Research Report

연구보고서 RE-103

국가 안전성 제고를 위한 소프트웨어안전 관리 등급 결정 기준 연구

A study on the criteria for the determination of software safety management levels to improve national safety

진회승/진용호/권장진

2021.07.

SPRi 소프트웨어정책연구소

이 보고서는 2020년도 과학기술정보통신부 정보통신진흥기금을 지원받아 수행한 연구결과로 보고서 내용은 연구자의 견해이며, 과학기술정보통신부의 공식입장과 다를 수 있습니다.

목 차

제1장 서 론 ····· 1

제1절 연구배경과 목적 ····· 1

1. 연구배경 ····· 1

2. 연구목적 ····· 3

제2절 연구방법 ····· 5

제2장 안전 등급제의 이론적 고찰 및 조사 방향 ····· 7

제1절 안전 등급제 개요 ····· 7

1. 안전 등급제 ····· 7

2. 정보시스템 등급제 ····· 8

3. 시설물 안전 등급제 ····· 14

제2절 시스템 안전 등급 ····· 15

1. IEC 61508의 시스템 안전등급 ····· 16

2. ISO 26262의 안전등급 ····· 18

3. 시스템 안전등급 결정 방법 및 조사 대상 ····· 18

제3절 소프트웨어 안전등급 ····· 19

1. 소프트웨어 안전등급이 필요한 이유 ····· 19

2. 안전표준의 소프트웨어 안전등급 결정 방법 및 조사 방향 ····· 22

제4절 소프트웨어안전 등급 적용 대상 ·····24
1. 주요정보통신기반시설 적용 대상 ·····24
2. 국가핵심기반 적용 대상 ·····27
3. 주요정보통신기반시설과 국가핵심기반에 기반한 적용 대상 ·····28
4. 공공기관 시스템 조사 방향 ·····29

제3장 산업 도메인별 안전등급 결정방법 조사 ·····30
제1절 조사 방향 ·····30
제2절 원자력 안전 ·····30
1. IAEA / IEC 관련 원자력 안전기준 ·····31
2. NRC / IEEE 관련 원자력 안전기준 ·····36
3. 시사점 ·····43
제3절 철도 안전 ·····45
1. 철도 안전 관련 국내외 법/제도 ·····45
2. 철도 안전 기준 ·····50
3. 시사점 ·····58
제4절 항공 안전 ·····60
1. 항공안전 관련 국내외 법/제도 ·····60
2. 항공 안전 기준 ·····62
3. 시사점 ·····71
제5절 전기용품 안전 ·····72

1. 전기용품 안전 관련 국내 법/제도 ····· 72
2. 전기용품 안전 기준 ····· 74
3. 시사점 ····· 79
제6절 의료 안전 ····· 81
1. 의료기기 안전 기준 (IEC 62304, ISO 14971) ····· 82
2. 시사점 ····· 84
제7절 미국 국방부 및 항공우주국 안전 ····· 85
1. 미국 국방 안전 기준 ····· 85
2. 미국 항공우주 안전 ····· 94
3. 시사점 ····· 106
제8절 각 표준의 안전등급 결정 방법에 대한 비교 분석 ····· 110
1. 시스템의 안전등급 상속 ····· 111
2. 시스템 위험 평가요소와 소프트웨어에 특화된 평가요소에 기반한 평가 ····· 111
3. 위험 심각도에 기반한 소프트웨어의 안전등급 평가 ····· 113

제4장 공공기관 시스템의 종류 및 등급제 조사 ····· 114
제1절 조사 방향 ····· 114
제2절 공공기관 시스템에 적용된 소프트웨어 관련 제도/기준 ····· 115
1. 국가기반시설 관리 체계 ····· 115
2. 공공기관/자치단체 정보시스템 관리 체계 ····· 120
3. 정보보호시스템 평가/인증 제도 (국내) ····· 125

4. 공공 정보/정보시스템 보안 등급 기준 (미국) ·····128
제3절 안전이 중요한 공공기관 시스템 조사 ·····132
1. 공공 정보시스템 분류 기준 ·····132
2. 기반시설 분류 기준 ·····136

제5장 공공기관 시스템 위험요인 조사 ·····146
제1절 위험분석 대상 시스템 선정 ·····146
1. 공공기관 시스템 유형 분류 ·····146
2. 공공기관 시스템 위험분석 ·····148
제2절 위험분석 결과 및 평가 고려사항 ·····151

제6장 안전등급에 따른 안전활동 및 기술 조사 ·····154
제1절 조사 방향 ·····154
제2절 산업일반 안전 표준 (IEC 61508) ·····155
1. 개요 ·····155
2. 안전활동 및 기술 조사 ·····155
3. 시사점 ·····161
제3절 철도 분야 안전 표준 (IEC 62279) ·····162
1. 개요 ·····162
2. 안전활동 및 기술 조사 ·····162
3. 시사점 ·····169

제4절 자동차 분야 안전 표준 (ISO 26262) ·····169
1. 개요 ·····169
2. 안전활동 및 기술 조사 ·····169
3. 시사점 ·····174
제5절 항공 분야 안전 표준 ·····175
1. 개요 ·····175
2. 안전활동 및 기술 조사 ·····175
3. 시사점 ·····179
제6절 의료 분야 안전 표준 ·····179
1. 개요 ·····179
2. 안전활동 및 기술 조사 ·····179
3. 시사점 ·····181
제7절 항공우주 분야 안전 표준 ·····182
1. 개요 ·····182
2. 안전활동 및 기술 조사 ·····182
3. 시사점 ·····190
제8절 국방 분야 안전 표준 ·····190
1. 개요 ·····190
2. 안전활동 및 기술 조사 ·····190
3. 시사점 ·····193

제7장 공공기관 시스템 소프트웨어 안전등급 결정방안 도출 ·····195

제1절 소프트웨어 안전등급 결정체계 방향성 도출 ·····195

1. 소프트웨어 안전등급 결정체계 방향성 도출 ·····195

2. 전문가 검토 및 소프트웨어 안전등급 결정 방안 선정 (방안 1) ·····197

제2절 소프트웨어 안전등급 결정체계 구축 ·····199

1. 용어 정의 ·····200

2. 위험 식별 ·····201

3. 위험 평가 ·····205

4. 소프트웨어 안전등급 결정 ·····211

5. 안전등급 선정 항목 및 지표에 대한 전문가 자문 ·····219

제8장 공공기관 시스템 소프트웨어 안전등급별 관리방안 도출 ·····221

제1절 소프트웨어 안전등급별 관리방안 도출 ·····221

1. 도메인별 안전표준들의 세부 안전활동 비교 ·····221

2. 소프트웨어 안전등급별 활동 비교 분석 ·····229

3. 소프트웨어 안전등급별 후보 관리방안 도출 ·····234

4. 전문가 검토 및 소프트웨어 안전등급별 관리방안 선정(관리방안 2) ···237

제2절 안전활동에 대응하는 산출물 및 안전기법, 수단 정리 ·····239

1. 각 표준별 산출물 비교 ·····239

2. 각 표준별 안전기법 및 수단 비교 ·····246

3. 안전활동 세부 정의 ·····251

제9장 결론 ····· 265

제1절 연구의 요약 ····· 265

제2절 향후 연구 ····· 265

제3절 연구의 한계 ····· 267

표 목 차

<표 1-1> 차량에서 소프트웨어 사용도 ····· 1

<표 1-2> 전문가 자문 그룹 ····· 6

<표 2-1> 정보시스템의 국가·사회적 중요도에 따른 등급산정 ····· 9

<표 2-2> 시설물의 안전등급 기준 ····· 14

<표 2-3> 위험등급 ····· 17

<표 2-4> IEC 60730의 안전등급 기준 ····· 24

<표 2-5> 전자적 침해 행위로부터 보호해야 할 필요가 있다고 인정되는 시설 기준 25

<표 2-6> 주요정보통신기반시설 지정대상의 분류 ····· 25

<표 2-7> 소프트웨어안전을 확보할 필요가 있는 시설 기준 ····· 27

<표 2-8> 국가핵심기반 지정 기준 ····· 27

<표 2-9> 소프트웨어안전을 확보할 필요가 있는 시스템 기준 ····· 28

<표 3-1> IAEA SSG-30 - 심각도 기준 ····· 33

<표 3-2> IAEA SSG-30 - 안전등급 분류기준 ····· 34

<표 3-3> IAEA SSG-30 - 안전등급 정의 ····· 34

<표 3-4> EUR - 안전등급 분류 기준 ····· 35

<표 3-5> 한국 원자로 안전등급 규정 - 안전등급 기준 ····· 37

<표 3-6> 경수로형 원전 규제기준 및 지침 - 전력계통 안전등급 기준 ····· 39

〈표 3-7〉 경수로형 원전 규제기준 및 지침 - 계측제어계통 안전등급 기준 ·····40
〈표 3-8〉 APR1400-SPM - 소프트웨어 안전등급 분류기준 ·····42
〈표 3-9〉 철도 - 소프트웨어에 대한 안전등급 체계 ·····56
〈표 3-10〉 철도 - 소프트웨어 제어 구분 ·····57
〈표 3-11〉 철도 - 소프트웨어 안전등급 결정 매트릭스 ·····58
〈표 3-12〉 철도 - 실패 조건 분류 기반의 개발 보증등급 부여 기준 ·····67
〈표 3-13〉 KS C IEC 61508 - 평가항목 분류 시 고려해야 하는 항목 ·····75
〈표 3-14〉 KS C IEC 60730 - 안전 관련 소프트웨어 등급 분류 기준 ·····78
〈표 3-15〉 의료 - IEC 62304 소프트웨어 안전등급 결정 기준 ·····83
〈표 3-16〉 의료 - ISO 14971 정성적 심각도 평가 기준 (3단계) ·····83
〈표 3-17〉 의료 - ISO 14971 정성적 심각도 평가 기준 (6단계) ·····84
〈표 3-18〉 미국방 - 소프트웨어 등급에 따른 활동 ·····87
〈표 3-19〉 미국방 - MIL-STD-882B 심각도 기준 ·····87
〈표 3-20〉 미국방 - 제어 유형에 대한 판단 기준 ·····88
〈표 3-21〉 미국 국방 - MIL-STD-882 심각도 분류 기준 ·····89
〈표 3-22〉 미국 국방 - MIL-STD-882 발생가능성 분류 기준 ·····89
〈표 3-23〉 미국 국방 - MIL-STD-882 소프트웨어 제어 유형 ·····92
〈표 3-24〉 미국 국방 - MIL-STD-882 소프트웨어 제어 유형 ·····93
〈표 3-25〉 NASA 소프트웨어 안전 연구의 발생가능성 평가 기준 ·····95
〈표 3-26〉 NASA 소프트웨어 안전 연구의 영향 평가 기준 ·····97
〈표 3-27〉 NASA-STD-8719.13 - 소프트웨어의 안전 중요도 판단 체크리스트 ·····98
〈표 3-28〉 NASA-STD-8739.8 - 소프트웨어의 안전 중요도 판단 체크리스트 ·····99
〈표 3-29〉 NASA 소프트웨어 제어유형 결정을 위한 주요 특성 ·····101

〈표 3-30〉 NASA-STD-8719.13 소프트웨어 제어 유형 평가 기준 ·····101
〈표 3-31〉 주요 산업 도메인 별 안전 기준의 안전등급 결정 유형 ·····110

〈표 4-1〉 발생가능성 등급 판단 기준표 ·····116
〈표 4-2〉 피해 규모 등급 판단 기준표 ·····116
〈표 4-3〉 영향요인 별 가중치 ·····117
〈표 4-4〉 영향요인 별 피해등급 판단기준표 (예시) ·····117
〈표 4-5〉 위험도 판정 기준표 ·····117
〈표 4-6〉 발생가능성 등급 판단 기준표 ·····118
〈표 4-7〉 피해규모 등급 판단 기준표 ·····119
〈표 4-8〉 피해규모 등급 판단 기준표 ·····119
〈표 4-9〉 위험도 평가 예시 ·····120
〈표 4-10〉 행정기관/공공기관 정보시스템 등급 평가항목 - 피해범위 ·····122
〈표 4-11〉 행정기관/공공기관 정보시스템 등급 평가항목 - 가용성 ·····123
〈표 4-12〉 FIPS PUB 199 - 보안등급 평가항목 ·····129
〈표 4-13〉 자치단체 정보시스템 장애 예방 및 지침 - 중요도 시스템 평가기준 ····133
〈표 4-14〉 재난 및 안전관리 기본법 시행령 - 분야별 국가핵심기반 지정 기준 ····137
〈표 4-15〉 국가기반체계 보호계획 수립지침 - 국가기반시설 지정 현황 ·····138
〈표 4-16〉 훈령 - 국가중요시설의 분류 및 지정 ·····141
〈표 4-17〉 정보통신기반시설 지정 예시 ·····142
〈표 4-18〉 행정안전부 - 주요정보통신기반시설 세부시설 지정기준 ·····143
〈표 4-19〉 사회기반시설사업의 종류 (예시) ·····144

〈표 5-1〉 시스템 유형 구분 ·····147
〈표 5-2〉 각 시스템 유형에 해당하는 공공기관 시스템(예) ·····147
〈표 5-3〉 분석 대상 공공기관 시스템 및 시스템 유형 식별 ·····148
〈표 5-4〉 위험등급 ·····149

〈표 6-1〉 조사 대상 분야 및 관련 표준 ·····154
〈표 6-2〉 IEC 61508 표준의 안전활동 ·····156
〈표 6-3〉 소프트웨어 안전 등급에 따른 기법 및 수단 - IEC 61508 ·····157
〈표 6-4〉 IEC 62279 표준의 안전활동 ·····163
〈표 6-5〉 소프트웨어 안전등급에 따른 산출물 작성 - IEC 62279 ·····164
〈표 6-6〉 소프트웨어 안전 등급에 따른 기법 및 수단 - IEC 62279 ·····166
〈표 6-7〉 ISO 26262 표준의 안전활동 ·····171
〈표 6-8〉 소프트웨어 안전 등급에 따른 표기법 - ISO 26262 ·····172
〈표 6-9〉 소프트웨어 안전 등급에 따른 설계원칙 - ISO 26262 ·····173
〈표 6-10〉 소프트웨어 안전 등급에 따른 방법 - ISO 26262 ·····173
〈표 6-11〉 소프트웨어 안전 등급에 따른 활동 - DO-178C ·····177
〈표 6-12〉 소프트웨어 안전 등급에 따른 활동 - IEC 62304 ·····181
〈표 6-13〉 소프트웨어 안전 등급에 따른 활동 - NASA-STD ·····184
〈표 6-3〉 소프트웨어 안전 등급에 따른 활동 - NASA-GB ·····184
〈표 6-15〉 소프트웨어 안전 등급에 따른 안전기법 및 수단 - NASA-STD-8719-13C ·····187

〈표 7-1〉 용어 정의 ·····200
〈표 7-2〉 공공시스템과 관련된 위험 ·····201

〈표 7-3〉 예시 - 주요 안전관련 기능 ·····203
〈표 7-4〉 예시 - 항공등화감시제어시스템의 주요 기능 ·····204
〈표 7-5〉 예시 - 소프트웨어 위험요인과 영향 ·····205
〈표 7-6〉 예시 - 위험영향력 판단 기준 ·····206
〈표 7-7〉 예시 - 소프트웨어 위험관여도 판단 기준 ·····207
〈표 7-8〉 소프트웨어 위험관여도 판단 기준표 - 기술적 판단 기준(예시) ·····208
〈표 7-9〉 예시 - 소프트웨어 안전등급 판단 기준 ·····210
〈표 7-10〉 예시 - 소프트웨어 안전등급 판정 ·····213
〈표 7-11〉 예시 - 소프트웨어 안전등급 판정 대상 시스템 정보 ·····215
〈표 7-12〉 예시 - 소프트웨어 안전등급 판정 대상 시스템 기능 설명 ·····217
〈표 7-13〉 전문가 검토 결과 ·····219

〈표 8-1〉 각 표준 별 안전활동 비교 - 산업일반 및 철도, 자동차 분야 ·····222
〈표 8-2〉 각 표준 별 안전활동 비교 - 항공우주 및 국방 분야 ·····223
〈표 8-3〉 각 표준 별 안전활동 비교 - 항공 및 의료 분야 ·····226
〈표 8-4〉 각 표준의 안전등급과 본 연구에서 제안한 안전등급 비교 ·····229
〈표 8-5〉 수행 활동 측면에서의 세부 관리방안 ·····231
〈표 8-6〉 검토 활동 측면에서의 세부 관리방안 ·····232
〈표 8-7〉 분석 활동 측면에서의 세부 관리방안 ·····234
〈표 8-8〉 전문가 검토 결과 ·····237
〈표 8-9〉 표준별 산출물 비교 - 항공우주, 국방, 항공, 의료 분야 ·····240
〈표 8-10〉 표준별 산출물 비교 - 산업일반, 철도, 자동차 분야 ·····242
〈표 8-11〉 분석 활동 측면에서의 세부 관리 방안 ·····246

〈표 8-12〉 소프트웨어안전요구사항 정의 활동 구성 ·····252
〈표 8-13〉 소프트웨어안전요구사항 검토 활동 구성 ·····252
〈표 8-14〉 소프트웨어안전요구사항 분석 활동 구성 ·····253
〈표 8-15〉 소프트웨어안전아키텍처 설계 활동 구성 ·····253
〈표 8-16〉 소프트웨어안전아키텍처 검토 활동 구성 ·····255
〈표 8-17〉 소프트웨어안전아키텍처 분석 활동 구성 ·····256
〈표 8-18〉 소프트웨어안전상세설계 활동 구성 ·····257
〈표 8-19〉 소프트웨어안전상세설계 검토 활동 구성 ·····258
〈표 8-20〉 소프트웨어안전상세설계 분석 활동 구성 ·····258
〈표 8-21〉 소프트웨어안전구현 활동 구성 ·····259
〈표 8-22〉 소프트웨어안전구현 검토 활동 구성 ·····259
〈표 8-23〉 소프트웨어안전구현 분석 활동 구성 ·····260
〈표 8-24〉 소프트웨어단위테스트 수행 활동 구성 ·····260
〈표 8-25〉 소프트웨어단위테스트 검토 활동 구성 ·····261
〈표 8-26〉 소프트웨어통합테스트 수행 활동 구성 ·····261
〈표 8-27〉 소프트웨어통합테스트 검토 활동 구성 ·····262
〈표 8-28〉 소프트웨어테스트 수행 활동 구성 ·····263
〈표 8-29〉 소프트웨어테스트 검토 활동 구성 ·····264

그 림 목 차

[그림 1-1] 보잉 737 맥스의 에디오피아 항공 302편 추락 사고 현장 ·····2

[그림 1-2] 연구 방법 ·····5

[그림 2-1] 등급산정 절차 ·····9

[그림 2-2] 정보시스템 특성을 반영하는 등급산정 세부내용 ·····10

[그림 2-3] 등급별 보안관리 기준 ·····11

[그림 2-4] 정보시스템 5등급 ·····12

[그림 2-5] 정보시스템 등급분류 절차 ·····13

[그림 2-6] 등급별 보안관리 수준 차별화 내용 예시 ·····13

[그림 2-7] Tolerable risk and ALARP ·····16

[그림 2-8] IEC 61508 소프트웨어 개발 시 등급별 필요한 기술 ·····18

[그림 2-9] 소프트웨어안전 등급 결정방법(1) ·····23

[그림 2-10] 주요정보통신기반 시설 지정 현황 ·····26

[그림 2-11] 행정안전부 소관 주요정보통신기반 시설 지정 현황 ·····26

[그림 3-1] 원자력 - IAEA NS-G-1.3에 의한 시스템의 안전 분류 ·····32

[그림 3-2] 원자력 안전등급 평가 기준 ·····43

[그림 3-3] 원자력 - 안전등급 비교 ·····45

[그림 3-4] 철도안전법 체계 ·····46

[그림 3-5] 유럽 ERA TSI의 참조 표준 ·····49

[그림 3-6] 철도 - IEC 62278 위험 평가 절차 ·····51
[그림 3-7] 철도 - IEC 62278 시간 기반 발생빈도 분류 기준 ·····52
[그림 3-8] 철도 - IEC 62278 거리 기반 발생빈도 분류 기준 ·····53
[그림 3-9] 철도 - IEC 62278 RAM 관련 심각도 분류 기준 ·····53
[그림 3-10] 철도 - IEC 62278 금전적 피해 관련 심각도 분류 기준 ·····53
[그림 3-11] 철도 - IEC 62278 RAMS 관련 심각도 분류 기준 ·····54
[그림 3-12] 철도 - IEC 62278 인명 및 환경 피해 관련 심각도 분류 기준 ·····54
[그림 3-13] 철도 - IEC 62278 위험 수용성 단계 (2단계) ·····54
[그림 3-14] 철도 - IEC 62278 위험 수용성 단계 (4단계) ·····55
[그림 3-15] 철도 - IEC 62278 위험 수용성 분류 기준 ·····55
[그림 3-16] 철도분야 안전등급 평가 기준 ·····59
[그림 3-17] 항공법 체계 ·····61
[그림 3-18] 항공 - 안전 관련 표준 ·····64
[그림 3-19] 항공 - ARP 4761 실패 조건 영향에 따른 분류 ·····65
[그림 3-20] 항공 - ARP 4761 실패 조건 분류에 따른 발생가능성 및 개발보증등급 목표 ····66
[그림 3-21] 항공 - ARP 4754 최상위 기능에 대한 개발 보증등급 할당 기준 ·····68
[그림 3-22] 항공 - DO-178C의 실패 조건에 대한 분류 기준 ·····70
[그림 3-23] 항공분야 안전등급 평가 기준 ·····71
[그림 3-24] 전기용품 안전 관련 국내 법제도 ·····73
[그림 3-25] 전기용품 안전기준 목록 ·····74
[그림 3-26] KS C IEC 61508 - 평가항목 및 지표 예 ·····76
[그림 3-27] KS C IEC 61508 - 리스크 그래프: 일반적인 도식 ·····77
[그림 3-28] KS C IEC 61508 - 위해 사건 심각도 매트릭스 ·····78

[그림 3-29] 전기용품 분야 안전등급 평가 기준 - IEC 60730 ·····79
[그림 3-30] 전기용품 분야 안전등급 평가 기준 - IEC 61508 ·····80
[그림 3-31] 의료 - IEC 62304 소프트웨어 안전 등급 결정 절차 ·····82
[그림 3-32] 의료분야 안전등급 평가 기준 ·····84
[그림 3-33] 미국 국방 - 소프트웨어 위험원 심각도 매트릭스 ·····87
[그림 3-34] 미국 국방 - MIL-STD-882 위험 평가 매트릭스 ·····91
[그림 3-35] 미국 국방 - MIL-STD-882 소프트웨어 위험 지수 - 위험 등급 관계 ··94
[그림 3-36] 미국 항공우주 - NESC 위험 매트릭스 ·····98
[그림 3-37] NASA-STD-8719.13 소프트웨어 제어 위험 등급 ·····103
[그림 3-38] NESC 위험 평가 기준: 위험 심각도 ·····104
[그림 3-39] 미국 항공우주 - NESC 위험 평가 기준: 발생가능성 ·····105
[그림 3-40] 미국 항공우주 - NASA-STD-8719.13 소프트웨어 위험 등급 ·····105
[그림 3-41] 미국 항공우주 - NASA-GB-8719.13 시스템-소프트웨어 위험등급 관계 ·····106
[그림 3-42] 미국 국방 분야 안전등급 평가 기준 ·····107
[그림 3-43] 미국 항공우주 분야 안전등급 평가 기준 ·····108
[그림 3-44] 소프트웨어의 관여도(Software Control Category) ·····112
[그림 3-45] MIL-STD-882E의 소프트웨어 분류 ·····112
[그림 3-46] IEC 62304 및 IEC 60730의 소프트웨어 분류 기준 ·····113

[그림 4-1] 행정기관/공공기관 정보시스템 등급산정 절차 ·····121
[그림 4-2] 행정기관/공공기관 정보시스템 중요도 평가기준 (예시) ·····124
[그림 4-3] 보안적합성 검증제도 - 제품유형별 검증 기준 ·····126
[그림 4-4] 공통평가기준 - 보안보증등급 ·····127

[그림 4-5] FIPS PUB 199 - Potential Impact Level ·····130
[그림 4-6] SP 800-60 - Type-based impacts for ‘Management and Support Information’ ·····131
[그림 4-7] SP 800-60 - Type-based impacts for ‘Mission Information’ ·····131
[그림 4-8] 범정부 서비스참조모형 ·····133
[그림 4-9] Mission-based information type ·····135
[그림 4-10] Services delivery support information ·····136
[그림 4-11] Government resource management information ·····136

[그림 5-1] 공공기관 시스템 유형 분류 ·····146

[그림 6-1] IEC 61508 안전활동 적용 절차 ·····155
[그림 6-2] IEC 62279 표준의 안전활동 적용 절차 ·····163
[그림 6-3] ISO 26262 표준의 안전활동 적용 절차 ·····170
[그림 6-4] DO-178C 표준의 안전활동 적용 절차 ·····176
[그림 6-5] IEC 62304 표준 안전활동 적용 절차 ·····180
[그림 6-6] Waterfall Lifecycle Model ·····182
[그림 6-7] Spiral Lifecycle Model ·····183
[그림 6-8] Incremental Development Lifecycle Model ·····183
[그림 6-9] 다양한 안전활동 적용 절차 예시 ·····191
[그림 6-10] Level of Rigor 및 예시 ·····192
[그림 6-11] LoR Task 예 ·····193

[그림 7-1] 공통 평가기준 정의 ·····196

[그림 7-2] 소프트웨어 안전등급 결정 절차 ·····200
[그림 7-3] 구조적 측면으로 위험 분류 ·····202
[그림 7-4] 예시 - 기능 특성에 따른 소프트웨어 위험관여도 결정 방법 ·····210

[그림 8-1] 수행 활동 측면에 대한 분석 - 항공우주, 국방, 의료, 항공 분야 ·····230
[그림 8-2] 수행 활동 측면에 대한 분석 - 산업일반, 철도, 자동차 분야 ·····230
[그림 8-3] 검토 활동 측면에 대한 분석 - 항공우주, 국방, 의료, 항공 분야 ·····232
[그림 8-4] 검토 활동 측면에 대한 분석 - 산업일반, 철도, 자동차 분야 ·····232
[그림 8-5] 분석 활동 측면에 대한 분석 - 항공우주, 국방, 의료, 항공 분야 ·····233
[그림 8-6] 분석 활동 측면에 대한 분석 - 산업일반, 철도, 자동차 분야 ·····234
[그림 8-7] 소프트웨어 안전등급별 후보 관리방안 1 ·····236
[그림 8-8] 소프트웨어 안전등급별 후보 관리방안 2 ·····236
[그림 8-9] 소프트웨어 안전등급별 후보 관리방안 3 ·····237

요 약 문

1. 제 목 : 국가 안전성 제고를 위한 소프트웨어안전 관리 등급 결정 기준 연구

2. 연구목적 및 필요성

(1) 추진 배경

ㅇ 소프트웨어안전 중요성의 부각

- 4차 산업혁명에 따른 디지털 전환이 산업 혁신의 핵심으로 인식됨에 따라 국가 기반시설 및 안전 중요 제품에 소프트웨어안전 중요성이 더욱 부각되고 있음
- 국가핵심기반과 안전 중요 제품에 포함된 소프트웨어가 복잡해지고 크기가 커짐에 따라 소프트웨어 안전 확보에 어려움이 있음

ㅇ 소프트웨어 안전관리를 위한 공통기준 부재

- 산업별 국제표준마다 안전등급 판정 기준이나 적용방식이 상이하고, 하드웨어 단위에서 안전등급이 결정되는 반면 소프트웨어 관련 안전관리를 위한 표준은 미흡함
- 안전 소프트웨어 개발자가 모든 도메인의 표준을 숙지하기 어려움

(2) 연구의 목적

ㅇ 소프트웨어 특성을 반영한 소프트웨어 안전등급에 대한 연구

- 하드웨어 단위에서 안전등급이 결정되며 소프트웨어를 위한 공통적인 안전 등급 판정 기준이 부재하여, 하드웨어 등급에 의해 상속되는 소프트웨어 안전등급이 아닌 소프트웨어 특성을 반영한 안전 등급을 연구

ㅇ 공공기관 시스템 대상 소프트웨어 안전등급을 통한 소프트웨어 안전관리 연구

- 공공기관 시스템 대상 소프트웨어 안전관리 등급을 개발하고 소프트웨어 안전등급별 안전관리 활동 연구

3. 연구의 구성 및 범위

(1) 연구의 구성

ㅇ 본 연구의 구성은 총 9장으로 구성됨

- 1장은 서론으로써 연구의 배경 및 필요성, 연구목적 및 방법 등을 기술하고, 2장은 안전 등급제의 이론적 고찰 및 소프트웨어 안전등급제 기준 항목 및 지표 도출을 위하여 조사 방향을 설정함
- 3장은 산업 도메인별 안전등급 결정방법 조사 내용을 정리함
- 4장에서는 공공기관 시스템의 종류 및 등급제를 조사하며, 5장에서는 공공기관 시스템의 위험요인을 조사함
- 6장에서 안전등급에 따른 안전활동 및 기술을 조사함
- 조사 내용을 기반으로 7장에서 공공기관 시스템의 소프트웨어 안전등급 결정방안을 도출하고, 8장에서 공공기관 시스템의 소프트웨어 안전등급별 관리방안을 도출함
- 9장은 본 연구의 요약과 시사점, 향후 연구로 구성됨

(2) 연구의 방법

ㅇ 안전등급 판단의 지표와 항목을 결정하기 위한 기본적인 연구틀은 다음과 같음

- 기초자료 수집을 위한 안전중요시스템 표준과 기존 문헌 연구
- 소프트웨어안전 전문가·도메인 전문가의 의견을 수렴하는 자문회의 개최
- 문헌 연구 및 자문회의를 통하여 소프트웨어 안전등급 결정을 위한 항목 및 지표 도출

ㅇ 기초자료 수집을 위한 안전중요시스템 표준과 기존 문헌 연구를 수행함

- 문헌 연구를 통하여 소프트웨어 안전등급의 필요성 도출
- 산업 도메인별 등급 판단을 위한 안전기준을 분석하여 안전등급 결정방

법 및 관련 제도, 안전 관련 기준 조사

- 공공기관 시스템에 적용되는 안전기준의 특성을 도출하기 위하여 관련 제도 및 기준, 국내외 다양한 등급제 사례, 공공기관 시스템의 종류 및 분류기준 분석
- 각 산업 도메인별 주요 안전표준에 정의된 안전활동 및 기술 조사

ㅇ 문헌 연구 및 자문회의를 통하여 소프트웨어 안전등급 결정을 위한 항목 및 지표를 도출함

- 기존 표준의 등급 선정 항목 및 지표를 조사하고 공공기관 시스템의 위험요인 및 시스템의 특성을 분석하여, 공공기관 시스템에 대한 소프트웨어 안전등급 결정방안 도출
- 소프트웨어 안전등급별 안전활동을 기반으로 한 공공기관 시스템의 소프트웨어 안전등급별 관리방안 도출

4. 연구 내용 및 결과

(1) 안전 등급제의 이론적 고찰 및 조사방안 제시

ㅇ 안전 등급제 개요

- 등급제의 첫 번째 목적은 시스템의 개발(또는 구축)과 관리 효율성을 위하여 일정한 기준으로 등급을 분류하여, 등급에 따라 적절한 활동을 수행하는 것임. 안전과는 직접적인 관련이 없으나 본 목적에 부합하는 사례로 정보시스템 등급제 사례를 제시함
- 두 번째 목적은 목적물, 시스템을 평가한 결과에 따라 등급을 분류하여 현황 정보를 제공하고, 체계적인 관리를 하는 것. 사례로 안전과 관련이 있는 시설물 안전 등급제를 제시함

ㅇ 시스템 안전 등급제

- 시스템 안전 등급 사례로 IEC 61508. ISO 26262를 요약 제시함

- 시스템 안전 등급 결정방법을 요약하고, 조사 대상 표준을 제시

ㅇ 소프트웨어 안전등급

- 소프트웨어 안전등급이 필요한 이유는 소프트웨어 안전 확보를 위한 필수 활동이며, 또한 소프트웨어 안전등급에 의해 효율적 안전관리가 가능하기 때문임
- 하드웨어 안전등급과 소프트웨어 안전등급 결정방법을 비교하면 다음과 같이 소프트웨어 안전등급을 결정하는 방법을 분류할 수 있음
  1) 시스템 안전등급을 상속하여 소프트웨어 안전 등급에 활용하는 방법
  2) 시스템 안전등급과 소프트웨어적 특성을 이용하여 소프트웨어 안전등급을 결정하는 방법
  3) 소프트웨어 안전등급 결정을 위해 소프트웨어적 특성만을 사용하는 방법
- 소프트웨어 안전등급 판정 기준 항목과 지표를 결정하기 위한 조사는 위의 세 가지 방법을 기준으로 조사하되 각각 표준별 특성도 고려하여 조사함. 조사 분석은 도출된 소프트웨어 안전등급 기준이 각 도메인에 공통적으로 적용이 가능하도록 결과를 도출함

ㅇ 소프트웨어안전 등급 적용 대상 및 표준 조사 방향 제시

- 소프트웨어안전 표준은 전통적으로 안전을 중요하게 다룬 도메인을 식별하여 관련 제도 및 관련 안전기준을 조사하고, 특히 소프트웨어 안전등급에 대한 평가 기준을 상세하게 다룬 도메인의 자료 조사함
- 공공기관 시스템에 적용되는 안전기준의 특성을 도출하기 위한 관련 제도 및 기준을 조사함
- 주요정보통신시반시설 및 국가핵심기반 적용 대상을 검토하고 소프트웨어안전 등급에 적용 대상 기준을 도출함. 소프트웨어 안전 등급 결정 방안과 항목, 지표 결정을 위한 국내외 공공기관 시스템 및 기반시설 분류 기준을 조사함

(2) 소프트웨어 안전관리 등급제 구축을 위한 조사

ㅇ 소프트웨어 안전등급 결정방법에 대한 조사 및 분류

- 소프트웨어 안전등급 결정 방안 선정을 위하여, 전통적으로 안전을 중요하게 다루는 도메인(원자력, 철도, 항공, 전기용품, 의료, 국방, 항공우주 등)의 관련 제도 및 등급 판단에 적용되는 안전기준을 조사하였음.
- 조사 내용은 크게 소프트웨어 안전등급을 결정하는 다양한 유형 및 방법, 소프트웨어 안전등급 평가항목과 지표로 구성됨

ㅇ 안전등급의 평가요소, 판단항목 및 관련 지표에 대한 조사

- 안전등급의 평가요소, 판단항목 및 관련 지표는 크게 시스템 수준과 소프트웨어 수준에서 고려하는 평가 요소를 구분하여 접근하였으며, 평가요소를 산정하는 다양한 접근방법 또는 세부 판단기준에 대하여 조사를 수행함
- 모든 도메인에서 위험의 심각도(Severity)를 평가항목으로 사용하는 것을 확인할 수 있었으며, 세부 항목으로는 인명 피해, 금전/환경적 손실, 시스템 기능/성능 손실 등이 많이 사용되고 있었음.
- 위험 발생가능성(Frequency/Probability/Likelihood)은 대부분의 도메인에서 시스템 수준의 평가항목으로 사용하나, 소프트웨어 평가항목으로는 사용하고 있지 않았음. 그 이유는 소프트웨어의 위험 발생가능성은 정량적 도출이 어렵기 때문임
- 이 외에도, 소프트웨어 특성을 고려한 평가항목으로 위험관여도 및 중복 안전장치의 존재 여부 등이 있음

(3) 공공기관 시스템 등급 결정을 위한 요인 조사

ㅇ 공공기관 시스템의 종류 및 등급제 조사

- 공공기관 시스템에 적용된 소프트웨어 관련 등급 결정방법, 공공기관 시스템에 적용된 소프트웨어 등급 결정을 위한 평가항목 및 지표에 대해 조사를 수행함
- 국가기반시설 위험평가 기준의 경우, 산업 안전 표준과 달리 시스템 외부

요인(예, 자연재해)으로 인한 위험에 대해서도 고려하고 있었으며, 공공 분야의 특성으로 인해 사회적 피해 측면의 평가항목을 고려하고 있었음

- 공공기관과 행정기관 정보시스템 관리 체계의 경우, 특정 위험보다는 시스템 자체의 국가·사회적 및 보안 측면의 중요도에 근거하여 등급을 평가하였으며, 공공시스템 특성을 반영하여 국가 안전보장(또는 국가 존립) 관련 항목에 대한 고려 비중이 높았음
- 국내 정보보호시스템 평가/인증 제도의 경우, 정보보호시스템 공통평가기준을 통해 국가 및 공공기관이 도입하는 보안제품의 유형에 따라 달성해야 하는 등급을 사전 정의하고 있음.
- 미국의 공공 정보시스템 보안등급 기준은 위험분석보다 시스템 자체에 대한 평가에 근거하여 등급을 부여하고 있음. 시스템을 정보 유형에 따라 분류하고, 기본적인 등급을 사전에 정의하여 제시하는 형태이며, 평가항목으로는 보안목표에 해당하는 기밀성, 무결성, 가용성을 고려하고 있음

o 공공기관 시스템 분류 조사

- 공공기관 시스템에 적용되는 안전기준의 특성을 도출하기 위하여 안전이 중요한 공공기관 시스템에 대하여 조사를 수행하였음. 이를 위해, 국내 및 미국에서의 공공 정보시스템 분류기준을 조사하고, 기반시설 분류기준(국가기반시설, 국가중요시설, 정보통신기반시설, 사회기반시설)에 대하여 조사를 수행함
- 국내에서는 전자정부법을 근거로 하여 정보시스템 분류기준을 제시하고 있으며, 정보기술아키텍처 서비스 분류 체계를 따르고 있음. 미국에서는 FISMA (Federal Information System Management Act)를 근거로 하여 정보시스템 분류기준을 제시하고 있음
- 재난 및 안전관리 기본법을 통해 국가기반시설 분류기준을 확인하였으며, 통합방위법을 통해 국가중요시설 분류기준을 조사하였음. 또한, 정보통신기반 보호법을 통해 정보통신기반시설 분류, 사회기반시설에 대한 민간투자법을 통해 사회기반시설 분류기준을 확인할 수 있었음

ㅇ 공공기관 시스템 위험요인 조사

- 공공기관 시스템의 특성을 분석하여 해당 특성에 따른 유형을 구분하고, 각 시스템 유형에 포함되는 공공기관 시스템을 선정하여 해당 공공기관 시스템의 위험요인을 조사함. 해당 위험요인 분석을 통해 시스템 유형별 안전등급을 분류하고, 안전등급 평가 시 고려해야 하는 사항들을 도출하였음

공공기관 시스템 유형 구분

시스템 유형	설명
유형 1	수집된 정보를 기반으로 소프트웨어 판단에 따른 자율 제어 시스템
유형 2	제어자의 판단에 따라 현장 설비를 제어하는 시스템
유형 3	수집된 정보를 모니터링하여 제어자에게 관련 정보를 제공하는 시스템 - 현장 설비를 제어하는데 활용되는 제어 정보 제공 - 모니터링 및 분석을 통해 시설에 대한 특정 안전 상태 정보 제공 . 예) 유독 가스 알람 설비 제어 모니터링및분석을통해자연재해,인재등의재난정보제공
유형 4	수집된 정보를 해당 환경에 노출된 관계자들에게 제공하는 시스템 - 식품, 의약품 등의 안전 관련 정보 제공 - 기후, 기상, 환경, 생활 정보 등의 일반 정보 제공

(4) 소프트웨어 안전관리 등급에 따른 적용 기술 조사

ㅇ 소프트웨어 안전등급에 따른 안전활동 및 기법에 대한 포괄적인 조사

- 사회 안전과 관련된 각 분야(산업 일반, 철도, 자동차, 의료, 항공, 항공우주, 국방)의 주요 안전표준을 선정하고, 선정된 안전표준에서 정의하고 있는 안전활동 및 기술 등의 관리방안을 조사하였음.

- 일부 표준들은 안전등급에 따른 안전활동의 수행을 차등 적용하는 형식으로 관리방안을 제시하고 있었으며, 또 다른 일부 표준들은 안전등급에 구분 없이 기본적으로 안전활동을 수행하되, 안전 기법 및 수단을 차등 적용하는 방식으로 관리방안을 제시하고 있었음.

- 철도 및 항공 분야 표준의 경우, 검토 및 검증 활동의 수행에 대한 독립성 수

준을 부여하고 있었으며, 항공우주 분야의 경우, 독립성 수준에 대한 중요성은 언급하고 있으나 구체적인 방안은 정의하고 있지 않았음

(5) 공공기관 시스템 소프트웨어 안전등급 결정방안 도출

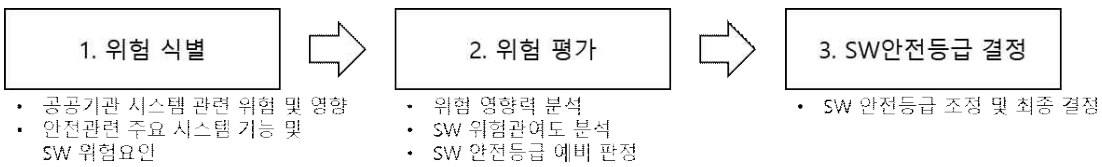
ㅇ 소프트웨어 안전등급 결정체계 방향성 도출

- 아래 세 가지 방안 중 **첫 번째 방안**으로 선정
- **미국방 표준(MIL-STD-882E)과 NASA 표준(NASA-STD-8719-13C) 접근방법에 기반한 것으로, 안전에 대한 "기본등급"을 우선 결정한 이후, 여러 조정 요인들을 기반으로 안전등급을 "조정" 하는 방안**
- 시스템이 충족시켜야 할 안전 요구사항을 정의하고, 특정 안전 요구사항을 만족시켰을 때, 보장되는 안전등급(Safety Assurance Level)을 정의하는 방법
- 공공기관 시스템 기능에 대하여 잠정적인 등급을 사전에 정의하는 방안

ㅇ 소프트웨어 안전등급 결정체계 구축

- 소프트웨어 안전등급 결정절차는 아래와 같다.

소프트웨어 안전등급 결정 절차

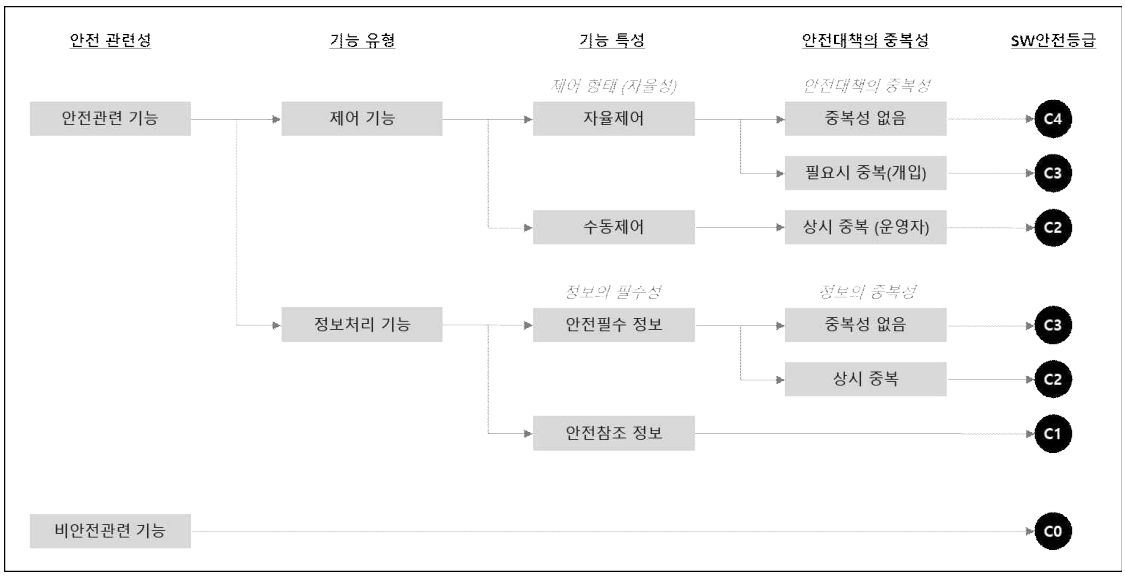


- 위험영향력(S)과 소프트웨어 위험관여도(C)로 소프트웨어안전 예비등급을 결정함

위험영향력 분석에 의한 위험영향력 판단

위험영향력	판단 기준
S4	다음 항목 중 하나 이상 해당 인적 피해 - 1명 이상의 사망, 또는 2명 이상의 전치 3개월 ~ 상해자, 또는 이상의 전치 2주 ~ 상해자 발생 경제적 피해 - 10억 이상의 손실 기반시설 피해 - 50% 이상 및 일주일 이상의 국가기반시설 기능 장애 야기
S3	다음 항목 중 하나 이상 해당 인적 피해 - 1명 이상의 전체 3개월 ~ 상해자, 또는 5명 이상의 전치 2주 ~ 상 경제적 피해 - 1000만원 이상 ~ 10억원 미만 기반시설 피해 - 30% 이상 및 하루 이상의 국가기반시설 기능 장애 야기
S2	다음 항목 중 하나 이상 해당 인적 피해 - 1명 이상의 전치 2주 ~ 상해자 경제적 피해 - 1000만원 미만 기반시설 피해 - 10% 이상 및 1시간 이상의 국가기반시설 기능 장애 야기
S1	다음 항목 중 하나 이상 해당 인적 피해 - 경미한 상해 경제적 피해 - 경미한 손실 기반시설 피해 - 10% 미만 및 1시간 미만의 국가기반시설 기능 장애 야기
S0	불편함을 느끼거나 피해 없음

기능 특성에 따른 소프트웨어 위험관여도 결정 방법



소프트웨어 안전등급 판단 기준

		위험영향력				
		S4	S3	S2	S1	S0
소프트웨어 위험관여도	C4	VH	VH	H	M	L
	C3	VH	H	H	M	L
	C2	H	H	M	M	L
	C1	M	M	M	M	L
	C0	L	L	L	L	L

VH(Very High, 매우 높음), H(High, 높음), M(Medium, 중간), L(Low, 낮음)

* 위험영향력과 소프트웨어 위험관여도는 숫자가 높을수록 높음

- 조직의 안전관련 방침 및 시스템 특성, 위험 발생 가능성을 추가 고려 등의 종합적으로 판단하여 소프트웨어 안전등급결정

(6) 공공기관 시스템 소프트웨어 안전등급별 관리방안 도출

○ 소프트웨어 안전활동, 기법, 수단의 등급별 적용방안 마련을 위한 분석

- 소프트웨어 안전등급에 따른 안전활동 및 기법의 조사 결과를 기반으로, 분야별 주요 표준에서 언급하고 있는 안전활동들을 단계별 주요 활동 '수행', 이전단계 결과물 대비 일관성 및 완전성 '검토', 단계별 활동 수준에서 야기될 수 있는 위험 요소 '분석' 측면으로 재 구조화함
- 재 구조화된 안전활동의 등급별 수행 여부, 수행의 수준 및 독립성 수준 등을 기준으로 '수행', '검토', '분석' 측면으로 비교 분석하고, 후보 관리방안을 도출함. 이후, 표준별 산출물과 안전 기법 및 수단을 비교하여, 후보 관리방안에 정의된 각 안전활동에 대응하는 산출물 및 안전 기법을 정리함

○ 후보 관리방안 도출하고 전문가의 검토 후 **후보 관리방안 2**가 현시점에서 가장 적절할 것으로 판단

- 후보 관리방안 1은 안전 관련 개발 및 검토 활동은 등급에 구분 없이 모두 수행함. 등급에 따른 차이는 분석 활동의 수행 유무, 검토 활동의 독립성 수준임
- **후보 관리방안 2는 '수행', '검토', '분석' 활동 모두 안전 등급에 따라 구분하여 수행함. 검토 활동의 독립성 수준도 등급에 따라 다름**
- 후보 관리방안 3은 단계 별 메인 활동은 등급에 구분 없이 모두 수행함. 등급에

따른 차이는 검토 및 분석 활동의 수행 유무, 검토 활동의 독립성 수준임

ㅇ 안전활동에 대응하는 산출물 및 안전기법, 수단을 정리함

(7) 소프트웨어 안전관리 등급제 검증을 위한 전문가 연구반 운영

ㅇ 전문가 그룹 검토 수행

- 소프트웨어안전 관련 분야에 종사하는 산·학·연의 전문가를 섭외하여, 연구 방향성 및 연구 결과를 검토할 전문가 그룹을 구성함. 원자력, 국방, 항공, 철도, 자동차 분야 등 다양한 분야에서 활발히 활동하고 있는 전문가로 구성됨
- 전문가 검토 결과를 통해 소프트웨어 안전등급 결정방안 도출 결과와 소프트웨어 안전등급에 따른 관리방안 도출 결과에 대하여 미비점 및 연구 결과의 유효성을 확인함
- 전문가 검토에 의한 식별된 미비점은 연구자의 판단에 의해 선별적으로 수용함으로써, 연구 결과의 방향성 및 신뢰성을 높임

5. 정책적 활용 내용

ㅇ 본 연구는 소프트웨어 안전 등급 기준과 평가 항목, 지표(안)을 제시함으로써 소프트웨어 안전등급제 시행을 위한 제도 개발의 기초 자료로써 활용됨

6. 기대효과

ㅇ 소프트웨어 안전등급제 및 안전등급에 따른 관리방안을 개발함으로써, 소프트웨어안전 관리를 위한 기본적인 체계가 마련될 수 있음.

ㅇ 해당 소프트웨어 안전등급제를 공공기관 시스템에 선제 적용해 봄으로써, 국가기반시설 및 안전 중요 제품에 대한 소프트웨어안전을 도모하고, 소프트웨어안전을 체계적으로 확보할 수 있으며, 다양한 안전관련 산업 분야에서 보다 안전성이 제고된 제품개발을 지원할 수 있음.

SUMMARY

This study deals with the process of deriving software safety level selection plans, and safety management plans for each software safety level for public institution systems and national infrastructure. The reason for the need for a common software safety level is to safe software of safety critical systems which is centered on hardware safety management, and to provide software developers and domain experts with necessary technologies for software safety activities and safety management. It is also to efficiently set the cost and time to secure safety, which are obstacles for software safety.

In order to determine the items and indicators of safety level and apply them to public institution systems, this study conducts a investigation on how to determine safety levels in major industrial domains and public institution safety management systems.

First, in order to establish a software safety level determination method, domains such as aviation, nuclear power, and railroads, which is traditionally important to safety, is selected, and safety standards is investigated. The content of investigation is composed of various types and methods for determining software safety level, and evaluation items and indicators for software safety level.

It is confirmed that most industry domains use the severity of risk as an assessment item. In addition, it is confirmed that the level of risk involvement, and the availability of redundant safety devices through hardwares and operators were commonly used as evaluation items considering software characteristics.

Second, The software safety level in this study aims to be applied to safety software of public institutions subject to the'Guidelines for securing software safety', a notice of the Software Promotion Act. In order to derive the characteristics of the safety standards applied to the system of public institutions, the case of the type and rating system of public institution systems was investigated.

Lastly, based on the results of the investigation and analysis, a plan for determining the software safety level of public institution systems and a management plan according to the software safety level was derived. The derived results verified validity and objectivity through software safety expert review by field.

Through this study, it is expected that a basic structure for software safety management will be prepared, and in keeping with the 4th industrial revolution, it will contribute to the enhancement of software safety in various industrial fields.

CONTENTS

Chapter 1 Introduction
Section 1 Research Background and Purpose
Section 2 Research Method

Chapter 2 Theoretical Review and Investigation Direction of Safety Rating System
Section 1 Overview of Safety Rating System
Section 2 System Safety Level
Section 3 Software Safety Level
Section 4 Subjects of Software Safety level

Chapter 3 Investigation of Safety Level Determination Method for Each Industrial Domain
Section 1 Investigation Direction
Section 2 Nuclear Safety
Section 3 Railway Safety
Section 4 Aviation Safety
Section 5 Safety of Electrical Appliances
Section 6 Medical Safety
Section 7 US Department of Defense and Aerospace Safety
Section 8 Comparative Analysis of the Safety Class Determination Method of Each Standard

Chapter 4 Investigation of Types and Rating System of Public Institutions
Section 1 Investigation Direction
Section 2 Software related systems/standards applied to public institution systems
Section 3 Investigation of Public Institution Systems where Safety is Important

Chapter 5 Investigation of System Risk Factors in Public Institutions
Section 1 Selection of Systems for Risk Analysis
Section 2 Risk Analysis Results and Evaluation Considerations

Chapter 6 Safety Activities and Technology Investigations According to Safety Level
Section 1 Investigation Direction

Section 2 General Industrial Safety Standard (IEC 61508)
Section 3 Railway Safety Standards (IEC 62279)
Section 4 Safety standards for the automotive sector (ISO 26262)
Section 5 Safety Standards for Aviation Sector
Section 6 Safety Standards in the Medical Field
Section 7 Safety Standards in the Aerospace Sector
Section 8 Safety Standards in the Defense Sector

Chapter 7 Determining the System Software Safety Level for Public Organizations
Section 1 Derivation of the Direction of the Software Safety Level Decision
Section 2 Establishment of Software Safety Level Determination System

Chapter 8 Derivation of Management Plans by System Software Safety Level for Public Institutions
Section 1 Derivation of Candidate Management Plan
Section 2 Arrangement of Outputs, Safety Techniques, and Means in Response to Safety Activities
Section 3 Expert Review

Chapter 9 Conclusion
Section 1 Summary of Research
Secton 2 Future Research

제1장 서 론

제1절 연구배경과 목적

1. 연구배경

4차 산업혁명의 영향으로 소프트웨어의 사용이 확대됨에 따라 소프트웨어 중요성이 강조되고 있다. 국가핵심기반[1]과 안전 중요 제품에 소프트웨어의 영향력도 커지고 있다. 예를 들어 자동차에서 소프트웨어 사용현황을 보면 다음 표와 같으며 연결기반 자율주행 차량(Connected Automated Vehicle, CAV)에서는 통신까지 추가되면서 소프트웨어는 더욱 많이 사용하게 된다.

<표 1-1> 차량에서 소프트웨어 사용도

분류	수동 안전 기술	능동 안전 기술
목적	피해를 최소화	사고 예방
예시	에어백, 안전벨트, 머리지지대	제동거리 단축 시스템, 주차보조 시스템, 차선이탈방지/유지 시스템
소프트웨어 의존도	적음	많음
적용범위	차량 영역	차량 및 주위 환경

자료 : 홍성수 외 (2019.10), 소프트웨어가 주도하는 차량 안전 기술, 오토저널 41(10)에서 편집

소프트웨어에 대한 의존도가 높아짐에 따라 프로그램의 규모가 커지고 복잡해지며 시스템의 안전에 중요한 기능을 직접 지원하거나 구현할 가능성이 높아졌다.[2] 이에 따라 소프트웨어안전을 확보하기는 어려워지고, 이는 안전

1) "국가핵심기반"이란 에너지, 정보통신, 교통수송, 보건의료 등 국가경제, 국민의 안전 · 건강 및 정부의 핵심기능에 중대한 영향을 미칠 수 있는 시설, 정보기술시스템 및 자산 등을 말한다. (재난 및 안전관리 기본법)

2) Matthew John Squair(2005), Issues in the Application of Software Safety Standards, the 10th Australian Workshop on Safety Related Programmable Systems (SCS' 05)

중요시스템에 커다란 영향을 준다. 예를 들어, 프리미엄급 자동차에는 현재 100개의 마이크로프로세서가 포함되어 있으며 약 1억 라인의 소프트웨어 코드에서 실행된다.[3] 복잡하고 거대한 소프트웨어의 코드는 안전 요구사항을 만족하도록 개발하기도 어려울 뿐만 아니라, 안전 보증도 쉽지 않다.

또한, 소프트웨어가 안전중요시스템을 제어하면서 소프트웨어에 의한 직접적인 위험성이 커지고 있다. Lucas Layman et al.(2010)은 NASA의 프로그램을 조사한 결과, 49-70%의 위험한 상태가 소프트웨어로 인해 발생할 수 있거나 소프트웨어가 위험한 상태의 예방에 관여한다는 것을 발견했다.[4]

항공기의 경우는 더욱 심각한 안전상의 문제가 발생하게 되는데 그 사례로 보잉 747 맥스 사고를 들 수 있다. 2018년과 2019년 두 차례 일어난 보잉 737 맥스의 사고는 승무원과 탑승자 346명 전원이 사망하였다. 이 사고의 원인은 보잉 737 MAX 기종에 장착되는 MCAS (Maneuvering Characteristics Augmentation System)이라는 소프트웨어의 결함이었다. 그동안 고려대상이 아닌 새로운 위험, 소프트웨어 오류가 심각한 사고의 원인이 된 것이다.

[그림 1- 1] 보잉 737 맥스의 에디오피아
항공 302편 추락 사고 현장

자료 : The national (2019.3.11.), Ethiopian Airlines flight ET302 crashes en route to Kenya, killing 157

3) J. Gapper(2016), Software is steering auto industry - FT.com, Financ. Times
4) Lucas Layman et al.(2010), The Role and Quality of Software Safety in the NASA Constellation Program

자동차, 항공, 철도 등의 안전중요시스템은 각각의 안전 표준에 따라 개발이 되나, 소프트웨어 개발자를 위한 통합된 소프트웨어 안전 표준은 현재 존재하고 있지 않다. 소프트웨어 개발자가 각각의 자동차, 항공, 철도 등의 도메인 표준을 모두 숙지하기는 쉽지 않은 상황이다.[5] 또한 각 도메인마다 안전 등급을 부여하기 위한 위험분석과 사고율, 안전등급에 각각 다른용어를 사용하여 하나로 통일하고 매칭하는 작업이 필요하다.[6] 이에 소프트웨어 안전 확보를 위한 소프트웨어안전 표준 및 제도를 연구하여 소프트웨어 개발자나 도메인 전문가가 소프트웨어에게 통합된 소프트웨어 안전 표준을 제공할 필요가 있다.

2. 연구목적

본 연구의 목적은 소프트웨어안전을 체계적으로 확보할 수 있는 관리 등급을 개발하고 이를 지속적으로 유지할 수 있는 평가·관리 체계를 마련하는 것이다. 이를 위한 구체적인 목표는 『소프트웨어안전 관리 등급제』를 시행하기 위한 항목과 지표를 설정하는 것이다.

안전중요시스템(Safety-Critical System)이란 시스템의 문제가 인간의 생명, 신체, 시스템 자산과 환경 등에 심각하게 영향을 주는 시스템을 말한다. 자동차, 철도와 항공 등 안전중요시스템은 안전 확보를 위하여 도메인마다 제공된 안전 표준에 따라 개발되고 관리된다. 안전중요시스템은 위험의 정도와 사고 가능성에 따라 안전등급을 나누어 개발되고 있으나, 소프트웨어 경우는 소프트웨어가 포함된 상위 시스템의 안전등급을 그대로 사용하며, 특수한 표준을 제외하고는 소프트웨어만의 안전등급이 존재하지 않는다.

소프트웨어는 대체로 소프트웨어가 포함된 안전중요시스템 위험분석에 따라 도출된 위험원이 상속되어 그 위험원을 제거하도록 개발된다. 그 이유는 소프트웨어의 문제는 독립적으로는 위험하지 않으며, 관련 시스템에 영향을

5) B. Gallina, I. Sljivo, O. Jaradat, Towards a safety-oriented process line for enabling reuse in safety critical systems development and certification, in: Proc. 2012 IEEE 35th Software Eng. Work. SEW 2012

6) Jean-Paul Blanquart et al.(2011), Criticality categories across safety standards in different domains

주어 위험한 사고를 일으키게 된다고 지금까지 생각되어 왔기 때문이다.

4차 산업혁명으로 소프트웨어의 중요성이 증가한 이 시점에서 소프트웨어의 원인으로 일어나는 위험이 상위 시스템의 위험원을 분석하여 결정된 위험보다 높을 수 없는 것인지 검토해 볼 필요가 있다. 소프트웨어에 의한 안전중요시스템의 제어가 증가하면서 시스템의 위험으로 발생하는 문제뿐만 아니라, 소프트웨어의 영향에 의한 시스템의 새로운 위험 요소에 대한 검토가 필요하다.

본 보고서는 소프트웨어 위험 요소를 고려한 소프트웨어 안전등급에 대해 검토하고 소프트웨어 안전등급을 결정하는 평가항목과 지표를 연구하여, 안전이 중요한 도메인에서 활동하는 소프트웨어 개발자와 도메인 전문가에게 안전중요 제품 개발에 도움을 주고자 한다.

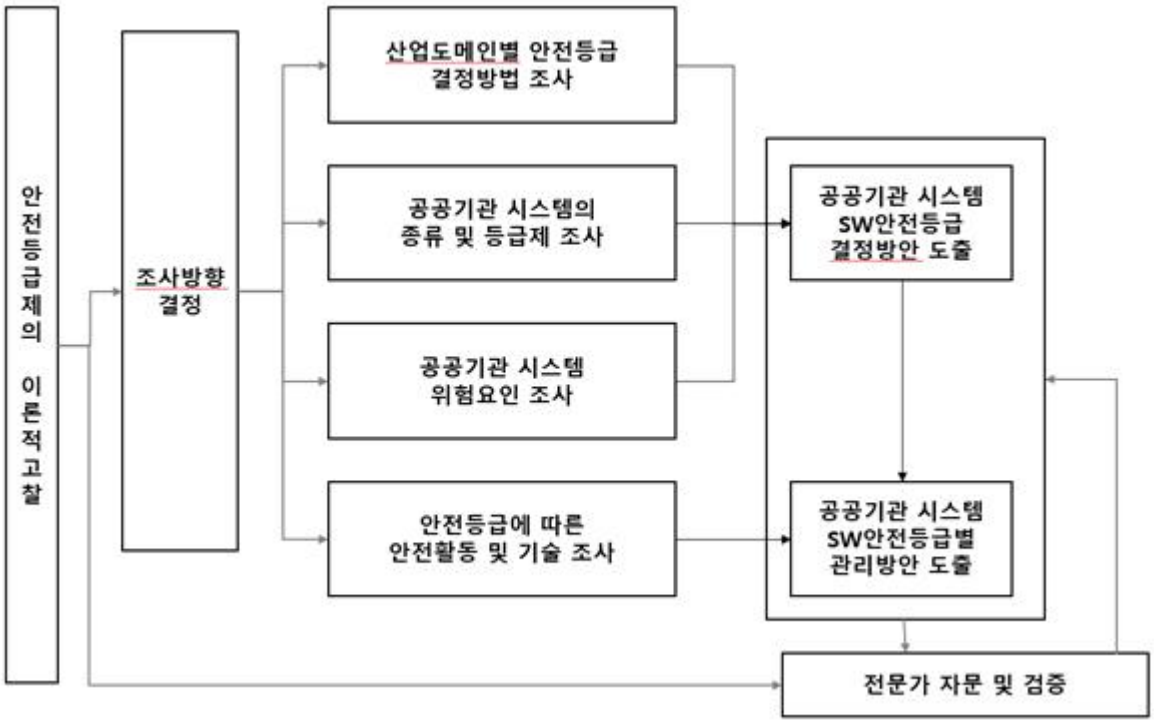
본 보고서는 특히 공공기관 시스템과 기반시설의 유형과 특성을 조사하여 에 공공기관 시스템과 기반시설을 위한 소프트웨어 안전등급 결정방안을 제시한다.

제2절 연구방법

소프트웨어안전 관리를 위한 등급제 구축을 위한 항목 및 지표 마련 연구를 위해 다음과 같은 활동을 바탕으로 안전등급의 기본 틀을 마련하였다.

1. 기초자료 수집을 위한 안전중요시스템 표준과 기존 문헌 연구
2. 소프트웨어안전 전문가·도메인 전문가의 의견을 수렴하는 자문회의 개최
3. 문헌 연구 및 자문회의를 통하여 소프트웨어 안전등급 결정을 위한 항목 및 지표 도출

[그림 1- 2] 연구 방법



문헌 연구로는 등급제 필요성을 도출하기 위해 연구자료를 분석하고 국내외 등급체계 관련 연구를 통한 등급체계 구축의 필수요소를 도출한다. 안전등급을 결정하기 위한 ISO 등 국제 안전표준의 안전등급 판단항목 및 지표를 조사한다. 공공기관 시스템에 우선 적용을 목표로 공공기관 시스템의 특성을 파악하여 현장적용성을 제고한다.

도메인별 소프트웨어안전 특성 적용을 위한 도메인 관련 요인, 하드웨어 안전과는 다른 소프트웨어안전의 특성을 파악하기 위한 자문회의를 실시한

다. 실현 가능한 등급제를 적용하고 향후 시스템 안전관리의 효율성 제고를 위하여 소프트웨어안전 시스템이 필요한 수요 그룹의 의견을 수렴한다.

자료 분석 및 전문가 의견을 종합하여 소프트웨어안전 등급 결정을 위한 후보 방안을 도출하고, 각 방안에 대한 소프트웨어안전 등급 선정을 위한 항목 및 지표 도출의 안을 마련한다. 항공, 철도와 자동차 등의 안전표준의 등급별 안전활동을 조사하여 등급별 안전활동을 정리하고 분석한다.

도출된 안전등급 결정을 위한 방안을 등급제를 적용할 수요그룹과 소프트웨어안전 전문가의 의견을 종합하여, 등급 결정방법을 정한다. 등급 선정 항목 및 지표는 안전 전문가 자문회의를 실시하여 등급별 지표를 검증한다.

이와 같이 국내외 표준 및 등급 관련 법제도, 보고서 분석을 통해서 가능한 등급 결정 방안을 도출하고, 공공기관 시스템의 특성을 반영한 등급 선정 지표와 항목을 결정한다. 전문가 자문을 통한 등급제 연구 결과의 신뢰도를 향상시킨다.

조사 및 분석 결과를 분야별 안전 분야 도메인 및 소프트웨어안전 전문가를 대상으로 전문가 그룹을 구성하고 검증한다. 전문가 구성은 다음과 같다.

〈표 1-2〉 전문가 자문 그룹

분류	세분류	수	비고
도메인 전문가	철도, 국방, 항공, 자동차	각 1명	연구기관, 기업
소프트웨어안전 전문가	소프트웨어안전 평가	3명	연구기관
	소프트웨어안전 검증	1명	대학
	소프트웨어안전 컨설팅	3명	기업

본 연구결과 중 전문가에게 소프트웨어 안전등급 결정방안과 항목 결정방향, 결정된 소프트웨어 안전등급 체계, 소프트웨어 안전등급별 관리방안 선정 등을 검증받고, 전문가의 조언에 따라 수정하였다,

제2장 안전 등급제의 이론적 고찰 및 조사 방향

제1절 안전 등급제 개요

본 절에서는 안전 등급제의 목적을 설명하고, 국가 정보시스템과 시설물의 안전등급을 기술한다. 국가 시스템의 안전등급은 효율적인 위험의 사전 대비를 위하여 안전이 중요한 시스템을 선정하여 안전등급을 결정한 후 등급별로 적합한 방법으로 개발·운영한다. 시설물의 안전등급은 구축 후 사후 관리를 위한 것으로 특정 수준 이상의 안전등급을 유지하도록 관리한다.

1. 안전 등급제

등급제란 특정 목적을 달성하기 위해 품질, 가치, 양 등의 특징에 따라 목적물, 시스템을 분류하는 것을 말한다. 등급제의 첫 번째 목적은 시스템의 개발(또는 구축)과 관리 효율성을 위하여 일정한 기준으로 등급을 분류하여, 등급에 따라 적절한 활동을 수행하는 것이다. 즉 위험의 예방 및 대비의 목적이 강하다. 두 번째 목적은 목적물, 시스템을 평가한 결과에 따라 등급을 분류하여 현황 정보를 제공하고, 체계적인 관리를 하는 것이다. 두 번째 목적은 개발 시부터 위험에 대한 예방의 목적보다 구축 이후에 시스템의 안전성에 대한 반복적 점검에 의한 사후 관리의 목적이 강하다.

첫 번째 목적에 해당하는 안전등급제 중 하나는 『화학물질관리법에 의한 위해관리계획서 이행등급』이다. 사고대비물질 97종을 물질별 지정 수량이상 취급 시 “위해관리계획서”를 작성하여 화학물질안전원에 제출하고, 영업허가를 득한 후 사업장의 취급시설을 운영하도록 하는 절차가 있다. 이때 위험 수준에 따라 위해관리계획서의 내용이 달라진다. 1수준은 화학사고 발생 시 피해 영향 범위에 주민이 없고 최근 5년간 화학사고가 발생하지 않은 사업장이고, 2수준은 1수준에 해당되지 않으면서 공정안전보고서 및 안전성 향상계획서 등 타 법에서의 화학사고 예방제도의 제출 대상이 아닌 경우, 3수준은 1, 2수준에 해당되지 않는 경우로 구분되고 있다.[7)]

7) 애스앰애이(2019), 위해관리계획서 이행등급 산정 세부기준 마련 연구

두 번째 목적에 해당하는 안전등급은 “화학물질관리법에 의한 위해관리계획 이행점검”에 의한 등급이다. 위해관리계획의 이행점검 평가항목과 세부평가기준에 따라 이행점검과 이행수준 평가를 수행한다. 평가점수의 총합에 따라 정기점검 기간을 달리 정한다.[8)]

본 연구에서 수행하려고 하는 『소프트웨어안전 등급제』의 경우는 첫 번째 목적에 주력하려고 한다. 『시설물 안전등급제』의 경우는 노후화에 대비하기 위하여 시설물의 현재 상태를 양호, 불량으로 판정하여 불량의 경우는 시설물을 교체하거나 개선하는 활동을 위해 등급제를 시행한다. 운영 시에 등급제를 시행하여 시설물의 위험을 제거하고자 하는 활동이다. 이는 두 번째 목적에 해당하는 것이다.

소프트웨어안전 등급제 시행을 위한 기초 연구로 국내 다른 분야의 등급제를 조사한다. 안전과 관련이 없는 일반 시스템 등급제와 안전에 관련된 등급제를 조사한다.

2. 정보시스템 등급제

정보시스템 등급제의 경우는 시스템 장애나 중단의 사전 대비를 위하여 또는 보안 사고에 대비하기 위하여 시스템 장애・피해・보안사고 발생 시 예상되는 위험수준에 따라 등급을 결정한 후 등급별로 적합한 방법으로 운영한다. 예를 들면 등급이 높은 시스템은 장애에 대비하기 위하여 서버 관제 시스템이나 재해복수 시스템을 운영한다. 등급의 높은 시스템의 경우 장애를 대비하기 위한 시스템을 운영하고, 백업 등의 활동을 한다. 안전시스템과는 등급을 결정하는 항목은 다르나, 등급을 결정하는 방법에 대해 검토하기 위해 정보시스템 등급에 대해 조사하였다.

가. 지방자치단체 정보시스템 등급

행정안전부에서는 지방자치단체가 구축・운영하는 정보시스템의 장애 예방 및 대응을 위해 정보시스템 등급제를 시행한다. 다음 시스템에 대해 정보시스템 5등급을 부여한다.[9)]

---

8) 환경부(2020), 화학물질관리법
9) 행정자치부(2017.6.9.), 자체단체 정보시스템 장애 예방 및 대응 지침 제9조

- 재해복구시스템
- 개발 및 테스트 용도 시스템
- 단순 정보용 홈페이지 시스템, 단순 메일 기능 시스템
- 백업 및 소산 용도 시스템

크게 3단계로 나누어진 등급 산정절차에 따라 정보시스템 등급은 아래와 같이 결정된다.

[그림 2-1] 등급산정 절차

<표 2-1> 정보시스템의 국가・사회적 중요도에 따른 등급산정

등급	1등급	2등급	3등급	4등급	5등급
판단기준 (기밀성/무결성)	국가 안전보장 관련	국제통상, 국민생명, 경제	국민건장, 복지 등	사회활동, 문화	단순정보 제공

첫째 단계는 기밀성, 무결성 관점에서 정보시스템이 장애 또는 피해 발생 시 예상되는 위험수준을 국가・사회적 중요도에 따라 1~5단계의 등급을 나눈다. 정보시스템은 대분류(18개), 소분류(145개)에 따라 분류되어 있다. 소분류의 기밀성과 무결성 등급은 공개 가능 여부, 대국민 영향, 개인정보 포함여부 등에 따라 정한다. 소분류의 등급은 결정된 기밀성과 무결성 중 높은 등급을 선택한다.

둘째는 정보시스템의 가용성 측면에서 특성을 반영하여 1등급 이하의 단계를 변화시킨다. 정보시스템의 중단・장애 시 피해범위를 고려하여 시스템 특성을 산정한다. 피해 범위에는 일평균 사용자수, 처리시간 증가, 이용 빈도 등을 포함한다.

[그림 2-2] 정보시스템 특성을 반영하는 등급산정 세부내용

지표			점수				
			1점	2점	3점	4점	5점
5점 (지표 1)	정보시스템 중단시 피해 범위*		경미한 불편	처리불편 또는 지연	경제적 손실 또는 처리 오류 발생	중대한 문제 발생	심각한 문제 발생
5점 (지표 2)	일평균 사용자 수 (5점)	행정	전체 5% 이하	전체 25%이하	전체 50% 이하	전체 75% 이하	전체 75% 초과
		대민	1백명 이하	1천명 이하	1만명 이하	10만명 이하	10만명 초과
	처리시간 증가 (5점)		없음	50% 증가	100% 증가	200% 증가	300% 증가
	이용 빈도 (5점)		매년	분기별	매달	매주	매일
	연계 기관 수 (5점)		없음	2개 이하	5개 이하	10개 이하	10개 초과

마지막으로 기관 신뢰도 평가를 통해 5등급을 분류한다. 국가 안전보장과 관련되는 국방, 외교, 치안, 사법, 정보, 방첩과 관련된 기관 등은 1등급을 상향조정한다.

지방자체단체 정보시스템의 경우는 관리하는 정보가 안전에 관련된 내용이 아니고, 안전정보라도 다른 수단에 의해 중복되어 관리될 수 있다면 안전과 관련된 시스템은 아니다. 그러나 시스템 및 자료의 중요성에 따라 중단·장애의 등급을 결정하는 방법은 안전 등급 결정에 활용이 가능한 지 검토하는데 참고가 된다. 세단계로 등급을 결정하는데 첫 번째 단계는 정보시스템의 종류에 따라 정보시스템의 분류한 후 등급 결정 항목에 따라 등급을 산정한다. 두 번째 단계는 정보시스템의 특성을 반영하여 등급을 조정한다. 마지막 단계로 기관신뢰도를 고려하여 등급을 결정한다.

공공기관 안전 시스템의 경우도 안전 시스템을 철도, 항공, 원자력의 기능에 따라 시스템을 분류한 후 초기 등급을 산정하고, 시스템의 특성을 반영하는 방법으로 안전 등급을 결정할 수 있을지 검토할 예정이다.

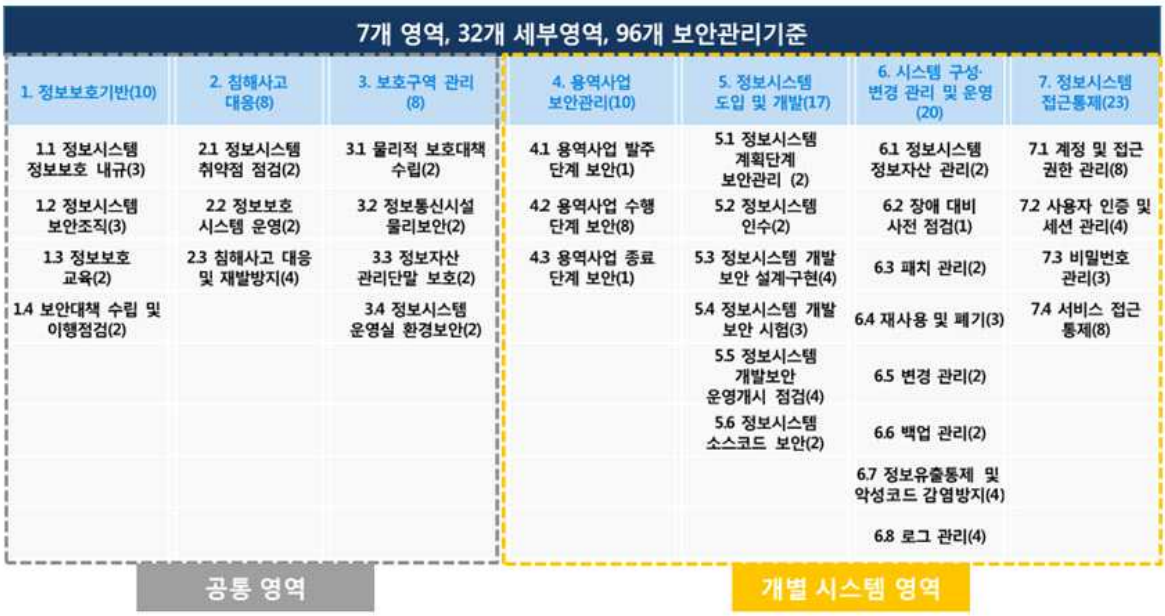
나. 정보시스템 보안 등급

또한, 행정안전부는 행정기관 등의 장이 정보시스템을 구축·운영함에 있어 소관 정보시스템의 중요도, 가용성 등에 따라 등급을 분류하고 등급별

장애관리, 행정정보 관리, 보안관리 등을 수행하게 하였다. [10]

국방, 외교, 통일 등 중요한 업무를 다루는 시스템은 높은 등급을 부여하여 보안을 강화하여 관리하며, 단순 정보 제공을 위한 시스템은 낮은 등급을 부여하여 기본적이고 최소한의 보안관리를 시행한다. 이는 중요한 시스템의 보안관리는 강화하고, 자원을 효율적으로 관리하는 장점이 있다. 등급별 정보시스템 관리의 다른 장점은 기관 담당자들이 보안업무를 수행하는데 있어 업무가이드 역할을 한다는 것이다.

[그림 2-3] 등급별 보안관리 기준



자료 : 행정안전부 보도자료(2019.6.27.) 행안부, '정보시스템 등급별 보안관리' 제도 확산 나선다.

이 제도는 기관 담당자들이 정보시스템에 대해 수행해야 하는 보안관리 업무를 7개 분야 76개 항목으로 제시하고 있다. 76개 항목에 대해 세부 업무 수행 기준을 명시하여 체계적인 관리에 도움을 준다. 이는 소프트웨어안전 등급의 취지와도 일치한다. 단지 보호의 목표가 보안과 안전으로 다르다.

정보시스템 등급분류 기준은 다음과 같다. 시스템이 관리하는 정보 또는 서비스의 기밀성, 무결성 등의 중요성과 사용자수, 연계 기관수 등 가용성에 따라 1~5등급을 부여한다.

10) 행정안전부(2019.8.23.) 행정기관 및 공공기관 정보시스템 구축·운영 지침 제48조의 2

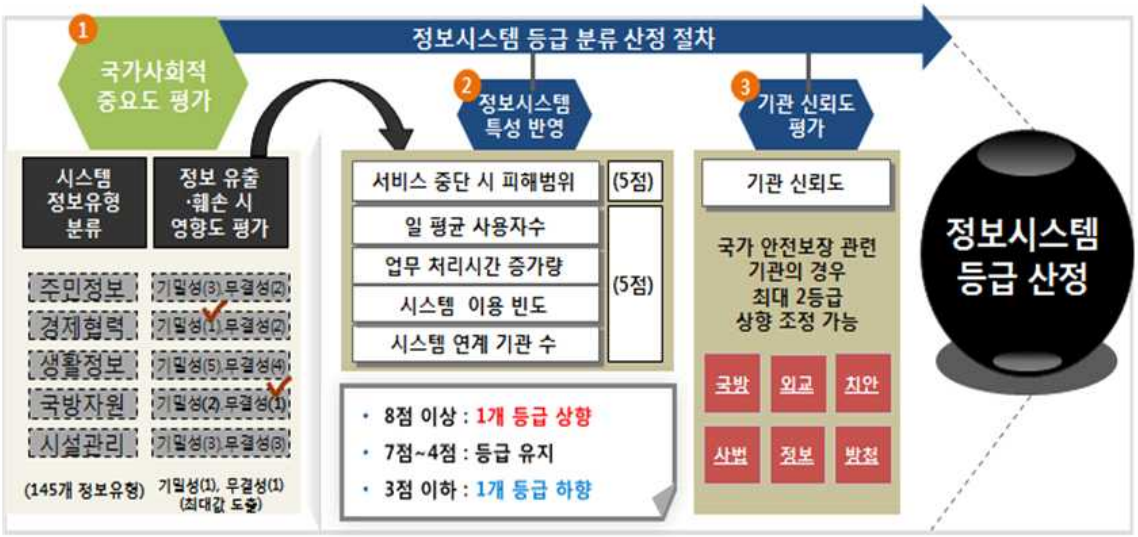
[그림 2-4] 정보시스템 5등급

자료 : 행정안전부 보도자료(2019.6.27.) 행안부, '정보시스템 등급별 보안관리' 제도 확산 나선다.

등급분류의 절차는 시스템의 국가·사회적 중요도를 평가하고 시스템 특성을 반영한 후 기관 신뢰도 평가를 종합하여 정보시스템의 등급을 분류한다. 첫째, 국가·사회적 중요도를 평가는 주민정보, 경제협력, 생활정보, 국방자원, 시설관리 등 145개 정보 유형의 시스템의 정보 유출·훼손 시 영향도를 평가하여 기본 등급을 정하는 것이다. 서비스 중단 시 피해범위, 일평균 사용자수, 시스템 이용 빈도, 시스템 연계 기관 수의 정보시스템 특성을 반영하여 등급의 상향, 하향을 정한다. 또한 국방, 외교, 치안 등 기관 신뢰도에 따라 최대 2등급을 상향 조절가능하다. 이와 같은 절차에 의해 정보시스템 등급이 산정된다.

등급을 결정하는 방법은 장애 관리를 위한 "가. 지방자치단체 정보시스템 등급"과 많이 다르지는 않다. 그러나 시스템의 보안 등급별 활동은 장애를 관리하기 위한 방법과 다르다.

[그림 2-5] 정보시스템 등급분류 절차



자료 : 행정안전부 보도자료(2019.6.27.) 행안부, '정보시스템 등급별 보안관리' 제도 확산 나선다.

이와 같이 분류된 등급기준에 따라 모든 정보시스템에 대해 기본적인 보안지침(국가정보보안기본지침 등)은 준수하도록 규정되었으며, 보안관리 수준은 3단계(H, M, L)로 차별 관리한다.

[그림 2-6] 등급별 보안관리 수준 차별화 내용 예시

기준	1~2등급 (H)	3등급 (M)	4~5등급 (L)
취약점 점검	정보통신기반시설 취약점 점검항목(**상, 중**)에 따라 **외부점검**(연1회), **대내외 웹서비스**에 대해 **모의침투시험**	정보통신기반시설 취약점 점검항목(**상**)에 따라 **자체점검**(연1회), **대외 웹서비스** **모의침투시험**	정보통신기반시설취약점 점검항목(**상**)에 따라 **자체점검**(연1회), **대외 웹서비스** **취약점 진단도구**로 진단
취약점 조치	즉시조치 불가능한 취약점 모니터링(**분기 1회**)	즉시조치 불가능한 취약점 모니터링(**반기 1회**)	즉시조치 불가능한 취약점 모니터링(**연 1회**)
저장매체 불용처리	**물리적** 완전파쇄	**자기적 충격**에 의한 파쇄	**완전포맷 3회 이상** 수행
로그 기록 검토	로그검토 **(월 1회)**	로그검토 **(분기 1회)**	로그검토 **(반기 1회)**
로그 위변조 방지	로그 접근권한 최소화, 로그 별도백업**(3년 이상)**	로그 접근권한 최소화, 로그 별도백업**(6개월 이상)**	

자료 : 행정안전부 보도자료(2019.6.27.) 행안부, '정보시스템 등급별 보안관리' 제도 확산 나선다.

이와 같은 등급분류 개념과 절차, 등급별 관리 수준은 관리하는 대상과 관리 방법만 다를 뿐 소프트웨어안전 등급제에 활용을 할 수 있다. 단지 보안과 안전을 특성이 다른 점을 고려하여 안전의 특성에 맞게 적절하게 차용하는 것이 필요하다.

3. 시설물 안전 등급제

국토교통부는 시설물의 안전 점검과 적정한 유지관리를 통하여 재해와 재난을 예방하고 시설물의 효용성의 증진시키기 위해 “시설물의 안전 및 유지관리에 관한 특별법”을 제정하여 시행하고 있다. 개발 시 위험 예방의 목적보다는 시설물의 구축 이후에 시설물 안전 사후 관리에 목적이 있다.

시설물의 안전검검 실시결과에 따라 해당 시스템의 안정등급을 지정하고 있다. 안전점검 및 정밀안전진단을 시행하고 종합적으로 평가하여 시설물은 상태에 따라 안전등급의 5개로 나뉘는데 기준은 다음과 같다.

<표 2-2> 시설물의 안전등급 기준

안전등급	시설물의 상태
A(우수)	문제점이 없는 최상의 상태
B(양호)	보조부재에 경미한 결함이 발생하였으나, 기능 발휘에는 지장이 없으며 내구성증진을 위하여 일부의 보수가 필요한 상태
C(보통)	주요부재에 경미한 결함 또는 보조부재에 광범위한 결함이 발행하였으나 전체적인 시설물의 안전에는 지장이 없으며, 주요부재에 내구성, 기능성 저하 방지를 위한 보수가 필요하거나 보조부재에 간단한 보강이 필요한 상태
D(미흡)	주요부재에 결함이 발생하여 긴급한 보수, 보강이 필요하며 사용제한 여부를 결정하여야 하는 상태
E(불량)	주요부재에 발생한 심각한 결함으로 인하여 시설물의 안전에 있어 즉각 사용을 금지하고 보강 또는 개축을 하여야 하는 상태

자료 : 국토교통부(2020), 시설물의 안전 및 유지관리에 관한 특별법 시행령

시설물의 안전 및 유지관리 계획의 목표는 안전등급 A,B 시설물 비중을

95%로 유지하는 것이다.[11]

제2절 시스템 안전 등급

국방안전 표준인 MIL-STD-882E는 시스템의 정의를 “명시된 결과를 가지고 명시된 환경 내에서 지정 기능을 수행하는데 필요한 하드웨어, 소프트웨어, 자재, 시설, 인력, 데이터 및 서비스를 구성해 놓은 것”이라고 하였다. 시스템은 여러 가지 뜻으로 쓰이나, 시스템 안전에서 시스템은 하드웨어, 소프트웨어, 인력, 데이터, 환경 등을 모두 포함하는 구성물이다

안전중요시스템은 도메인마다 표준을 다르게 가지고 있다. 대표적인 안전표준으로 전기/전자/프로그래밍 가능한 전기장치의 안전성 표준인 IEC 61508이 있다.[12] 이 표준에서 파생된 자동차 안전표준은 ISO 26262이며, 철도 표준은 IEC 62278이 있다. IEC 61508, ISO 26262는 하드웨어와 소프트웨어의 표준이 포함되어 있으며, 철도의 경우는 소프트웨어 표준으로 IEC 62279가 존재한다. 대부분의 안전표준에서는 하드웨어를 기준으로 안전등급을 정하고 소프트웨어 안전등급은 하드웨어 안전등급과 동일하게 설정한다.

각 표준의 내용과 안전 등급 결정방법은 기존 연구에서 수행하였으므로 간단히만 정리한다. IEC 61508, 자동차, 철도, 항공 등 각 도메인의 안전표준을 이용하는 안전 선진국인 미국, 유럽 등에서는 철도, 항공 시스템은 인증기관을 지정하고 안전표준에 따라 인증을 시행한 후 시장출시가 가능하다. 자동차의 경우는 표준에 따라 시스템을 생산하나, 미국과 유럽의 관리 시스템이 다른데 미국의 경우는 승인없이 출시가 가능하다. 그러나 안전사고 발생 시 제조물책임법에 따라 소비자는 소송을 제기할 수 있으므로, 자동차 제작사는 제작 과실의 의무를 피하기 위해 표준에 따라 자동차를 제작해야 한다.[13] 표준에 따라 시스템개발 시 가장 중요하게 수행하는 작업은 위험 분석과 등급의 결정이다. 등급에 따라 수행하는 요구사항이 달라지고 시스템의 안전도가 다르게 나타나기 때문이다.

IEC 61508과 ISO 26262(자동차 안전표준)에서 안전등급을 설정하는 기준을

11) 국토교통부(2017), 제4차 시설물의 안전 및 유지관리 기본계획(2018 ~ 2022)
12) IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems
13) 트라이즈컨설팅((2015), 소프트웨어안전 산업동향조사

기술한다.시설물에 대한 안전 목표는 동일하며, 안전 목표에 미흡한 정도에 따라 등급을 선정하고 관리한다. 소프트웨어 안전등급에 경우 이와는 다르게 대상 소프트웨어의 안전 목표가 안전 중요도에 따라 다르며, 안전 목표에 따라 요구되는 안전활동의 수준이 다르게 된다.

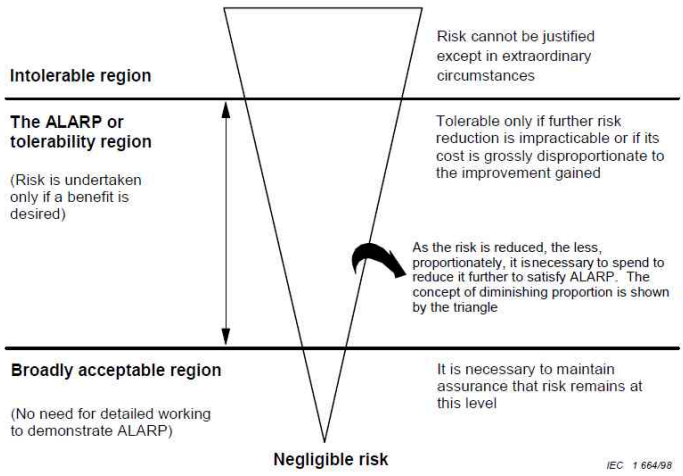
1. IEC 61508의 시스템 안전등급

IEC 61508에서 안전등급은 안전 무결성 수준(SIL, Safety Integrity Level)이라 부른다. SIL은 4단계로 분류되며 각 수준에 따라 주어진 시간 안에 요구되는 안전 기능을 성공적으로 수행할 수 있는 확률을 말한다. 고장 발생확률을 산출하기가 어려워서, 여러 가지 방법을 사용하여 SIL을 결정할 수 있다.

SIL을 결정하는 방법으로는 ALARP(As Low As Reasonably Practicable) 방법, 양적 방법, Risk Graph 방법 등이 있다.[14)]

ALARP 방법은 자체적으로도 사용이 가능하지만, 정성적 방법과 정량적 방법에서도 사용가능하다. 정성적 방법의 경우는 발생 빈도가 2등급이나 3등급을 조건을 충족하도록 안전 기능의 요구사항을 추가하는 방식이다. 정량적 방법의 경우는 빈도와 수치를 지정하고, 개발 자본과 운영비용을 추가하여 2등급이나 3등급을 충족시키도록 SIL 요구사항을 증가하는 것이다.

[그림 2-7] Tolerable risk and ALARP



자료 : IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems, Part 5

14) IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems, Part 5

ALARP에서 등급은 다음과 같이 정의한다.

<표 2-3> 위험등급

위험등급	상태
1등급	받아들이기 어려운 위험
2등급	위험감소를 구현하기 어렵거나, 사용한 비용에 비하여 개선 결과의 효과가 부족한 경우에만 용인될 수 있는 바람직하지 못한 위험
3등급	위험감소 비용이 개선 효과를 넘는 경우의 허용 가능한 위험
4등급	무시해도 될 정도의 위험

위와 같은 등급은 발생 가능성과 결과의 심각성에 따라 결정이 된다.[15)]

Risk Graph 방법은 정량적인 방법으로 SIL은 위험 요소의 지식으로부터 결정된다. 이 방법은 4가지 요소를 결합하여 그래프를 이용하여 SIL을 결정하는데, 그 요소는 '심각성(Consequence)', '위험에 노출되는 시간(Frequency of, and exposure time in, the hazardous zone)', '위험회피 가능성(Possibility of avoiding the hazardous event)', '기능실패 가능성(Probability of the unwanted occurrence)' 등으로 구성된다.[16)]

IEC 61508은 소프트웨어 개발 단계별로 필요한 문서를 정의하고 있으며, IEC 61508은 등급별, 개발 단계별로 안전을 확보하기 위한 기술들을 소개하고 있다. 예를 들면 다음 표는 소프트웨어 설계 및 개발 단계의 상세설계에서 필요한 기술들을 보여준다.

15) 트라이즈컨설팅((2015), 소프트웨어안전 산업동향조사
16) 송지환 외(2018), 소프트웨어안전 분야 선정기준 및 소프트웨어안전공통기준 도출 연구

[그림 2-8] IEC 61508 소프트웨어 개발 시 등급별 필요한 기술

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1a	Structured methods **	C.2.1	HR	HR	HR	HR
1b	Semi-formal methods **	Table B.7	R	HR	HR	HR
1c	Formal design and refinement methods **	B.2.2, C.2.4	---	R	R	HR
2	Computer-aided design tools	B.3.5	R	R	HR	HR
3	Defensive programming	C.2.5	---	R	HR	HR
4	Modular approach	Table B.9	HR	HR	HR	HR
5	Design and coding standards	C.2.6 Table B.1	R	HR	HR	HR
6	Structured programming	C.2.7	HR	HR	HR	HR
7	Use of trusted/verified software elements (if available)	C.2.10	R	HR	HR	HR
8	Forward traceability between the software safety requirements specification and software design	C.2.11	R	R	HR	HR

자료 : IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems, Part 3

2. ISO 26262의 안전등급

자동차 표준인 ISO 26262에서 안전등급은 ASIL(Automotive Safety Integrity Level)이다. ASIL도 IEC 61508과 비슷하게 4등급으로 나누어져 있다. 자동차 표준에서 등급을 나누는 기준은 심각성(Severity), 위험 노출 시간(Probability of exposure regarding operational situations), 통제가능성(Controllability)이다.[17]

등급은 A,B,C,D로 나뉘며 D가 가장 높은 등급이다. 이 표준의 경우는 등급이 높을수록 요구되는 추천 요구사항이 높아지며, 등급에 따라 추천되는 사항을 표로 정리하고 있다.

3. 시스템 안전등급 결정 방법 및 조사 대상

도메인마다 시스템 안전등급을 결정하기 위한 위험분석 방법과 위험원은 다르나, 시스템 안전등급을 결정하기 위한 항목은 비슷하다. 이 절에서는 IEC 61508과 자동차 표준(ISO 26262)의 등급 결정방법에 대해 정리하였는

17) ISO 26262, Road vehicle Functional safety, Part 3

데, 철도나 항공 표준들도 시스템 안전등급을 결정하기 위한 항목은 위험 발생도와 피해 심각도가 공통 항목으로 포함되어 있다. 각 표준별 상세한 등급 선정 항목 및 지표를 분석하기 위해 『제3장 산업 도메인별 안전등급 결정방법 조사』에서 원자력, 철도, 항공, 전기용품, 의료, 국방, 항공우주 등의 표준을 조사하도록 하겠다.

제3절 소프트웨어 안전등급

1. 소프트웨어 안전등급이 필요한 이유

가. 안전 중요도에 따른 소프트웨어안전 확보

소프트웨어안전 등급제는 개발 및 운영 시에 안전을 확보하기 위해 소프트웨어의 에러를 제거하고 안전기능을 추가하는 정도를 결정하기 위해 소프트웨어의 “위험 영향력”과 “소프트웨어 위험관여도”등의 항목에 따라 안전등급을 결정하고 관리하는 것이다. 소프트웨어안전 등급이 높을수록 반드시 해야 하는 소프트웨어안전 활동 요구사항이 많아지게 된다.

소프트웨어안전 등급은 위험도에 따라 어느 정도의 안전을 확보할 것인지에 대한 기준이 되기 때문에 필요하다. IEC 61508에서는 [그림 2-8] IEC 61508 소프트웨어 개발 시 등급별 필요한 기술과 같이 등급에 따라 적용해야 하는 기술이 늘어나고, 그에 따라 안전도가 높아지고, 안전 검증도 더 상세하고 정확하게 할 수 있다.

나. 통합적이고 체계적인 소프트웨어안전 관리

자동차, 항공, 철도 등의 안전중요시스템은 각각의 안전 표준에 따라 개발이 되나, 소프트웨어 개발자를 위한 통합된 소프트웨어 안전표준은 현재 존재하지 않다. 소프트웨어 개발자가 각각의 자동차, 항공, 철도 등의 도메인 표준을 모두 숙지하기는 쉽지 않은 상황이다.[18] 또한 자동차, 항공, 철도 등

18) B. Gallina, I. Sljivo, O. Jaradat, Towards a safety-oriented process line for enabling reuse in

의 도메인 전문가가 소프트웨어안전 확보 요건이나 기술을 습득하기는 더욱 어렵다. 그러므로 안전소프트웨어 개발자와 자동차, 항공, 철도 등 도메인 전문가가 쉽게 접할 수 있고, 각 표준 간 최신 기술을 포함하는 소프트웨어안전활동과 기술을 소프트웨어 안전등급에 따라 제시할 필요가 있다.

다. 소프트웨어안전 관리 효율성 확보

또 다른 이유는 보장된 안전도에 따라 비용이 결정되기 때문이다. IEC 61508의 ALARP의 개념과 같이 안전은 100% 보장이 어려우며, 안전도 상승 대비 비용의 상승이 너무 커서 안전도 상승에 의미가 없을 수도 있다. 소프트웨어 안전 확보의 경우도 시스템 안전 확보와 동일하게 안전 대비 비용을 고려해야 한다.

John A McDermid (2001)는 안전한 소프트웨어를 위해 소프트웨어의 안전도를 높이고 안전 기능을 추가하는데 비용과 시간이 상당히 필요하다고 했다.[19] Matthew John Squair(2005)는 소프트웨어의 중요성이 높을수록 무결성 수준 및 관련 개발 노력이 높아 지므로 안전한 소프트웨어를 생산하는데 더 많은 비용이 든다고 했다.[20] W. Eric Wong,(2014)은 불필요한 추가 비용 지출을 피하기 위해서는 위험이 낮은 시스템에 엄격한 안전 표준을 적용하는 것은 피해야 하고 표준은 시스템의 최소 위험 수준에 대한 지침을 제공해야 한다고 했다.[21]

그러므로 위험도의 심각성에 따라 소프트웨어 개발 시 들어가는 비용과 시간을 조절한 필요가 있다. 즉, 위험도 및 발생확률 등의 요인이 높아 상위 안전등급을 받은 소프트웨어의 경우는 하위 안전등급을 받은 소프트웨어에 비해 개발 비용 및 기간이 많게는 2배 이상 들어가게 된다. W. Eric Wong(2014)에 따르면 안전 보장 활동은 프로젝트에서 개발 시간과 가격을

---

safety critical systems development and certification, in: Proc. 2012 IEEE 35th Software Eng. Work. SEW 2012

19) John A McDermid(2001), Software Safety: Why is there no Consensus?, 21th ISSC(International System Safety Conference)

20) Matthew John Squair(2005), Issues in the Application of Software Safety Standards, the 10th Australian Workshop on Safety Related Programmable Systems (SCS' 05)

21) W. Eric Wong et al.(2014), Evaluating Software Safety Standards: A Systematic Review and Comparison, 2014 Eighth International Conference on Software Security and Reliability

높이기 때문에 안전표준은 안전과 비용을 동시에 고려해야 한다고 한다. 그는 일반 소프트웨어에 비해 가장 높은 안전등급의 소프트웨어를 개발하는 비용은 75%에서 150%보다 더 많게 들어간다고 했다.[22] 그 이유는 안전등급이 높아질수록 적용해야 하는 기술, 도구 등이 많아지고 복잡해지며, 대상 소프트웨어 테스트 및 검증도 더 세밀하게 해야 한다.

“국방 장비의 안전 관련 소프트웨어에 대한 요구사항[23](DEF STAN 00-55)” 에는 소프트웨어 안전 등급별로 수행해야 하는 활동들을 제공하고 있다. 이는 등급별로 해야 하는 활동들을 다음과 같이 분류하고 있다.

- M : 필수 수행

- J1 : 조항 또는 조항의 일부를 따르지 않으면 정당화 필요하다. 정당화는 **소프트웨어 무결성의 미미한 향상이 규정 준수를 통해 얻어지거나** 규정 준수 비용이 이익에 비해 과도하다는 것을 나타낼 수 있다.

- J2 : 조항에 설명된 역할, 방법, 제품 또는 활동의 누락 또는 불이행에 대한 정당성이 제공되어야 하지만, 개별 조항 또는 조항의 일부를 준수하지 않는다는 상세한 정당화는 필요하지 않다. 정당화는 컴플라이언스가 소프트웨어의 무결성을 크게 향상시키지 못하거나 컴플라이언스 비용이 이익을 얻기 위해 과도하다는 것을 나타낼 수 있다.

DEF STAN 00-55 표준에서는 안전 활동을 수행하지 않아도 되는 이유를 두 가지로 제공하고 있다. 첫 번째는 해당 안전 활동을 수행하는 것이 국방 장비 안전에 큰 영향을 주지 않는 경우이다. 두 번째는 ‘J1’의 경우와 같이 해당 안전 활동을 수행하는 것에 대한 규정 준수 비용이 이익에 비해 과도할 경우이다. 표준에서 안전 등급에 따라 수행해야 하는 기능을 결정할 때 고려하는 요소로 “비용”이 중요하게 간주되는 것을 확인할 수 있다.

반면에 C. Abis(200)은 록히드마틴은 C-130J 항공기를 일반 시스템 비용의 절반으로 DO-178B 레벨 A로 개발할 수 있다고 했다. 이는 표준에서 요구하는 바를 정형적인 프로세스를 적용한다면, 오히려 적은 비용으로 개발이 가능하다고도 할 수 있다. 이는 시스템의 등급을 정하고 등급마다 정형적인

22) W.Eric Wong(2014), Evaluating Software Safety Standards: A Systematic Review and Comparison, 2014 Eighth International Conference on Software Security and Reliability

23) UK Ministry of Defence(1997), DEF STAN 00-55 REQUIREMENTS FOR SAFETY RELATED SOFTWARE IN DEFENCE EQUIPMENT PART 2: GUIDANCE

프로세스를 사용한다면 안전을 확보하면서 비용을 절감하는 좋은 방법이 된다고 할 수 있겠다.

2. 안전표준의 소프트웨어 안전등급 결정 방법 및 조사 방향

시스템 안전등급에 관해서는 본장 제2절 시스템 안전 등급제에서 정리한 바와 같이 항공, 철도, 원자력 등 도메인마다 표준을 가지고 있으며, 각 표준마다 시스템 안전등급과 소프트웨어안전 등급을 정하는 방식이 다르다.

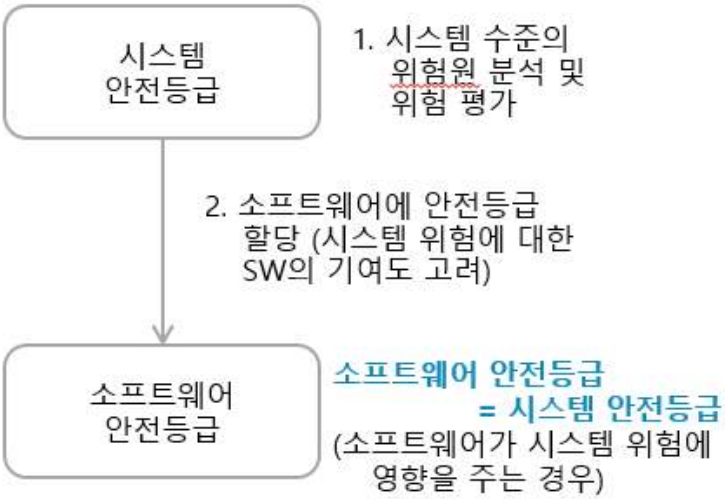
대부분의 소프트웨어안전 등급은 시스템 안전에 대한 중요도에 따라 시스템 안전 등급과 동일하게 결정된다.[24] 대부분의 도메인에서 시스템의 위험은 위험 심각도와 발생률에 따라 정하지만, 각 도메인 마다 위험 심각도와 발생율 정하는 방식과 기준은 차이가 있다.[25]

그러므로 시스템 표준에 따라 소프트웨어안전 등급을 결정하는 방법이 다르게 된다. 그러나 유사한 원칙은 등급결정과 관련된 위험원에 대해 소프트웨어가 원인이 된다면, 소프트웨어안전 등급은 시스템 안전등급을 그대로 상속한다. 소프트웨어 수준에서 추가적인 요소들에 대한 평가를 수행하지 않는다. IEC 61508 (산업일반), IEC 62278/62279 (철도 분야, DO-178C (항공 분야), ISO 26262 (자동차 분야) 등이 사용하는 방법이다.

24) John A McDermid(2001), Software Safety: Why is there no Consensus?, 21th ISSC(International System Safety Conference)

25) Jean-Paul Blanquart et al.(2011), Criticality categories across safety standards in different domains

[그림 2-9] 소프트웨어안전 등급 결정방법(1)



두 번째 방법은 시스템에서 산출한 위험도와 소프트웨어적 특성을 포함하여 소프트웨어안전 등급을 결정하는 방법이다. 그 예로 국방표준(MIL-STD-882)이 있다.[26] 즉 시스템 위험에 대한 심각도(Severity)와 발생가능성(likelihood)에 대한 평가와 소프트웨어가 해당 시스템 위험에 관여하는 정도(Software Control Category)를 평가하여 소프트웨어 안전 등급을 분류한다.

마지막 방법은 시스템 수준의 위험평가에 대한 고려 없이 소프트웨어 수준에서 소프트웨어 안전등급을 평가하는 방법이다. 소프트웨어 외부요소에 의한 위험감소를 고려하여 소프트웨어로 인해 발생가능한 위험의 심각도에 따라 소프트웨어안전 등급을 결정한다. 그 사례로는 IEC62304 (의료), IEC 60730 (자동전자제어장치) 등의 표준이 있다.

26) John A McDermid(2001), Software Safety: Why is there no Consensus?, 21th ISSC(International System Safety Conference)

<표 2-4> IEC 60730의 안전등급 기준

안전등급	정의
A Class	장비의 안전을 위해 의존하지 않는 제어 기능 사례 : room thermostats, humidity controls, lighting controls, timers, and 소프트웨어itches
B Class	제어된 장비의 안전하지 않은 작동을 방지하기 위한 제어 기능 사례 : thermal cut-offs and door locks for laundry equipment
C Class	특수 위험을 방지하기 위한 제어 기능 (폭발 제어 장비 등) 사례 : automatic burner controls and thermal cut-outs for closed, un-vented water heater systems

자료 : IEC 60730, Safety Standard for Household Appliances

3장에서 조사하고자 하는 표준은 소프트웨어 등급을 결정하는 세 가지 방법을 모두 포함하고 있다. 각 표준들에 대해 소프트웨어 안전등급을 결정하는 방법에 대해 자세히 조사하고, 어느 방안이 소프트웨어 안전등급 결정에 공통적으로 사용가능한 지 분석하고자 한다.

제4절 소프트웨어안전 등급 적용 대상

본 절에서는 소프트웨어안전 등급을 적용해야 하는 대상을 선정하기 위하여 『정보통신기반 보호법』의 주요정보통신기반시설 지정[27]대상과 분류, 지정 현황 등을 검토한다. 『재난 및 안전관리 기본법(약칭 : 재난안전법)』의 제26조(국가핵심기반의 지정 등)를 검토한다.

주요정보통신기반시설과 국가핵심기반 지정대상을 검토하고 공공기관 시스템의 소프트웨어안전 등급 적용 대상 선정 시 참고할 수 있는 부분에 대해 언급하고자 한다.

1. 주요정보통신기반시설 적용 대상

『정보통신기반 보호법』에서는 각 중앙행정기관의 장에게 소관 분야의 정보통신기반시설 중 하위 5가지 기준에 의해 전자적 침해 행위로부터 보

27) 정보통신기반보호법 제8조(주요정보통신기반시설의 지정 등)

호해야 할 필요가 있다고 인정되는 시설에 대하여 주요정보통신기반시설로 지정할 수 있게 하고 있다.

<표 2-5> 전자적 침해 행위로부터 보호해야 할 필요가 있다고 인정되는 시설 기준

1) 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2) 해당 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3) 다른 정보통신기반시설과의 상호연계성
4) 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5) 침해사고의 발생가능성 또는 그 복구의 용이성

자료 : 정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)

국가정보원과 과학기술정보통신부에서는 『주요정보통신기반시설 지정평가기준 가이드라인』을 제공하고 있다. 가이드라인에 따르면 주요정보통신기반시성 지정대상을 다음과 같이 분류하고 있다.

<표 2-6> 주요정보통신기반시설 지정대상의 분류

정보통신 및 미디어	유무선 통신 시설, 포털, IDC, 방송국, 신문사 등	**식품의약품 관리**	식품의약품 관리 기관 등
금융기관	은행, 증권사, 신용카드사, 화폐 발행 및 유통 기관 등	**보건복지**	병의원, 혈액원, 백신 제조업체, 복지 관련 기관 등
교통수송	철도, 공항, 항만, 도로・교량, 교통제어체계 등	**정부기관**	중앙행정부처 및 지방자치단체, 입법부, 사법부 등
에너지	원자력을 제외한 발전시설, 변전시설, 정유시설, 도시가스 배관시설 등	**사회안전시설**	치안, 소방 등과 관련된 기관
		건설・환경	건설업체, 소각장, 매립지, 독성물질 취급 시설 등
원자력	원자력 발전시설, 방사성 유출물 저장 시설 등	**지리정보**	지도 제작 및 유통 기관 등
식・용수	정수장, 하수처리장 등	**기타**	연구소, 본인 확인 기관 등

자료 : 국가정보원・미래창조과학부(2014), 주요정보통신기반시설 지정평가기준 가이드라인

본 가이드에서는 중앙행정기관에서 수립하는 공통기준인 1차 평가기준과, 지정대상시설 관리기관이 수행하는 2차 평가기준을 제공한다. 1차 평가기준은 <표 2-6> 주요정보통신기반시설 지정대상의 분류에 따라 서비스 대상,

범위, 피해 등의 기준을 다르게 설정하고 시설에 따른 특성을 추가한 기준도 제공하고 있다. 2차 평가기준은 제어시스템을 포함한 분야와 그렇지 않은 분야의 평가항목 및 점수를 다르게 산정하도록 하고 있다.

2019년 12월 기준으로 공공분야 141개와 관리기관 265개 시설, 민간분야 91개와 관리기관 149개 시설 등 총 414개의 주요정보통신기반시설을 지정·관리 중이다.

[그림 2-10] 주요정보통신기반 시설 지정 현황

	2013	2014	2015	2016	2017	2018	2019
공공	135	193	227	243	252	262	265
민간	74	99	127	142	141	149	149
합계	209	292	354	385	393	411	414

자료 : 국가정보원 등(2020), 2020 국가정보보호백서

행정안전부는 국가안보 및 경제사회에 미치는 영향 등을 고려하여 주요정보통신기반시설을 지정(2019년 12월 기준 102개)하여 관리하고 있으며, 주요정보통신기반시설을 보호하기 위하여 취약점 분석·평가, 보호대책 수립 등의 지원과 기술 가이드 배포 등을 수행하고 있다.

[그림 2-11] 행정안전부 소관 주요정보통신기반 시설 지정 현황

합계	제어시스템(50)						정보시스템(52)		
102	철도운영	교통신호	상수도	지역난방	U-CITY	물재생	긴급구조	시·도 행정	행안부
	12	12	16	2	5	3	19	17	16

자료 : 국가정보원 등(2020), 2020 국가정보보호백서

<표 2-5> 전자적 침해 행위로부터 보호해야 할 필요가 있다고 인정되는 시설 기준을 안전에 적용해 보면 <표 2-7> 소프트웨어안전을 확보할 필요가 있는 시설 기준과 같이 변경해야 하는 부분이 있다.

〈표 2-7〉 소프트웨어안전을 확보할 필요가 있는 시설 기준

1) 해당 ‘소프트웨어안전 중요시스템’을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2) 해당 기관이 수행하는 업무의 ‘소프트웨어안전 중요시스템’에 대한 의존도
3) 다른 ‘소프트웨어안전 중요시스템’과의 상호연계성
4) 소프트웨어 안전사고의 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5) 안전 사고의 발생가능성 또는 그 복구의 용이성

4) 소프트웨어 안전사고의 경우 국가안전보장과 경제사회에 미치는 **피해 규모 및 범위**, 5) 안전 사고의 **발생가능성** 또는 그 복구의 용이성는 시스템 안전등급을 정할 때의 기준인 ‘위험 발생도’와 ‘피해 심각도’와 같은 의미이다. 3) 다른 ‘소프트웨어안전 중요시스템’과의 상호연계성은 소프트웨어에서 피해의 규모 및 범위와 연관되어있는 요소이다. 소프트웨어 시스템은 항공, 자동차 등의 시스템보다는 다른 소프트웨어시스템과 연계가 용이하고 복잡하기 때문이다.

2. 국가핵심기반 적용 대상

재난안전법에서 “국가핵심기반“이란 에너지, 정보통신, 교통수송, 보건의료 등 국가경제, 국민의 안전·건강 및 정부의 핵심기능에 중대한 영향을 미칠 수 있는 시설, 정보기술시스템 및 자산 등을 말한다.

〈표 2-8〉 국가핵심기반 지정 기준

1) 다른 국가핵심기반 등에 미치는 연쇄효과
2) 둘 이상의 중앙행정기관의 공동대응 필요성
3) 재난이 발생하는 경우 국가안전보장과 경제·사회에 미치는 피해 규모 및 범위
4) 재난의 발생 가능성 또는 그 복구의 용이성

자료 : 재난안전법 제26조(국가핵심기반의 지정 등)

3. 재난이 발생하는 경우 국가안전보장과 경제·사회에 미치는 피해 규모 및 범위, 4. 재난의 발생 가능성 또는 그 복구의 용이성 기준은 주요정보통신시반시설과 보안사고와 재난이라는 방어 대상만 다를 뿐 '피해 규모 및 범위', '발생가능성' 기준은 동일하다. 주요정보통신기반시설과 다른 기준은 2. 둘 이상의 중앙행정기관의 공동대응 필요성이라는 기준이다. '둘 이상의 중앙행정기관의 공동대응'에도 불구하고 안전 확보에 면에서 철도, 항공, 자동차 등 각 안전관리 기관이 달라, 체계적인 예방, 대비, 대응, 복구가 어렵다. 특히 소프트웨어안전이 중요한 자율주행차의 경우는 영국 사례를 살펴보더라도 경제.에너지.산업 전략부의 협업을 통해 관리를 하고 있다.[28] 그러므로 소프트웨어안전 시스템의 관리도 중앙행정기관의 공동대응 필요성을 검토해 볼 필요가 있다.

3. 주요정보통신기반시설과 국가핵심기반에 기반한 적용 대상

주요정보통신기반시설과 국가핵심기반 지정 기준을 통합하면 다음과 같은 기준이 도출된다.

〈표 2-9〉 소프트웨어안전을 확보할 필요가 있는 시스템 기준

1) 해당 '소프트웨어안전 중요시스템'을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2) 해당 기관이 수행하는 업무의 '소프트웨어안전 중요시스템'에 대한 의존도 및 둘 이상의 중앙행정 기관의 공동대응 필요성
3) 다른 '소프트웨어안전 중요시스템'과의 상호연계성
4) 소프트웨어 안전사고의 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5) 안전 사고의 발생가능성 또는 그 복구의 용이성

위의 기준에 대해 소프트웨어 안전등급 대상 시스템을 선정하기 위해서는 세

28) 진회승 외(2018), 소프트웨어 안전 산업 동향조사 18p 해외 선진사례 조사-자율주행차 관련 정책 및 지침/가이드 동향-영국

부 기준이 도출되어야 한다. 이를 위해 다음과 같은 조사를 시행하고자 한다.

4. 공공기관 시스템 조사 방향

소프트웨어 안전등급 적용 대상 선정은 본 연구의 범위는 아니나, 향후 등급제를 시행할 경우 중요한 요소이므로 공공기관 시스템의 위험요인과 시스템 특성을 조사함과 동시에 공공기관 시스템 종류 및 분류에 대한 기초조사를 수행한다.

제4장에서 공공기관 시스템의 소프트웨어 안전등급 결정방안을 도출하기 위한 공공기관 시스템의 유형과 특징을 조사하기 위하여 국내외 공공시스템 분류 기준을 조사한다. 국가기반시설 지정 기준을 조사하고, 위험도 평가 예시를 살펴 본다. 주요정보통신기반시설 지정 예를 조사하기 위하여 각 부처 고시를 조사한다. 지정된 주요정보통신기반시설은 고시를 통해 발표하게 되어있었으나 현재는 보안 확보를 위해 발표하지 않는다.

공공기관 시스템과 국가기반시설에 안전등급을 적용 대상을 검토하기 위하여 국내외 안전중요시스템의 분류기준에 대해 조사한다. 미국은 표준 기술연구원에서 정보시스템 보안 기준 및 분류 기준을 제시하고 있다.

국내는 재난 및 안전관리 기본법에서 국가 핵심 기반 분류기준을 제시한다. 통합방위법에 의한 국가중요시설 분류기준을 검토한다. 민간투자법은 사회기반시설을 각종 생산활동의 기반이 되는 시설, 해당 시설의 효용을 증진시키거나 이용자의 편의를 도모하는 시설 및 국민생활의 편익을 증진시키는 시설로 정의하고 있으며, 제시한 세부기준을 조사한다.

제3장 산업 도메인별 안전등급 결정방법 조사

제1절 조사 방향

본 장에서는 주요 산업 도메인에서 안전등급을 결정하는 방법들에 대하여 조사한다. 먼저, 원자력, 철도, 항공 등 전통적으로 안전을 중요하게 다룬 도메인을 식별하여 관련 제도 및 안전기준을 조사하고, 의료, 국방, 항공우주 등 소프트웨어 안전등급에 대한 평가 기준을 보다 상세하게 다룬 도메인의 자료를 조사한다.

먼저 각 도메인 관련 국내외 법제도를 조사하고, 각 도메인의 안전등급 기준 관련 문서를 검토하여 안전등급 평가 기준을 조사한다. 조사를 바탕으로 소프트웨어 안전등급의 결정 방법, 소프트웨어 안전등급 평가항목과 지표, 소프트웨어 안전등급 구분 등의 시사점을 도출한다.

조사 대상은 다음과 같다.

ㅇ원자력 안전 기준

ㅇ철도 안전기준

ㅇ항공 안전기준

ㅇ전기용품 안전기준

ㅇ의료 안전기준

ㅇ미국 국방 안전기준

ㅇ미국 항공우주 안전기준

제2절 원자력 안전

원자력 분야의 안전기준은 크게 IAEA / IEC 관련 표준과 NRC / IEEE 관련 표준으로 구분된다. IAEA / IEC 관련 표준은 주로 유럽 쪽에서 안전기준으로 사용되고 있으며,

NRC / IEEE 관련 표준은 우리나라, 미국 등에서 안전기준으로 사용되고 있다. 본 절에서는 두 표준에서 정의하고 있는 안전등급 분류 기준에 대해서 살펴 본다.

1. IAEA / IEC 관련 원자력 안전기준

가. IAEA 안전기준

IAEA NS-G-1.3[29]에 의하면 I&C (Instrumentation and Control) 시스템은 크게 2가지 분류-안전에 중요한 시스템(important to safety)과 안전에 중요하지 않은 시스템-로 구분된다. 안전에 중요한 시스템은 아래와 같이 2개의 하위 분류로 구분된다.

ㅇ 안전 시스템 (Safety system)

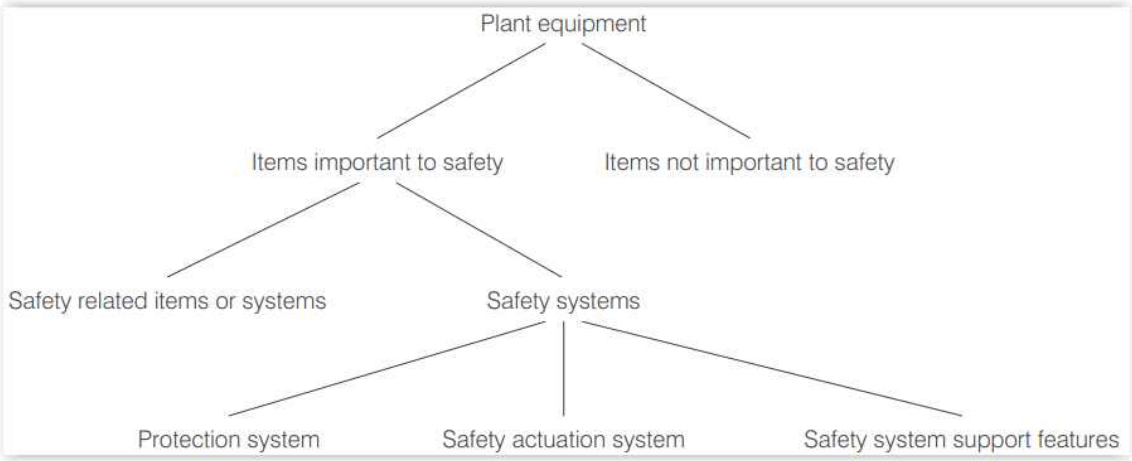
- 원자로의 안전정지 또는 노심 잔열 제거에 필수적인 시스템
- 예상운전과도상태(AOO: anticipated operational occurrences)나 설계기준사고(DBA: design basis accidents)의 결과를 제한하는 시스템
- [그림 3-1]과 같이 보호 시스템, 안전 작동 시스템, 안전 시스템 지원 기능이 포함됨

ㅇ 안전 관련 시스템 (Safety-related system)

- 안전 시스템은 아니나 안전에 중요한 기능을 수행하는 시스템
- 예시: 원자로 제어 및 제한 시스템 (reactor control and limitation system), HMI 패널 (human-machine interface panel), 방사능 감시 시스템 (radiation monitoring systems)

29) IAEA Safety Standard Series, Safety Guide, No. NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants

[그림 3-1] 원자력 - IAEA NS-G-1.3에 의한 시스템의 안전 분류



자료: IAEA Safety Standard Series, No. NS-G-1.3

IAEA SSR-2/1[30]에서는 시스템의 안전에 대한 분류가 시스템이 수행하는 기능(function)과 안전에 대한 중요성(safety significance)에 기반하여야 한다고 명시하고 있다.[31] 이와 관련하여, 다음 기능을 수행하는 시스템을 안전에 중요한 시스템으로 정의하고 있다.[32]

- ㅇ 반응도 제어 (Control of reactivity)
- ㅇ 노심잔열제거 (Removal of heat from the reactor and from the fuel store)
- ㅇ 방사선 누출물 차단 (Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases)

또한, 해당 안전기준에서는 안전에 중요한 시스템 간 간섭이 없어야 함을 강조하고 있으며, 여러 기능을 수행하는 시스템의 경우, 가장 중요한 기능의 안전등급으로 시스템의 안전등급을 분류하고 있다. IAEA SSR-2/1에서 정의하고 있는 시스템의 안전 중요성 판단 시 고려해야 하는 요소는 다음과 같다.[33]

- ㅇ 시스템에 의해 수행되는 안전기능
- ㅇ 안전기능 수행의 실패로 인한 결과 (consequences)

---

30) IAEA Safety Standards, Specific Safety Requirements, No. SSR-1/2, Safety of Nuclear Power Plants: Design
31) IAEA SSR-2/1 Requirement 22
32) IAEA SSR-2/1 Requirement 4
33) IAEA SSR-2/1 Requirement 22

ㅇ 안전기능이 호출되는 빈도 (frequency)

ㅇ 위험발생이 가능한 이벤트(postulated initiating event) 이후 안전기능이 호출되는 시간 (time) 또는 기간 (period)

IAEA SSG-30[34]은 IAEA SSR-2/1의 안전분류 요구사항에 따라 안전등급을 분류하기 위한 구체적인 기준을 제시하고 있다. 안전 중요성에 대하여 다음과 같은 요소를 고려하도록 가이드하고 있으며, <표 3-1>와 같이 안전기능 수행 실패로 인한 결과의 심각도(Severity) 분류 기준을 정의하고 있다.

ㅇ 안전 중요성에 대한 고려 요소

- 안전기능 수행의 실패로 인한 결과 (consequences)
- 안전기능과 관련된 위험발생가능한 이벤트(postulated initiating event)의 발생빈도 (frequency)
- 안전상태(safe state) 또는 통제상태(controlled state)를 달성하는데 기여 정도 (significance of the contribution)

<표 3-1> IAEA SSG-30 - 심각도 기준

심각도	설명
High	기능 수행의 실패로 최악의 경우, 다음과 같은 영향을 미칠 때 - 설계기준사고(design basis accident)에 대한 기준치 이상의 방사선 물질의 누출 야기 - 설계기준사고(design basis accident)에 대한 주요 물리적 파라미터의 값이 정해진 기준치 초과 야기
Medium	기능 수행의 실패로 최악의 경우, 다음과 같은 영향을 미칠 때 - 예상운전과도상태(anticipated operational occurrences)에 대한 기준치 이상의 방사선 물질의 누출 야기 - 예상운전과도상태(anticipated operational occurrences)에 대한 주요 물리적 파라미터의 값이 정해진 기준치 초과 야기
Low	기능 수행의 실패로 최악의 경우, 다음과 같은 영향을 미칠 때 - 작업자에게 허용된 기준치 이상 방사능 노출 야기

자료 : IAEA Specific Safety Guide. No. SSG-30

34) IAEA Safety Standards, Specific Safety Guide, No. SSG-30, Safety Classification of Structure, System and Components in Nuclear Power Plants

또한, 해당 심각도 분류 기준과 발생빈도 및 시스템 상태를 고려하여 안전등급을 구분할 수 있도록 분류기준을 제시하고 있다. <표 3-2>와 <표 3-3>을 통해 안전등급 분류 기준과 각 안전등급에 대한 설명을 확인할 수 있다.

<표 3-2> IAEA SSG-30 - 안전등급 분류기준

심각도 / 기능	High	Medium	Low
예상 작동 발생 후, 제어 상태에 도달하는 기능	Safety Category 1	Safety Category 2	Safety Category 3
설계기반사고 이후, 통제 상태에 도달하는 기능	Safety Category 1	Safety Category 2	Safety Category 3
안전 상태에 도달한 후, 유지하기 위한 기능	Safety Category 2	Safety ategory 3	Safety Category 3
설계확장 조건의 결과 완화를 위한 기능	Safety C ategory 2/3	Safety Category 3	Safety Category 3

자료 : IAEA Specific Safety Guide. No. SSG-30

<표 3-3> IAEA SSG-30 - 안전등급 정의

심각도	설명
Safety category 1	• 예상운전과도상태 또는 설계기준사고 후 통제상태(controlled state)에 도달하는 데 필요한 기능이고 심각도가 **High**인 기능
Safety category 2	• 예상운전과도상태 또는 설계기준사고 후 통제상태(controlled state)에 도달하는 데 필요한 기능이고 심각도가 **Medium**인 모든 기능, 또는 • 안전상태(safe state)에 도달하거나 오랫동안 그 상태를 유지하는데 필요한 기능이고 심각도가 **High**인 기능. 또는 • Safety category 1으로 분류된 기능의 백업 기능을 수행하고 노심용융(core melt)없이 설계확장조건 (design extension conditions)을 제어하는데 필요한 기능
Safety category 3	• 예상운전과도상태 또는 설계기준사고에서 작동하는 기능이고 심각도가 **Low**인 기능. 또는, • 안전상태(safe state)에 도달하거나 오랫동안 그 상태를 유지하는데 필요한 기능이고 심각도가 **Medium**인 기능. 또는, • Safety category 2로 분류되지는 않으나 설계기준사고의 영향을 완화하는데 필요한 기능이고 심각도가 **High**인 기능. 또는, • 원자로 정지(reactor trip) 또는 공학적 안전 기능의 작동 빈도를 줄이기 위한 기능. 또는, • 사고 발생에 있어 발전소 운영자와 비상 서비스에 필요한 정보를 제공하기 위한 감시 기능

자료 : IAEA Specific Safety Guide. No. SSG-30

마지막으로, IAEA SSG-30에서는 추가적인 요소(예. 기능이 수행되어야 하는 시간 조건 등)을 고려하여 안전등급의 조정 가능성을 언급하고 있으며, 시스템이 서로 다른 등급을 할당 받은 다수의 기능으로 구성되어 있다면, 이 중 가장 높은 등급을 기준으로 안전등급이 정의됨을 할당하도록 가이드하고 있다.

나. IEC 61226[35] 안전기준

IEC 61226 안전기준은 IAEA SSR-2/1에서 제시하고 있는 안전등급 분류 전략을 기반으로 확장된 기준을 제시하고 있다. 각 기능, 시스템, 장비 (FSE: Function, System, Equipment)를 심층방어원칙 및 안전에 대한 중요도(important to safety)를 기준으로 4가지 등급으로 분류하고 있다.

- ㅇ Category A- 원전의 안전을 보장하는데 주 역할을 수행하는 기능
- ㅇ Category B- 안전확보를 위해 Category A의 보완적인 역할을 수행하는 안전기능
- ㅇ Category C- 안전기능 원전의 안전을 확보하는데 보조 또는 간접적인 역할을 수행하는 기능으로서 Category A 또는 Category B에 포함되지 않는 기능
- ㅇ Non-Classified- Category A, B, C에 속하지 않은 모든 비안전 기능

다. EUR (European Commission) 안전기준

EUR은 IAEA SSG-30의 기준을 기반으로 한다. EUR은 안전 중요성 외에 기능이 수행되는 시간 측면을 고려하여 안전등급의 분류기준을 정하고 있다. 다음 <표 3-4>에서 EUR의 안전등급 분류 기준을 설명하고 있다.[36]

<표 3-4> EUR - 안전등급 분류 기준

기능	참조 기준
F1A Function	주로 보호계통에 의해 수행되는 기능으로써, 설계기준사고 발생 시 발전소가 제어가능한 상태에 도달하기 위해 필요한 안전기능(설계

35) Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems
36) IEC 기술기준 및 계측제어계통 설계 방안, KEPCO E&C, 2012

	기준사고 발생 후 30분 이내에 수행되어야 함) - 원자로 정지 - 공학적안전계통 작동기능 등
F1B Function	설계기준사고 발생 후, 보호기능의 자동 작동 및 수행 후 30분이 지난 뒤부터, 발전소가 안전정지 상태에 도달할 때 까지 수행되는 안전기능 - 공학적 안전계통의 수동동작 - 사고 후 감시 및 운전기능 등
F2 Function	발전소가 안전정지 상태에 도달하고 24시간이 경과된 이후 시점부터 72시간까지 발전소를 안전정지 상태로 유지하는데 필요한 안전기능
NC (Non-classified) Function	그 외의 비안전 기능

자료 : KEPCO E&C, 2012, IEC 기술기준 및 계측제어계통 설계 방안

라. 주요 적용 요건

위에서 언급한 IAEA / IEC 관련 안전기준에서 언급하고 있는 적용 요건 관련 주요 참조 기준은 다음과 같다.[37]

ㅇ 소프트웨어

- IEC 60880 (Cat. A), IEC 62138 (Cat. B, C)
- IEC 61508 (System Integrity Level)
- IAEA GS-R-3 and ISO 9000

2. NRC / IEEE 관련 원자력 안전기준

가. 미국 원자력 안전기준 (10CFR50) & IEEE 안전기준

미국의 원자력과 관련된 안전규제 요건을 정의하고 있는 Code of Federal Regulations Title 10(이하, 10CFR)에서는, 전자장치에 대하여 안전 중요성에 따라 안전 관련(Safety-Related) 시스템과 비안전 관련(non Safety-Related) 시스템으로 구분하고 있다.[38] 안전 관련 시스템은 다음과 같이 정의된다.

37) IEC 기술기준 및 계측제어계통 설계 방안, KEPCO E&C, 2012
38) 10CFR50.49

ㅇ 설계기준사고 후, 다음을 보장하는 시스템

- The integrity of the reactor coolant pressure boundary;
- The capability to shut down the reactor and maintain it in a safe shutdown condition; or
- The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures

또한, 10CFR에서는 안전 관련 시스템의 정의가 IEEE 323-1974[39]에서 정의하고 있는 Class 1E에 해당하는 시스템을 참조하고 있음을 명시하고 있다. IEEE 323에서는 Class 1E에 대해서 다음과 같이 정의하고 있다.

ㅇ The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal or that are otherwise essential in preventing significant release of radioactive material to the environment.

나. 한국 원자력 안전기준 & 법규정에 의한 기준

한국의 원자력 안전은 원자력 안전법 / 시행령 / 시행규칙에 기반을 두고 있다. 안전등급의 분류에 대한 구체적인 기준은 원자로시설의 안전등급과 등급별 규격에 관한 규정(이후 원자로 안전등급 규정)에서 언급하고 있다. 원자로 안전등급 규정은 원자로시설의 설비에 대해 안전등급 1, 2, 3또는 비안전 등급으로 분류하도록 명시하고 있으며, 각 안전등급에 대한 기준은 다음 <표 3-5>과 같다.[40]

<표 3-5> 한국 원자로 안전등급 규정 - 안전등급 기준

안전등급	설명
안전등급 1	원자로냉각재 압력경계(고장이 발생할 경우 원자로냉각재 보충능력을 초과하는 원자로냉각재의 상실을 초래할 수 있는 부분)를 구성하는 설비의 내압부분과 그 지지물에 대하여 부여한다.
안전등급 2	원자로격납건물의 내압부분 및 그 지지물, 그리고 제5조에서 규정한 안전등급 1에 속하지 아니하면서 다음 각 호의 어느 하나의 안전기능을

39) IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations
40) 원자로시설의 안전등급과 등급별 규격에 관한 규정 제 5조, 6조, 7조, 8조

	수행하는 설비의 내압부분 및 그 지지물에 대하여 부여한다. - 핵분열생성물의 유출을 방지하는 역할을 하거나 방사성물질을 원자로격납건물 내에 억류 또는 격리하는 기능 - 비상시 원자로격납건물내에서 발생된 열 또는 방사성물질을 제거하는 기능(예 : 격납건물살수) - 비상시 원자로를 미임계 상태로 만들기 위하여 부반응도를 증가시키거나 또는 압력경계설비를 통한 정반응도의 증가를 억제하는 기능(예 : 붕산주입계통) - 비상시 노심에 직접 냉각재를 공급하여 노심냉각을 보장하는 기능(예 : 잔열제거, 비상노심냉각) - 비상시 노심의 냉각에 충분한 원자로냉각재를 공급하거나 유지하는 기능(예 : 핵연료 재장전용수 저장탱크)
안전등급 3	안전등급 1 또는 안전등급 2에 속하지 아니하며, 다음 각 호의 어느 하나의 안전기능을 수행하는 설비에 대하여 부여한다. - 원자로격납건물안의 수소농도를 허용 한계치 이내로 제어하는 기능. 다만, 원자로격납건물 경계 확장기능은 제외 - 안전등급 1, 2 또는 3의 설비를 보유하고 있는 원자로격납건물 외부의 한정된 공간(예 : 원자로제어실, 핵연료 건물)으로부터 방사성물질을 제거하는 기능 - 원자로를 미임계상태로 만들거나 유지하기 위하여 부반응도를 증가시키는 기능(예 : 붕산보충) - 노심냉각을 위해 원자로냉각재를 충분히 공급하거나 유지하는 기능(예 : 원자로냉각재 보충수계통) - 노심반응도 제어 또는 노심냉각능력을 확보하기 위하여 원자로내부의 기하학적 구조를 유지하는 기능(예 : 노심지지구조물) - 안전등급 1, 2 또는 3의 설비에 대하여 그 하중을 지지하거나 보호하는 기능(제9조에 따른 전력산업기술기준(이하 “KEPIC“이라 한다) MN 또는 이에 상응하는 ASME Code Sec. Ⅲ)의 범위에 포함되지 아니한 콘크리트 및 강재구조물에 해당 - 원자로제어실 또는 원자력발전소 외부의 사람들을 위하여 방사선을 차폐하는 기능 - 습식 저장된 사용후핵연료의 냉각유지기능(예 : 사용후핵연료 저장조 및 냉각계통) - 안전등급 1, 2 또는 3의 설비에 의하여 수행되는 안전기능을 보장하는 기능(예 : 안전등급 1, 2 또는 3의 열교환기로부터 열을 제거하는 기능, 안전등급 2 또는 3의 펌프 윤활기능, 비상 디젤기관의 연료급유기능) - 안전등급 1, 2 또는 3의 설비에 구동전원이나 동력을 공급하는 기능 - 안전등급 1, 2 또는 3의 설비가 안전기능의 수행에 필요한 수동 또는 자동작동을 위한 정보를 제공하거나 그 설비를 제어하는 기능

	- 안전등급 1, 2 또는 3의 설비가 안전기능의 수행에 필요한 전원을 공급하거나 신호를 송신하는 기능 - 안전등급 1, 2 또는 3의 설비가 적절한 안전기능을 수행하도록 보장하거나 유지하기 위한 수동 또는 자동의 연동기능 - 안전등급 1, 2 또는 3의 설비와 운전요원을 위하여 적절한 환경조건을 제공하는 기능 - 압력용기의 설계, 제작에 관한 기준(제9조에 따른 KEPIC MN 또는 이에 상응하는 ASME Code Sec. Ⅲ)이 적용되지 아니하는 안전등급 2에 해당하는 기능
비안전등급	안전등급 1, 2 또는 3에 속하지 아니하는 설비에 대하여 부여한다.

자료 : 원자로시설의 안전등급과 등급별 규격에 관한 규정

이에 기반하여 경수로형 원전 규제기준 및 규제지침은 설비에 대한 안전등급 분류 기준 뿐만 아니라, 전력계통과 계측제어계통에 대한 안전등급 분류 기준을 제시하고 있다. 다음 <표 3-6>, <표 3-7>에서 경수로형 원전 규제기준에서 정의하고 있는 전력계통과 계측제어계통에 대한 안전등급 기준을 확인할 수 있다.

<표 3-6> 경수로형 원전 규제기준 및 지침 - 전력계통 안전등급 기준

안전등급	설명
안전등급 1E(전기1급) 전력계통	원자로 정지, 격납용기 격리, 비상노심 냉각, 원자로격납건물 열제거 및 노심 잔열제거 기능을 수행하거나, 환경으로의 심각한 방사성물질 누출을 방지하는 데 필수적인 기능을 수행하는 구조물·계통·기기에 전력을 공급하는 계통을 안전등급 1E(전기1급) 전력계통이라 한다.
비안전등급(전기비1급) 전력계통	안전등급 1E(전기1급) 이외의 구조물·계통·기기에 전력을 공급하는 계통을 비안전등급(전기비1급) 전력계통이라 한다. 또한 발전소 정전사고(SBO) 대처능력을 제공하는 발전소 정전 사고 대처설비들도 비안전등급(전기비1급) 전력계통으로 분류한다.

경수로형 원전 규제기준 3장 설계공통 기준 (3.2.2)

계측제어계통의 안전등급에 대한 분류 기준은 경수로형 원전 규제지침에서 보다 상세하게 정의하고 있다.[41] 원자로 안전등급 규정에서 정한 '안전등급 3' 및 '비안전등급'에 해당하는 계측제어계통은 발전소설계기준에 따라 계측등급-I([42]IC-1), 계측등

41) 경수로형 원전 규제지침 8.1 계측제어계통의 안전등급 분류
42) IC: Instrumentation and Control Class

급-II(IC-2) 및 계측등급-III(IC-3)으로 분류한다. 계측등급-I, II 및 III은 각각 설계기준사건(Design Basis Event), 특정사건[43](Special Event) 및 정상운전 (Normal Operation)을 위한 계통에 해당된다.

<표 3-7> 경수로형 원전 규제기준 및 지침 - 계측제어계통 안전등급 기준

안전등급	설명
계측제어등급 1(IC 1)	계측제어등급 1은 원자력안전위원회고시 제2014-15호(원자로.15) 제7조(안전등급 3)에 의해 안전등급 3으로 분류된 계측제어설비로서, 원자력발전소의 설계기준사건 발생 시 안전기능을 수행한다. 대표적인 설비는 원자로정지계통 및 공학적안전설비작동계통이 있다. 이 외에도 안전기능을 지원하거나 안전과 관련되는 설비로서 안전정지계통의 계측제어설비, 정보계통 및 연동계통, 데이터통신계통, 수동제어설비, 표시기 및 기록계(원자로제어실, 원격정지실 및 현장제어반 포함) 등이 포함될 수 있다.
계측제어등급 2(IC 2)	계측제어등급 2는 계측제어등급 1에 포함되지 않는 계측제어설비로서, 특정사건 발생 시 별도의 보호 및 제어 기능을 수행한다. 대표적인 설비로는 다양성 보호계통, 다양성 수동제어기 및 표시기, 지진원자로자동정지계통, 심층방어 및 다양성 분석결과에 따라 선정된 계측제어계통 등이 있다.
계측제어등급 3(IC 3)	계측제어등급 3은 계측제어등급 1 및 2에 포함되지 않는 계측제어설비로서, 발전소 과도상태를 포함한 정상 운전에 필요한 계통이다. 대표적인 설비로는 발전소 운전에 필요한 계측제어계통, 발전소 상태감시 및 진단설비, 전산설비 및 경보계통, 화재감시 및 경보설비, 통신설비 등의 계측제어설비를 포함한다.

경수로형 원전 규제기준 3장 설계공통 기준 (3.2.2)

위의 등급을 분류하는 기준을 보면 시스템이 수행하는 기능에 따라 분류됨을 알 수 있다. 수행하는 기능은 안전에 대한 중요성에 대한 판단을 근거로 분류하고 있으며, 안전 중요성을 판단할 때 다양성(diversity), 중복성(심층방어 개념, defense-in-depth) 등의 요소를 고려하고 있다.

동 규제지침에서는 위의 안전등급에 따라 적용되어야 할 요건에 대해서 언급하고 있으며, 계측제어계통에 대한 요건이 소프트웨어를 포함한 적용 요건임을 알 수 있다. 계측제어계통 안전등급에 대한 적용 규제지침의 내용은 다음과 같다.

43) 특정사건이라 함은 설계기준사건에 속하지 않는 사건으로서 원자로가 정지되어야 할 조건임에도 정지되지 아니하는 과도상태, 원자로보호계통의 소프트웨어 공통원인고장에 따른 과도상태, 발전소 정전사건, 대규모 지진발생에 따른 과도상태 등을 포함한다.

ㅇ 계측제어등급 1은 규제지침 3.2, 3.3, 3.9, 8.2 ~ 8.10, 8.12 ~ 8.20 등을 포함하는 관련 요건 및 지침을 만족하여야 한다.

계측제어등급 1에 사용되는 소프트웨어[44]는 가장 엄격한 소프트웨어 품질보증요건과 기술기준을 적용하여 개발되어야 한다. 계측제어등급 1에 사용되는 소프트웨어는 KEPIC EME 3100(IEEE Std. 1012)에서 제시하는 무결성 등급 4에 해당하는 확인 및 검증활동이 요구되며, 소프트웨어 확인 및 검증 활동은 개발조직과 기술, 관리 및 재정적으로 독립된 조직에 의해 수행되어야 한다. 또한 소프트웨어 안전성 분석이 요구된다. 기성소프트웨어가 계측제어등급 1에 사용되는 경우 해당 소프트웨어는 계측제어등급 1에 상응하는 품질을 갖추고 있음이 입증되어야 한다. 만약, 계측제어등급 1에 사용되는 소프트웨어가 해당 요건을 만족하지 못하는 경우 이에 대한 정당성이 입증되어야 한다.

ㅇ 계측제어등급 2는 해당 계통이 수행하는 기능에 적합한 품질 및 신뢰성을 가져야 하며, 계측제어등급 1에 적용되는 요건 및 지침을 차등적으로 적용할 수 있다. 특히 동 계통의 기능 실패 또는 상실이 계측제어등급 1의 기능 수행에 영향을 미치지 않도록 관련 요건(예: 격리, 다양성 등)을 만족하여야 한다.

계측제어등급 2에 사용되는 소프트웨어는 수행하는 기능의 중요도에 상응하는 소프트웨어 품질보증요건 및 기술기준에 따라 개발되어야 한다. 계측제어등급 2에 사용되는 소프트웨어가 계측제어등급 1의 기능수행에 영향을 미칠 수 있는 위험요소를 내재하고 있다면 소프트웨어 안전성 분석을 수행해야 하며, 확인 및 검증 활동은 설계조직과 적절히 독립된 확인 및 검증조직에 의해 수행되어야 한다.

ㅇ 계측제어등급 3은 해당 계통이 수행하는 기능에 적합한 품질 및 신뢰성을 가져야 하며, 계측제어등급 1에 적용되는 요건 및 지침을 차등적으로 적용할 수 있다. 특히 동 계통의 기능 실패 또는 상실이 계측제어등급 1의 기능 수행에 영향을 미치지 않도록 관련 요건(예: 격리, 다양성 등)을 만족하여야 한다.

계측제어등급 3에 사용되는 소프트웨어는 발전소 운전에 적합한 신뢰성 있는 수준의 소프트웨어 품질보증요건 및 기술기준에 따라 개발되어야 한다.

---

44) 계측제어계통에 사용되는 소프트웨어에는 펌웨어, 운영체제, 응용소프트웨어 등이 있으며, FPGA(Field-Programmable Gate Array)/CPLD(Complex Programmable Logic Devices)논리회로, 기성소프트웨어(Pre-existing Software) 등을 포함할 수 있다.

규제지침에서 언급하고 있는 안전등급별 적용 요건은 계측제어등급 1에 대해서는 명확하게 제시하고 있지만, 계측제어등급 2, 3에 대해서는 '차등적으로 적용할 수 있다'고 해석의 여지를 남겨 두고 있다.

원자력 분야 안전 전문가에 의하면, 실제 개발 프로젝트에서도 계측제어등급 2, 3의 적용 요건에 대한 해석이 명확하지 않다고 한다. 다만 개발결과에 대한 검증 측면은 별도의 기준이 있어, 안전활동이 검증 중심으로 이루어지고 있다.

다. 한국 원자력 안전기준 - 한국 신형원전 기술기준[45]

한국 신형원전(APR 1400)은 한국이 독자적으로 개발한 차세대 원전 모델로, 신고리 3호기에 적용되었다. APR 1400은 유럽사업자요건(EUR) 인증 심사 및 미국 NRC의 설계검증도 통과하였다. 이러한 APR 1400 기술기준 중 소프트웨어 프로그램 매뉴얼(APR1400-SPM[46])에서 소프트웨어 안전등급에 대한 분류기준을 제시하고 있다. 계측제어계통에서 개발되거나 사용되는 모든 소프트웨어는 그 기능(functionality) 및 안전 중요성 (importance related to safety)에 따라 다음 <표 3-8>과 같이 분류된다.

<표 3-8> APR1400-SPM - 소프트웨어 안전등급 분류기준

안전등급	설명
Safety Critical(SC; Protection)	원자로 보호시스템(RPS) 시작, 엔지니어링된 안전기능의 작동 시스템(ESFAS) 제어작업 및 안전 종료를 위한 제어 작을 직접 수행하는데 필요한 기능을 포함한 소프트웨어
Important to safety (ITS)	다양한 작동 시스템(DAS, Diverse Actuation System) 제어 작업을 수행하는데 필요한 기능을 포함한 소프트웨어, 안전 중요 기능을 모니터링하거나 테스트하는데 의존하는 소프트웨어 또는 공장의 안전 중요 기능을 모니터링하는 소프트웨어
Important to availability (ITA)	공장 운영에 중요한 시스템 및 장비의 운영을 유지하기 위해 필요한 소프트웨어
General purpose (GP)	SC, ITS, ITA 클래스에 할당되지 않은 소프트웨어

자료 : KEPCO & KHNP, Software Program Manual for APR 1400

위의 소프트웨어 안전등급은 IEEE 1012[47]의 소프트웨어 분류 기준과 다음과 같이 매핑된다.

45) APR 1400 (Advanced Power Reactor 1400)
46) Software Program Manual for APR 1400, KEPCO & KHNP
47) IEEE Standard for System, Software, and Hardware Verification and Validation

○ **SC** : High (SIL 4), **ITS** : Major (SIL 3), **ITA** : Moderate (SIL 2), **GP** : Low (SIL 1)

또한, 시스템 수준의 안전등급과의 관계에 있어서 다음과 같이 명시하고 있다.

○ The software for the safety I&C systems is classified as one of the two software classes: SC class and ITS class. Both classes of the software for the safety I&C systems are implemented on Class 1E hardware.

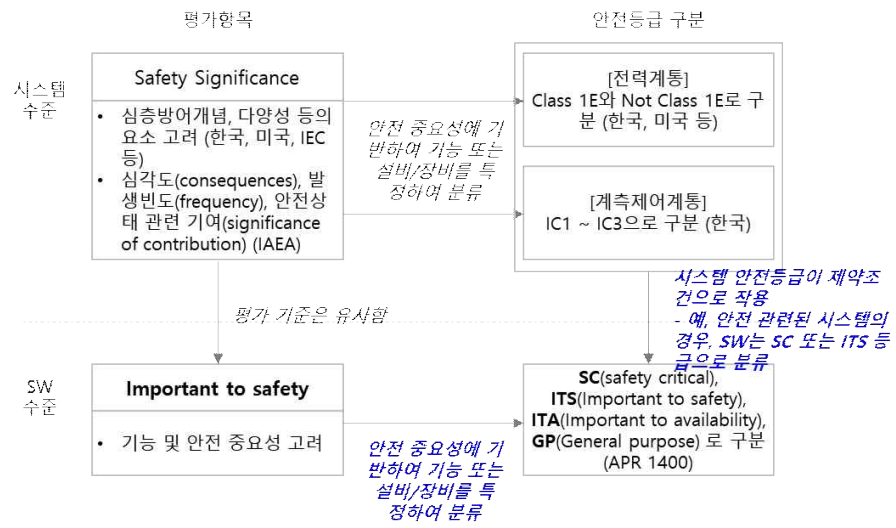
즉, 안전과 관련된 시스템으로 분류된 경우, 해당 시스템의 소프트웨어는 SC 등급 또는 ITS 등급으로 분류되어야 한다는 것을 뜻한다.

3. 시사점

가. 원자력 분야 안전등급 평가 기준

원자력 분야의 안전기준에서 정의하고 있는 안전등급 평가 기준은 조사 결과를 기반으로 다음 [그림 3-2]과 같이 정리할 수 있다. 소프트웨어 안전등급에 대한 평가항목으로 '안전 중요성'을 고려하고 있으며, 원자로 기능이 상당부분 표준화되어 있어 각 기능의 '안전 중요성' 수준이 정해져 있다.

[그림 3-2] 원자력 안전등급 평가 기준



나. 안전등급 기준이 명시된 문서

원자력 분야의 안전기준은 관련 법규정(예, 원자로시설의 안전등급과 등급별 규격에 관한 규정 등)에 등급 분류 기준이 명시되어 있으며, 다양한 표준 (IEC, IEEE 등)에서도 등급 분류 기준을 명시하고 있다. 다만, 나라마다 사용되는 기준에 차이가 있고, 표준에서 명시하고 있는 기준도 차이가 존재한다. 원자력 분야 전반에 걸쳐서 일관된 기준이 적용되고 있지는 않다.

다. 시스템 수준의 안전등급과의 연관성

시스템 수준에서나 소프트웨어 수준에서나 동일하게, 수행하는 **기능의 안전 중요성**을 고려하여 평가하고 있다. 참조되는 기준마다 차이가 있으나, 시스템 수준의 안전등급이 소프트웨어 안전등급을 판단할 때 일종의 제약조건으로 사용된다. 예를 들어, 한국 신형원전 기술기준에서는 시스템이 안전 관련된 것으로 평가된 경우, 소프트웨어는 SC 또는 ITS 등급 중 하나로 평가되어야 한다.

라. 소프트웨어 안전등급 평가항목 및 지표

위에서 살펴본 대부분의 기준에서 안전등급의 평가는 시스템이 수행하는 기능의 안전 중요성에 기반하고 있다. 안전 중요성에 대한 판단 시 다양성(diversity), 심층방어 개념(defense-in-depth)에 기반한 중복성 등의 요소를 고려하고 있다. 원자력 분야 내에서 원자력 발전소의 구조나 기능, 이를 기반으로 어떤 기능이 안전에 중요하다는 것에 대해 상당한 공통인식이 있는 것으로 판단된다.

이 외에 안전기능의 호출 빈도(frequence), 위험 관련 사건 발생후 안전기능이 호출되는 시간(time) 또는 기간(period)이 고려되기도 한다.

마. 소프트웨어 안전등급 결정방법 및 안전등급 구분

앞서 언급했듯이 적용되는 기준별로 차이가 있으나, 소프트웨어 안전등급은 기능의 안전등급 중요성에 기반하여 정성적으로 평가되는 경우가 많다.

안전등급 구분도 표준별 국가별로 다양하다. 이는 한 분야 내에서도 일관된 기준을 정립하는 것이 쉽지 않음을 보여준다. 국내의 경우, IC 1 ~ IC 3의 3등급 체계 또는 SC(SIL 4), ITS(SIL 3), ITA(SIL 2), GP(SIL 1)의 4등급 체계가 사용되고 있다.

[그림 3-3] 원자력 - 안전등급 비교

Organizations or Countries		Safety Classification of I&C Functions and Systems in nuclear plants			
Main international standard organizations					
IAEA NS-G-1.3		Systems Important to Safety			Systems not important to safety
		Safety	Safety-related		
IAEA SSG-30	Function	Safety category 1	Safety category 2	Safety category 3	
	System	Safety class 1	Safety class 2	Safety class 3	
IEC 61226		Systems Important to Safety			Non-classified
	I&C function	Category A	Category B	Category C	
	I&C system	Class 1	Class 2	Class 3	
IEEE		Systems Important to Safety			Non-safety-related
		Safety-related	[5]		
EUR[6]	Safety level of functions / I&C systems	F1A	F1B	F2	NS (non-safety)
MDEP member states					
Canada		Category 1	Category 2	Category 3	Category 4
France		F1A	F1B	F2	Non-classified
Finland		Class 2	Class 3	EYT/ STUK	EYT (classified non-nuclear)
UK		Class 1	Class 2	Class 3	Non-classified
United States		Systems Important to Safety			(not specified)
		Safety-Related	[5]		
India		IA	IB	IC	NINS
Japan		PS1/MS1	PS2/MS2	PS3/MS3	Non-nuclear safety
Korea		IC-1	IC-2		IC-3
Russia		Class 2	Class 3		Class 4 (Systems not important to safety)
Others nuclear states					
Switzerland		1	2	3	Non-classified
Germany	I&C function	Category 1	Category 2	Category 3	Non-classified
	I&C equipment	E1		E2	

자료 : Safety classification for I&C systems in nuclear power plants - current status & difficulties, World Nuclear Association, Sep. 2015

제3절 철도 안전

1. 철도 안전 관련 국내외 법/제도

가. 국내 법/제도

철도 관련 법으로는 철도산업발전기본법, 철도건설법, 철도안전법, 철도사업법, 도시철도법, 궤도운송법 등이 있다. 철도 안전과 관련된 내용은 철도안전법과 도시철도법에서 다루고 있다. 철도안전법은 기본적으로 철도산업발전기본법에 명시된 철도를 대상으로 하나, 철도안전에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 철도안전법 규정을 따르도록 하고 있다. 도시철도법은 도시철도와 관련된 안전기준을 제시하고 있으나, 기술적 특성이 차별화되지 않은 안전 분야에 대해서는 대부분 철도안전법 규정을 적용하고 있다.

철도 안전법과 관련된 법/규정은 다음과 같다.

[그림 3-4] 철도안전법 체계

자료 : NIPA, IEC 62279 기반 철도 분야 소프트웨어안전 가이드

철도안전법은 시행령과 시행규칙을 두고 있으며, 형식승인을 수행하기 위한 기술기준을 두고 있다. 철도 소프트웨어의 안전과 관련된 기준을 제시하고 있는 것은 철도차량 기술기준이다.

철도차량 기술기준에서는 고속철도차량(Part 31), 일반철도차량(Part 41 ~ 47), 도시철도차량(Part 51 ~ 57) 별로 안전에 대한 필수 요구사항(3.2 안전)을 제시하고 있다. 안전 요구사항은 차량한계, 주행안전, 충돌안전, 화재안전, 전기안전 등으로 분류하고 있으며, 위험도 분석 및 철도 소프트웨어에 대한 안전 요구사항을 별도로 설명하고 있

다. 철도차량 기술기준은 위험도 분석 절차에 대해 다음과 같이 설명하고 있다.[48)]

(1) 사고를 유발할 수 있는 위험사건을 식별하고 위험요인을 분석하여, 분석된 위험요인이 사고로 전개될 수 있는 사고시나리오를 작성한다.

(2) 각각의 사고시나리오에서 위험사건의 발생확률을 산정한다.

(3) 각각의 사고시나리오에서 사고가 피해에 미치는 영향을 분석하여 결과심각도를 산정한다.

(4) 각각의 사고시나리오에서 위험사건의 발생확률과 결과심각도를 산출하여 위험도 평가를 실시한다.

(5) 위험도평가 결과가 요구하는 안전수준을 만족하지 못하는 경우에는 그에 대한 원인을 분석하고 요구하는 안전수준에 적합하도록 안전대책을 수립한다.

(6) 수립된 안전대책이 요구하는 안전수준에 적합하며, 경제적 측면에서 적정한 것임을 확인하여 안전대책의 검증을 실시한다.

위험도는 위험사건의 발생확률과 결과심각도를 고려하여 평가하도록 명시하고 있다. 위험도 평가 방법은 가능한 한 정량적인 방법을 우선적으로 적용하도록 명시하고 있으며, 기술기준에서 제시하지 않은 세부사항에 대해서는 국가 규격 또는 국제 규격을 준용하도록 가이드하고 있다. 다음은 철도차량 기술기준에서 명시하고 있는 내용이다.

위험도분석은 가능한 한 정량적인 방법으로 실시하되, 정량적인 방법이 곤란한 경우에는 기존의 경험 또는 사례를 이용하거나 정성적인 방법을 적용할 수 있도록 하고 있다. 위험도분석의 세부기준에 관하여 본 기술기준에서 정하지 아니한 사항은 관련된 국가규격 및 국제규격을 준용할 수 있다.

철도 소프트웨어 대해서도 위에서 언급한 위험도 분석 기준에 따라 소프트웨어의 위험도 분석을 수행하도록 명시하고 있다. 또한 IEC 62279에서 제시하고 있는 안전활동을 수행하도록 하고 있다. 결과적으로 위험에 대한 소프트웨어 안전등급을 결정하는 기준은 IEC 62279[49)]를 따르도록 하고 있다고 판단할 수 있다. 다음은 철도차량 기술기준에서 명시하고 있는 내용이다.

---

48) 철도차량 기술기준 Part 31, 41~47, 51~57 3.2.6 위험도 분석

49) Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

ㅇ 위험도 분석에 따른 철도차량에 대한 예비위험도 분석을 통해 위험도 관리수준을 결정하고, 정해진 관리수준에 따라 신청자는 철도차량 소프트웨어 안전관리를 실시해야 한다.

ㅇ 신청자는 소프트웨어 안전확보를 위해 철도소프트웨어에 대한 국제표준 IEC 62279를 기반으로 안전활동을 하여야 한다.

나. 해외 법/제도

ㅇ 유럽의 법/제도

유럽연합에서 철도 안전 및 상호운영 관련 지침 (Directive 2004/49/EC, 2008/57/EC)를 제정하고, ERA(European Railway Agency)에서 유럽 철도 산업 및 관련 제조사들이 필수적으로 준수해야 할 요구사항들을 상호운영을 위한 기술사양서(TSI: Technical Specification for Interoperability) 형식으로 제공한다. 각 회원국은 관련 지침에 의거해서 자국의 철도 관련 법/제도를 개정하고, TSI를 근간으로 기술적으로 준수해야 할 요구사항을 제정하여 운영한다.

TSI에 소프트웨어 안전과 관련해서 필수적으로 참조해야 할 표준으로 EN 50128(IEC 62279)[50]을 명시하고 있어, 해당 표준의 적용은 법/제도적으로 강제된다.

50) Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems

[그림 3-5] 유럽 ERA TSI의 참조 표준

List of mandatory standards

The application of the version of the standards listed in the table below, and their subsequent amendments when published as harmonised standard in the certification process is an appropriate means to fully comply to the risk management process as set out in Annex I of the Commission Implementing Regulation (EU) No 402/2013, without prejudice for the provisions of chapter 4 and chapter 6 of this TSI.

No	Reference	Document name and comments	Version	Note
A1	EN 50126-1	Railway applications —The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS Process	2017	
			1999	1,2
A2	EN 50128	Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems	2011	
A3	EN 50129	Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling	2003	1
A4	EN 50159	Railway applications — Communication, signalling and processing systems	2010	1
A5	EN 50126-2	Railway Applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Systems Approach to Safety	2017	3

자료 : COMMISSION REGULATION (EU) 2016/919

ㅇ 미국의 법/제도

미국의 철도 안전에 관한 사항은 교통법(US Code Title 49, 이하 USC 49)와 하위법령(CFR Title 49, 이하 CFR 49)에 규정되어 있다. USC 49 철도 프로그램 중 안전에 관한 내용은 Part A에 규정되어 있으며, CFR 49는 Chapter 2. Federal Railroad Administration (FRA)과 Chapter 6. Federal Transit Administration (FTA)에서 철도안전에 관한 사항을 규정하고 있다.

CFR 49에서는 안전 시스템의 성능 표준 제정에 주안점을 두고, 안전 인증 획득을 위한 별도의 개발 방법 및 집행 기관, 공급자 프로세스 등을 정해 놓지 않았다. 관련 사업자들은 규정에서 권고하는 표준 중 하나를 사용하거나 자체적인 프로세스 및 절차, 분석 방법과 문서를 통해 FRA 규정의 요구사항을 만족하면 인증을 득할 수 있도록 하고 있다.

소프트웨어 안전의 경우도 AREMA C&S Manual Part 17.3 (recommended safety assurance) 및 유럽 표준인 EN 50128(IEC 62279)[51]의 사용을 유도하고 있으나, 규정에서 강제하고 있지는 않다.

ㅇ 일본의 법/제도

일본 국토교통성에서는 철도사업법의 국토교통성령(한국의 시행규칙에 해당)을 통해

51) Railway applications - Communication, signalling and processing systems

철도차량 및 용품, 궤도 및 기타 시설에 대한 기술기준을 규정하여 공표하고 있다. 철도차량 인증검사에 필요한 시행지침은 검증을 직접 수행하는 철도운영기관(인증대상 철도차량의 발주자)이 자체적으로 수립한다. 국립교통안전환경연구소(NTSEL)는 ISO/IEC Guide 65[52] 기반으로 철도용품에 대한 제품인증 기준을 만들어 운영하고 있다. 또한, 개별 분야의 기술적 안전과 신뢰성에 관한 국제 규격- IEC 62278(RAMS), IEC 62279(소프트웨어), IEC 62280[53](통신), IEC 62425[54](철도신호용전자장치)-에 대한 인정 및 상호인증을 통해, 일본 철도차량 및 용품 제조업체들의 해외 진출 시 안전 규격 인증 심사를 용이케 하고 있다.

2. 철도 안전 기준

철도 시스템에 관련된 안전 표준은 유럽의 규격을 기반으로 제정 및 준수되고 있다. 다음은 철도 분야에서 주로 활용되는 안전 관련 표준이다.

- IEC 62278 (EN 50126): Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- IEC 62279 (EN 50128): Railway Applications - Communication, signalling and processing systems - Software for railway control and protection systems
- IEC 62425 (EN 50129): Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signaling
- IEC 62280 (EN 50159): Railway applications - Communication, signalling and processing systems - Safety related communication in transmission system

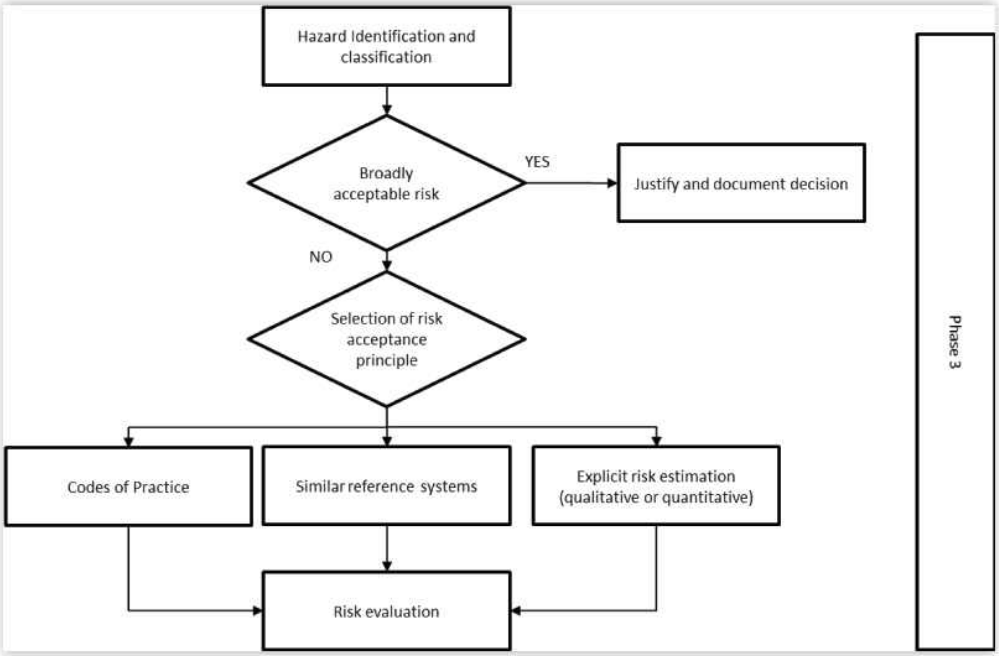
철도 분야에서 소프트웨어의 안전등급은 시스템의 안전등급 평가를 기반으로 한다. 본 절에서는 시스템 수준의 안전등급 평가 기준을 제시하고 있는 IEC 62278 (EN 50126)과 소프트웨어의 안전등급 기준을 제시하고 있는 IEC62279 (EN 50128)에 대해 살펴본다.

가. IEC 62278 (EN 50126)

52) General requirements for bodies operating product certification systems
53) Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems
54) Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

IEC 62278은 철도 시스템의 RAMS (Reliability, Availability, Maintainability and Safety)에 대한 요건을 제시하고 있는 표준이다. 철도 시스템에 대한 안전 요건은 시스템 수준에서의 위험에 대한 평가를 기반으로 한다. 위험에 대한 평가는 기대되는 손실 발생의 빈도(frequency of occurrence of Loss) 및 손실의 심각도(degree of severity of loss) 항목을 고려하여 이루어지며[55], 다음 [그림 3-6]에서 확인 가능한 절차를 거쳐 수행된다[56].

[그림 3-6] 철도 - IEC 62278 위험 평가 절차



자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

위험 평가 절차는 시스템의 위험원 식별에서부터 시작한다. 식별된 위험원에 대해서는 일차적으로 보편적으로 허용가능한 수준(broadly acceptable)에 해당하는지를 살펴본다. 평가는 전문가의 판단에 기반하며, 보편적으로 허용가능한 수준의 위험으로 판단되면, 안전 요건을 적용하지 않게 된다.

위험이 보편적으로 허용가능한 수준을 넘어선다고 판단한 경우, 위험 평가를 위해 세 가지 방법 중 하나를 선택하게 된다.

55) IEC 62278 5.8 Risk based approach
56) IEC 62278 6.3 Risk assessment

ㅇ 실천 규범의 사용 (use of codes of practice)

ㅇ 유사 시스템과의 비교 (comparison with a similar system as a reference)

ㅇ 명시적인 위험 평가 (Explicit risk estimation)

명시적인 위험 평가 방법은 Appendix C의 가이드로 제시하고 있다. 표준에서 제시하고 있는 가이드는 철도 시스템에 사용되는 전형적인 분류 기준이며, 책임 기관에서 대상 시스템에 맞게 조정해서 쓰도록 권고하고 있다. 표준에서는 발생 빈도(frequency of occurrence)와 심각도 분류(severity categories)에 대한 기준과 이를 기반으로 한 위험 분류 기준 (risk acceptance category)에 대해서 제시하고 있다.

발생빈도 측면에서는 시간(time) 기반의 평가 기준과 운행거리(distance) 기반의 평가 기준을 제시하고 있다.

[그림 3-7] 철도 - IEC 62278 시간 기반 발생빈도 분류 기준

Frequency level	Description	Example of a frequency range based on a single item operating 24 h/day	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5000 h/year
		Expected to happen	
Frequent	Likely to occur frequently. The event will be frequently experienced.	more than once within a period of approximately 6 weeks	more than about 150 times
Probable	Will occur several times. The event can be expected to occur often.	approximately once per 6 weeks to once per year	about 15 to 150 times
Occasional	Likely to occur several times. The event can be expected to occur several times.	approximately once per 1 year to once per 10 years	about 2 to 15 times
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.	approximately once per 10 years to once per 1 000 years	perhaps once at most
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.	approximately once per 1 000 years to once per 100 000 years	not expected to happen within the lifetime
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.	once in a period of approximately 100 000 years or more	extremely unlikely to happen within the lifetime

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[그림 3-8] 철도 - IEC 62278 거리 기반 발생빈도 분류 기준

Frequency level	Description	Example of a range of frequency
F1	Likely to occur often	more than once every 5 000 km per train
F2	Will occur several times	once every 25 000 km per train
F3	Might occur sometimes	once every 100 000 km per train

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

심각도 측면에서는 사람, 환경, 서비스, 자산 및 금전적 손해 관점에서 다양한 기준을 제시하고 있다.

[그림 3-9] 철도 - IEC 62278 RAM 관련 심각도 분류 기준

RAM severity category	Description
Significant (immobilising failure)	A failure that: • prevents train movement or • causes a delay to service greater than a specified time • and/or generates a cost greater than a specified level
Major (service failure)	A failure that: • prevents the system from achieving its performance and • does not cause a delay or cost greater than the minimum threshold specified for a significant failure
Minor	A failure that: • does not prevent a system achieving its specified performance and • does not meet criteria for Significant or Major failures

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[그림 3-10] 철도 - IEC 62278 금전적 피해 관련 심각도 분류 기준

Severity category	Financial consequences
SF1	The incident will incur people suing the company, severe impact to the public image of the company, and/or incur costs higher than 1 000 000 €.
SF2	The incident may have an impact on the public image of the company and/or incur costs higher than 100 000 €
SF3	The incident will not incur costs higher than 100 000 €

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[그림 3-11] 철도 - IEC 62278 RAMS 관련 심각도 분류 기준

Severity category	Consequences to persons or environment	Consequences on service/property
Catastrophic	• Affecting a large number of people and resulting in multiple fatalities, and/or • extreme damage to the environment	Any of the below consequences in presence of consequences to persons or environment
Critical	• Affecting a very small number of people and resulting in at least one fatality, and/or • large damage to the environment	Loss of a major system
Marginal	• No possibility of fatality, severe or minor injuries only, and/or • minor damage to the environment	Severe system(s) damage
Insignificant	• Possible minor injury	Minor system damage

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[그림 3-12] 철도 - IEC 62278 인명 및 환경 피해 관련 심각도 분류 기준

Severity category	Consequences to persons or environment
S1	Many equivalent fatalities (likely more than about 10) or extreme damage to the environment.
S2	Multiple equivalent fatalities (likely less than about 10) or large damage to the environment.
S3	Single fatality or severe injury or significant damage to the environment.
S4	Minor injuries or minor damage to the environment
S5	Possible minor injury

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

본 표준에서는 안전등급을 위험 수용성(risk acceptance) 관점에서 분류하고 있다. 위험 수용성에 대한 분류의 예는 다음과 같다.

[그림 3-13] 철도 - IEC 62278 위험 수용성 단계 (2단계)

Risk Acceptance Category	Actions to be applied
Unacceptable	The risk needs further reduction to be accepted
Acceptable	The risk is accepted provided adequate control is maintained

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

[그림 3-14] 철도 - IEC 62278 위험 수용성 단계 (4단계)

Risk Acceptance Category	Actions to be applied
Intolerable	The risk shall be eliminated
Undesirable	The risk shall only be accepted if its reduction is impracticable and with the agreement of the railway duty holders or the responsible Safety Regulatory Authority.
Tolerable	The risk can be tolerated and accepted with adequate control (e.g. maintenance procedures or rules) and with the agreement of the responsible railway duty holders.
Negligible	The risk is acceptable without the agreement of the railway duty holders.

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

앞서 살펴본 발생 빈도 및 심각도 평가항목의 조합을 통해 위험 수용성 수준을 분류하는 기준은 아래와 같다.

[그림 3-15] 철도 - IEC 62278 위험 수용성 분류 기준

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			

자료 : IEC 62278, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

나. IEC 62279 (EN 50128)

IEC 62279 (EN 50128)은 철도 시스템에 대한 소프트웨어 규격으로 철도 분야의 안전 관련 소프트웨어 개발, 시험, 검증 및 유지보수와 준수해야 할 일련의 요구사항을 제공한다.

해당 표준에서는 소프트웨어의 안전등급 (software safety integrity level)이 SIL 0 (가장 낮음), SIL1 ~ SIL4의 5 단계로 구분됨을 명시하고 있다. 또한, 소프트웨어 안전등급은 기본적으로 시스템 수준에서 평가되고 결정된다고 명시되어 있다. IEC 62278에서 명시한 기준에 의해 시스템의 기능에 대한 안전등급이 결정되고, 시스템 수준에서 해당 기능을 소프트웨어에 할당하면, 해당 소프트웨어는 시스템 기능에 부여된 안전등급을 그대로 상속하게 된다. 안전기능을 독립적인 복수 개의 구성요소가 구현하는 경우 등 안전등급을 조정할 수 있는 방법이 존재 하나, 기본적으로 시스템의 안전등급과 동일하게 소프트웨어의 안전등급이 결정된다.

다. 철도 소프트웨어 안전 기준 및 체계 구축 연구

한국철도기술연구원에서 2004~2007년(4년)에 걸쳐 수행된 철도 소프트웨어 안전기준 및 체계 구축에 관한 연구[57]에서는 철도 소프트웨어의 안전등급에 대한 분류 기준을 제시하고 있다.

해당 연구에서는 철도 차량 및 시설에 적용을 목적으로 개발 또는 사용되는 소프트웨어를 대상으로 하고 있으며, <표 3-9>와 같이 소프트웨어가 수행하는 기능의 안전 중요도에 따라 '소프트웨어 안전등급 0~4'의 5개 등급으로 분류하고 있다.

<표 3-9> 철도 - 소프트웨어에 대한 안전등급 체계

안전등급	설명
4	매우 높음
3	높음
2	중간
1	낮음
0	안전과 관련없음

자료 : 한국철도기술연구원, 2008, 철도 소프트웨어 안전기준 및 체계 구축 연구보고서

이 연구에서는 소프트웨어의 안전등급을 결정하기 위한 방법도 제시하고 있다. 우선, 소프트웨어의 안전등급은 소프트웨어가 탑재되는 시스템의 안전등급을 하위 시스템에 할당하는 과정을 통해 결정되는 것을 원칙으로 한다. 그래서 소프트웨어의 안전등급을

57) 한국철도기술연구원, 철도 소프트웨어 안전기준 및 체계 구축 연구보고서, 2008

결정하기 위한 사전 조건으로 다음을 제시하고 있다.

- ㅇ 시스템의 안전등급이 결정되어 있어야 한다.
- ㅇ 하위 시스템들의 역할과 그 연계를 규정할 수 있도록 충분히 상세한 시스템의 구조적 특성이 정의되어 있어야 한다.
- ㅇ 위험요소 목록과 각 위험요소에 대하여 위험요소를 초래할 수 있는 개시사건들 및 각 개시사건에 대한 위험도가 결정되어 있어야 한다.

소프트웨어의 안전등급을 결정하는 방법은 1) 소프트웨어 제어 특성에 대해 분류하고, 이후 2) 시스템의 안전등급과 소프트웨어 제어 특성을 조합하여 소프트웨어의 안전등급을 결정하는 것으로 정의하고 있다.

이 연구에서 제시하고 있는 소프트웨어 제어 특성에 따른 구분 기준은 다음 <표 3-10>과 같다. 제시된 기준에서는 소프트웨어 기능을 시스템의 제어 또는 운전원의 조치에 필요한 정보 제공 기능으로 구분하고 있으며, 소프트웨어 오동작으로 인한 위험요소 발생을 완화하기 위한 다른 독립적인 하위 시스템의 존재 여부를 고려하여 분류하고 있다.

<표 3-10> 철도 - 소프트웨어 제어 구분

소프트웨어 제어 범주	소프트웨어의 제어 특성
C1a	시스템의 기능을 독자적으로 제어하는 소프트웨어, 해당 소프트웨어의 오동작으로 인한 위험요소 발생을 완화하기 위한 다른 독립적인 하위 시스템이 존재하지 않아 해당 소프트웨어의 고장이 직접적으로 시스템의 위험요소를 발생시킨다.
C2a	시스템의 기능을 제어하는 소프트웨어. 해당 소프트웨어의 오동작으로 인한 위험요소 발생을 완화하기 위한 다른 독립적인 하위 시스템이 존재한다.
C2b	시스템의 위험요소를 탐지하고, 위험요소를 완화하기 위한 운전원의 조치를 요구사하는 기능을 수행하는 소프트웨어. 해당 소프트웨어의 오동작은 시스템의 위험요소를 발생시킨다.
C3a	시스템의 기능을 제어하는 소프트웨어. 해당 소프트웨어의 오동작으로 인한 위험요소를 방지할 수 있는 다중의 독립된 하위 시스템이 존재한다.
C3b	시스템의 위험요소를 탐지하고, 위험요소를 완화하기 위한 운전원의 조치를 요구하는 기능을 수행하는 소프트웨어. 그러나 해당 소

	프트웨어 외에도 다중의 독립적인 상태정보를 제공하는 독립적인 하위 시스템이 존재한다.
C4	시스템의 기능을 제어하지 않으며, 운전원 조치를 위한 정보를 제공하지도 않는 소프트웨어

자료 : 한국철도기술연구원, 2008, 철도 소프트웨어 안전기준 및 체계 구축 연구보고서

시스템의 안전등급과 소프트웨어의 제어 범주의 조합을 통한 소프트웨어의 안전등급 결정 기준은 다음 <표 3-11>와 같이 제시되어 있다.

<표 3-11> 철도 - 소프트웨어 안전등급 결정 매트릭스

소프트웨어 제어 범주	소프트웨어의 제어 특성			
	4	3	2	1
C1	4	3	2	1
C2a & C2b	3	2	1	0
C3a & C3b	2	1	0	0
C4	1	0	0	0

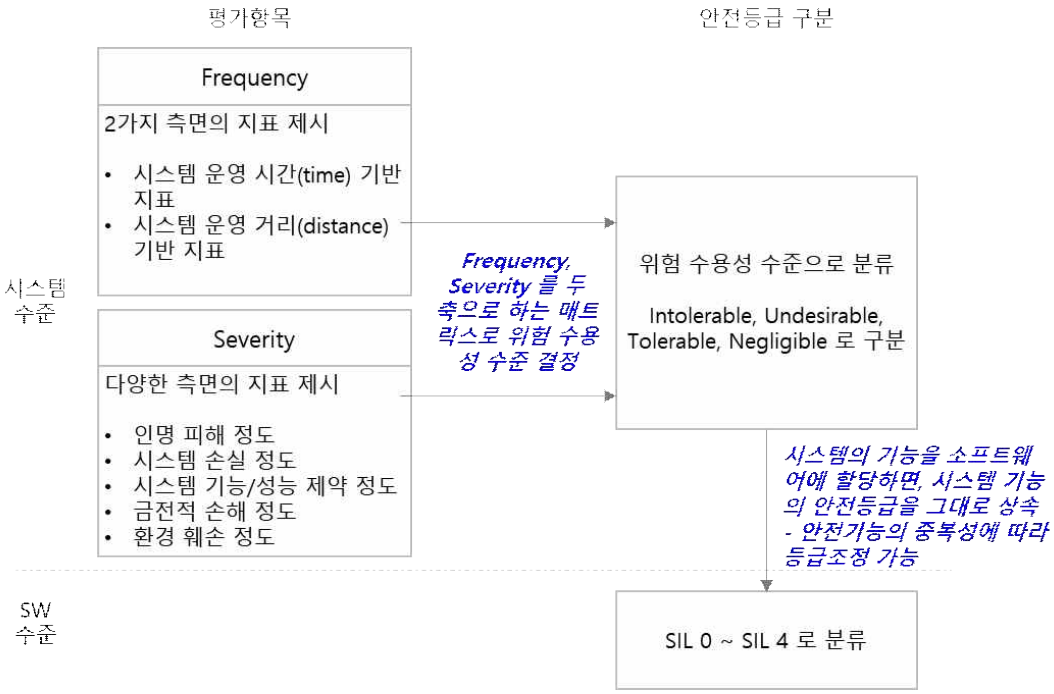
자료 : 한국철도기술연구원, 2008, 철도 소프트웨어 안전기준 및 체계 구축 연구보고서

3. 시사점

가. 철도분야 안전등급 평가 기준

철도 분야의 안전등급 평가 기준은 다음 [그림 3-16]과 같이 정리할 수 있다. 안전등급의 평가는 시스템 수준에서 이루어지며, 소프트웨어는 시스템의 안전등급을 상속받는다. 시스템 기능에 대하여 복수개의 하위 시스템을 구현하는 경우 소프트웨어의 등급이 조정될 수 있으며, 시스템 안전등급의 평가항목으로 발생빈도(Frequency)와 심각도(Severity)가 고려된다.

[그림 3-16] 철도분야 안전등급 평가 기준



나. 안전등급 기준이 명시된 문서

철도분야의 관련 법규정(예, 철도안전법, 도시철도법 등)에서는 안전등급 기준을 제시하고 있지는 않고, 기술기준(철도차량 기술기준)에서 시스템 수준에서 위험평가 시 발생확률 및 결과심각도를 고려해야 함을 명시하고 있다. 하지만 이 또한 상세한 기준을 제시하고 있지는 않다. 기술기준에서는 소프트웨어 안전활동을 위해 국가표준 또는 국제표준(IEC 62279)를 참조할 수 있음을 기술하고 있다.

다. 시스템 수준의 안전등급과의 연관성

철도분야에서 소프트웨어의 안전등급은 결과적으로 국제표준(IEC 62278, IEC 62279)을 따라서 정하게 된다. 국제표준에서는 기본적으로 시스템의 안전등급과 동일하게 소프트웨어의 안전등급이 결정되는 것으로 기술하고 있다. 즉, IEC 62278에서 명시한 기준에 의해 시스템의 기능에 대한 안전등급이 결정되고, 시스템 수준에서 해당 기능을 소프트웨어에 할당하면, 해당 소프트웨어는 시스템 기능에 부여된 안전등급을 그대로 상속하게 된다.

라. 소프트웨어 안전등급 평가항목 및 지표

IEC 62278에서는 시스템의 안전등급을 평가하기 위한 방법으로 발생 빈도(frequency of occurrence)와 심각도 분류(severity categories)에 대한 기준과 이를 기반으로 한 위험 분류 기준 (risk acceptance category)에 대해서 제시하고 있다. 발생빈도 측면에서는 시간(time) 기반의 평가 기준과 운행거리(distance) 기반의 평가 기준을 제시하고 있다. 심각도 측면에서는 사람, 환경, 서비스, 자산 및 금전적 손해 관점에서 다양한 기준을 제시하고 있다.

철도 소프트웨어의 안전기준을 제시하기 위해 수행된 연구에서는 소프트웨어의 제어 특성에 따른 소프트웨어 안전등급의 구분 기준을 제시하기도 하였다. 이 연구에서는 소프트웨어 기능을 시스템의 제어 또는 운전원의 조치에 필요한 정보 제공 기능으로 구분하고 있으며, 소프트웨어 오동작으로 인한 위험요소 발생을 완화하기 위한 다른 독립적인 하위 시스템의 존재 여부를 고려하여 분류하고 있다.

마. 소프트웨어 안전등급 결정방법 및 안전등급 구분

소프트웨어 안전등급은 IEC 62279에서 제시한 기준을 따르고 있다. 해당 표준에서는 소프트웨어 안전등급이 기본적으로 시스템 수준에서 평가되고 결정된다고 명시되어 있으며, 소프트웨어 안전등급은 SIL 0 (가장 낮음), SIL1 ~ SIL4의 5 단계로 구분된다.

제4절 항공 안전

1. 항공안전 관련 국내외 법/제도

가. 해외 법/제도

항공 분야의 안전은 국제 협약을 통해 그 기준이 상당 부분 일관되게 적용되고 있다. 1944년 54개국이 국제민간항공협약(Convention on International Civil Aviation Organization)인 시카고 협약에 서명하였다. 이 협약에 근거하여 국제민간항공기구(ICAO: International Civil Aviation Organization)가 설립되었다. 국제민간항공기구는 항공안전기준과 관련하여 모든 협약국들이 준수할 피요가 있는 표준과 권고 방식(SARPs:Standards and Recommended Practices)을 규정하고 있다.

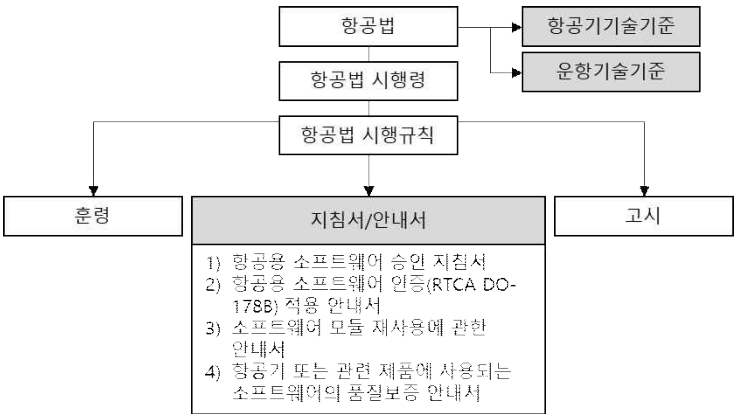
항공 분야에서는 항공기가 운항에 적합한 자체 안전성과 신뢰성을 갖고 있는지를 확

인하는 항공기 인증 제도를 운영하고 있다. 항공기 인증 제도는 설계 안전성을 입증하는 형식인증(Type Certification), 제작 안전성을 입증하는 제작인증(Production Certificatin), 비행 안전성을 입증하는 감항인증(Airworthiness Certification), 운영 안전성을 입증하는 계속감항성(Continued Airworthness)으로 구성된다.

항공기 인증 기준을 운영하는 대표적인 운영 기관으로는 국제민간항공기구(ICAO), 미국연방항공청(FAA), 유럽항공안전기구(EASA)가 있다. 국제민간항공기구에서는 항공기 운영과 항공기의 감항성에 관한 기준을 규정하고 있다. 미국연방항공국에서는 FAR(Federal Aviation Regulation)에서 각종 부품의 법적 인증 절차 및 항공기, 엔진, 프로펠러 등에 대한 감항기술기준을 규정하고 있으며, 이는 세계 각국의 감항기술기준에서 인용되고 있다. 유럽항공안전기구에서는 항공 인증을 위해 EC No. 1592/2002[58]에 의한 기술기준을 적용하고 있다. 기타 국가에서는 해당 기술기준을 기반으로 해당 국가의 감항인증 제도를 운영하고 있다.

국내에서는 미국연방항공청의 FAR에 기반한 KAS(Korean Airworthness Standards)를 기준으로 민간항공기의 감항 인증 제도를 운영하고 있다.

[그림 3-17] 항공법 체계



자료 : NIPA, DO-178C 기반 항공기 분야 소프트웨어안전 가이드

나. 국내 법제도

국내 항공우주 관련 법/제도는 산업통상자원부의 항공우주산업개발 촉진법, 과학기술정보통신부의 우주개발진흥법, 국토교통부의 항공법 등이 존재한다. 이 중 항공법에서 항공기의 감항인증 등을 포함한 항공기 안전에 대한 기준을 제시하고 있다. 항공법과

58) Regulation (EC) No 1592/2002 of the European Parliament and of the Council

관련된 법/규정은 다음과 같다.

ㅇ 항공법/시행령/시행규칙은 항공 안전관련 최상위 규정으로 소프트웨어 개발에 관련된 내용을 직접적으로 다루지는 않는다. 항공법에 의거하여 항공기 기술기준(Korean Airworthiness Standards)이 개발되어 있으며, 해당 기술기준에서 소프트웨어 개발은 RTCA DO-178[59] 또는 EUROCAE ED12[60]를 따르도록 명시하고 있다. 소프트웨어 안전등급은 해당 표준에서 제시하고 있는 기준을 따른다.

- 모든 시스템 소프트웨어 본 기술기준에서 요구하는 안전수준에 적합하고, 계통 내에서 의도하는 기능으로 작동되도록 설계되고, 검증되어야 한다. 소프트웨어의 설계 및 시험은 RTCA/ DO-178 또는 EUROCAE ED12에 따른다.[61]

또한 항공용 소프트웨어 개발자들에게 DO-178을 적용하는 방법과 절차 등을 안내하기 위해 다음과 같은 지침서 및 안내서를 제공하고 있다.

ㅇ 항공용 소프트웨어 승인 지침서: 항공용 소프트웨어 개발자들에게 DO-178B를 적용하는 방법과 절차 안내

ㅇ 항공용 소프트웨어 인증(RTCA DO-178B) 적용 안내서: 형식증명, 부가형식증명, 기술표준품 형식승인 업무를 수행하는데 있어서, DO-178B를 적용하는 방법과 절차 안내

ㅇ 소프트웨어 모듈 재사용에 관한 안내서: 소프트웨어 모듈 재사용에 관한 개발자 지침, 인증기관 지침 등을 안내

ㅇ 항공기 또는 관련 제품에 사용되는 소프트웨어의 품질보증 안내서: 항공기 또는 관련제품에 사용되는 소프트웨어의 품질보증 요구 조건에 대한 적합성을 입증하는데 필요한 절차 안내

2. 항공 안전 기준

항공 소프트웨어 개발과 관련된 표준은 다음과 같다.

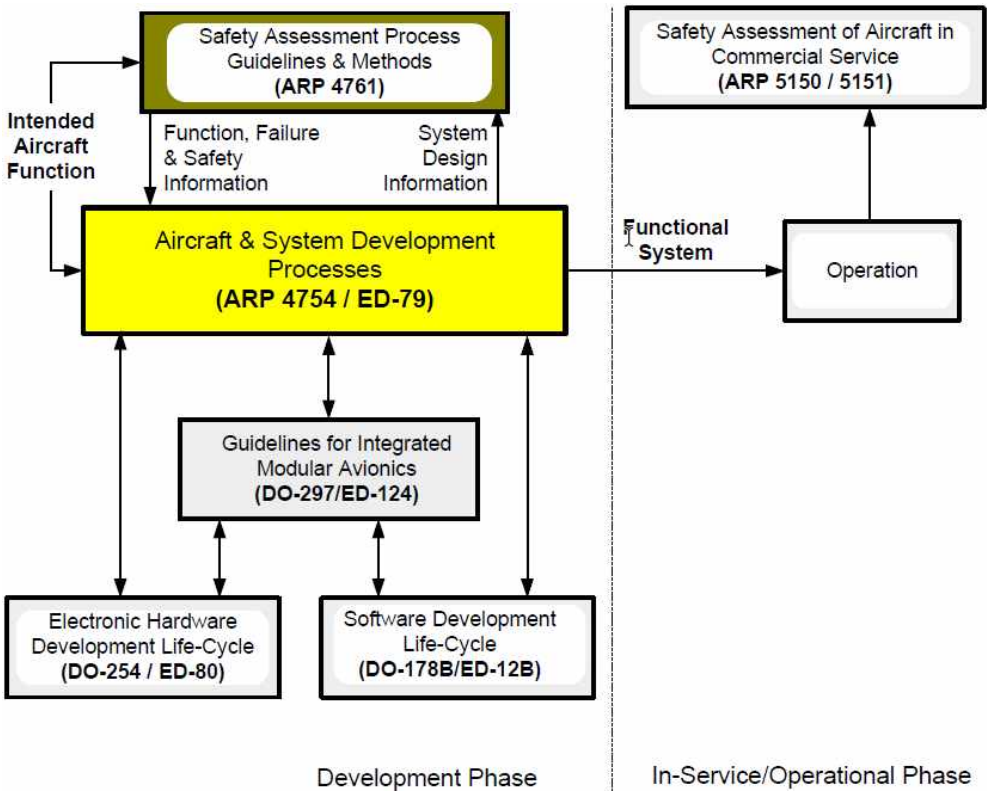
ㅇ ARP 4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: FHA 등의 안전성 평가 절차와 FMEA,

59) Software Considerations in Airborne Systems and Equipment Certification
60) Software Considerations in Airborne Systems and Equipment Certification
61) 항공기 기술기준 Part 1. 1.7.3 소프트웨어 인증

FTA 등의 안전분석 기법을 기술한 표준

- ARP 4754 Guidelines For Development Of Civil Aircraft and Systems: 항공기 시스템의 인증과 개발을 위해 수행해야 하는 절차를 기술한 표준
- DO-297 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations: 통합 항공 전자모듈의 인증을 위한 필요한 사항을 기술한 표준
- DO-254 Design Assurance Guidance for Airborne Electronic Hardware: 항공기에 탑재되는 하드웨어의 개발을 위해 수행해야 하는 계획과 개발 드의 프로세스를 정의한 표준
- DO-178 Software Considerations in Airborne Systems and Equipment Certification: 항공기에 탑재되는 소프트웨어의 개발을 위해 수행해야 하는 계획, 개발, 검증, 품질보증 등의 프로세스를 정의한 표준
- DO-278 Guidelines for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance: 항공 지상장비에 탑재되는 소프트웨어의 개발을 위해 수행해야 하는 계획과 개발 등의 프로세스를 정의한 표준

[그림 3-18] 항공 - 안전 관련 표준



자료 : ARP 4754, Guidelines For Development Of Civil Aircraft and Systems

가. ARP 4761

ARP 4761에서는 FHA(Functional Hazard Assessment) 기법을 통해 시스템의 실패 조건(failure conditions)을 식별하고, 이에 대해 심각도 관점에서 분류하는 기준을 제시한다. FHA는 다음과 같은 절차로 수행된다.[62]

1) 대상 시스템의 기능 식별

2) 식별된 기능과 관련된 실패 조건 식별

3) 실패 조건의 영향 결정 (항공기에 대한 영향)

4) 실패 조건의 영향에 대한 분류

5) 실패 조건에 대한 요구사항 할당 (분류에 따른 Probability, Development assurance level 결정)

62) ARP 4761 Appendix A

6) 요구사항을 검증할 방법 정의

이 중 4) 실패 조건의 영향에 대한 분류는 시스템의 실패가 항공기에 미치는 영향에 기반을 두고 있다. 실패가 항공기에 미치는 영향은 다음과 같이 크게 3가지 관점에서 고려되며, 이후 각 관점에 대한 영향의 크기에 따라 [그림 3-19]와 같이 심각도가 분류된다.

- ㅇ 안전 마진 / 비행 기능 감소
- ㅇ 승무원의 업무 부담 증가 / 물리적 고통
- ㅇ 승객의 불편 / 부작용

[그림 3-19] 항공 - ARP 4761 실패 조건 영향에 따른 분류

Failure Condition Severity Classification	FAA	Minor	Major	Severe Major	Catastrophic
	JAA	Minor	Major	Hazardous	Catastrophic
Failure Condition Effect	FAA & JAA	- slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants	- significant reduction in safety margins or functional capabilities - significant increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants	- large reduction in safety margins or functional capabilities - higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - adverse effects upon occupants	- all failure conditions which prevent continued safe flight and landing

자료: ARP 4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment

실패 조건의 분류를 기반으로 실패 조건의 발생 가능성에 대한 목표 및 개발 보증 수준을 정한다. 이에 대한 기준은 다음과 같다.

[그림 3-20] 항공 - ARP 4761 실패 조건 분류에 따른 발생가능성 및 개발보증등급 목표

Development Assurance Level	ARP 4754	Level D		Level C	Level B	Level A
Probability (Quantitative)	Per flight hour 1.0 1.0E-3 1.0E-5 1.0E-7 1.0E-9					
Probability (Descriptive)	FAA	Probable		Improbable		Extremely Improbable
	JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Severity Classification	FAA	Minor		Major	Severe Major	Catastrophic
	JAA	Minor		Major	Hazardous	Catastrophic

자료: ARP 4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment

ARP 4761은 안전 등급 (safety integrity level)이라는 개념 대신, 개발 보증 등급 (development assurance level) 개념을 사용하고 있다. 개발 보증이란 시스템이 인증 기준을 충족하도록 개발 오류가 식별되고 수정되었음을 적절한 수준의 확신으로 입증하는 데 사용되는 모든 계획되고 체계적인 조치를 뜻한다.

시스템의 개발 보증 수준은 시스템이 수행하는 기능의 실패 조건의 심각도에 따라 결정된다.

나. ARP 4754

ARP 4761의 기준에 의해 항공기의 기능에 부여된 개발 보증 등급과 관련된 안전목표는 기능 개발에 대한 보증등급(FDAL: Functional Development Assurance Level)과 수치적 분석(필요시)에 의해 충족된다. 해당 기능은 구현을 위해 시스템의 구성요소(item)에 할당되는데, 해당 구성요소에 할당된 개발 보증 등급은 IDAL(Item Development Assurance Level)이 된다.

ARP 4754는 FDAL과 IDAL을 부여하는 기준을 제시하고 있으며, FDAL 수준에 따라 부과되는 시스템 수준의 안전 요구사항에 대해 기술하고 있다. DO-178과 DO-254는 각각 소프트웨어와 하드웨어에 부여된 IDAL 수준에 따라 부과되는 구성요소(item) 수준의 안전 요구사항에 대해 기술하고 있다.

ARP 4754에서는 실패 조건의 분류를 기반으로 개발 보증등급을 부여하는 기준을 다음 <표 3-12>와 같이 제시하고 있다.

<표 3-12> 철도 - 실패 조건 분류 기반의 개발 보증등급 부여 기준

실패조건의 분류	개발 보증등급 부여 기준
Catastrophic	• 항공기/시스템 기능 또는 항목의 개발 오류로 인해 Catastrophic Failure(FC)가 **발생**할 수 있는 경우, 관련 개발 보증 프로세스에 Level A 할당됨 • 두 개 이상의 독립적으로 개발된 항공기/시스템 기능 또는 항목 간의 개발 오류의 조합으로 인해 **치명적인 실패 조건이 발생**할 수 있는 경우, 하나의 개발 보증 프로세스에 Level A가 지정되거나 두 개의 개발 보증 프로세스에 최소 Level B가 지정됨 • 다른 독립적으로 개발된 항공기/시스템 기능 또는 항목은 개발 보증 수준 Level C보다 낮지 않게 할당되며, 각 항목이 독립적임을 설정하는 개발 보증 프로세스는 Level A를 유지해야 함
Hazardous	• 항공기/시스템 기능 또는 항목의 개발 오류로 인해 위험 및 **심각한 고장 상태가 발생**할 수 있는 경우, 최소 Level B가 할당됨 • 두 개 이상의 독립적으로 개발된 항공기/시스템 기능 또는 항목 간의 개발 오류 조합으로 인해 **위험한 고장 또는 심각한 주요 상태가 발생**할 수 있는 경우, 하나의 개발 보증 프로세스에 최소 Level B가 지정되거나 두 개의 개발 보증 프로세스가 최소 Level C로 지정됨 • 기타 독립적으로 개발된 항공기/시스템 기능 또는 항목은 개발 보증 Level D보다 낮지 않게 할당되며, 각 항목이 실제로 독립적임을 설정하는 개발 보증 프로세스는 Level B를 유지해야 함
Major	• 항공기/시스템 기능 또는 항목의 개발 오류로 인해 **중대한 고장 상태가 발생**할 수 있는 경우, 관련 개발 보증 프로세스에 Level C가 할당됨 • 두 개 이상의 독립적으로 개발된 항공기/시스템 기능 또는 항목 간의 개발 오류의 조합으로 인해, **중대한 고장 상태가 발생**할 수 있는 경우, 하나의 개발 보증 프로세스에 최소 Level C가 지정되거나 두 개의 개발 보증 프로세스에 최소 Level D가 지정됨 • 각 항목이 실제로 독립적임을 설정하는 개발 보증 프로세스는 Level C를 유지해야 함
Minor	• 항공기/시스템 기능 또는 항목의 개발 오류로 인해 **경미한 고장 상태가 발생**할 수 있는 경우, 관련 개발 보증 프로세스가 최소 Level D로 할당됨 • 두 개 이상의 독립적으로 개발된 항공기/시스템 기능 또는 항목 간의 개발 오류의 조합으로 인해 **경미한 고장 조건이 발생**할 수 있는 경우, 하나의 개발 보증 프로세스가 최소 Level D에 할당됨

자료 : ARP 4754 Guidelines For Development Of Civil Aircraft and Systems

최상위에서 식별된 실패 조건이 단일 기능(function) 또는 시스템 구성요소(item)에

의해 기인하는 경우, 실패 조건의 심각도에 따라 다음과 같이 개발 보증등급이 결정된다.

[그림 3-21] 항공 - ARP 4754 최상위 기능에 대한 개발 보증등급 할당 기준

Top-Level Failure Condition Severity Classification	Associated Top-Level Function FDAL Assignment
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

자료 : ARP 4754 Guidelines For Development Of Civil Aircraft and Systems

하지만, 실패 조건이 복수의 기능 또는 시스템 구성요소에 의해 기인하는 경우, 기능 또는 시스템 구성요소 간의 독립성에 따라 다른 개발 보증등급이 부여될 수 있다.

다. RTCA DO-178C

RTCA DO-178C 표준에서는 시스템 수준에서의 안전 평가를 통해 고장 상태가 결정되고, 소프트웨어 컴포넌트가 해당 시스템 및 시스템 고장에 얼마만큼 관련되어 있는지 분석을 수행하여 소프트웨어의 등급을 결정한다. 소프트웨어 등급은 시스템 안전 평가 프로세스(System Safety Assessment Process)에 따라 결정된다. 즉, 시스템 수준에서 결정된 실패 조건(failure condition)에 소프트웨어가 어떻게 기여하는지를 판단하여 소프트웨어의 등급을 결정하며, 소프트웨어 등급은 소프트웨어를 개발하는데 필요한 엄격함(rigor)의 정도를 나타낸다.

RTCA DO-178C에서 실패 조건의 분류는 시스템의 실패가 항공기에 미치는 여향에 기반을 두고 있다. 이는 ARP 4761에서 정의하고 있는 기준과 매우 동일하며, 승객 또는 승무원의 사망 또는 부상을 조금 더 명시적으로 기술하고 있다.

o 비행기의 안전 마진 / 비행 기능 감소

- ㅇ 승무원의 업무 부담 증가 / 물리적 고통
- ㅇ 승객의 불편 / 사망 또는 부상

소프트웨어 등급은 위에서 언급한 시스템의 실패 조건 분류에 기반하여 A 등급 ~ E 등급의 5단계로 분류된다. 다음은 소프트웨어 등급을 분류하는 기준이다.

- ㅇ A 등급: 소프트웨어 오동작 또는 기능의 손실이 시스템 수준에서 'Catastrophic'의 실패 조건을 유발하거나 이에 기여할 때
- ㅇ B 등급: 소프트웨어 오동작 또는 기능의 손실이 시스템 수준에서 'Hazardous'의 실패 조건을 유발하거나 이에 기여할 때
- ㅇ C 등급: 소프트웨어 오동작 또는 기능의 손실이 시스템 수준에서 'Major'의 실패 조건을 유발하거나 이에 기여할 때
- ㅇ D 등급: 소프트웨어 오동작 또는 기능의 손실이 시스템 수준에서 'Minor'의 실패 조건을 유발하거나 이에 기여할 때
- ㅇ E 등급: 소프트웨어 오동작 또는 기능의 손실이 시스템 수준에서 'No Safety Effect'의 실패 조건을 유발하거나 이에 기여할 때

[그림 3-22] 항공 - DO-178C의 실패 조건에 대한 분류 기준

Category	Description
Catastrophic	Failure Conditions, which would result in multiple fatalities, usually with the loss of the airplane.
Hazardous	Failure Conditions, which would reduce the capability of the airplane or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be: • A large reduction in safety margins or functional capabilities; • Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely, or • Serious or fatal injury to a relatively small number of the occupants other than the flight crew.
Major	Failure Conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.
Minor	Failure Conditions which would not significantly reduce airplane safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.
No Safety Effect	Failure Conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the airplane or increase crew workload.

자료 : DO-178 Software Considerations in Airborne Systems and Equipment Certification

DO-178C는 소프트웨어 등급을 결정할 때 환경조건과 같은 외부 요인, 아키텍처 전략 등을 고려할 수 있다고 기술하고 있다.

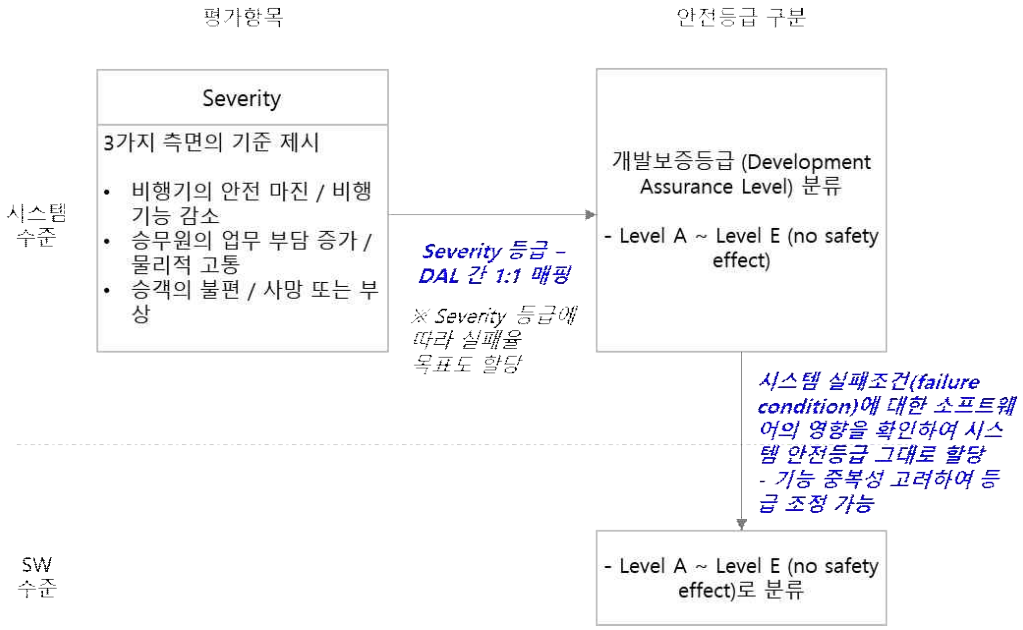
아키텍처에 대한 고려의 예로서 소프트웨어 컴포넌트 간 독립성을 들 수 있다. 소프트웨어 컴포넌트 간 독립성이 보장되어 있는 경우(software partitioning), 각 소프트웨어 컴포넌트에 개별적인 소프트웨어 등급이 부여될 수 있다. 그러나 독립성이 보장되지 않은 경우, 전체 소프트웨어가 동일한 등급을 부여 받는다. 소프트웨어가 하나 이상의 실패 조건에 영향을 미칠 때는 실패 조건의 분류 등급이 가장 높은 것을 기준으로 등급을 결정한다.

3. 시사점

가. 항공분야 안전등급 평가 기준

항공 분야의 안전등급 평가 기준은 다음 [그림 3-23]과 같이 정리할 수 있다. 안전등급의 평가는 시스템 수준에서 이루어지며, 소프트웨어는 시스템의 안전등급을 상속받는다. 시스템 실패조건이 복수개의 독립적인 하위 기능/시스템의 결함 조합에 의한 경우, 소프트웨어 등급은 하향 조정될 수 있으며, 시스템 안전등급의 평가항목으로 심각도(Severity)가 고려되었다.

[그림 3-23] 항공분야 안전등급 평가 기준



나. 안전등급 기준이 명시된 문서

항공분야의 관련 법규정(항공법/시행령/시행규칙 등)은 소프트웨어 안전 및 개발에 관련된 내용을 직접적으로 다루지는 않는다. 항공법에 의거하여 항공기 기술기준(Korean Airworthiness Standards)이 개발되어 있으며, 해당 기술기준에서 소프트웨어 개발은 RTCA/ DO-178C 또는 EUROCAE ED12를 따르도록 명시하고 있다. 소프트웨어 안전등급은 해당 표준에서 그 기준을 제시하고 있다.

다. 시스템 수준의 안전등급과의 연관성

항공분야에서 소프트웨어 안전등급은 시스템 안전 평가 프로세스에 따라 결정된다. 시스템 기능의 실패 조건을 식별하고, 해당 실패 조건이 항공기에 미치는 영향을 고려하여 실패 조건을 분류한다. 소프트웨어의 안전등급은 소프트웨어 기능이 실패 조건에 미치는 영향을 분석하여, 실패 조건의 분류 기준에 따라 등급이 결정된다.

라. 소프트웨어 안전등급 평가항목 및 지표

소프트웨어 안전등급 판단에 영향을 미치는 평가항목은 시스템 수준의 실패 조건에 대한 영향 심각도이다. 실패 조건의 영향 심각도를 판단하기 위한 기준으로 비행기의 안전 마진 / 비행 기능 감소, 승무원의 업무 부담 증가 / 물리적 고통, 승객의 불편 / 사상 등의 관점에서 정성적인 평가기준을 제시하고 있다.

마. 소프트웨어 안전등급 결정방법 및 안전등급 구분

소프트웨어 안전등급은 DO-178C에서 제시한 기준을 따르고 있다. 해당 표준에서는 소프트웨어 안전등급이 기본적으로 시스템 수준에서 평가되고 결정된다고 명시되어 있으며, 소프트웨어 안전등급은 A 등급(가장 높음) ~ E 등급(가장 낮음)의 5 단계로 구분된다.

제5절 전기용품 안전

1. 전기용품 안전 관련 국내 법/제도

국내에서는 우리 일상에서 사용되고 있는 제품의 안전성을 확보하기 위해 제품이 시장에 출시되기 전과 후를 기준으로 관련법을 제정하여 운영하고 있다. 제품시장 출시 전에는 “전기용품 및 생활용품 안전관리법” 및 “어린이제품 안전특별법”에 따른 제품인증제도를 중심으로 사전 안전관리가 요구되는 일부 제품에 대해서는 사업자가 최소한의 안전요구조건을 만족하는 제품을 시장에 출시토록 의무화하고 있으며, 인증을 받은 제품 및 기타 사전관리되고 있지 않은 제품에 대해서도 소비자의 안전에 위협을 가한 제품 또는 가할 여지가 있는 제품에 대해서는 “제품안전기본법”을 근거로 안전성 조사를 통해 시장 또는 소비자로부터 회수될 수 있도록 리콜제도를 운영하

고 있다.[63]

[그림 3-24] 전기용품 안전 관련 국내 법제도

자료 : 국가기술표준원 홈페이지 - 정책 - 제품안전

전기용품 및 생활용품 안전관리법은 안전과 관련된 전기용품을 대상으로 '안전인증 제도'의 운영을 명시하고 있다. 동법의 시행규칙 및 운영요령에서 안전관리대상 전기용품을 기술하고 있으며, 각 전기용품에 대한 안전요건은 별도의 기준을 제정하여 적용하고 있다.[64]

다음은 전기용품 안전기준 목록의 일부이다[65].

63) 국가기술표준원 홈페이지 - 정책 - 제품안전 (https://www.kats.go.kr/content.do?cmsid=37)
64) 전기용품 안전기준 (KC)
65) 국가기술표준원 홈페이지 - 정책 - 제품안전 - 안전기준열람 (https://www.kats.go.kr/content.do?cmsid=34)

[그림 3-25] 전기용품 안전기준 목록

기준번호	기준명	고시일	조회수	첨부파일
KC 10023	안정기 내장형 LED 램프	2020-05-14	902	
KC 60335-2-29	가정용 및 이와 유사한 전기기기의 안전성 제2-29부: 배터리 충전기의 개별 요구사항	2020-05-14	868	
KC 10030	LED조명 시스템	2019-07-30	1062	
KC 62196-1	플러그,소켓-아울렛, 자동차 커넥터,자동차 인렛 및 자동차 어댑터-전기자동차의 전도성 충전 제1부: 일반 요구사항	2019-06-28	1112	
KC 61851-1	전기차 충전시스템 제1부: 일반 요구사항	2019-06-28	1054	
KC 62619	산업용 리튬이차전지 안전	2019-10-21	1929	
KC 62133	휴대용 밀폐 2차 전지 안전	2019-02-15	4555	
KC 10025	형광램프 대체형 LED 램프 - 컨버터 내장형	2018-11-05	3566	
KC 60598-2-8	등기구 제2-8부: 손전등 - 개별요구사항	2018-11-05	2989	
KC 62133	휴대용 밀폐 2차 전지 안전	2018-09-06	3884	

자료 : 국가기술표준원 홈페이지 - 정책 - 제품안전

KC 62619[66]은 배터리 시스템의 안전에 대한 요구사항을 정의하고 있다. 시스템의 안전등급과 관련해서 전지 관리 시스템(BMS)이 '안전 무결성 기준(SIL)'에 적합하게 설계되어야 한다고 명시하고 있으며, 등급 결정을 위한 세부 기준을 제시하고 있지는 않다. 다만 참조 규격으로 KS C IEC 61508[67], KS C IEC 60730-1[68] 등을 명시하고 있다. 시스템 또는 소프트웨어의 안전 등급을 결정하는 기준은 해당 표준을 따른다.

2. 전기용품 안전 기준

가. KS C IEC61508

KS C IEC61508에서는 안전무결성수준(SIL)을 결정하는 방법으로 정량적 방법과 정성

66) 전기용품 안전기준 (KC) - 산업용 리튬이차전지 안전
67) 전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 기능안전성
68) 전기용품안전기준 - 가정용 및 이와 유사한 자동 제어장치 - 제1부:일반 요구사항

적 방법을 기술하고 있다[69]. 정량적 방법은 시스템의 평균 고장 확률 등의 데이터를 활용하는데, 소프트웨어의 경우 이런 정량적인 고장율 개념을 적용하는 것에 논란이 있는 상태이다. 이 때문에 본 연구에서 안전무결성수준 결정을 위한 정량적 방법은 별도로 소개하지 않는다.

안전무결성수준을 결정하기 위한 정성적 방법은 다음과 같은 평가항목 및 세부 평가항목에 기반한다.

- o 위해한 사건의 결과
- o 위해한 사건의 빈도
  - 위해 구역의 빈도와 그에 대한 노출 시간
  - 위해한 사건을 피할 가능성
  - 불의의 발생 확률 (발생된 위해 경우의 확률)

또한, <표 3-13>, [그림 3-26]과 같이 위의 평가항목에 대한 분류 시 고려해야 하는 항목과 지표에 대한 예를 제시하고 있다.

<표 3-13> KS C IEC 61508 - 평가항목 분류 시 고려해야 하는 항목

고려 사항	설명
위해한 사건의 결과	• 사람에 대한 상해와 사망 • 환경 또는 물질 손상
위해 구역의 빈도와 그에 대한 노출 시간	• 위해 구역에서의 노출 정도
위해한 사건을 피할 가능성	• 공정에 대한 감독 여부 • 위해한 사건의 발전 비율 • 위험 인식의 용이성 • 위해한 사건의 방지 수단의 가용성 • 유사 시스템에 대한 안전 경험
불의의 발생 확률	• 유사 시스템에 대한 안전 경험

자료 : KS C IEC 61508, 전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 기능안전성

69) KS C IEC 61508-5 KS C IEC61508-5 프로그램 가능한 전자장치 안전관련 시스템의 기능안전성 — 제5부: 안전무결성수준 결정 방법의 예

[그림 3-26] KS C IEC 61508 - 평가항목 및 지표 예

리스크 파라미터		구분	비고
결과(*C*)	C_1 C_2 C_3 C_4	경상 한 명 이상의 사람의 심각하고 영구적인 상해; 한 명의 사망 몇 사람 사망 매우 많은 수의 사람 사망	1. 구분 체계는 사람에 대하 상해와 사망에 따라 개발되었다. 환경 또는 물질 손상에 대해서도 기타 구분 계획을 개발할 필요가 있다. 2. C_1, C_2, C_3, C_4의 해석에 대하여, 사고의 결과와 정상적인 구제조치를 고려하여야 한다.
위해 구역의 빈도와 그에 대한 노출시간(*F*)	F_1 F_2	위해 구역에서의 노출이 드물거나 가끔 있음. 위해 구역에서의 노출이 빈번하거나 항상 있음.	3. 위 **비고** 1. 참조
위해한 사건을 피할 가능성(*P*)	P_1 P_2	일정 조건에서 가능 거의 불가능	4. 이 파라미터는 다음을 고려한다. – 어떤 공정의 운영[감독되거나(즉, 숙련 및 비숙련 직원에 의해 운영되는) 감독되지 않음.] – 위해한 사건의 발전 비율(예 : 갑자기, 급속히, 천천히) – 위험 인식 용이(예 : 즉시 보이고, 기술적 수단 또는 기술적 수단 없이 발견됨.) – 위해한 사건의 방지(예 : 회피 수단의 실시가 가능함, 또는 불가능함, 또는 일정 조건에서 가능함.) – 실제 안전 경험(이런 경험이 동일 EUC나 유산 EUC에 대해 존재해도 되거나 존재하지 않는 것이 좋다.)
불의의 사건 발생 확률(*W*)	W_1 W_2 W_3	불의의 사고 발생을 간과할 확률이 거의 적으며 불의의 사고 발생 가능성이 거의 없음. 불의의 사고 발생을 간과할 확률이 적으며 불의의 사고 발생 가능성이 약간 있음. 불의의 사고 발생을 간과할 확률이 비교적 높으며 불의의 사고 발생 가능성이 자주 있음.	5. *W* 인자의 목적은 안전관련 시스템 (E/E/PE나 기타 기술)을 추가하지 않고 기타 기술 위험 감소 시설만 포함시킨 경우의 불의의 사고 발생 빈도를 측정하는 것이다. 6. EUC, EUC 제어 시스템 및 유사 EUC 및 EUC 제어 시스템에 대한 경험이 거의 또는 전혀 없다면, 결산에 의해 W 인자의 측정되어도 된다. 이런 경우 최악의 경우가 예측되어야 한다.

자료 : KS C IEC 61508, 전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 기능안전성

위에서 언급된 평가항목을 기반으로 안전등급을 결정하는 방법으로는 리스크 그래프 방법이 제시되고 있다. 리스크 그래프를 작성하는 방법은 다음과 같다. 해당 예시에서는 안전무결성수준을 1~4 등급으로 구분하고 있다.

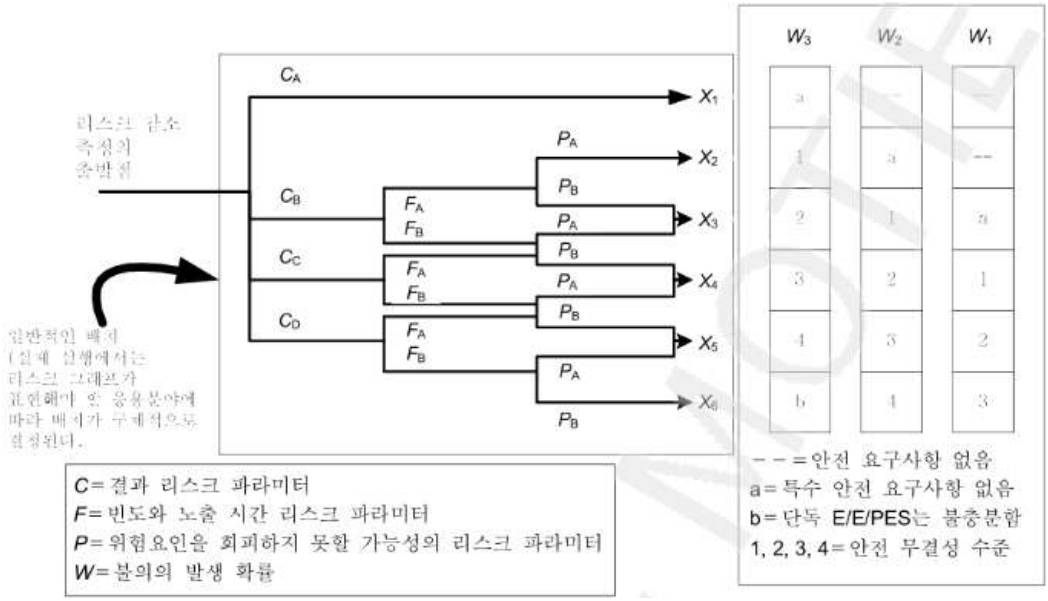
1) 평가항목과 이에 대한 분류자(리스크 파라미터)의 조합을 통해 1차 분류 수행

- 사용되는 평가 항목: 위해한 사건의 결과, 위해 구역의 빈도와 그에 대한 노출시간, 위해한 사건을 피할 가능성

2) 1차 분류된 결과는 불의의 사건 발생 확률을 고려하여 분류를 조정함

3) 조정된 결과는 안전등급과 매핑됨

[그림 3-27] KS C IEC 61508 - 리스크 그래프: 일반적인 도식



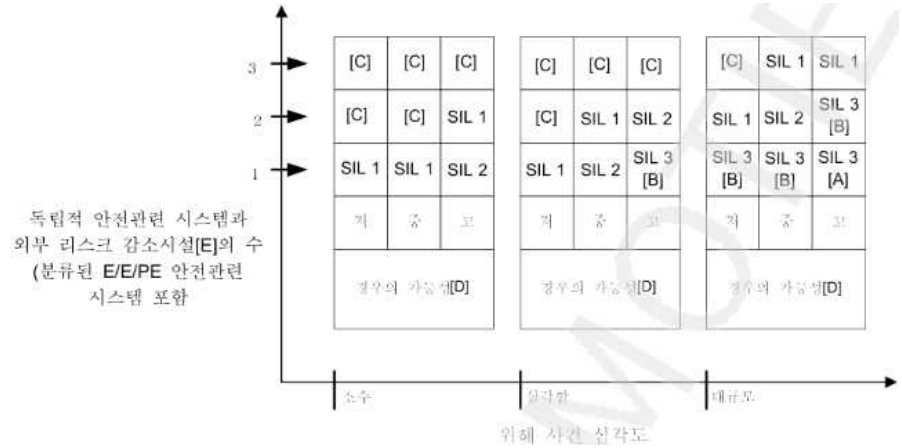
자료 : KS C IEC 61508, 전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 기능안전성

KS C IEC61508에서 제시하고 있는 또 다른 정성적 안전무결성수준의 결정 방법은 위해 사건 심각도 매트릭스이다. 이 방법에서는 다음과 같은 평가항목을 기준으로 안전무결성수준을 판단한다. (이 방법의 경우, 세부적인 평가지표는 제시하지 않고 있다.)

- ㅇ 위해 사건의 심각도 (severity)
- ㅇ 위해 사건의 발생가능성 (likelihood)
- ㅇ 대상 시스템 또는 외부시스템에서 상호독립적으로 구현된 안전기능의 개수

위의 평가항목에 대한 평가를 기준으로 다음과 같이 입체적인 매트릭스 구조를 통해 안전무결성수준을 결정할 수 있다.

[그림 3-28] KS C IEC 61508 - 위해 사건 심각도 매트릭스



자료 : KS C IEC 61508, 전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 기능안전성

위의 기준에 의해 결정된 안전무결성 수준 및 요구사항은 해당 안전기능을 구현할 시스템 혹은 하위 시스템에 할당된다. 소프트웨어의 안전등급도 이러한 할당 방식에 의해 결정된다[70].

나. KS C IEC60730

KS C IEC 60730은 난방기, 에어컨과 같은 가정용 자동제어장치의 안전에 대한 요건을 정의하고 있다. 이 표준에서는 전자 제어장치에 대한 요구사항을 정의하고 있으며, 해당 부분에서 안전과 관련한 소프트웨어의 등급을 분류하는 기준을 제시하고 있다.[71] 소프트웨어의 등급 분류 기준은 <표 3-14>과 같다.

<표 3-14> KS C IEC 60730 - 안전 관련 소프트웨어 등급 분류 기준

소프트웨어 등급	등급 분류 기준
A등급 제어장치	안전이 기기에 의존하지 않는 제어장치 예) 온도조절장치
B등급 제어장치	기기의 불안전 상태를 예방하도록 설계된 제어장치 예) 온도 제한장치, 압력 제한장치 등
C등급 제어장치	폭발과 같은 위험한 상황을 예방하기 위해 설계된 제어장치 예) 버너 조절 시스템, 밀폐 온수기의 온도차단장치

자료 : KS C IEC 60730, 전기용품안전기준 - 가정용 및 이와 유사한 자동 제어장치

70) KS C IEC 61508-1 7.6 안전 요구사항 할당
71) KS C IEC 60730-1 부속서 H.2.22 제어장치 기능의 종류에 따른 정의

이 표준에서 제시하고 있는 소프트웨어 안전등급의 평가항목은 소프트웨어 기능으로 인해 발생 가능한 위험의 심각도이다. 이 표준에서는 소프트웨어 안전등급에 따라 적용되어야 할 요구사항에 대해서도 상세하게 정의하고 있다.[72)]

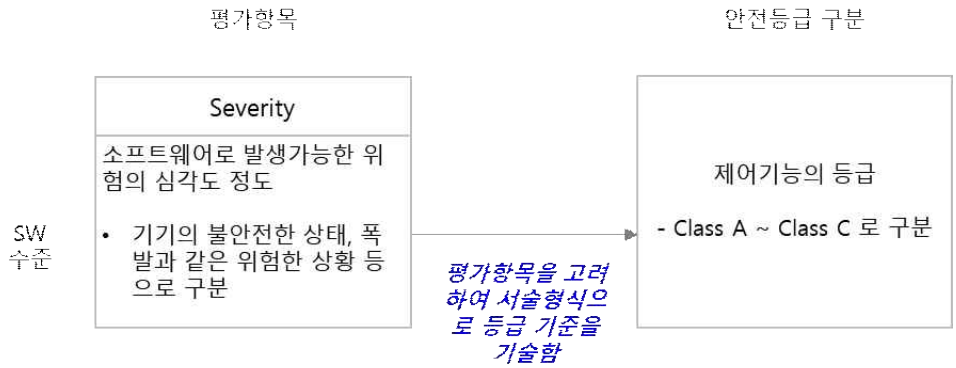
- ㅇ 소프트웨어 구조에 대한 요구사항
- ㅇ 고장/에러 제어장치에 대한 안전장치
- ㅇ 에러를 회피하기 위한 안전활동
- ㅇ 원격 작동하는 제어장치 기능

3. 시사점

가. 전기용품 분야 안전등급 평가 기준

전기용품 분야의 안전등급 평가 기준은 다음 [그림 3-29]와 [그림 3-30]와 같이 정리될 수 있다. 먼저, IEC 60730 표준 기반의 안전등급 평가 기준은, 시스템 수준의 안전분석 또는 안전등급 결정체계에 대한 별도의 언급 없이 소프트웨어 안전등급 결정을 위한 기준을 제시한다. 소프트웨어 안전등급을 결정하기 위한 평가항목으로, 위험 심각도가 고려된다.

[그림 3-29] 전기용품 분야 안전등급 평가 기준 - IEC 60730

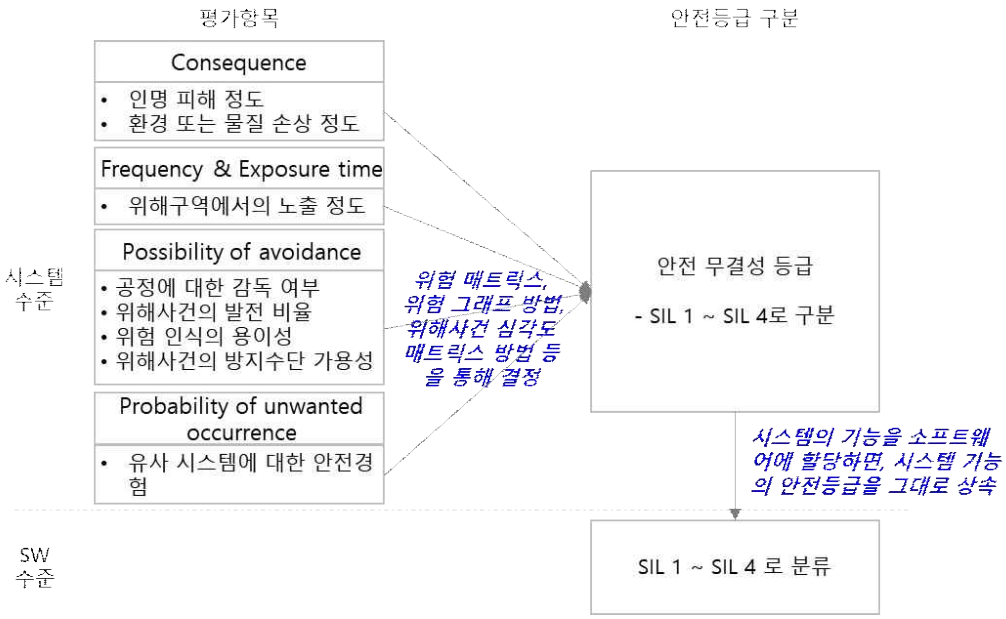


IEC 61508 표준 기반의 안전등급 평가 기준은, 시스템 수준에서 안전등급 평가가 이

72) KS C IEC 60730-1 부속서 H.11.12 소프트웨어를 사용하는 제어장치

루어지며, 소프트웨어는 시스템의 안전등급을 상속 받는다. 시스템의 안전등급의 평가 항목으로 위험 심각도, 노출도, 회피 가능성, 사건발생확률 등이 고려되며, 안전등급 결정을 위해 위험 매트릭스, 위험 그래프, 위해사건 심각도 매트릭스 등의 다양한 방법을 제시하고 있다.

[그림 3-30] 전기용품 분야 안전등급 평가 기준 – IEC 61508



나. 안전등급 기준이 명시된 문서

전기용품 분야의 관련 법규정(전기용품 및 생활용품 안전관리법, 어린이제품 안전특별법 등)은 소프트웨어 안전에 관련된 내용을 다루지는 않는다. 다만 해당 법제도를 기반으로 제품인증제도를 운영하고 있으며, 각 제품에 대한 안전요건은 별도의 전기용품 안전기준(KC)을 제정하여 적용하고 있다.

전기용품 안전기준은 시스템을 개발하기 위한 안전 요구사항을 명시하고 있으며, 시스템 또는 소프트웨어의 안전등급에 대해서는 관련 표준문서를 참조하도록 하고 있다. 산업용 리튬이차전지 안전기준의 경우, KS C IEC 61508과 KS C IEC 60730을 참조하도록 하고 있다. 해당 표준에서는 시스템 또는 소프트웨어 수준의 안전등급을 결정하는 기준을 제시하고 있다.

다. 시스템 수준의 안전등급과의 연관성

전기용품 분야에서 소프트웨어 안전등급은 관련 표준(KS C IEC 61508 또는 KS C IEC 60730)에 다라 결정된다.

KS C IEC 61508에서는 시스템 수준에서 안전등급(안전무결성수준, SIL)이 결정되고, 소프트웨어에 이를 할당하는 방식으로 소프트웨어의 안전등급이 결정된다. KS C IEC 60730에서는 소프트웨어 기능으로 인해 발생 가능한 위험의 심각도를 기반으로 소프트웨어 자체의 안전등급을 판단하도록 기준을 제시하고 있다.

라. 소프트웨어 안전등급 평가항목 및 지표

KS C IEC 61508에서 시스템의 안전등급을 평가할 때 다음과 같은 항목을 고려한다.

- ㅇ 위해한 사건의 결과
- ㅇ 위해 구역의 빈도와 그에 대한 노출 시간
- ㅇ 위해한 사건을 피할 가능성
- ㅇ 불의의 발생 확률
- ㅇ 대상 시스템 또는 외부시스템에서 상호독립적으로 구현된 안전기능의 개 수

각 평가항목에 대한 분류 기준으로 정량적 방법과 정성적 방법을 제시하고 있으나, 정량적 방법의 경우 고장율 개념을 사용하고 있어 소프트웨어에 적용하는 데는 어려움이 있을 것으로 판단된다. 해당 표준은 각 평가항목에 대한 정성적 분류 기준도 제시하고 있다. KS C IEC 60730은 소프트웨어 기능으로 인해 발생 가능한 위험의 심각도를 평가항목으로 제시하고 있으며, 심각도의 정도에 대한 정성적 기준을 제시하고 있다.

마. 소프트웨어 안전등급 결정방법 및 안전등급 구분

KS C IEC 61508은 안전무결성수준을 등급 1(가장 낮음) ~ 등급 4(가장 높음)의 4단계로 구분하고 있다. KS C IEC 60730은 소프트웨어 등급을 등급 A(가장 낮음) ~ 등급 C(가장 높음)의 3단계로 구분하고 있다.

제6절 의료 안전

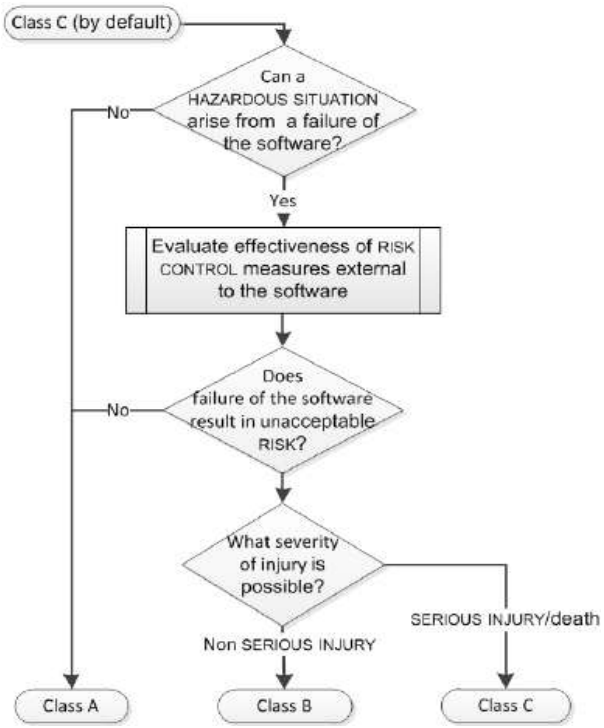
의료 분야의 안전 표준으로 ISO 14971[73]과 IEC 62304[74]가 대표적이다. ISO 14971은

의료기기 또는 시스템에 대한 위험관리 표준으로 시스템 수준의 위험 평가 기준을 제시하고 있다. IEC 62304는 의료기기 시스템에 포함되어 있는 소프트웨어의 안전성을 확보하기 위해 필요한 개발과 유지보수 활동에 대한 요건을 제시하고 있다. 이 표준에서는 소프트웨어의 안전등급을 평가하기 위해 소프트웨어 수준에서 기준을 제시하고 있다. 다른 도메인의 표준과는 달리 소프트웨어 수준에서 판단할 수 있는 기준을 제시하고 있어 본 연구에서 이를 살펴보고자 한다.

1. 의료기기 안전 기준 (IEC 62304, ISO 14971)

IEC 62304는 의료기기에 사용되는 소프트웨어의 안전등급을 평가하기 위한 절차 및 기준을 제시하고 있다[75]. 소프트웨어 안전등급 결정 절차는 다음과 같다.

[그림 3-31] 의료 - IEC 62304 소프트웨어 안전 등급 결정 절차



자료 : IEC 62304, Medical device software — Software life cycle processes

73) Medical Devices - Application Of Risk Management To Medical Devices
74) Medical device software — Software life cycle processes
75) IEC 62304 4.3 Software safety classification

소프트웨어 안전등급의 결정을 위해 다음의 특성을 고려하며, 해당 특성을 기반으로 소프트웨어 안전등급을 결정한다. <표 3-15>에서는 소프트웨어 안전등급 결정을 위한 기준을 설명하고 있다.

- ㅇ 소프트웨어 실패로 인한 위험상황(Hazardous Situation) 발생 여부
- ㅇ 대상 소프트웨어 이외의 시스템에 의한 안전장치(Risk control measures)의 존재 여부
- ㅇ 위험으로 인한 인명 피해의 심각도 (Severity of Injury)

<표 3-15> 의료 - IEC 62304 소프트웨어 안전등급 결정 기준

안전등급	안전등급 결정 기준
안전등급 A (Software Safety Class A)	• 소프트웨어 시스템이 위험 상황에 기여하지 않거나, • 소프트웨어 시스템이 외부의 위험관리 조치를 고려한 후, 허용 가능한 수준의 위험에 기여함
안전등급 B (Software Safety Class B)	• 소프트웨어 시스템이 외부의 위험관리 조치를 고려한 후, 허용 불가능한 수준의 위험에 기여를 하며, 이로 인한 피해는 심각하지 않은 부상의 정도임
안전등급 C (Software Safety Class C)	• 소프트웨어 시스템이 외부의 위험관리 조치를 고려한 후, 허용 불가능한 수준의 위험에 기여를 하며, 이로 인한 피해는 사망 또는 심각한 부상의 정도임

자료 : IEC 62304, Medical device software — Software life cycle processes

이 표준은 위의 기준을 제시하면서 소프트웨어 실패 확률은 1(100%)로 가정한다고 명시하고 있다. 하지만, 해당 표준에서는 피해의 심각도에 대한 기준이 제시되고 있지 않다. 피해 심각도에 대한 기준은 ISO 14971을 참조할 수 있다. 다음 <표 3-16>, <표 3-17>은 ISO 14971에서 제시하고 있는 피해 심각도 기준의 예이다[76].

<표 3-16> 의료 - ISO 14971 정성적 심각도 평가 기준 (3단계)

심각도	설명
Significant	사망 또는 손실
Moderate	복구 가능하거나 경미한 부상
Negligible	약간의 부상 또는 부상이 없음

자료 : ISO 14971, Medical Devices - Application Of Risk Management To Medical Devices

76) ISO 14971 Annex D.3 Risk estimation

<표 3-17> 의료 - ISO 14971 정성적 심각도 평가 기준 (6단계)

심각도	설명
Catastrophic	환자의 사망
Critical	영구적인 손상 또는 생명을 위협하는 부상 발생
Serious	전문적인 의학적 개입이 필요한 부상 또는 장애 발생
Minor	전문적인 의학적 개입이 필요하지 않은 일시적 부상 또는 장애 발생
Negligible	불편하거나 일시적인 불쾌함 발생

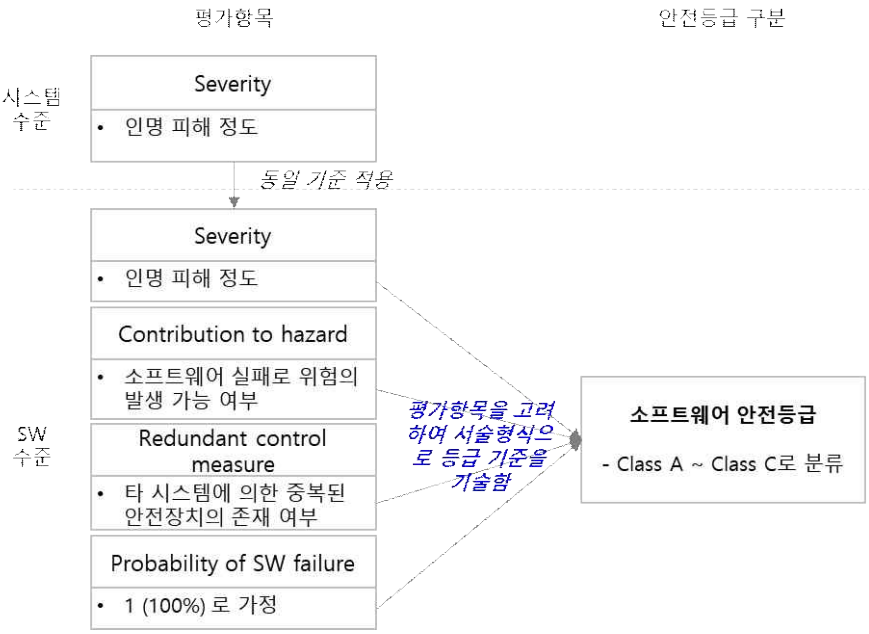
자료 : ISO 14971, Medical Devices - Application Of Risk Management To Medical Devices

2. 시사점

가. 의료분야 안전등급 평가 기준

의료분야의 안전등급 평가 기준은 다음 [그림 3-32]과 같이 정리될 수 있다. 시스템 수준의 안전분석 또는 안전등급 결정 체계에 대한 별도의 언급없이 소프트웨어 안전등급 결정을 위한 기준을 제시하고 있다. 소프트웨어 안전등급에 대한 평가항목으로 심각도, 위험 관여도, 중복된 외부 안전장치를 고려하고 있다.

[그림 3-32] 의료분야 안전등급 평가 기준



나. 시스템 수준의 안전등급과의 연관성

의료기기에 대한 소프트웨어 안전 표준(IEC 62304)는 시스템 수준의 안전 분석에 대한 참조없이 소프트웨어의 안전등급을 평가할 수 있는 기준을 제시하고 있다.

다. 소프트웨어 안전등급 평가항목 및 지표

의료 분야에서 소프트웨어 안전등급 평가 시 고려하고 있는 평가항목은 다음과 같다.

- ㅇ 소프트웨어 실패로 인한 위험상황(Hazardous Situation) 발생 여부
- ㅇ 대상 소프트웨어 이외의 시스템에 의한 안전장치(Risk control measures)의 존재 여부
- ㅇ 위험으로 인한 인명 피해의 심각도 (Severity of Injury)

해당 표준에서는 이에 대한 구체적인 기준은 제시하고 있지는 않다.

라. 소프트웨어 안전등급 결정방법 및 안전등급 구분

소프트웨어 안전등급은 Class A(가장 낮음) ~ Class C(가장 높음)의 3단계로 구분하고 있다.

제7절 미국 국방부 및 항공우주국 안전

미국 국방부(Department of defense)와 항공우주국(NASA)의 안전 표준은 소프트웨어에 특화된 안전등급 기준에 대하여 가장 많은 고려를 하고 있는 표준 중 하나이다. 다른 도메인들의 안전 표준은 대부분 시스템 수준에서 결정된 안전등급을 소프트웨어가 상속받는 방식으로 소프트웨어의 안전등급을 결정한다. 하지만 미국 국방부 및 항공우주국의 안전 표준은 시스템 수준의 위험에 대한 평가 뿐만 아니라, 소프트웨어의 특성을 소프트웨어 안전등급을 결정하는데 중요한 평가항목으로 고려하고 있다. 이러한 이유로 이 절에서 해당 표준들에 대해 상세하게 살펴보고자 한다.

1. 미국 국방 안전 기준

미국 국방부는 국방부 지침 DoDI 5000.02[77]에 따라, 국방 시스템 / 제품 / 장비 / 기반시설의 위험요인(hazard)을 제거하거나, 이로 인한 위험의 최소화를 위한 시스템 공학적 접근방법을 포함하는 시스템 안전 표준인 MIL-STD-882[78]를 제정하였다. MIL-STD-882는 시스템 수준에서 위험을 평가하고 등급을 분류하는 기준[79]과 소프트웨어가 시스템 위험에 미치는 영향을 평가하고 안전등급을 분류하는 기준[80]을 제시한다. 소프트웨어 안전등급 분류에 대한 기준은 MIL-STD-882C 버전부터 포함되었는데, 이에 대한 기반이 되는 연구[81]가 있어, 본 장에서는 해당 연구에 대한 조사 내용도 설명하고자 한다. 소프트웨어와 관련된 안전활동 수행을 위한 세부사항은 별도의 핸드북을 통해 가이드하고 있다[82].

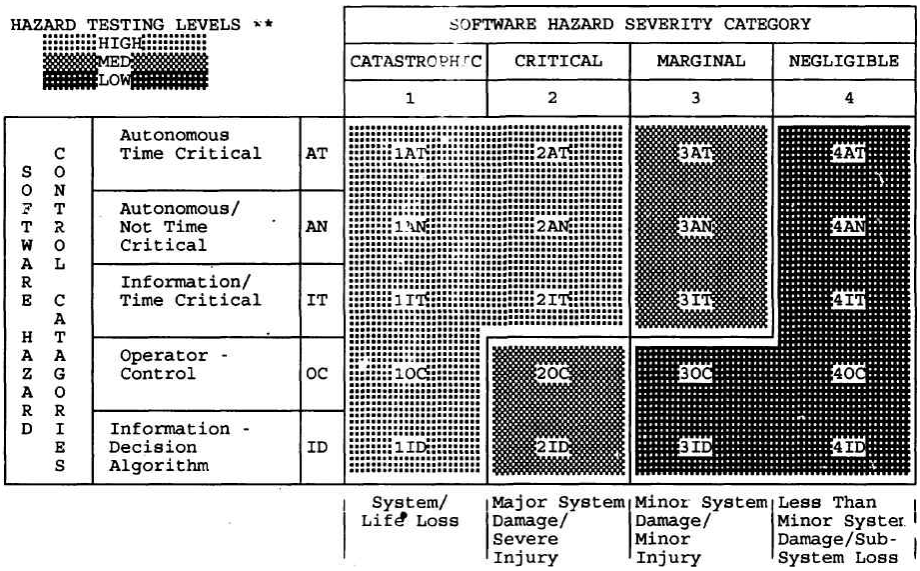
가. 소프트웨어 시스템 안전 가이드 (Software System Safety Guide)

MIL-STD-882C 표준의 기반 연구인 소프트웨어 시스템 안전 가이드에서는 [그림 3-33]과 같이 소프트웨어 위험원 심각도 매트릭스(Software Hazard Criticality Matrix)를 정의하고 있다. 해당 매트릭스는 하드웨어 기반의 위험 평가표와 유사하나 소프트웨어에 대한 테스트 수준을 결정하기 위한 등급 구분을 목적으로 하고 있다. 평가는 소프트웨어 위험원에 대한 심각도(severity) 유형과 제어(control) 유형의 두 가지 항목을 기반으로 수행한다.

소프트웨어 등급의 결정은 소프트웨어 제어 유형보다는 심각도 유형에 보다 의존적임을 알 수 있다. 즉, 소프트웨어가 제어 기능을 수행하거나 정보 제공 기능을 수행하는 경우와 상관없이, 그로 인한 위험의 심각도가 높으면 등급이 높게 결정될 수 있다.

77) DOD INSTRUCTION 5000.02 - OPERATION OF THE ADAPTIVE ACQUISITION FRAMEWORK
78) DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY
79) MIL-STD-882E 4.3.3
80) MIL-STD-882E 4.4
81) Software system safety guide (CECOM-TR-92-2), US Army Communications/Electronics Command
82) Joint Software Systems Safety Engineering Handbook

[그림 3-33] 미국 국방 - 소프트웨어 위험원 심각도 매트릭스



자료: Software system safety guide (CECOM-TR-92-2), US Army Communications/Electronics Command

두 평가항목을 기반으로 소프트웨어 등급은 높음(High), 중간(Medium), 낮음(Low)으로 구분하며, <표 3-18>과 같이 각 등급에 따라 필요한 분석과 테스트 활동의 정도를 규정하고 있다.

<표 3-18> 미국방 - 소프트웨어 등급에 따른 활동

소프트웨어 등급	필요 활동
High	주요 분석활동 및 테스트 활동 수행
Medium	요구사항 및 설계에 대한 높은 수준의 분석, 심층적인 테스트 수행
Low	관리 활동의 검토를 통해 허용되는 높은 수준의 분석 및 테스트 활동

자료: Software system safety guide (CECOM-TR-92-2), US Army Communications/Electronics Command

심각도 유형은 소프트웨어 위험원이 시스템 수준의 위험에 미치는 영향 정도를 기반으로 평가한다. 본 가이드에서 심각도 유형을 구분하기 위한 세부 기준은 제시하고 있지는 않으며, MIL-STD-882B 표준을 참고하고 있다. MIL-STD-882B의 심각도 기준은 다음 <표 3-19>와 같다.

자료 : MIL-STD-882B SYSTEM SAFETY PROGRAM REQUIREMENTS

<표 3-19> 미국방 - MIL-STD-882B 심각도 기준

심각도	기준
Catastrophic (I)	시망 또는 시스템 손실
Critical (II)	심각한 부상 또는 직업병, 주요 시스템 손상
Marginal (III)	경미한 부상 또는 직업병, 경미한 시스템 손상
Negligible (IV)	경미한 부상 또는 직업병 미만, 경미한 시스템 손상 미만

또한, 해당 가이드에서는 <표 3-20>과 같이 제어 유형에 대한 판단 기준을 제시하고 있으며, 다음의 특성들을 고려하고 있다.

- ㅇ 안전 관련된 기능의 수행 여부
- ㅇ 소프트웨어 기능의 구분: 제어 기능 vs. 정보 제공
- ㅇ 기능 수행의 시간 제약: 즉각적으로(실시간으로) 사람/운영자의 대응 가능성 여부
- ㅇ 소프트웨어 기능의 자율성: 기능 완료를 위한 사람/운영자의 개입의 필요성 여부
- ㅇ 독립적인 안전장치의 중복 존재 여부

<표 3-20> 미국방 - 제어 유형에 대한 판단 기준

제어 유형	판단 기준
Autonomous Time Critical	소프트웨어는 잠재적으로 위험한 하드웨어 시스템, 하위 시스템 또는 구성 요소에 대한 자율적 제어를 실행하며, 위험 발생을 방지하기 위한 실시간적인 사람의 개입 가능성이 존재하지 않음. 소프트웨어 오류 또는 이벤트 방지 실패는 직접적인 위험의 발생으로 이어짐. 예) 항공기 자동 착륙 시스템
Autonomous/Not Time Critical	소프트웨어는 잠재적으로 위험한 하드웨어 시스템, 하위 시스템 또는 구성 요소에 대한 제어를 실행하며, 위험을 완화하기 위해 독립적인 안전 시스템 및 사람의 개입이 가능함. 그러나 이러한 시스템 자체는 안전에 적합하지 않은 것으로 간주되며, 이에 대한 시정 조치가 필요할 수 있음 예) 비행 제어 시스템을 뜨르는 자동 지형 시스템
Information / Time Critical	소프트웨어는 위험을 완화하기 위해 즉각적인 운영자의 조치가 필요한 정보를 표출함. 소프트웨어 오류는 위험 발생을 방지하도록 설계되거나 그렇지 않을 수 있음. 예) 미사일 범위 제어 안전 비행 경로 매개변수 등
Operator Control	소프트웨어 아이템은 잠재적으로 위험한 하드웨어 시스템, 하위 시스템 또는 제어 기능을 완료하기 위하여 사람의 조치가 필요한 구성 요소에

	대해 명령을 할당함. 각 위험 이벤트에 대하여 몇 가지 중복적이고 독립된 안전장치가 존재함 예) 전통적인 항공기의 무기 방출 시스템
Information Decision Algorithm	소프트웨어는 안전에 중요한 결정을 내리는데 사용되는 정보를 생성함. 각 위험 이벤트에 대하여 몇 가지 중복적이고 독립된 안전 장치가 존재함
Not Safety Related Software	소프트웨어는 위험한 기능을 제어하지 않음

자료: Software system safety guide (CECOM-TR-92-2), US Army Communications/Electronics Command

나. 시스템 안전 표준 (MIL-STD-882)

MIL-STD-882 표준에서는 시스템 수준에서 위험을 평가하는 기준을 제시하고 있다. 위험은 심각도(severity)와 발생가능성(probability) 측면에서 평가된다. 이 중 심각도에 대한 평가는 인명 피해, 환경에 대한 영향, 금전적 손실을 기준으로 등급을 분류한다.

<표 3-21> 미국 국방 - MIL-STD-882 심각도 분류 기준

심각도 등급	설명	분류 기준
1	Catastrophic	다음 중 하나 이상을 유발 가능: 사망, 영구적 완전 장애, 회복 불가한 중대한 환경 영향 또는 $10M 이상의 금전적 손실
2	Critical	다음 중 하나 이상을 유발 가능: 영구적 부분 장애, 3명 이상의 입원을 유발할 수 있는 직업병이나 상해, 회복 가능한 중대한 환경 영향 또는 $1M ~ $10M의 금전적 손실
3	Marginal	다음 중 하나 이상을 유발 가능: 1일 이상 결근을 유발하는 직업병이나 상해, 회복 가능한 중간정도의 환경 영향 또는 $100K ~ $1M의 금전적 손실
4	Megligible	다음 중 하나 이상을 유발 가능: 결근을 유발하지 않는 직업병이나 상해, 최소한의 환경 영향 또는 $100K 이하의 금전적 손실

자료 : MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY

위험의 발생가능성에 대한 평가는 위험의 발생 확률을 고려하여 수행한다. 표준에서는 정량적인 근거자료가 있을 경우에 이를 우선적으로 사용할 것을 권고하고 있다. 다음 <표 3-22>는 표준에서 제시하고 있는 발생가능성에 대한 분류 기준이다.

<표 3-22> 미국 국방 - MIL-STD-882 발생가능성 분류 기준

발생 가능성	설명	Individual Item	Fleet/Inventory	Quantitative
A	Frequent	Likely to occur often in the life of an item	Continuously experienced	Probability of occurrence greater than or equal to 10^{-1}
B	Probable	Will occur several times in the life of an item	Will occur frequently	Probability of occurrence less than 10^{-1} but greater than or equal to 10^{-2}
C	Occasional	Likely to occur sometime in the life of an item	Will occur several times	Probability of occurrence less than 10^{-2} but greater than or equal to 10^{-3}
D	Remote	Unlikely, but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur	Probability of occurrence less than 10^{-3} but greater than or equal to 10^{-6}
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced in the life of an item	Unlikely to occur, but possible	Probability of occurrence less than 10^{-6}
F	Eliminated	Incapable of occurrence within the life of an item. This category is used when potential hazards are identified and later eliminated		

자료 : MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY

최종적으로 위험에 대한 등급은 위험의 심각도와 발생가능성을 두 축으로 하는 위험 평가 매트릭스를 통해 결정된다.

[그림 3-34] 미국 국방 - MIL-STD-882 위험 평가 매트릭스

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

자료 : MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY

MIL-STD-882 표준에서는 소프트웨어에 대한 위험 평가를 수행할 때 평가항목으로 발생가능성을 적용하기 어려우며, 통계적 자료에 기반한 산정이 어렵다고 언급하고 있다. 이는 소프트웨어의 기능이 어플리케이션에 따라 다르게 적용되고, 이 때문에 소프트웨어의 신뢰성을 산정하는 것이 어렵다고 보고 있다. 이러한 이유로 소프트웨어의 위험에 대한 기여도 평가시 위험 심각도 (severity)와 하드웨어에 대한 제어 정도 (degree of control)를 고려하도록 가이드 하고 있다. 위험 심각도에 대한 평가 기준은 위에서 언급한 시스템 수준의 위험 평가 기준을 준용하도록 하고 있다.

소프트웨어의 제어 정도에 대한 기준은 앞서 살펴본 소프트웨어 시스템 안전 가이드의 기준과 유사하다. 다음은 본 표준에서 소프트웨어 제어 정도를 평가하기 위해 고려하는 소프트웨어 특성이다. 기존 안전 가이드에 비해 안전 관련 정도를 추가적으로 구분(예, safety-cirtical, safety-related, not safety-significant)한 정도가 차이점이라 할 수 있다.

- ㅇ 소프트웨어 기능의 안전 관련 정도: Safety-significant (safety-critical, safety-related), not safety-significant
- ㅇ 소프트웨어 기능의 구분: 제어 기능 vs. 정보 제공
- ㅇ 기능 수행의 시간 제약: 즉각적으로(실시간으로) 사람/운영자의 대응 가능성 여부

ㅇ 소프트웨어의 자율성: 기능이 완료되기 위해 사람/운영자의 개입의 필요성 여부

ㅇ 독립적인 안전장치의 중복 존재 여부

기존 안전 가이드와 큰 차이점은 제어 유형의 의미에 있다. 기존 가이드에서는 소프트웨어 특성에 기반하여 단순히 유형을 분류해 놓은 성격이 강한 반면, 본 표준에서는 소프트웨어 특성이 안전에 미치는 중요도를 고려하여 등급을 구분하였다. 즉, 소프트웨어의 자율성, 독립적인 안전장치의 중복 존재 여부, 안전 관련 정도에 대한 특성을 기반으로 안전에 보다 중요한 영향을 미치는 소프트웨어 기능에 대해 등급 1을 부여하고, 중요도가 낮아짐에 따라 등급 2 ~ 5까지 순차적으로 부여하였다. 이는 소프트웨어 위험에 대한 등급을 결정할 때 기존과는 다른 영향을 미치게 됨을 의미한다. 다음 <표 3-23>은 본 표준에서 제시하고 있는 소프트웨어 제어 유형에 대한 구분 기준이다.

<표 3-23> 미국 국방 - MIL-STD-882 소프트웨어 제어 유형

제어 유형	설명	분류 기준
1	Autonomous	• 잠재적으로 안전에 중요한 하드웨어 시스템, 하위시스템 또는 구성 요소의 재난 및 위험 발생을 방지하기 위해 사전 정의된 안전 감지 및 개입 없이 자율적인 통제 권한을 행사하는 소프트웨어 기능
2	Semi-Autonomous	• 잠재적으로 안전에 중요한 하드웨어 시스템, 하위시스템 또는 구성 요소의 재난 및 위험 발생을 방지하기 위해 사전 정의된 안전 감지 및 개입을 위한 시간을 확보하기 위한 제어 권한을 행사하는 소프트웨어 기능 • 사고 발생 또는 위험을 완화하거나 제어하기 위해 운영자가 조속히 사전 정의된 조치를 취하도록 요구하는 안전 관련 정보를 표시하는 소프트웨어 항목. 소프트웨어 예외, 오류, 결함 또는 지연은 사고 발생 또는 예방을 수행하지 못함
3	Redundant Fault Tolerant	• 안전 기능이 중요한 하드웨어 시스템, 하위 시스템 또는 업무 수행을 위해 지시 기능이 필요한 구성요소에 명령을 지시하는 소프트웨어 기능. 시스템 탐지 및 기능적 반응은 기 정의된 각 위험 상태에 대한 중복적이고 독립적인 내결함성 포함 • 중요한 결정을 내리는 데 필요한 안전에 필수적인 정보를 생성하는 소프트웨어. 이 시스템은 위험한 조건, 탐지 및 디스플레이에 대한 다수의 중복적이고 독립적인 내결함성 메커니즘 포함
4	Influential	• 소프트웨어는 운영자의 결정을 지원하기 위한 안전 관련 정보를 생성하지만, 사고 회피를 위해 운영자의 조치를 요구하지 않음

5	No Safety Impact	• 소프트웨어 기능이 안전에 중요한 하드웨어 시스템, 하위 시스템 또는 구성 요소에 대해 명령 또는 제어 권한이 없으며 안전에 중요한 정보를 제공하지 않음 • 소프트웨어는 안전 관련 또는 시간에 민감한 데이터 또는 제어 기기의 상호 작용에 필요한 정보를 제공하지 않음. 소프트웨어는 안전에 중대한 또는 시간에 민감한 데이터를 전송하거나 해결하지 않음

자료 : MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY

소프트웨어 안전 심각도 매트릭스는 <표 3-24>과 같이 소프트웨어 위험에 대한 심각도 및 제어 유형 평가를 기반으로 소프트웨어 중요도 지수 (소프트웨어CI: Software Criticality Index)를 도출한다.

<표 3-24> 미국 국방 - MIL-STD-882 소프트웨어 제어 유형

소프트웨어 제어 유형	심각도 등급			
	Catastrophic	Critical	Marginal	Negligible
1	소프트웨어CI 1	소프트웨어CI 1	소프트웨어CI 3	소프트웨어CI 4
2	소프트웨어CI 1	소프트웨어CI 2	소프트웨어CI 3	소프트웨어CI 4
3	소프트웨어CI 2	소프트웨어CI 3	소프트웨어CI 4	소프트웨어CI 4
4	소프트웨어CI 3	소프트웨어CI 4	소프트웨어CI 4	소프트웨어CI 4
5	소프트웨어CI 5	소프트웨어CI 5	소프트웨어CI 5	소프트웨어CI 5

자료 : MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY

앞서 언급한 대로 소프트웨어 제어 유형에 대한 의미가 바뀌면서, 소프트웨어 중요도 지수를 결정하는데 제어 유형이 미치는 영향도가 기존 안전 가이드와는 차이가 있다. 기존 안전 가이드에서는 소프트웨어 등급을 결정하는데 제어 유형보다는 심각도가 많은 영향을 미친 반면, 이 표준에서는 제어 유형의 비중이 심각도의 비중과 유사하다. 이런 기준의 변화로 인해 심각도 등급이 높다고 할지라도 제어 유형의 등급이 낮으면 소프트웨어 등급은 낮게 결정되는 것을 볼 수 있다.

소프트웨어 중요도 지수는 위험 등급 및 소프트웨어 활동에 부과되는 요건(LOR: Level of Rigor)과 연결된다.

[그림 3-35] 미국 국방 - MIL-STD-882 소프트웨어 위험 지수 - 위험 등급 관계

RELATIONSHIP BETWEEN SwCI, RISK LEVEL, LOR Tasks, AND RISK		
Software Criticality Index (SwCI)	Risk Level	Software LOR Tasks and Risk Assessment/Acceptance
SwCI 1	High	• If SwCI 1 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as HIGH and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 1 LOR tasks or prepare a formal risk assessment for acceptance of a HIGH risk.
SwCI 2	Serious	• If SwCI 2 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as SERIOUS and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 2 LOR tasks or prepare a formal risk assessment for acceptance of a SERIOUS risk.
SwCI 3	Medium	• If SwCI 3 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as MEDIUM and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 3 LOR tasks or prepare a formal risk assessment for acceptance of a MEDIUM risk.
SwCI 4	Low	• If SwCI 4 LOR tasks are unspecified or incomplete, the contributions to system risk will be documented as LOW and provided to the PM for decision. The PM shall document the decision of whether to expend the resources required to implement SwCI 4 LOR tasks or prepare a formal risk assessment for acceptance of a LOW risk.
SwCI 5	Not Safety	• No safety-specific analyses or testing is required.

자료 : MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY

2. 미국 항공우주 안전

미국 항공우주국(NASA: National Aeronautics and Space Administration)은 NASA 센터, 프로그램, 프로젝트 및 시설에서 사용되는 소프트웨어 안전을 보장하기 위한 요건을 제공하기 위해 NASA 소프트웨어 안전 표준 NASA-STD-8719.13[83]을 제정하였다. NASA 소프트웨어 안전 가이드 NASA-GB-8719.13는 소프트웨어 안전을 구현하기 위한 세부 사항을 제공한다.

NASA 소프트웨어 보증 및 안전 표준인 NASA-STD-8739.8[84]은 소프트웨어 공학 및 품질활동에 대한 요건을 제공하기 위해 제정되었으며, NASA 소프트웨어 안전 표준과의 호환성, IV&V 활동 추가 등을 위해 확장되었다.

또한, 본 연구에서는 NASA의 소프트웨어 안전 등급에 대한 평가 기준을 보다 잘 이해하기 위해, 이와 관련된 초기 연구자료에 대해서도 살펴본다.

83) NASA SOFTWARE SAFETY STANDARD
84) Software Assurance and Software Safety Standard

가. NASA 소프트웨어 안전 관련 연구

NASA에서는 외부전문가와 함께 NASA에서 사용될 위험 평가 체계에 대한 연구를 수행하였다. 본 절에서는 이 연구의 수행 결과[85]에 대해서 설명한다.

이 연구에서는 위험의 평가 항목으로 NASA 프로그램/프로젝트의 실패 확률(probability)/발생가능성(likelihood)과 이에 미치는 영향(impact)/결과(consequence)를 언급하고 있다.

이 중, 발생가능성(likelyhood)에 대해서 정성적인 기준과 확률에 기반한 정량적 기준을 제시하고 있다. 정량적 기준은 각종 도메인의 사고 데이터(예, 운행거리, 사고빈도 등)를 기반으로 해당하는 확률을 도출하였다. <표 3-25>에서는 해당 발생가능성에 대한 평가 기준에 대하여 설명하고 있다.

<표 3-25> NASA 소프트웨어 안전 연구의 발생가능성 평가 기준

Level	Description
Level 1 (Very Low)	- 설명 : 발생 가능성은 운영 기회 당 **0.000001 (10-6) 미만**으로 추정됨 - 예 : 승객의 비행기 탑승 기회 당 치명적인 충돌 - 간략 설명 : 항공 여행은 우리 사회가 매일 참여하는 가장 안전한 활동 중 하나임. 잦은 실패를 용납하지 않는 매우 성숙된 기술들이며, 장애 발생 시 향후 쟁애 발생을 방지하기 위해 광범위한 자원을 투자함
Level 2 (Low)	- 설명 : 가능성은 낮지만 발생할 수 있음. 발생 가능성은 운영 기회 당 **0.000001에서 0.001 (10-6 and 10-3)** 사이로 추정됨 - 예 : 승용차 여행 당 사망자 수 - 간략 설명: 해당 범주는 일반인이 수용할 수 있는 것으로, 사회에서 받아들이는 거의 모든 위험을 나타냄 - Assumptions: 운영 기회를 산출하기 위해 승용차 여행이 평균 약 70마일이라 가정함. 여객 버스 여행은 평균 약 70마일이었음. 이 여행 당 평균 마일은 가상의 목적으로만 사용하였으며, 이 평균값이 합리적이라고 판단하였음. 하지만 해당 운행을 확인하는 객관적인 증거가 존재하지는 않음
Level 3 (Moderate)	- 설명 : 이벤트 수명 중 일정 시간 동안 발생 가능성이 있음. 발생 가능성은 운영 기회 당 **0.001에서 0.01 (10-3 ~ 10-2)**로 추정됨 - 예 : 오토바이 여행 당 사망자 - 간략 설명 : 해당 범주는 우리 사회가 수용 가능한 위험 또는 불가능한 위험에 대해 분리된 것으로 보일 수 있는 사건을 나타냄. 많은 사람들이 해당 활동을 피하기 위해 의식적인 선택을 하는 반면, 어떠한 사람들은 여전히 위험

85) Kelly D. Moses and Roy W. Malone, Development of risk assessment matrix for NASA engineering and safety center, 2004

	을 받아들이고 해당 활동을 수행함.
Level 4 (High)	- 설명 : 수명 중 어느 정도 발생할 것으로 예상됨. 발생 가능성은 운용 기회 당 **0.01에서 0.10 (10-2 ~ 10-1)**으로 추정됨 - 예 : 미국 ELV 출시(1998 ~ 2001) 및 심장 개방 수술 - 간략 설명 : 해당 범주의 사건은 여전히 사회 전체에서 위험한 것으로 간주하고 있음. 인간의 죽음을 수반하는 경우, 개인 또는 건강 관련 문제에 대해 명확하고 의식적으로 선택하는 것은 허용되는 위험임
Level 5 Very High)	- Narrative: 자주 발생할 가능성이 있음. 발생 가능성은 운영 기회 당 **0.10 (10-1)** 보다 클 것으로 추정됨 - 예 : 뇌 수술 중, 또는 그 결과로 인한 사망 - 간략 설명 : 해당 범주의 실제 사례는 일반적으로 세 가지 범주로 구분될 수 있음. 1) Stupid stunts: 사회 전체가 해당 범주에서 사망률이나 부상률을 허용하지 않으며, 우리는 해당 범주를 피하는 방식으로 진화함. Lesser of the Two Evils: 두가지 옵션 중 사용 가능한 옵션이 높은 실패율을 수반하는 경우가 있음. 매우 위험한 수술이 이 범주에 속함. 3) Easily/Cheaply replaceable item or, rarely re-used items : 해당 범주는 특히 새로운 기술 및 낮은 사용율의 부품 및 시스템을 고려하여 추가 조사를 위해 권장됨

자료 : Kelly D. Moses and Roy W. Malone, Development of risk assessment matrix for NASA engineering and safety center, 2004

실패에 미치는 영향(consequence)은 건강과 환경에 미치는 영향, 미션 성공에 대한 영향, 국가적 중요도의 3가지 관점에서 기준을 제시하고 있으며, 해당 관점에서 영향을 분류하는 기준은 <표 3-26>를 통해 확인할 수 있다.

ㅇ 건강과 환경에 대한 영향 (Safety, Health, Environment)

- 생명, 건강, 작업 환경, 자연 환경 등에 미치는 영향

ㅇ 미션 성공에 대한 영향 (Mission Success)

- 주요 미션 목표(MMOs: Major Mission Objectives), 보조 미션 목표(Supplemental Mission Objectives), 하드웨어로 손실로 인한 금전적 손실에 미치는 영향

ㅇ 국가적 중요도 (National Significance)

- 국가 위상(prestige), 가시성(visibility), 대민 관계(public relations)에 미치는 영향

<표 3-26> NASA 소프트웨어 안전 연구의 영향 평가 기준

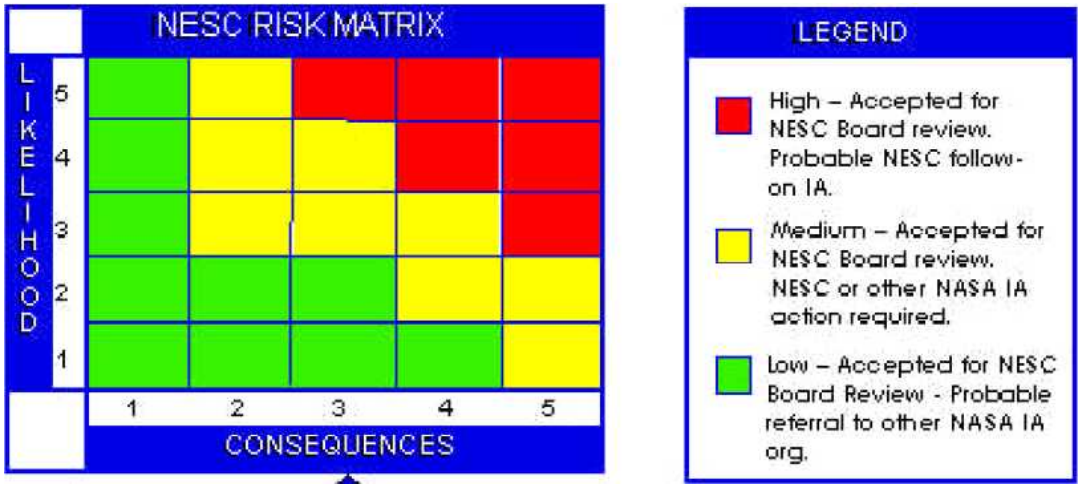
Level	Description		
	Safety, Health, Environment	Mission Success	National Significance

1	- Minimal/no safety or health plan violations - Minimal to no environment impacts	- Hardware loss between 200k and 1 million USD - Failure to any one supplemental objective	Minimal or no identified national prestige or visibility
2	- Could result in injury or illness not resulting in lost work day - Minimal environmental damage	- Hardware loss between 1 M and 10 M USD - Failure to meet > 50% of supplemental objectives	Low national prestige and visibility
3	- Could result in injury or occupational illness resulting in one or more lost work day - Mitigatable environmental damage w/o law violation	- Hardware loss between 10M and 100 M USD - Failure to any one MMO	Moderate national prestige and visibility
4	- Could result in permanent partial disability, injuries or occupational illness - Reversible environmental damage – law violation	- Hardware loss between 100 M and 250 M USD - Failure to meet > 50% MMOs	Significant national prestige and visibility
5	- Could result in death or perm. total disability - Irreversible severe environmental damage that violate law or regulation	- Hardware loss over 250 M USD - Failure to all MMOs	High national prestige and visibility

자료 : Kelly D. Moses and Roy W. Malone, Development of risk assessment matrix for NASA engineering and safety center, 2004

위험 평가는 위에서 소개한 두 개의 평가항목을 축으로 하는 위험 매트릭스를 이용하여 수행된다. 이 연구에서 위험은 높음(High), 중간(Medium), 낮음(Low)의 3 등급으로 분류하고 있다.

[그림 3-36] 미국 항공우주 - NESC 위험 매트릭스



자료 : Kelly D. Moses and Roy W. Malone, Development of risk assessment matrix for NASA engineering and safety center, 2004

나. NASA 소프트웨어 안전 표준 (NASA-STD-8719.13, NASA-STD-8739.8)

NASA 소프트웨어 안전 표준 NASA-STD-8719.13에서는 소프트웨어 안전 중요도 평가를 위한 절차와 기준을 제시하고 있다. 소프트웨어 안전 중요도 평가는 두 단계로 이루어 진다. 첫 번째 단계는 소프트웨어의 안전 중요성(safety-criticality)을 평가하는 단계이다. 이 단계에서 사용하는 방법을 소프트웨어 안전 리트머스 시험(software safety litmus test)라고 한다. 두 번째 단계는 소프트웨어의 위험 등급을 평가하는 소프트웨어 위험 평가(software risk assessment) 단계이다. 실질적인 소프트웨어의 안전 등급은 두 번째 단계에서 결정된다.

ㅇ 단계 1: 소프트웨어 안전 리트머스 시험 (Software Safety Litmus Test)

소프트웨어 안전 리트머스 시험은 시스템 수준의 안전 평가시 소프트웨어의 관여도에 대한 상위 수준의 첫 지표이다. 시스템이 안전에 중요하다고(safety-critical) 판단한 경우, 이 시스템에 포함된 소프트웨어 또한 안전에 중요하다고 가정하고 시작할 수 있다. 실질적으로는 소프트웨어가 안전에 중요한지 여부를 판단하기 위해 다음 <표 3-27>과 같은 체크리스트를 활용한다.

<표 3-27> NASA-STD-8719.13 - 소프트웨어의 안전 중요도 판단 체크리스트

체크리스트
• Causes or contributes to a system hazard/condition/event. • Provides control or mitigation for a system hazards/condition/event . Controls safety critical functions. . Mitigates damage if a hazard/condition/event occurs. . Detects, reports, and/or takes corrective action, if the system reaches a potentially hazardous state. • Processes safety critical commands (including autonomous commanding) • Resides on the same processor as safety critical software and is not logically separated from the safety critical software • Processes data or analyzes trends that lead directly to safety decisions (e.g., determining when to turn power off to a wind tunnel to prevent system destruction) • Provides full or partial verification or validation of safety critical systems, including hardware or software subsystems. (e.g., this can include models and simulations)

자료 : NASA-STD-8719.13, NASA SOFTWARE SAFETY STANDARD

NASA 소프트웨어 보증 및 안전 표준(NASA-STD-8739.8)에서는 시스템 안전에 영향을 미치는 소프트웨어를 식별하기 위해 <표 3-28>과 같이 보다 구체적인 체크리스트를 제공하고 있다. 이는 소프트웨어가 안전을 위협하는 원인(causes)을 제공하는 경우와 안전을 보장하기 위한 제어(control) 기능에 대한 것이다.

<표 3-28> NASA-STD-8739.8 - 소프트웨어의 안전 중요도 판단 체크리스트

체크리스트
• Does software control any of the safety-critical hardware? • Does software perform critical reconfiguration of the system during the mission? • Does the software perform redundancy management for safety-critical hardware? • Does the software determine when to perform a critical action? • Does the software trigger logic to meet failure tolerance requirements? • Does the software monitor hazard inhibits, safety-critical hardware/software, or issue a caution and warning alarm used to perform an operational control? • Does the software process or display data used to make safety-critical decisions? • Does the flight or ground software manipulate hazardous system effectors during prelaunch checkouts or terminal count? • Does the software perform analysis that impacts automatic or manual hazardous operations?

- Does the software serve as an interlock preventing unsafe actions?
- Does the software contain stored command sequences that remove multiple inhibits from a hazard?
- Does the software initiate any stored command sequences, associated with a safety-critical activity?
- Does software violate any hazard inhibits or hardware redundancy independence (channelized communication/power paths, stored command sequences/scripts, FDIR false positive, etc.)?
- Can the software controls introduce new hazard causes?
- Are the software safety-critical controls truly independent?
- Can common cause faults affect the software controls?
- Can any of the software controls used in operational scenarios cause a system hazard?
- Does the software control 소프트웨어itch-over to a backup system if a failure occurs in a primary system?
- Is the software that makes safety-critical decisions fault-tolerant?
- Does the software provide an approach for recovery if the system monitoring functions fail?
- Does the software allow the operators to disable safety-critical controls unintentionally?
- Does the software provide safety-critical cautions and warnings?
- Is the software capable of diagnosing and fixing safety-critical faults that might occur in operations?
- Does the software provide health and status of safety-critical functions?
- Does the software process safety-critical commands (including autonomous commanding)?
- Can software that provides full or partial verification or validation of safety -critical systems generate a hazard if it has a defect, fault, or error?
- Can a defect, fault, or error in the software used to process data or analyze trends lead to safety decisions that cause a system hazard?
- Do software capabilities exist against the potential use cases and planned operations throughout all phases of use, and through transitions between those phases/states?

자료 : NASA-STD-8739.8, Software Assurance and Software Safety Standard

ㅇ 단계 2: 소프트웨어 위험 평가 (Software Risk Assessment)

시스템 위험에 대한 소프트웨어의 관여도를 평가할 때, 소프트웨어 기능에 대해 단독으로 평가하기보다는 시스템 내에서 소프트웨어가 하는 역할에 초점을 맞출 필요가 있다. 소프트웨어 위험 평가는 시스템 안전 분석으로부터 도출된 정보(예, 실패의 발생 가능성, 심각도, 시스템 복잡도, 소프트웨어 크기, 하드웨어/소프트웨어 상충점 등)를 활용해서 수행한다. 소프트웨어 위험 평가는 다음의 세 단계를 거쳐 수행된다.

1) 소프트웨어 안전 리트머트 시험(소프트웨어가 안전에 중요한지(safety-critical) 평가)

2) 소프트웨어 제어 유형(control category) 결정

3) 소프트웨어 위험 등급(software risk index) 결정

소프트웨어 위험 평가의 첫 번째 단계는 평가 대상 소프트웨어를 식별하는 것이다. 소프트웨어 위험 평가는 소프트웨어 안전 리트머스 시험을 통해 안전에 중요하다고 평가된 소프트웨어를 대상으로 한다.

두 번째 단계인 소프트웨어 제어 유형 결정을 위해서 소프트웨어의 다양한 특성이 고려된다. 주요하게 고려되는 소프트웨어 특성은 다음 <표 3-29>와 같다.

<표 3-29> NASA 소프트웨어 제어유형 결정을 위한 주요 특성

소프트웨어 특성	
주요 고려사항	• 안전에 중요한 기능의 제어 여부 및 위험요인 발생에 대한 관여 (degree of control) • 시스템의 복잡도(complexity)와 실패의 발생가능성 (likelihood of failure) • 기능 수행의 시간 제약: 다른 시스템 또는 운영자의 대응 가능성 여부 (time -criticality) • 소프트웨어의 자율성: 기능이 완료되기 위해 운영자의 개입의 필요성 여부 (level of autonomy) • 소프트웨어 기능의 구분: 제어(control) 기능 vs. 정보(safety data) 제공 • 독립적인 안전장치의 중복 존재 여부 (redundant safety measures)
추가 고려사항	• 소프트웨어 안전성 및 성숙도 • 공통 원인 고장 • 입증되지 않은 기술 사용 • 고장 허용 수준 • 재사용된 소프트웨어 보장을 위한 프로세스 • 소프트웨어 엔지니어링 및 소프트웨어 보증 프로세스의 견고성 • 하드웨어 기능을 소프트웨어로 교체하기 위한 평가 프로세스 • 인간과 시스템 간 상호작용 및 해당 상호작용과 관련된 훈련의 정도

자료 : NASA-STD-8719.13, NASA SOFTWARE SAFETY STANDARD

위에서 언급한 특성들이 고려된 소프트웨어 제어 유형 평가 기준은 다음과 같다.

<표 3-30> NASA-STD-8719.13 소프트웨어 제어 유형 평가 기준

Software	Description

Control Category	
IA*	• 소프트웨어가 안전 중요 기능의 부분 또는 전체를 자동 제어하는 경우 • 복잡한 서브시스템을 가지고 있고 병렬 프로세서로 상호작용을 하거나 다중 인터페이스가 있는 복잡한 시스템이 존재하는 경우 • 일부 또는 전체의 안전 중요 기능이 시간에 많은 영향을 받는 경우
IIA & IIB*	• 위험을 감지하고 사용자에게 안전 조치의 필요성을 알리는 경우 • 병렬프로세싱은 없지만, 소수의 인터페이스 및 서브시스템으로 다소 복잡한 시스템을 가지는 경우 • 사용자나 자동화된 시스템이 위험 통제에 필요한 시간 내에 조치를 수행할 수 있는 경우
IIIA & IIIB	• 몇 개의 완화 시스템을 통해 위험을 방지할 수 있는 경우 • 안전 중요 정보를 제공하는 여분의 방식이 있는 경우 • 완화 시스템이 중요한 시간 안에 동작하는 경우
IV	• 위험을 제어하지 않으며 사용자를 위한 안전 중요데이터를 생성하지 않는 경우 • 2~3개의 서브시스템으로 이루어진 단순한 시스템인 경우 • 시간이 중요한 요소가 되지 않는 경우

* A = software control of hazard/condition/event. B = Software generates safety data for the system

자료 : NASA-STD-8719.13, NASA SOFTWARE SAFETY STANDARD

소프트웨어 위험 평가의 마지막 단계는 소프트웨어 위험 등급을 결정하는 것이다. 소프트웨어 위험 등급에 대한 평가는 두 가지 접근방법으로 제시되고 있다. 첫 번째 접근방법은 소프트웨어 제어 유형과 시스템 수준에서 정의된 위험 심각도 유형을 고려한 평가 방법이다. 이에 대한 기준은 다음과 같다.

[그림 3-37] NASA-STD-8719.13 소프트웨어 제어 위험 등급

Software Control Category	Hazard/Condition/Event Category			
	Negligible/Marginal	Moderate	Critical	Catastrophic
IA	3 (Moderate)	2 (Medium)	1 (High)	1 (High)
IIA & IIB	5 (Low)	3 (Moderate)	2 (Medium)	1 (High)
IIIA & IIIB	5 (Low)	5 (Low)	3 (Moderate)	2 (Medium)
IV	5 (Low)	5 (Low)	4 (Marginal)	3 (Moderate)

자료 : NASA-STD-8719.13, NASA SOFTWARE SAFETY STANDARD

소프트웨어 위험 등급은 다음과 같이 정의된다.

- 1 : High Risk, Software controls catastrophic or critical hazards
- 2 : Medium Risk, Software control of catastrophic or critical hazards is reduced, but still significant.
- 3 : Moderate Risk, Software control of moderate hazards
- 4 : Marginal Risk, Software control of moderate to marginal hazards
- 5 : Low Risk, Negligible hazard or little software control

시스템 수준의 심각도 유형을 평가하는 기준은 NESC(NASA Engineering and Safety Center)의 위험 평가 기준을 참고할 수 있다.

[그림 3-38] NESC 위험 평가 기준: 위험 심각도

If the risk scenario occurs, what are the consequences?						
CONSEQUENCES	Level	1	2	3	4	5
	Safety, Health, & Environment	Minimal/no safety or health plan violations; Minimal/no environmental impacts	Could result in injury or illness not resulting in lost work days; Minimal environmental damage	Could result in injury or illness resulting in one or more lost work days; Mitigatable env. damage	Could result in permanent partial disability; Reversible environmental damage	Could result in death or permanent total disability ; Irreversible severe environmental damage
	Mission Success (Crewed & Non-Crewed Missions)	Hardware loss < $100K and/or Failure to meet any one Major Mission Objective (MMO)	Hardware loss $100k -$1M and/or Failure to meet > 10% of MMOs	Hardware loss $1M - $10M and/or Failure to meet > 25% of MMOs	Hardware loss $10M - $50M and/or Failure to meet > 50% MMOs	Hardware loss > $50 M and/or Failure to meet all MMOs

자료 : NESC(NASA Engineering and Safety Center)

이 기준은 앞서 언급한 NASA 소프트웨어 안전 연구를 기반으로 최근의 상황을 반영하여 갱신된 것이다. 기존 기준과의 차이점으로는 국가적 중요도(National Significance) 관점의 내용이 빠졌고, 미션 성공(Mission Success)에 대한 영향 관점에서 비용 기준이 조정된 점이다.

소프트웨어 위험 등급을 결정하기 위한 두 번째 방법은 위에서 정의한 소프트웨어 위험 등급에 추가적으로 위험의 발생가능성을 고려하는 것이다. 이 표준은 소프트웨어 위험의 발생가능성은 시스템 수준에서 평가된 내용을 그대로 상속하는 것으로 가이드하고 있다.

시스템 수준의 발생가능성에 대한 평가 기준은 다음과 같다. NASA 소프트웨어 안전 연구에서 제시한 기존 기준과의 차이점은 정량적 기준을 유인 임무(crewed missions)과 무인 임무(non-crewed missions)으로 구분하여 제시하고 있다. 유인 임무에 대한 정량적 수치는 기존 기준과 동일하다. 정성적인 기준에서도 위험 대응방안에 대한 고려가 포함되어 있다.

위험의 발생가능성을 고려한 소프트웨어 위험 등급은 다음과 같다.

[그림 3-39] 미국 항공우주 - NESC 위험 평가 기준: 발생가능성

How likely is this condition, situation, or risk scenario?					
LIKELIHOOD	Level	Probability	Qualitative Guidance (Crewed and Non-Crewed Missions)	Quantitative Guidance: Crewed Missions	Quantitative Guidance: Non-Crewed Missions
	5	Highly Likely	Likely to occur multiple times. Existing controls have little or no effect.	Estimated probability greater than 0.10 (>10%)	Estimated probability greater than 0.50 (>50%)
	4	Likely	Expected to occur. Existing controls have serious uncertainties or limitations.	Between 0.01 and 0.10 (1% - 10%)	Between 0.25 and 0.50 (25% - 50%)
	3	Moderate	Significant potential to occur. Existing controls have some uncertainties or limitations.	Between 0.001 and 0.01 (0.1% - 1%)	Between 0.05 and 0.25 (5% - 25%)
	2	Unlikely	Unlikely but possible to occur. Existing controls have minor uncertainties or limitations.	Between 0.000001 and 0.001 (0.0001% - 0.1%)	Between 0.01 and 0.05 (1% - 5%)
	1	Highly Unlikely	Not likely to occur. Strong controls are in place.	Less than 0.000001 (< 0.0001%)	Less than 1% (< 1%)

자료 : NESC(NASA Engineering and Safety Center)

[그림 3-40] 미국 항공우주 - NASA-STD-8719.13 소프트웨어 위험 등급

Software Control Risk Index Levels	Likelihood of Occurrence				
	Improbable	Unlikely	Possible	Probable	Likely
SW 1 (High)	4	3	2	1	1
SW 2 (Medium)	5	4	3	2	1
SW 3 (Moderate)	6	5	4	3	2
SW 4 (Marginal)	7	6	5	4	3
SW 5 (Low)	7	7	6	5	4

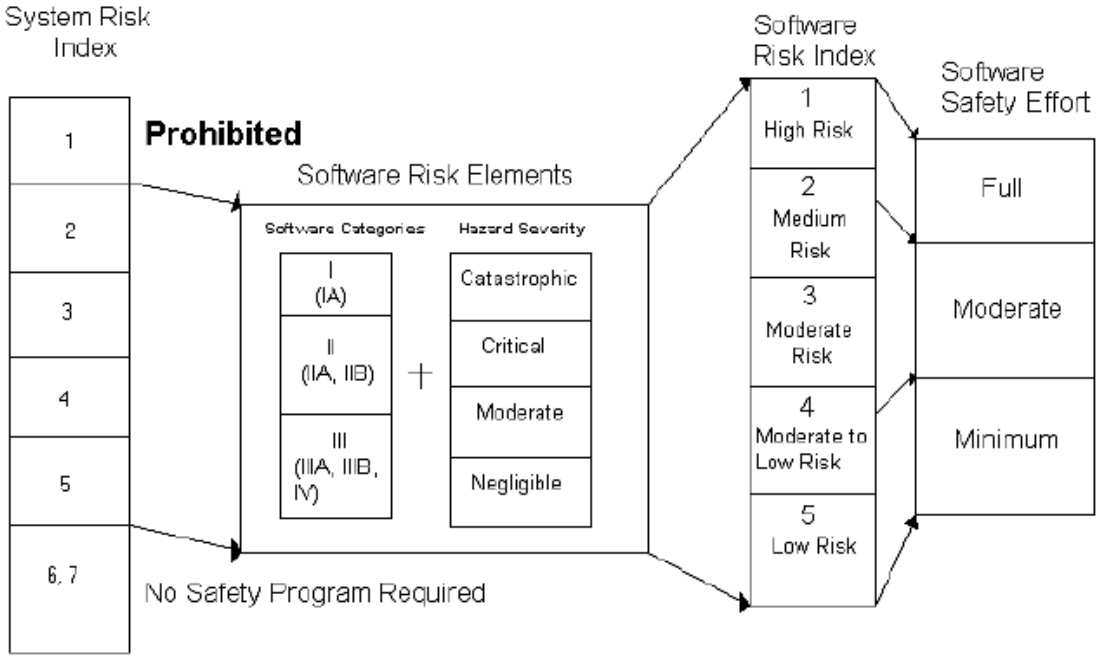
1 = Highest Priority (Highest Software Risk), 7 = Lowest Priority (Lowest Software Risk)

자료 : NASA-STD-8719.13, NASA SOFTWARE SAFETY STANDARD

소프트웨어 위험 등급 결정에 위험 발생가능성의 평가항목을 적용하는 것은 실질적으로 안전 등급을 낮추는 효과가 있다. 그러나 NASA 소프트웨어 안전 가이드에서는 발생가능성을 적용한 소프트웨어 위험 등급에 대해서는 언급하고 있지 않다.

마지막으로 NASA 소프트웨어 안전 가이드에서 시스템 위험 등급과 소프트웨어 위험 등급 간의 관계에 대해서 다음과 같이 정리하고 있다.

[그림 3-41] 미국 항공우주 - NASA-GB-8719.13 시스템-소프트웨어 위험등급 관계



자료 : NASA-STD-8719.13, NASA SOFTWARE SAFETY STANDARD

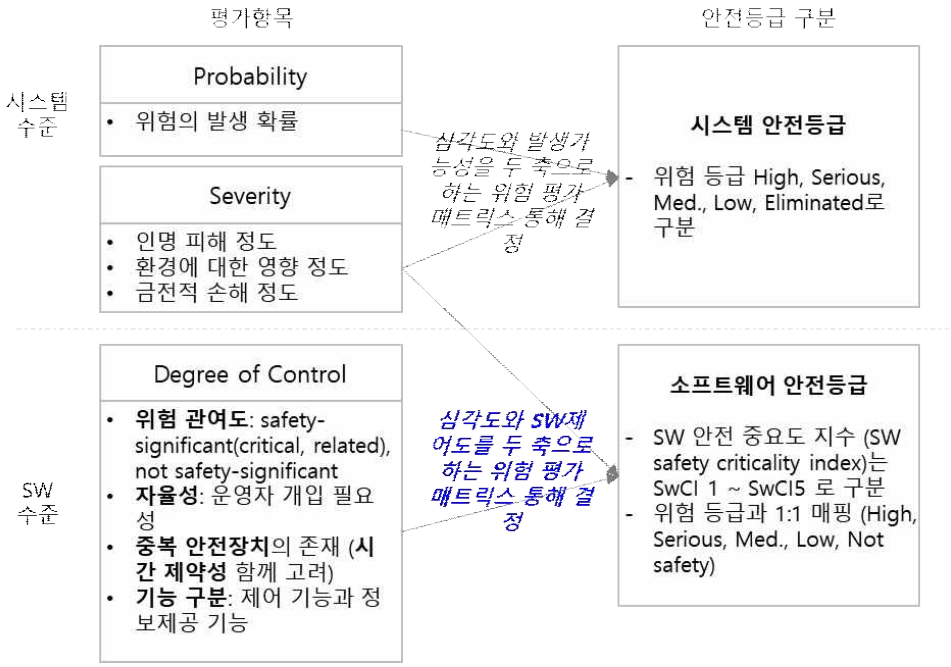
시스템 위험 등급은 소프트웨어 위험 등급 결정에 기본적인 입력으로 사용되며, 소프트웨어 제어 유형에 따라 소프트웨어 위험 등급이 조정된다. 시스템 위험 등급 중 최상위 등급(1)은 허용되지 않기 때문에 제외되고, 최하위 등급(6, 7)은 안전 활동이 필요 없기 때문에 소프트웨어 위험등급 평가 시 고려 대상에서 제외된다.

3. 시사점

가. 미국 국방 분야 안전등급 평가 기준

미국 국방 분야의 안전등급 평가 기준은 다음 [그림 3-37]와 같이 정리될 수 있다. 시스템 수준의 위험 평가항목 중 심각도의 평가 결과를 소프트웨어 수준 위험평가에서 그대로 활용하며, 소프트웨어의 위험 평가항목으로 발생가능성은 적용하기 힘들고 소프트웨어 제어도 적용이 적절하다고 기술하고 있다.

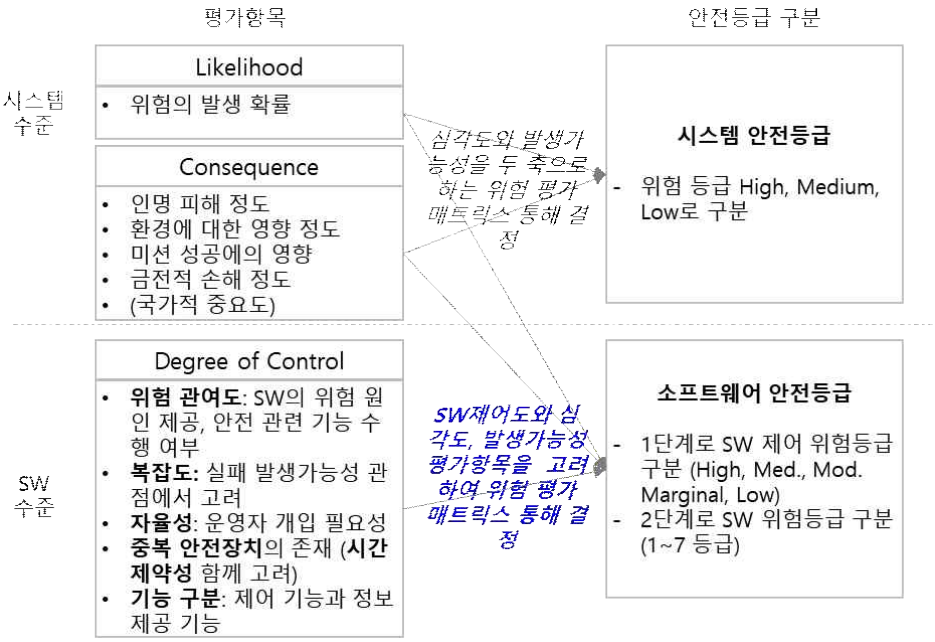
[그림 3-42] 미국 국방 분야 안전등급 평가 기준



나. 미국 항공우주 분야 안전등급 평가 기준

미국 항공우주 분야의 안전등급 평가 기준은 다음 [그림 3-43]과 같이 정리될 수 있다. 시스템 수준의 위험 평가항목 중 심각도와 발생가능성의 평가결과를 소프트웨어 수준 위험평가에 그대로 활용한다. 소프트웨어 안전등급에 대한 평가항목으로 시스템 수준의 심각도 및 발생가능성과 소프트웨어 제어도를 함께 고려한다.

[그림 3-43] 미국 항공우주 분야 안전등급 평가 기준



다. 시스템 수준의 안전등급과의 연관성

미국 국방 분야와 항공우주 분야 모두 시스템 수준의 안전등급이 소프트웨어 안전등급을 결정하는데 기본적인 입력으로 사용된다. 두 분야의 차이점은 국방 분야에서는 시스템 수준의 위험 평가항목 중 심각도(severity)만을 활용하는 반면, 항공우주 분야에서는 심각도와 발생가능성(likelihood)을 모두 활용하는 방안을 제시하고 있다.

하지만 두 분야에서는 다른 도메인의 안전 기준과는 다르게 소프트웨어가 시스템 위험에 관여하는 정도에 대해 구체적인 기준을 제시하여 평가하고 있다. 이와 관련된 평가항목이 소프트웨어 제어 유형이다. 소프트웨어의 안전 등급은 시스템 안전등급을 기반으로 하지만, 소프트웨어 제어 유형에 따라 그 등급을 조정하는 방식을 취하고 있다.

라. 소프트웨어 안전등급 평가항목 및 지표

두 분야의 평가항목은 시스템 수준과 소프트웨어 수준으로 구분할 수 있다.

미국 국방 분야의 시스템 수준 평가항목으로는 심각도(Severity) 항목을 사용하고 있으며, 이에 대한 평가시 인명 피해, 환경에 대한 영향, 금전적 손실 측면에 대해 고려하고 있다. 소프트웨어 수준에서는 소프트웨어가 시스템 위험에 미치는 영향을 평가하

기 위한 지표로 소프트웨어 제어 유형 항목을 사용하고 있다. 소프트웨어 제어 유형을 결정하기 위해 고려하는 특성은 다음과 같다.

- ㅇ 소프트웨어 기능의 안전 관련 정도
- ㅇ 소프트웨어 기능의 구분 (제어 vs. 정보 제공)
- ㅇ 기능 수행의 시간 제약
- ㅇ 소프트웨어의 자율성
- ㅇ 독립적인 안전장치의 중복 존재 여부

미국 항공우주 분야에서 사용하는 시스템 수준 평가항목은 심각도(Severity)와 발생가능성(Likelihood)이다. 이 중 심각도는 건강과 환경에 대한 영향, 미션 성공 및 국가 중요도 등의 측면의 평가를 통해 결정된다(국가적 중요도 측면은 최근 평가기준에서는 제외됨). 발생가능성은 정성적인 기준과 정량적 기준을 제시하고 있다. 정량적 기준은 운행거리, 사고빈도 등의 과거 데이터를 기반으로 단위 운행 당 사고 확률로 정의하고 있다. 최근 기준에서는 유인 임무의 경우와 무인 임무의 경우를 구분하여 발생가능성에 대한 기준을 제시하고 있다.

소프트웨어 수준에서는 국방 분야와 동일하게 소프트웨어 제어 유형 항목을 고려하고 있다. 유형을 분류하는 기준 또한 국방 분야의 기준과 유사하게 제시하고 있다. 추가적으로 고려해야 할 소프트웨어 특성도 언급하고 있으나 상세한 기준을 제시하고 있지는 않다.

- ㅇ 안전에 중요한 기능의 제어 여부 및 위험요인 발생에 대한 관여 (degree of control)
- ㅇ 시스템의 복잡도(complexity)와 실패의 발생가능성 (likelihood of failure)
- ㅇ 기능 수행의 시간 제약 (time-criticality)
- ㅇ 소프트웨어의 자율성 (level of autonomy)
- ㅇ 소프트웨어 기능의 구분 (제어(control) vs. 정보(safety data) 제공)
- ㅇ 독립적인 안전장치의 중복 존재 여부 (redundant safety measures)

마. 소프트웨어 안전등급 결정방법 및 안전등급 구분

미국 국방 분야에서 소프트웨어 안전등급은 위험에 대한 심각도(severity)와 소프트웨

어 제어 유형(software control category)을 두 축으로 하는 소프트웨어 안전 중요도 매트릭스를 이용하여 결정한다. 소프트웨어 안전등급은 소프트웨어CI(Software Criticality Index) 1(가장 높음) ~ 소프트웨어CI 5(가장 낮음)으로 구분된다.

미국 항공우주 분야에서 소프트웨어 안전등급은 두 단계의 매트릭스를 적용하여 결정하고 있다. 먼저 위험에 대한 심각도와 소프트웨어 제어 유형을 두축으로 하는 소프트웨어 제어 위험 매트릭스를 이용하여 소프트웨어 제어 위험 등급을 결정하고, 소프트웨어 제어 위험 등급과 위험의 발생가능성을 두축으로 하는 소프트웨어 위험 매트릭스를 이용하여 최종적인 소프트웨어 위험 등급을 결정한다. 이를 통한 소프트웨어 위험 등급은 1(가장 높음) ~ 7(가장낮음)의 7 단계로 구분된다. 그러나 실제 안전에 대한 요건은 Red(1~2), Orange(3), Yellow(4), Green(5~7)의 4 단계로 구분하여 적용하고 있다.

제8절 각 표준의 안전등급 결정 방법에 대한 비교 분석

본 절에서는 지금까지 조사한 각 표준별 안전등급 결정 방법들에 대하여 비교 분석을 수행하도록 한다. 2절부터 7절까지는 전통적으로 안전을 중요하게 다룬 주요 산업 도메인을 대상으로 소프트웨어 안전등급의 결정방법 및 안전등급 결정 시 고려되어야 하는 평가항목과 지표들에 대하여 조사하였다. 그 결과, 안전등급의 결정방법은 시스템의 안전등급 상속, 시스템 위험 평가요소와 소프트웨어에 특화된 평가요소에 기반한 평가, 위험 심각도에 기반한 소프트웨어의 안전등급 평가와 같이 크게 3가지 유형으로 구분되는 것을 확인할 수 있었다.

다음 <표 3-31>에서는 현재까지 조사한 주요 산업 도메별 안전 기준들의 안전등급 결정 유형이 어떻게 구분되는지 보여주고 있다.

<표 3-31> 주요 산업 도메인 별 안전 기준의 안전등급 결정 유형

주요 산업 도메인	관련 기준	안전등급 결정 유형
2절. 원자력 안전	IAEA SSR-2/1 & SSG-30, IEC 61226, US 10CFR50, IEEE 323, 한국원자로안전규정, 경수로형원전규제기준/지침, APR1400	- 시스템의 안전등급 상속
3절. 철도 안전	IEC 62278(EN 50126),	- 시스템의 안전등급 상속

	IEC 62279(EN 50128)	
4절. 항공 안전	ARP 4761, ARP 4754, DO-178C	- 시스템의 안전등급 상속
5절. 전기용품 안전	KS C IEC 61508, KS C IEC 60730	- 시스템의 안전등급 상속 - 위험 심각도에 기반한 소프트웨어의 안전등급 평가
6절. 의료 안전	IEC 62304, ISO 14971	- 위험 심각도에 기반한 소프트웨어의 안전등급 평가
7절. 미국 국방부 및 항공우주국 안전	MIL-STD-882, Software system safety guide, NASA-STD-8719.13, NASA-GB-8719.13, NESC Risk assessment matrix	- 시스템 위험 평가요소와 소프트웨어에 특화된 평가요소에 기반한 평가

1. 시스템의 안전등급 상속

시스템의 안전등급 상속은 [그림 3-44]에서 보이는 바와 같이, 시스템 수준에서 평가된 안전등급을 관련 소프트웨어가 그대로 상속하여 소프트웨어의 등급을 구분하는 방법이다. 소프트웨어 수준에서 추가적인 요소에 대한 평가를 수행하지 않으며, 등급결정과 관련된 위험원에 대해 소프트웨어가 원인이 될 수 있는지를 판단한다.

원자력 분야, 철도 분야, 항공 분야, 전기용품 분야의 안전 기준에서 해당 안전등급 결정 유형을 활용하여 소프트웨어의 안전등급을 결정하고 있다.

원자력 안전을 제외하고, 철도 및 항공, 전기안전 안전 분야(IEC 61508)에서는 안전등급의 평가는 시스템 수준에서 수행되고, 소프트웨어는 시스템의 안전등급을 상속받도록 정의하고 있었다. 원자력 안전에서는 시스템 수준의 안전등급이 소프트웨어 안전등급을 결정하는데 제약조건의 성격으로 사용됨을 확인할 수 있었다.

이외, 해당 안전등급 결정 유형은 다음과 같은 공통적인 특정을 갖는다.

- ㅇ 시스템 안전등급의 평가항목으로 심각도(severity)가 고려됨
- ㅇ 발생빈도 및 확률은 각 표준마다 고려하는 관점이 상이함
- ㅇ 시스템 실패 조건이 복수 개의 하위 기능/시스템의 결함 조합에 의한 경우, 소프트웨어의 안전등급을 조정할 수 있음

2. 시스템 위험 평가요소와 소프트웨어에 특화된 평가요소에 기반한 평가

시스템 위험 평가요소와 소프트웨어에 특화된 평가요소에 기반한 평가 방법은 시스템 위험의 평가결과를 기반으로 소프트웨어에 특화된 평가요소를 추가로 고려하여, 소프트웨어 맞는 별도의 안전등급을 부여하는 방법이다. 시스템 위험에 대한 심각도(Severity) 평가와 소프트웨어가 해당 심각도에 관여하는 정도(Software Control Category)를 평가하여 소프트웨어를 분류한다. [그림 3-44], [그림 3-45]에서 소프트웨어가 해당 심각도에 관여하는 정도와 이를 기반으로 한 소프트에어 분류를 확인할 수 있다.

[그림 3-44] 소프트웨어의 관여도(Software Control Category)

SW Control Category		Description
1	Autonomous	Software functionality that exercises autonomous control authority over potentially safety-significant hardware systems, subsystems, or components without the possibility of predetermined safe detection and intervention by a control entity to preclude the occurrence of a mishap or hazard.
2	Semi-autonomous	Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems, or components, allowing time for predetermined safe detection and intervention by independent safety mechanisms to mitigate or control the mishap or hazard. Software item that displays safety-significant information requiring immediate operator entity to execute a predetermined action for mitigation or control over a mishap or hazard. Software exception, failure, fault, or delay will allow, or fail to prevent, mishap occurrence.
3	Redundant fault tolerant	Software functionality that issues commands over safety-significant hardware systems, subsystems, or components requiring a control entity to complete the command function. The system detection and functional reaction includes redundant, independent fault tolerant mechanisms for each defined hazardous condition Software that generates information of a safety-critical nature used to make critical decisions. The system includes several redundant, independent fault tolerant mechanisms for each hazardous condition, detection and display.
4	Influential	Software generates information of a safety-related nature used to make decisions by the operator, but does not require operator action to avoid a mishap
5	No safety impact	Software functionality that does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Software does not provide safety-significant or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of safety-significant or time sensitive data

자료 : MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY

[그림 3-45] MIL-STD-882E의 소프트웨어 분류

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

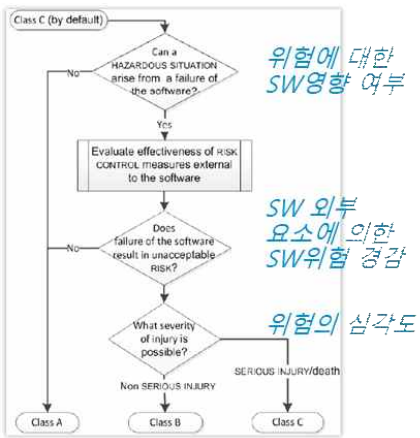
자료 : MIL-STD-882E, DEPARTMENT OF DEFENSE STANDARD PRACTICE: SYSTEM SAFETY

시스템 수준의 위험 평가항목 중 ‘심각도’의 평가 결과를 소프트웨어 수준 위험평가에서 그대로 활용하는 것을 확인할 수 있었다. 미국 항공우주 안전 기준에서는 ‘발생가능성’의 평가 결과도 포함된다. 또한 해당 안전등급 결정 유형에서는 모든 표준이 ‘심각도’와 ‘소프트웨어가 해당 심각도에 관여하는 정도’의 조합으로 소프트웨어 안전등급을 도출하는 것을 확인할 수 있다.

3. 위험 심각도에 기반한 소프트웨어의 안전등급 평가

위험 심각도에 기반한 소프트웨어의 안전등급 평가는 소프트웨어로 인해 발생가능한 위험의 심각도에 따라 안전등급을 결정하는 방법이다. 시스템 수준의 위험평가에 대한 고려 없이 소프트웨어 수준에서 평가가 가능하다. [그림 3-46] 과 같이 의료안전 표준 IEC 62304 및 자동전자제어장치 관련 표준 IEC 60730[86]에서 해당 접근 방법과 유사한 안전등급 결정방법이 적용되었으며, 필요에 따라 소프트웨어 외부요소에 의한 위험 감소도 고려하여 소프트웨어 안전등급을 구분한다.

[그림 3-46] IEC 62304 및 IEC 60730의 소프트웨어 분류 기준



등급	정의
A	Control functions, which are not intended to be relied upon for the safety of the equipment. Examples are: room thermostats, humidity controls, lighting controls, timers, and switches
B	Control functions, which are intended to prevent unsafe operation of the controlled equipment. Examples are: thermal cut-offs and door locks for laundry equipment
C	Control functions, which are intended to prevent special hazards (e.g., explosion of the controlled equipment). Examples are: automatic burner controls and thermal cut-outs for closed, un-vented water heater systems

자료 : IEC 62304, Medical device software — Software life cycle processes
자료 : IEC 60730, Safety Standard for Household Appliances

해당 안전등급 결정 유형에서는, 시스템 수준의 안전분석 또는 안전등급 결정 체계에 대한 별도의 언급 없이 소프트웨어 안전등급 결정을 위한 기준을 제시하고 있다. 또한, 소프트웨어 안전등급에 대한 평가항목으로 ‘심각도’ 및 ‘위험 관여도’, ‘중복된 외부 안전장치’를 고려하고 있음을 확인할 수 있었다.

86) Safety Standard for Household Appliances

제4장 공공기관 시스템의 종류 및 등급제 조사

제1절 조사 방향

본 장에서는 공공기관 시스템의 종류와 기존에 적용되고 있는 다양한 국내외 등급제에 대해 조사한다. 먼저, 공공기관 시스템에 적용되는 안전 기준의 특성을 도출하기 위하여 관련 제도 및 기준을 조사하고, 안전이 중요한 공공기관 시스템에 대하여 조사하도록 한다.

조사 내용은 크게 공공기관 시스템에 적용된 소프트웨어 관련 등급 결정방법, 공공기관 시스템에 적용된 소프트웨어 등급 결정을 위한 평가항목 및 지표, 안전이 중요한 공공기관 시스템 및 이에 대한 분류로 구성되며, 조사 대상은 다음과 같다.

ㅇ 공공기관 시스템에 적용된 소프트웨어 관련 제도/기준

- 국가기반시설 관리 체계(재난안전관리)
- 공공기관/자치단체 정보시스템 관리 체계
- 정보보호시스템 평가/인증 제도(국내)
- 공공 정보/정보시스템 보안 등급 기준(미국)

ㅇ 안전이 중요한 공공기관 시스템

- 공공 정보시스템 분류 기준(국내, 미국)
- 기반시설 분류 기준(국가기반시설, 국가중요시설, 정보통신기반시설, 사회기반시설)

제2절 공공기관 시스템에 적용된 소프트웨어 관련 제도/기준

1. 국가기반시설 관리 체계

가. 관련 법제도

재난 및 안전관리 기본법은 각종 재난으로부터 국토를 보존하고 국민의 생명 · 신체 및 재산을 보호하기 위하여 재난 및 안전관리체제 확립, 재난의 예방 · 대비 · 대응 · 복구와 안전문화활동, 그 밖에 재난 및 안전관리에 필요한 사항을 규정하고 있다. 이 법에서는 재난 예방을 위한 방안 중 하나로 국가핵심기반시설을 지정하고 이에 대한 보호계획을 수립하여 관리하도록 하고 있다.

국가기반체계 보호계획 수립지침은 재난 및 안전관리 기본법에 의거하여 국가기반시설에 대한 보호계획을 작성하는 기준을 제시하고 있다. 이 지침에서 보호계획은 국가기반시설에 발생가능한 위험에 기반하여 수립된다. 이를 위해 국가기반시설의 위험을 분석하고, 관리 우선순위를 지정하기 위해 위험등급을 산정한다. 본 장에서는 국가기반체계 보호계획 수립지침과 이를 기반으로 해양수산부에서 수립한 국가기반시설 보호 계획(2018)에서 제시하고 있는 위험등급 평가 기준에 대해 살펴 본다.

나. 국가기반체계 보호계획 수립지침의 위험도 등급 평가 기준

국가기반체계 보호계획 수립지침에서 위험도 등급은 위험성과 영향력의 2개 항목에 대한 평가를 기반으로 이루어 진다. 각 항목에 대한 평가 기준과 위험도 등급 부여 기준은 다음과 같다.

ㅇ 위험성 평가 기준

- 식별된 위험에 대해 ‘발생가능성’ 등급과 ‘피해 규모’ 등급을 산정하고 이 둘을 곱하여 산출함

위험성 = 발생가능성 등급 X 피해 규모 등급

<표 4-1> 발생가능성 등급 판단 기준표

등급	발생 확률	판단 기준
5	매우 높음	1일 1회 정도 발생할 가능성
4	높음	1개월 1회 정도 발생할 가능성
3	보통	1년 1회 정도 발생할 가능성
2	낮음	3년 1회 정도 발생할 가능성
1	매우 낮음	10년 1회 정도 발생할 가능성

자료 : 국민안전처 재난관리실(2016.12), 2017 국가기반체계 보호계획 수립지침

<표 4-2> 피해 규모 등급 판단 기준표

등급	피해 규모	판단기준
5	매우 높음	즉시 교체 필요
4	높음	교체 필요
3	보통	즉시 보수·보강 필요
2	낮음	보수·보강 필요
1	매우 낮음	보수·보강 불필요

자료 : 국민안전처 재난관리실(2016.12), 2017 국가기반체계 보호계획 수립지침

○ 영향력 평가 기준

- 식별된 위험으로 인한 영향요인 별 피해 등급과 가중치를 가중 합산하여 산출함

영향력 = ∑(영향요인 별 가중치 x 피해등급)

- 영향 요인으로는 인적, 경제적, 사회적 요인이 고려됨

. 인적피해 : 기관내에서의 인명피해 및 주변지역의 인명피해 파급까지 고려

. 경제적피해 : 기관내의 재무적 손실을 기준으로 판단 함

. 사회적피해 : 기관내에서 발생할 경우 사회적으로 미치는 영향을 고려

<표 4-3> 영향요인 별 가중치

영향요인	가중치
인적 피해	0.5

경제적 피해	0.3
사회적 피해	0.2

자료 : 국민안전처 재난관리실(2016.12), 2017 국가기반체계 보호계획 수립지침

<표 4-4> 영향요인 별 피해등급 판단기준표 (예시)

등급	심각도	판단 기준	
5	매우 높음	인적 피해	사망 발생
		경제적 피해	10억 이상 손실
		사회적 피해	광역 단위 사회적 불안·불편, 심리적 피해 등 발생
4	높음	인적 피해	전치 4주 이상
		경제적 피해	1000만원 이상, 10억 미만
		사회적 피해	도시 내 사회적 불안·불편, 심리적 피해 등 발생
3	보통	인적 피해	전치 2주 이상, 4주 미만
		경제적 피해	1000만원 미만
		사회적 피해	구(區)·소도시 단위 사회적 불안·불편, 심리적 피해 등 발생
2	낮음	인적 피해	경미한 상해
		경제적 피해	경미한 손실
		사회적 피해	동(洞)·마을 단위 사회적 불안·불편, 심리적 피해 등 발생
1	매우 낮음	인적 피해	상해 없음
		경제적 피해	피해 없음
		사회적 피해	개인 단위 사회적 불안·불편, 심리적 피해 등 발생

자료 : 국민안전처 재난관리실(2016.12), 2017 국가기반체계 보호계획 수립지침

○ 위험도 판정 기준

- 위험성 등급과 영향력 등급을 두 축으로 하는 매트릭스를 이용하여 높음, 보통, 낮음 등급으로 구분함

<표 4-5> 위험도 판정 기준표

영향력 / 위험성	매우 높음 (4.1~5.0)	높 음 (3.1~4.0)	보 통 (2.1~3.0)	낮 음 (1.1~2.0)	아주 낮음 (1.0 이하)
매우 높음 (21~25)	높음	높음	보통	낮음	낮음
높 음 (16~20)	높음	높음	보통	낮음	낮음
보 통 (11~15)	높음	높음	보통	낮음	낮음
낮 음 (6~10)	높음	보통	보통	낮음	낮음
아주 낮음 (1~5)	높음	보통	낮음	낮음	낮음

자료 : 국민안전처 재난관리실(2016.12), 2017 국가기반체계 보호계획 수립지침

다. 해양수산부 국국가기반시설 보호 계획(2018)의 위험도 등급 평가 기준

본 계획은 국가기반체계 보호계획 수립지침을 기반으로 해양수산수 기반시설 특성에 맞도록 조정된 기준을 제시하고 있다.

○ 발생가능성 평가 기준

- 위험의 발생 빈도를 기준으로 등급을 결정함

<표 4-6> 발생가능성 등급 판단 기준표

등급	발생 확률	판단 기준
4	매우높음	빈번하게 연속적으로 발생 / 1일 1회 정도 발생
3	높음	종종 발생 / 1개월 1회 정도 발생
2	낮음	가끔씩 발생 / 1년 1회 정도 발생
1	매우 낮음	거의 발생하지 않음 / 10 년 1회 정도 발생

자료 : 해양수산부(2018.2), 2018 국가기반시설 보호 계획

○ 피해규모 평가 기준

위험의 영향력에 대해 시설/시스템 피해, 인적 피해, 경제적 피해, 사회적 피해 (사회적 불안/불편, 심리적 피해 등) 관점에서 기준을 제시함

<표 4-7> 피해규모 등급 판단 기준표

등급	피해 규모	판단기준
4	매우높음	즉시 교체 필요 / 사망발생 / 10억 이상의 경제적 피해/ 광역 단위 사회적 불안·불편, 심리적 피해 등 발생 / 50%이상 및 일주일 이상의 국가기반시설 기능 장애 야기
3	높음	교체 필요 / 전치 4주 이상 상해 발생 / 1000만원 이상 10억 미만의 경제적 피해 / 도시 내 사회적 불안·불편, 심리적 피해 등 발생 / 30%이상 및 하루 이상의 국가기반시설 기능 장애 야기
2	낮음	즉시 보수·보강 필요 / 전치 2주 이상, 4주 미만 상해 발생/ 1000만원 미만의 경제적 피해/ 구(區)·소도시 단위 사회적 불안·불편, 심리적 피해 등 발생 / 10%이상 및 1시간 이상의 국가기반시설 기능 장애 야기
1	매우 낮음	보수·보강 필요 / 경미한 상해 발생 / 경미한 경제적 피해 / 동(洞)·마을 단위 사회적 불안·불편, 심리적 피해 등 발생 / 5% 이하 및 1시간 미만의 국가기반시설 기능 장애 야기

자료 : 해양수산부(2018.2), 2018 국가기반시설 보호 계획

○ 위험도 평가 기준

위험도는 ‘발생가능성 등급’과 ‘피해규모 등급’ 산출 후, ‘위험도 판정 기준표’를 적용하여 위험도를 4단계로 구분하여 판정함

<표 4-8> 피해규모 등급 판단 기준표

발생가능성 / 피해규모	4. 매우높음 (자주 발생)	3. 높음 (종종 발생)	2. 낮음 (가끔 발생)	1. 매우낮음 (거의 없음)
4. 매우높음 (치명적 위험)	1등급	1등급	2등급	3등급
3. 높음 (중대한 위험)	1등급	2등급	3등급	4등급
2. 낮음 (상당한 위험)	2등급	3등급	4등급	5등급
1. 매우낮음	3등급	4등급	5등급	5등급

(낮은 위험)				

자료 : 해양수산부(2018.2), 2018 국가기반시설 보호 계획

<표 4-9> 위험도 평가 예시

시설 (세분화 2단계)	세부시설 (세분화 3단계)	주요 위험요인	발생 가능성	피해 규모	위험도 등급
정보시스템	항만운영시스템	지진으로 인한 IT시스템 마비	1	4	3등급
부두시설 등	부두시설	풍수해 등에 따른 시설피해	2	3	3등급
	하역시설	풍수해 등에 따른 시설피해	2	3	3등급
업무장비	하역장비	풍수해 등에 따른 시설피해	2	2	4등급
	예선	풍수해 등에 따른 시설피해	2	2	4등급
유틸리티 설비	비상발전기	풍수해 등에 따른 시설피해	2	2	4등급

자료 : 해양수산부(2018.2), 2018 국가기반시설 보호 계획

라. 시사점

위에서 살펴 본 위험도 등급 평가기준의 특징은 다음과 같이 요약할 수 있다.

- ㅇ 산업 안전 표준과 달리 시스템 외부요인(예, 자연재해)으로 인한 위험에 대해서도 고려함
- ㅇ 위험 평가 수준(시스템 vs. 소프트웨어)에 대한 구분 없음
- ㅇ 산업 안전표준과 유사하게 평가항목으로 ‘발생가능성’과 ‘피해규모/영향력 ' 을 고려함
- ㅇ 공공 분야의 특성으로 인해 ‘사회적 피해 ' 측면의 평가항목을 고려함

2. 공공기관/자치단체 정보시스템 관리 체계

가. 관련 법제도

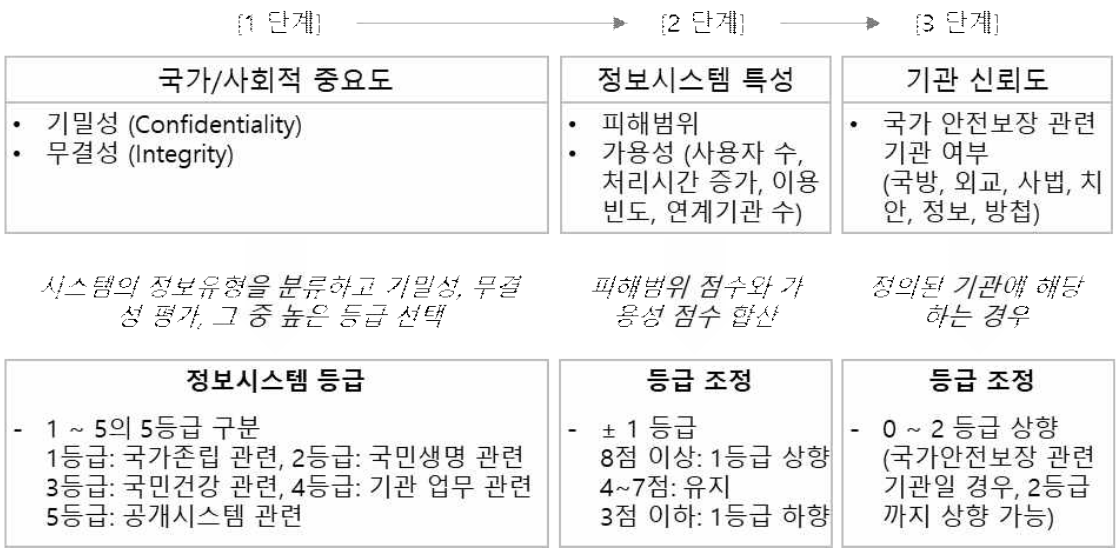
전자정부법은 행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정하고 있는 법이다. 전자정부법은 정보시스템에 대한 관리 기준도 제시하고 있다. 전자정부법 56조는 정보통신망과 행정정보 등에 대한 보안대책 마련을, 56조의 2는 정보시스템의 장애 예방 및 대응을 위한 방안 마련을 요구하고 있다.

행정기관 및 공공기관 정보시스템 구축운영지침 제48조의2는 정보시스템의 장애관리, 행정정보 관리, 보안관리 등을 위해 중요도, 가용성 등을 고려하여 등급을 분류하라고 기술하고 있다. 자치단체 정보시스템 장애 예방 및 대응 지침은 정보시스템의 등급 결정을 위한 절차 및 기준을 제시하고 있다. 또한, 2019년에 행정안전부의 보도 자료[87]를 통해 등급 결정 기준에 대해 추가 설명을 하고 있다.

나. 정보시스템 등급 평가 기준

해당 자료에서는, 정보시스템에 대한 등급산정을 [그림 4-1]과 같이 3단계로 제시하고 있다.

[그림 4-1] 행정기관/공공기관 정보시스템 등급산정 절차



자료 : 행정자치부 예규 제 90호, 2017.6.9., 자치단체 정보시스템 장애 예방 및 대응 지침

87) 행안부, ‘정보시스템 등급별 보안관리’ 제도 확산 나선다 (2019.6.27.)

○ 정보시스템 등급산정 단계

- 1 단계: 정보시스템에 대한 장애·피해 발생 시, 예상되는 위험 수준을 국가·사회적 중요도(세부 평가항목 – 기밀성, 무결성)를 평가하여 1~5등급을 기본 등급을 결정한다.
- 2단계: 정보시스템에 대한 장애·피해 발생시, 발생되는 피해범위와 정보시스템의 특성(사용자수, 처리시간, 이용빈도, 연계기관 수)을 분류하여 1단계에서 결정된 등급을 조정한다.
- 3단계: 국가 안전보장과 관련된 기관(국방, 외교, 사법, 치안, 정보, 방첩)에서 운영하는 시스템의 경우, 등급을 상향 조정할 수 있다.

또한, 등급산정에 대한 평가항목 및 기준으로 중요도(기밀성/무결성), 정보시스템 특성(피해범위 및 가용성), 기관에 대한 신뢰도로 구성하고 있다. 각 항목에 대한 세부 내용은 다음과 같다.

○ 중요도 (기밀성/무결성): 정보기술아키텍처(EA) 서비스분류체계(SRM)를 기준으로 정보시스템의 국가 · 사회적 중요도를 5등급 평가 (서비스 또는 정보 유형에 따라 사전 정의된 기밀성, 무결성 등급 부여)

- 공개가능 정보인 경우 기밀성은 5등급, 무결성은 4등급(국민불편 시) 또는 5등급(영향이 미미할 경우) 하향
- 개인정보를 포함하는 경우, 기밀성을 3등급으로 상향(정보중요도 등급이 4등급 또는 5등급인 경우에 한함)
- 기밀성, 무결성 기준이 다른 경우에는 높은 등급 선택, 동일한 정보시스템이 여러 개 분류체계에 해당되는 경우 분류체계의 등급 중 가장 높은 등급을 선택

○ 정보시스템 특성: 피해범위

<표 4-10> 행정기관/공공기관 정보시스템 등급 평가항목 – 피해범위

배점	구분	설명
5	심각한 문제발생	• 기관업무의 심각한 문제나 영향 발생할 수 있는 경우 • 전 국민 생명의 위험이 발생할 수 있는 경우 • 전 국가 차원의 안보/치안의 위험이 발생할 수 있는 경우

		• 국가경제의 심각한 손실이 발생할 수 있는 경우 • 국민생활(경제·사회활동)의 심각한 장애가 발생 할 수 있는 경우
4	중대한 문제발생	• 기관업무의 중요한 문제나 영향이 발생할 수 있는 경우 • 특정 국민의 생명이 위험할 수 있는 경우 • 지역 차원의 안보/치안의 지장이 발생할 수 있는 경우 • 국가경제의 중요한 손실이 발생할 수 있는 경우 • 국민생활(경제·사회활동)의 중요한 장애가 발생할 수 있는 경우 • 해당 기관에 법적 책임 발생할 수 있는 경우
3	경제적손실 또는 처리오류 발생	• 기관업무 수행에 문제가 발생할 수 있는 경우 • 개인 및 소규모 지역 단위의 국민생명에 대한 위험이 발생할 수 있는 경우 • 소규모 지역 안보 및 치안의 지장이 발생할 수 있는 경우 • 국가경제의 손실이 발생할 수 있는 경우 • 국민생활(경제·사회활동)의 장애가 발생할 수 있는 경우 • 대국민 서비스 지연 및 민원이 발생할 수 있는 경우
2	처리불편 또는 지연	• 기관업무 수행의 지연이 발생할 수 있는 경우 • 국민건강 증진의 지장이 발생할 수 있는 경우 • 안보 및 치안의 경미한 지장이 발생할 수 있는 경우 • 국가경제의 소규모 손실이 발생할 수 있는 경우 • 국민생활(경제·사회활동)의 불편이 발생할 수 있는 경우 • 내부업무 지연이 발생할 수 있는 경우
1	경미한 불편	• 해당 시스템이 없더라도 대국민 서비스나 내부업무 처리가 가능한 경우 • 국가안보, 사회질서 유지, 국가 경제이익, 국민생명과 관련이 없거나 경미한 경우

자료 : 행정자치부 예규 제 90호, 2017.6.9., 자치단체 정보시스템 장애 예방 및 대응 지침

○ 정보시스템 특성: 가용성

<표 4-11> 행정기관/공공기관 정보시스템 등급 평가항목 - 가용성

일평균 사용자 수(5점)	**행정**	전체 5% 이하	전체 25% 이하	전체 50% 이하	전체 75% 이하	전체 75% 초과
	대민	1백명 이하	1천명 이하	1만명 이하	10만명 이하	10만명 초과
처리시간 증가(5점)		없음	50% 증가	100% 증가	200% 증가	300% 증가
이용 빈도(5점)		매년	분기별	매달	매주	매일

연계 기관 수(5점)	없음	2개 이하	5개 이하	10개 이하	10개 초과

자료 : 행정자치부 예규 제 90호, 2017.6.9., 자치단체 정보시스템 장애 예방 및 대응 지침

○ 기관 신뢰도: 국가 안전보장과 관련되는 국방, 외교, 치안, 사법, 정보, 방첩 관련 기관 등은 2등급까지 상향조정(-2등급) 가능

[그림 4-2] 행정기관/공공기관 정보시스템 중요도 평가기준 (예시)

번호	대분류	소분류	분류체계 설명	등급기준	
			등급상향 기준 설명	C	I
1	주민생활	주민정보	주민과 관련된 정보(호적, 등본, 제증명) 관리 및 각종 요청서류 제공 서비스를 위한 정보	3	2
2		생활정보	주민의 생활과 관련된 편의정보 및 공공시설 정보를 제공하는 서비스를 위한 정보	5	4
3		가계금융	가계 재정의 안정을 지원하기 위하여 제공되는 대출 보증 및 직접대출 서비스	3	2
4		가계생활안정	가계생활의 안정을 위한 비금융(보육지원, 위탁 교육, 관련 시설 운영) 형태의 지원 서비스	3	3
5		선거·투표	국민이 선거 및 투표 활동을 수행하기 위해 국가가 지원하는 서비스	3	3
			✔ 선거의 투·개표 결과정보 등 위·변조 시 국정운영에 심각한 피해가 예상되는 경우 무결성 2등급	-	2
6		인권보호	국민이 권리를 행사하고 보호받기 위해 국가가 지원하는 서비스	3	3
			✔ 인권보호 정보의 유출시 국민의 권리행사보호에 피해 예상 시 기밀성 2등급	2	-
7	환경	주거환경개선	쾌적한 주거환경을 위해 제공되는 주거환경시설 개선, 생활편의시설 건설 등에 해당하는 서비스	5	4
8		주거환경정화	쾌적한 주거환경 조성을 위해 각종 쓰레기 및 폐기물 처리 등에 해당하는 서비스	5	4
9		환경보전	자연환경을 보호하는 목적으로 환경파괴 행위 감시 및 환경보호 활동 지원 등의 서비스를 위한 정보	5	4
10		환경오염	환경오염과 관련된 직간접적인 행위 및 환경오염 물질 관리 등의 서비스를 위한 정보	5	3
11		기상관측	항공, 해상, 육상에 관련된 기상정보를 관측·예측 및 수집, 관리하기 위한 기초데이터 서비스	5	2
12		기상예보	기상에 따른 재난·재해 사전예방을 위한 기상 예측 및 예보 서비스	5	2
13		기후예측	기후의 변화에 대한 사전 대응을 효과적으로 수행하기 위한 기후예측 서비스	5	2
14	국가인프라	상수도	안정적이고 깨끗한 상수 생산 및 공급을 위하여 제공되는 서비스	3	2
15		하수도	안정적인 쾌적한 하수 처리를 위하여 제공되는 서비스를 위해 처리하는 정보	3	2
16		전기에너지	전기에너지의 안정적인 생산과 공급을 지원하기 위한 서비스	2	2
			✔ 에너지 관련 정보 중 원자력(핵)에너지와 연관되어 유출 시 치명적인 피해가 예상되는 경우 기밀성 1등급	1	-
17		가스에너지	가스에너지의 안정적인 유통과 공급을 지원하기 위한 서비스	2	2
			✔ 에너지 관련 정보 중 원자력(핵)에너지와 연관되어 유출 시 치명적인 피해가 예상되는 경우 기밀성 1등급	1	-
18		석유에너지	석유에너지의 안정적인 유통과 공급을 지원하기 위한 서비스	2	2
			✔ 에너지 관련 정보 중 원자력(핵)에너지와 연관되어 유출 시 치명적인 피해가 예상되는 경우 기밀성 1등급	1	-
19		석탄에너지	석탄에너지의 안정적인 생산·유통 ·공급을 지원하기 위한 서비스	2	2
			✔ 에너지 관련 정보 중 원자력(핵)에너지와 연관되어 유출 시 치명적인 피해가 예상되는 경우 기밀성 1등급	1	-
20		도로교통	도로교통 및 관련 시설유지관리 등의 활동 및 정보제공을 위한 서비스	4	3
			✔ 비상지 동원물품 관리와 연관된 정보의 유출 시 국가안보에 심각한 피해 예상 시 기밀성 2등급	2	-
21		해상교통	해상교통과 관련된 시설(항만)의 유지관리 및 선박운행정보 등의 제공 서비스를	4	3

자료 : 행정자치부 예규 제 90호, 2017.6.9., 자치단체 정보시스템 장애 예방 및 대응 지침

다. 시사점

위에서 살펴 본 행정기관 및 공공기관 정보시스템 등급평가 기준의 특징은 다음과 같이 요약할 수 있다.

- ㅇ 특정한 위험보다는 시스템 자체의 국가사회적 및 보안 측면의 중요도에 근거하여 등급을 평가함
- ㅇ 시스템을 서비스 또는 정보유형에 따라 분류하고 기본적인 등급을 사전에 정의하여 제시함
- ㅇ 평가항목으로 보안 관련 평가항목(기밀성, 무결성, 가용성 등)의 비중이 큼
- ㅇ 또한 공공시스템의 특성을 반영하여 '국가 안전보장(또는 국가 존립)' 관련 항목에 대한 고려 비중이 큼
- ㅇ 피해범위 평가 지표의 단위가 산업 안전표준의 것과 다름 (예, 전국민/특정국민/소규모지역국민의 생명 vs. 사망/중상/…)

3. 정보보호시스템 평가/인증 제도 (국내)

가. 관련 법제도

국내 정보보호시스템 평가/인증 제도는 전자정부법 및 국가정보화기본법에 의거한다. 전자정부법 56조는 보통신망과 행정정보 등에 대한 보안대책 마련을 요구하고 있다. 국가정보화 기본법 38조는 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지키도록 할 수 있음을 명시하고 있다.

국가정보원은 전자정부법 제56조에 근거하여 국가 · 공공기관이 도입하는 정보보호시스템 · 네트워크 장비 등 보안기능이 탑재된 IT제품의 보안 안전성을 검증하는 보안적합성 검증제도를 운영하고 있다. 중앙행정기관과 주요정보통신기반시설 관리기관 및 광역시 · 도(교육지원청 포함)는 정보보호시스템 · 네트워크 장비 도입후 국가정보원에 보안적합성 검증을 신청하여야 하며 검증과정에서 발견된 취약점을 제거한 후에 운용하여야 한다.

나. 보안적합성 검증 기준

국가 · 공공기관이 도입하는 정보보호시스템과 네트워크 장비는 유형에 따라 공통평가기준(CC: Common Criteria)인증 또는 보안기능 확인서 등 사전 인증을 획득해야 한다. 침입차단시스템 등 23종 제품은 우리나라(IT보안인증사무국)를 비롯, CCRA회원국이 발행한 CC 인증을 받아야 하며, 네트워크 장비는 보안기능 확인서를 받아야 한다.

아울러 가상사설망(VPN), 소프트웨어 기반 보안USB, 호스트 자료유출방지 등 3종 제품은 검증필 암호모듈을 탑재해야 한다. 또한, 23종 이외 기타 제품은 보안기능 확인서를 사전에 발급받아 활용할 수 있다.

[그림 4-3] 보안적합성 검증제도 - 제품유형별 검증 기준

도입 요건	제품 유형	필수 확인 사항
CC 인증	침입차단시스템(FW) 침입방지시스템(IPS)(침입탐지포함) 가상사설망 제품 통합보안관리제품 웹 방화벽 운영체제(서버) 접근통제 제품 DB 접근통제 제품 네트워크 접근통제 제품 인터넷전화 보안 제품 무선침입방지시스템 무선랜 인증 제품 가상화 제품(Hypervisor) 네트워크 자료유출방지 제품 호스트 자료유출방지 제품(매체제어 제품 포함) 디지털 복합기(완전삭제 또는 데이터 암호화) 스마트폰 보안관리 제품 스팸메일 차단시스템 패치관리시스템 망간자료전송제품 DDoS 대응장비 안티바이러스 제품 소스코드 보안약점 분석도구 스마트카드	**※ CC 인증 필수 유형 제품** ①보호프로파일(PP)을 준수하였을 경우 해당 인증등급 수용 가능 ②준수한 보호프로파일이 없는 국내용 CC 등을 획득한 경우 EAL 2 이상 ③스마트카드 제품은 EAL4 이상 **※ CC 인증 범위** 도입기관이 사용하고자 하는 보안기능이 인증범위(TOE)에 포함되었는지 여부 **※ CC 인증 및 보안기능 확인서** 다양한 하드웨어에 탑재, 배포되는 경우 인증보고서 또는 보안기능 확인서에 해당 H/W 모델명이 기재 되었는지 확인 **※ 검증필 암호모듈** 가상사설망(VPN) · S/W 기반 보안USB · 호스트 자료유출방지 등 3종 유형은 검증필 암호모듈 탑재 필요
보안기능 확인서 (舊 보안기능 시험결과서)	가상화 관리제품 S/W 기반 보안USB 제품 네트워크 장비	

자료 : 한국정보보안기술원, Korea Information Security Technology

다. 정보보호시스템 공통평가기준 (CC)

공통평가기준(CC)은 IT 제품의 정보 보안평가 인증을 위한 평가 기준으로 앞서 설명한 보안적합성 검증제도의 검증 기준으로도 사용되고 있다. 공통평가기준은 다음 2가지 유형의 보안 요구사항을 제시하고 있다.

ㅇ 보안 기능 요구사항 (Functional requirements) : 보안 제품이 가져야 하는 보안 기능을 정의함

- 예시: identification & authentication, audit, user data protection, cryptographic support

ㅇ 보증 요구사항 (Assurance requirements) : 보안 기능 요구사항 만족에 대한 보증을 얻는 방법과 관련된 요구사항을 정의함

- 예시: development, configuration management, life cycle support, testing, vulnerability analysis

[그림 4-4] 공통평가기준 - 보안보증등급

EAL1	Functionally Tested
EAL2	Structurally Tested
EAL3	Methodically Tested & Checked
EAL4	Methodically Designed, Tested & Reviewed
EAL5	Semi-formally Designed & Tested
EAL7	Semi-formally Verified Design & Tested
EAL7	Formally Verified Design & Tested

자료 : Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components

공통평가기준에서는 7단계의 보안 보증등급을 정의하고 있다. 보안 보증등급은 특정 수준의 보안 수준을 달성하기 위해 필요한 요구사항을 정의한 것으로, 시스템에 대한 평가를 기반으로 부여되는 안전등급의 개념과는 차이가 있다. 보안 분야에서는 필요한 보안 보증등급 수준을 사용자가 정의하도록 하고 있다. 국가 · 공공기관이 도입하는 정보보안 관련 제품의 경우, 국가정보원에서 필요한 보안 보증등급 수준을 정하여 적용하고 있다.

공통평가기준의 내용을 기반으로 특정 시스템 유형별로 구체적인 보안 요구사항을 제시하기 위해 보호 프로파일(Protection profile)과 보안목표명세서(Security target)을 정하여 사용하고 있다.

라. 시사점

위에서 살펴 본 보안 적합성 검증 기준 및 정보보호시스템 공통평가기준의 특징은 다음과 같이 요약할 수 있다.

- ㅇ 국가 · 공공기관이 도입하는 보안제품의 유형에 따라 달성해야 하는 등급(EAL)을 사전 정의함
- ㅇ 정보보호시스템 공통평가기준(CC)의 보증등급(EAL)은 은 '미리 정의된 보증수준 or 보증패키지 (보증요구사항들의 집합)' 의 개념으로 사용자가 달성 수준을 정할 수 있음 (시스템에 대한 평가를 기반으로 부여되는 안전등급의 개념과는 차이가 있음)
- ㅇ 제품 유형별로 구체적인 보안 요구사항(PP, ST)을 제공함

4. 공공 정보/정보시스템 보안 등급 기준 (미국)

가. 관련 법제도

미국의 정보보안 관련 법제도의 근간은 FISMA(Federal Information Security Modernization Act)이다. 미국 표준기술연구원 (NIST: National Institute of Standards and Technology)은 RMF(Risk Management Framework)를 개발하여 위험관리의 전체 생명주기에 대한 프레임워크 제공하고 있다. 전체 RMF 중 보안등급의 평가기준은 FIPS PUB 199[88], SP 800-60[89]를 통해서 제공하고 있다.

나. 보안등급 평가 기준

FIPS PUB 199는 보안등급을 평가하기 위한 평가항목으로 기밀성 (Confidentiality), 무

88) FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems

89) Special Publication 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

결성 (Integrity), 가용성(Availability)을 제시하고 있다. 각 평가항목은 다음 <표 4-12>과 같이 정의된다.

<표 4-12> FIPS PUB 199 - 보안등급 평가항목

보안등급 평가항목	설명
Confidentiality	“개인 정보 보호 및 독점 정보 보호 수단을 포함하여 정보 액세스 및 공개에 대한 승인 된 제한 유지…“[44 U.S.C., Sec. 3542] 기밀성 손실은 정보의 무단 공개입니다.
Integrity	“부적절한 정보 수정 또는 손실에 대한 보호, 정보 부인 방지 및 신뢰성 보장…“[44 U.S.C., Sec. 3542] 무결성 손실은 정보의 무단 수정 또는 손실입니다.
Availability	“정보에 대한 적시적이고 안정적인 접근 및 사용 보장…“[44 U.S.C., SEC. 3542] 가용성 손실은 정보 또는 정보 시스템에 대한 접근 또는 사용의 중단입니다.

자료 : FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems

각 항목에 대한 평가는 해당 항목의 부족 또는 손실로 인한 영향(impact)에 기반하여 이루어진다. 영향 판단 시 고려해야 할 세부항목은 다음과 같이 정의된다.

- ㅇ Degradation in mission capability,
- ㅇ Damage to org. asset,
- ㅇ Financial loss,
- ㅇ Harm to individuals

FIPS PUB 199에서 정의하고 있는 영향 수준에 대한 평가 기준은 다음 [그림 4-5]과 같다.

[그림 4-5] FIPS PUB 199 - Potential Impact Level

Potential Impact	Definitions
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[7] A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

자료 : FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems

기본적으로 보안 등급평가는 각 항목별로 수행된다. 하나의 시스템에 다양한 정보 유형이 존재하는 경우, 그 중 가장 높은 평가등급으로 결정된다. 시스템 전체 수준의 보안 등급은 기밀성, 무결성, 가용성 평가등급 중 가장 높은 등급으로 결정된다.

SP 800-60은 정보/정보시스템 유형 별로 잠재 보안등급을 제시하고 있다. 다음은 이에 대한 일부 예이다.

[그림 4-6] SP 800-60 - Type-based impacts for ‘Management and Support Information’

Table C-2: Type-based Impacts for Federal Information and Information Systems

Security Categorization of Management and Support Information

	Confidentiality	Integrity	Availability
Controls and Oversight			
Corrective Action (Policy/Regulation)	Low	**Low**	**Low**
Program Evaluation	Low	**Low**	**Low**
Program Monitoring	Low[3]	Low	Low
Regulatory Development			
Policy and Guidance Development	Low	Low	**Low**
Public Comment Tracking	**Low**	**Low**	**Low**
Regulatory Creation	Low	Low	**Low**
Rule Publication	**Low**	**Low**	**Low**
Planning and Budgeting			
Budget Formulation	Low	Low	**Low**
Capital Planning	Low	Low	**Low**
Enterprise Architecture	Low	Low	**Low**
Strategic Planning	Low	Low	**Low**
Budget Execution	Low	Low	**Low**
Workforce Planning	Low	**Low**	**Low**
Management Improvement	Low	Low	**Low**
Budgeting & Performance Integration	Low	Low	**Low**
Tax and Fiscal Policy	Low	Low	**Low**
Internal Risk Management and Mitigation			
Contingency Planning	Moderate	**Moderate**	Moderate
Continuity of Operations	Moderate	**Moderate**	Moderate

자료 : Special Publication 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

[그림 4-7] SP 800-60 - Type-based impacts for ‘Mission Information’

Table D-2: Security Categorization of Mission Information

	Confidentiality	Integrity	Availability
Defense & National Security	**Nat'l Security**	**Nat'l Security**	**Nat'l Security**
Homeland Security			
Border Control and Transportation Security	Moderate	Moderate	Moderate
Key Asset and Critical Infrastructure Protection	**High**	**High**	**High**
Catastrophic Defense	**High**	**High**	**High**
Executive Functions of the EOP[23]	**High**	**Moderate**	**High**
Intelligence Operations[24]	**High**	**High**	**High**
Disaster Management			
Disaster Monitoring and Prediction	Low	**High**	**High**
Disaster Preparedness and Planning	Low	Low	Low
Disaster Repair and Restoration	**Low**	**Low**	**Low**
Emergency Response	Low	**High**	**High**

자료 : Special Publication 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

다. 시사점

위에서 살펴 본 보안등급 평가 기준의 특징은 다음과 같이 요약할 수 있다.

- ㅇ 특정한 위험보다는 시스템 자체에 대한 평가에 근거하여 등급을 평가함
- ㅇ 시스템을 정보유형에 따라 분류하고 기본적인 등급을 사전에 정의하여 제시함
- ㅇ 평가항목으로 보안목표에 해당하는 기밀성, 무결성, 가용성을 고려함
- ㅇ 영향력을 판단할 때 반테러 미션에 대해 고려함
- ㅇ 국방, 국가안보, 국가기밀 등과 관련된 정보 또는 정보시스템은 별도로 정의된 기준에 따라 관리됨

제3절 안전이 중요한 공공기관 시스템 조사

1. 공공 정보시스템 분류 기준

가. 공공기관 및 행정기관 정보시스템 분류(국내)

공공기관 및 행정기관 정보시스템 분류를 위한 관련 법제도로 전자정부법이 존재한다. 전자정부법은 행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정하고 있는 법으로써, 전자정부법은 정보시스템에 대한 관리 기준도 제시하고 있다. 전자정부법 56조는 정보통신망과 행정정보 등에 대한 보안대책 마련을, 56조의 2는 정보시스템의 장애 예방 및 대응을 위한 방안 마련을 요구하고 있다. 전자정부법을 근거로 자치단체 정보시스템 장애 예방 및 대응 지침은 정보시스템의 등급 결정을 위한 절차 및 기준을 제시하고 있다.

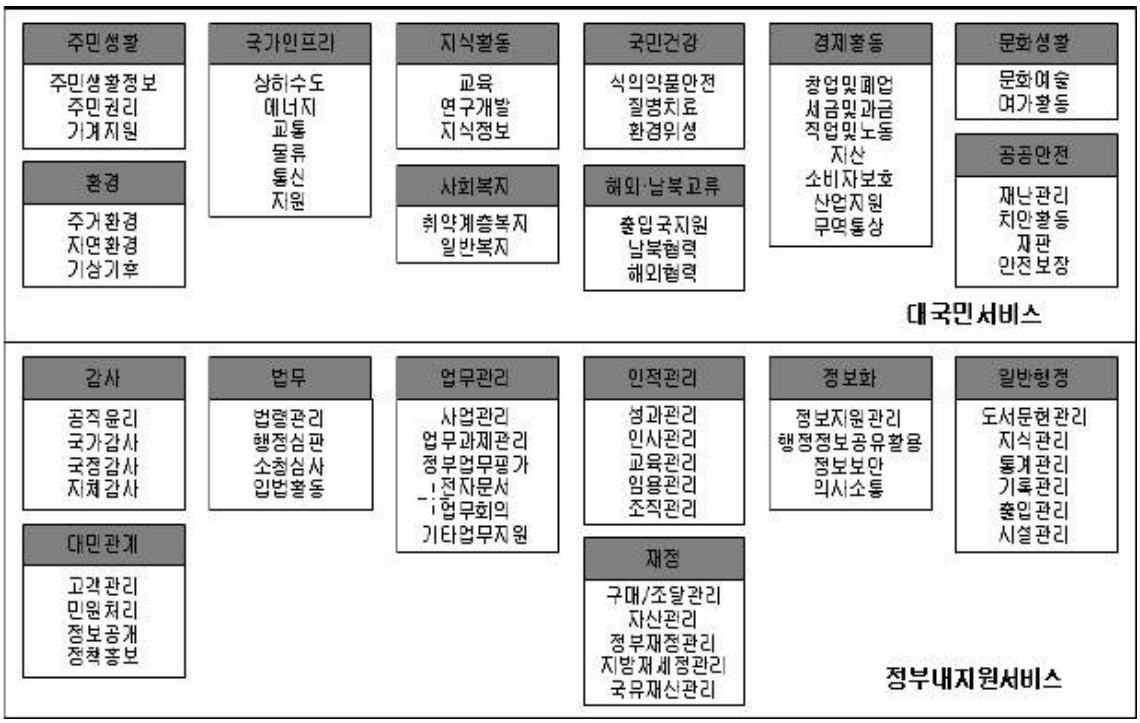
또한, 자치단체 정보시스템 장애 예방 및 장애 지침은 정보기술아키텍처(EA) 서비스 참조모형(SRM)[90]하고 있는 기준에 따라 정보시스템을 분류하고, 이 지침에서 제시하고 있는 기준에 따라 평가된 중요도를 제시하고 있다. 범정부 서비스 참조모형은 공공부문의 업무를 지원하기 위한 응용 서비스 기능을 분류한 것으로 업무에 대응되는 응용

90) 범정부 서비스참조모형 2.2, 행정안전부 (2012)

서비스를 효율적으로 식별할 수 있도록 정의되었다.

이 지침에서는 정보시스템은 크게 대국민 서비스, 정부내 지원 서비스의 2개 분야에서 18개의 중분류 145개의 소분류로 구분된다. <표 4-13>에서는 해당 정보시스템 분류에 대한 예를 보여주고 있다.

[그림 4-8] 범정부 서비스참조모형



<표 4-13> 자치단체 정보시스템 장애 예방 및 지침 - 중요도 시스템 평가기준

번호	대분류	소분류	분류체계 설명	등급기준	
			등급상향 기준 설명	C	I
1	주민생활	주민정보	주민과 관련된 정보(호적, 등본, 제증명) 관리 및 각종 요청서류 제공 서비스를 위한 정보	3	2
2		생활정보	주민의 생활과 관련된 편의정보 및 공공시설 정보를 제공하는 서비스를 위한 정보	5	4
3		가계금융	가계 재정의 안정을 지원하기 위하여 제공되는 대출 보증 및 직접대출 서비스	3	2
4		가계생활 안정	가계생활의 안정을 위한 비금융(보육지원, 위탁 교육, 관련 시설 운영) 형태의 지원 서비스	3	3
5		선거・투표	국민이 선거 및 투표 활동을 수행하기 위해 국가가 지원하는 서비스	3	3

			✔ 선거의 투·개표 결과정보 등 위·변조 시 국정운영에 심각한 피해가 예상 되는 경우 무결성 2등급	-	2
6		인권보호	국민이 권리를 행사하고 보호받기 위해 국가가 지원하는 서비스	3	3
			✔ 인권보호 정보의 유출시 국민의 권리행사·보호에 피해 예상 시 기밀성 2등급	2	-
7	환경	주건환경 개선	쾌적한 주거환경을 위해 제공되는 주거환경시설 개선, 생활편의시설 건설 등에 해당하는 서비스	5	4
8		주건환경 정화	쾌적한 주거환경 조성을 위해 각종 쓰레기 및 폐기물 처리 등에 해당하는 서비스	5	4
9		환경보전	자연환경을 보호하는 목적으로 환경파괴 행위 감시 및 환경보호 활동 지원 등의 서비스를 위한 정보	5	4
…		…	…	…	…
…	일반 행정	…	…	…	…
144		시설관리	기관시설 유지관리 및 시설의 안전이용을 위해 제공하는 정보와 서비스	3	3
145			✔ 시설관리 관련 정보의 유출 시 주요시설 침투 등 심각한 피해가 예상되는 경우 기밀성 2등급	2	-

자료 : 행정자치부 예규 제 90호, 2017.6.9., 자치단체 정보시스템 장애 예방 및 대응 지침

나. 공공 정보시스템 분류 (미국)

미국 표준기술연구원 (NIST: National Institute of Standards and Technology)은 FISMA (Federal Information Security Modernization Act)를 근거로 RMF(Risk Management Framework)를 개발하여 위험관리의 전체 생명주기에 대한 프레임워크 제공하고 있다. RMF 하에 FIPS PUB 199[91], SP 800-60[92]은 정보시스템의 보안등급 기준 및 정보시스템 분류에 따라 참조등급(Provisional impact level)을 제시하고 있다.

또한, SP 800-60은 OMB(Office of Management and Budget)' s Business Reference Model (BRM) section of Federal Enterprise Architecture를 기반으로 정보시스템을 분류하고 있다. 정보시스템은 크게 다음과 같은 3가지 유형으로 구분된다.

91) FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems

92) Special Publication 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

- Mission-based information type: 26개 중분류, 92개 소분류
- Services delivery support information: 8개 중분류, 42개 소분류
- Government resource management information type: 5개 중분류, 35개 소분류

[그림 4-9] Mission-based information type

Mission Areas and Information Types

D.1 Defense & National Security	**D.7 Energy**	**D.14 Health**
Strategic National & Theater Defense	Energy Supply	Access to Care
Operational Defense	Energy Conservation and Preparedness	Population Health Mgmt and Consumer Safety
Tactical Defense	Energy Resource Management	Health Care Administration
D.2 Homeland Security	Energy Production	Health Care Delivery Services
Border and Transportation Security	**D.8 Environmental Management**	Health Care Research and Practitioner Education
Key Asset and Critical Infrastructure Protection	Environmental Monitoring and Forecasting	**D.15 Income Security**
Catastrophic Defense	Environmental Remediation	General Retirement and Disability
Executive Functions of the Executive Office of the President (EOP)	Pollution Prevention and Control	Unemployment Compensation
D.3 Intelligence Operations	**D.9 Economic Development**	Housing Assistance
Intelligence Planning	Business and Industry Development	Food and Nutrition Assistance
Intelligence Collection	Intellectual Property Protection	Survivor Compensation
Intelligence Analysis & Production	Financial Sector Oversight	**D.16 Law Enforcement**
Intelligence Dissemination	Industry Sector Income Stabilization	Criminal Apprehension
Intelligence Processing	**D.10 Community & Social Services**	Criminal Investigation and Surveillance
D.4 Disaster Management	Homeownership Promotion	Citizen Protection
Disaster Monitoring and Prediction	Community and Regional Development	Leadership Protection
Disaster Preparedness and Planning	Social Services	Property Protection
Disaster Repair and Restoration	Postal Services	Substance Control
Emergency Response	**D.11 Transportation**	Crime Prevention
D.5 International Affairs & Commerce	Ground Transportation	*Trade Law Enforcement*
Foreign Affairs	Water Transportation	**D.17 Litigation & Judicial Activities**
International Development and Humanitarian Aid	Air Transportation	Judicial Hearings
Global Trade	Space Operations	Legal Defense
D.6 Natural Resources	**D.12 Education**	Legal Investigation
Water Resource Management	Elementary, Secondary, and Vocational Education	Legal Prosecution and Litigation
Conservation, Marine and Land Management	Higher Education	Resolution Facilitation
Recreational Resource Management and Tourism	Cultural and Historic Preservation	**D.18 Federal Correctional Activities**
Agricultural Innovation and Services	Cultural and Historic Exhibition	Criminal Incarceration
	D.13 Workforce Management	Criminal Rehabilitation
	Training and Employment	**D.19 General Sciences & Innovation**
	Labor Rights Management	Scientific and Technological Research and Innovation
	Worker Safety	Space Exploration and Innovation

Mode of Delivery

Services Delivery Mechanisms and Information Types

D.20 Knowledge Creation & Management	**D.22 Public Goods Creation & Management**	**D.24 Credit and Insurance**
Research and Development	Manufacturing	Direct Loans
General Purpose Data and Statistics	Construction	Loan Guarantees
Advising and Consulting	Public Resources, Facility and Infrastructure Management	General Insurance
Knowledge Dissemination	Information Infrastructure Management	**D.25 Transfers to State/ Local Governments**
D.21 Regulatory Compliance & Enforcement	**D.23 Federal Financial Assistance**	Formula Grants
Inspections and Auditing	Federal Grants (Non-State)	Project/Competitive Grants
Standards Setting/Reporting Guideline Development	Direct Transfers to Individuals	Earmarked Grants
Permits and Licensing	Subsidies	State Loans
	Tax Credits	**D.26 Direct Services for Citizens**
		Military Operations
		Civilian Operations

자료 : Special Publication 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

[그림 4-10] Services delivery support information

Services Delivery Support Information		
C.2.1 Controls and Oversight	**C.2.4 Internal Risk Management & Mitigation**	**C.2.8 General Government**
Corrective Action (Policy/Regulation)	Contingency Planning	Central Fiscal Operations
Program Evaluation	Continuity of Operations	Legislative Functions
Program Monitoring	Service Recovery	Executive Functions
C.2.2 Regulatory Development	**C.2.5 Revenue Collection**	Central Property Management
Policy & Guidance Development	Debt Collection	Central Personnel Management
Public Comment Tracking	User Fee Collection	Taxation Management
Regulatory Creation	Federal Asset Sales	Central Records & Statistics Management
Rule Publication	**C.2.6 Public Affairs**	*Income Information*
C.2.3 Planning & Budgeting	Customer Services	*Personal Identity and Authentication*
Budget Formulation	Official Information Dissemination	*Entitlement Event Information*
Capital Planning	Product Outreach	*Representative Payee Information*
Enterprise Architecture	Public Relations	*General Information*
Strategic Planning	**C.2.7 Legislative Relations**	
Budget Execution	Legislation Tracking	
Workforce Planning	Legislation Testimony	
Management Improvement	Proposal Development	
Budgeting & Performance Integration	Congressional Liaison Operations	
Tax & Fiscal Policy		

Special Publication 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

[그림 4-11] Government resource management information

Government Resource Management Information		
C.3.1 Administrative Management	**C.3.3 Human Resource Management**	**C.3.5 Information & Technology Management**
Facilities, Fleet, and Equipment Management	HR Strategy	System Development
Help Desk Services	Staff Acquisition	Lifecycle/Change Management
Security Management	Organization & Position Mgmt	System Maintenance
Travel	Compensation Management	IT Infrastructure Maintenance
Workplace Policy Development & Management	Benefits Management	Information Security
C.3.2 Financial Management	Employee Performance Mgmt	Record Retention
Accounting	Employee Relations	Information Management
Funds Control	Labor Relations	System and Network Monitoring
Payments	Separation Management	Information Sharing
Collections and Receivables	Human Resources Development	
Asset and Liability Management	**C.3.4 Supply Chain Management**	
Reporting and Information	Goods Acquisition	
Cost Accounting/ Performance Measurement	Inventory Control	
	Logistics Management	
	Services Acquisition	

Special Publication 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

2. 기반시설 분류 기준

가. 국가기반시설 분류

재난 및 안전관리 기본법[93]은 재난 예방을 위한 방안 중 하나로 국가핵심기반시설을

93) [시행 2020. 6. 9.] [법률 제17383호, 2020. 6. 9., 일부개정]

지정하고 이에 대한 보호계획을 수립하여 관리하도록 하고 있다. 이 법에서는 국가핵심기반을 지정하는 기준을 제시하고 있다. 동법의 시행령과 국가기반체계 보호계획 수립지침 등에서는 국가핵심기반 시설로 분류하는 세부 기준 및 실제 국가기반시설로 지정한 대상에 대해서 기술하고 있다.

또한, 재난 및 안전관리 기본법에서는 다음 <표 4-14>과 같이 국가핵심기반 시설로 분류하는 기준을 제시하고 있으며, 동법 시행령에서는 분야별로 국가핵심기반을 지정하는 보다 구체적인 기준을 제시하고 있다.

- ㅇ 다른 국가핵심기반 등에 미치는 연쇄효과
- ㅇ 둘 이상의 중앙행정기관의 공동대응 필요성
- ㅇ 재난이 발생하는 경우 국가안전보장과 경제 · 사회에 미치는 피해 규모 및 범위
- ㅇ 재난의 발생 가능성 또는 그 복구의 용이성

<표 4-14> 재난 및 안전관리 기본법 시행령 - 분야별 국가핵심기반 지정 기준

분야별	지정 기준
에너지	전력·석유·가스 공급에 필요한 생산·공급시설과 비축시설
정보통신	교환기 등 주요 통신장비가 집중된 시설 및 정보통신 서비스의 전국 상황 감시시설 국가행정을 운영·관리하는 데 필요한 기간망과 주요 전산시스템
교통수송	인력 수송과 물류 기능을 담당하는 체계와 실제 운용하는데 필요한 교통·운송시설 및 이를 통제하는 시설
금융	은행 및 투자매매업·투자중개업을 운영하는 데에 필요한 시설이나 체계
보건의료	응급의료서비스를 제공하는 시설과 이를 지원하는 혈액관리 업무를 담당하는 시설
원자력	원자력시설의 안정적 운영에 필요한 주제어장치가 집중된 시설과 방사성폐기물을 영구 처분하기 위한 시설
환경	폐기물관리법에 따른 생활폐끼물 처리를 위한 수집부터 소각·매립끄지의 계통상의 시설
정부중요 시설	중앙행정기관이 입주하고 있는 주요 시설
식용수	식용수 공급을 위한 담수부터 정수까지 계통상의 시설
문화재	문화재보호법 제2조제3항제1호에 따른 국가지정문화재로서 문화재청장이 특별히 관리할 필요가 있다고 인정하는 문화재

공통구	국토의 계획 및 이용에 관한 법률 제2조9호에 따른 공통구로서 행정안전부장관 또는 국토부장관이 특별히 관리할 필요가 있다고 인정하는 공통구

국가기반체계 보호계획 수립지침에서 지정하고 있는 국가기반시설은 다음 <표 4-15>와 같다.

<표 4-15> 국가기반체계 보호계획 수립지침 - 국가기반시설 지정 현황

분야 별		계	지정 시설
에너지 (42) (산업부)	전 력	20	화력(12) : 삼천포•영흥•보령•인천•하동•신인천•부산복합•당진•울산화력본부, 태안•평택•서인천 발전본부 원자력(4) : 고리•한빛•월성•한울 원자력발전소 수력(2) : 양양 양수발전소, 팔당 수력발전소 전기(2) : 한국전력거래소(중앙전력관제센터, 중부지사)
	가 스	4	생산기지(인수,저장,기화,송출)(3) : 평택, 인천, 통영, 삼척
	석 유	18	생산시설(5) : SK에너지 울산, SK인천석유화학 인천, GS칼텍스 여수, S-Oil 온산, 현대오일뱅크 대산 공장 비축시설(9) : 한국석유공사 울산•거제•여수•서산•평택•구리•용인•곡성•동해지사 수송시설(4) : 대한송유관공사 서울•경인•대전•충청지사
정 보 통 신* (21) (미래부)	통신망	12	통신교환국사(7) : KT 광화문•혜화지사, 용인교환국, LGU+ 종합연구소, SKT 분당사옥(NW관리센터), 보라매•둔산사옥(교환/전송실) 망관리센터(4) : KT 전국망센터, LGU+ 안양종합상황실, 상암교환국, SK 브로드밴드 동작종합정보센터 해저케이블육양국(1) : KT 송정해저케이블육양국
	전산망	9	전산망(7) : 외교정보전용망, 우정사업정보센터, 정부통합전산센터, 국가정보통신망, G4C시스템, 주민등록전산정보센터, 광주정부통합전산센터 정보센터(2) : 고용보험전산망, 국민건강보험공단
교 통 수 송 (35) (국토부, 해수부)	철 도	1	철도(1) : 한국철도공사(전국 철도시설)
	항 공	9	항공교통센터(1) : 인천 중구 공항(8) : 인천국제, 김포, 김해, 제주, 울산, 양양, 여수, 무안공항
	화 물	2	내륙컨테이너기지(2) : 의왕, 양산 ICD
	도 로	1	고속국도(1) : 한국도로공사 성남 교통정보센터
	지하철	10	지하철(10) : 서울메트로, 서울도시철도공사, 부산교통공사, 인천교통공사, 대전•대구• 광주도시철도공사, 서울시9호선운영(주), 신분당선, 공항철도
	항 만	12	무역항(12) : 부산•인천•여수•광양•마산•울산•동해묵호•군산•목포•포항•평택당진•대산항
금융(8) (재정부, 금융위)	금융	8	한국•한국수출입•산업•중소기업은행 금융결제원, 한국거래소, 코스콤, 한국예탁결제원

분야 별		계	지정 시설
보 건 의 료 (31) (복지부)	의료 서비스	12	병원(12) : 국립중앙의료원, 서울•부산•경북•충남•충북•전남•전북대학교병원, 길병원, 단국대 부속병원, 연세대 원주 세브란스병원, 목포 한국병원
	혈 액	19	혈액원(16) : 대한적십자사 혈액관리본부, 서울남부•서울동부•서울서부•부산•대구경북인천・울산・경기・강원・충북・대전세종충남・전북・광주전남・경남・제주 혈액원 혈액검사센터(3) : 중앙・중부・남부 혈액검사센터
원 자 력 (36) (원안위)	원자력	36 (5)	원자력발전소(4) : 고리・한빛・월성・한울 원자력본부 ※ 4개소 35개 시설(주제어실, 방사능방재시설 등) 방사성폐기물처분시설(1) : 중・저준위 방사성폐기물처분시설
환경(5) (환경부)	매립	5	쓰레기매립장(5) : 수도권매립지관리공사, 부산시 생곡매립장, 대구시 환경자원매립장, 광주시 광역위생매립장, 대전시 환경자원매립장
식용수 (80) (국토부, 환경부)	댐	30	다목적댐(16) : 소양강・충주・횡성・안동・임하・합천・남강・밀양・대청・용담・섬진강・주암・부안・보령・장흥・군위댐 생공용수댐(14) : 대곡・사연・대암•선암•영천•안계•구천•연초•광동•달방•수어•운문•평림•감포
	정수장	50	광역정수장(20) : 반월•시흥•성남•수지•와부•덕소•일산・송전・청주・충주・석성・보령・천안・고산・화순・구미・사천・고양・덕정・반송 지방정수장(30) : 서울 암사・강북, 부산 화명・덕산, 대구 매곡・고산, 인천 부평・수산, 광주 용연・덕남, 대전 송촌・월평, 울산 회야・천상, 성남 복정, 부천 까치울, 안양 비산・포이・청계통합, 안산 안산・연성, 군포 군포, 김포 고촌, 춘천 소양, 여수 둔덕, 목포 몽탄, 김해 삼계・명동, 창원 칠서, 진주 제2정수장
정부중요시설**(13) (정부청사관리소)	정부중요시설	13	중앙행정기관(13) : 정부서울청사, 정부과천청사, 정부대전청사, 정부세종청사, 국방부, 대검찰청, 방위사업청, 경찰청, 농촌진흥청, 기상청, 국가기상위성센터, 국가기상슈퍼컴퓨터센터, 국가태풍센터

나. 국가중요시설 분류

통합방위법[94]은 적에 의하여 점령 또는 파괴되거나 기능이 마비될 경우 국가안보와 국민생활에 심각한 영향을 주게 되는 시설을 국가중요시설로 지정하여 관리하도록 하고 있다. 국가중요시설 지정 및 방호 훈령은 국가중요시설을 중요도 등급에 따라 분류하는 기준과 구체적으로 국가중요시설을 지정하여 제시하고 있다.

국가중요시설 지정 및 방호 훈령은 국가중요시설을 다음과 같이 정의하고 있다.

94) [시행 2017. 7. 26.] [법률 제14839호, 2017. 7. 26., 타법개정]

ㅇ “국가중요시설”이라 함은 공공기관, 공항, 항만, 주요산업시설 등 적에 의하여 점령 또는 파괴되거나 기능이 마비될 경우 국가안보 및 국민생활에 심대한 영향을 미치는 시설을 말한다.

또한 시설의 기능·역할의 중요성과 가치의 정도에 따라 시설을 가급, 나급, 다급으로 구분하는 기준을 다음과 같이 제시하고 있다.

ㅇ “가”급 : 적에 의하여 점령 또는 파괴되거나, 기능 마비시 광범위한 지역의 통합방위작전수행이 요구되고, 국민생활에 결정적인 영향을 미칠 수 있는 시설

ㅇ “나”급 : 적에 의하여 점령 또는 파괴되거나, 기능 마비시 일부 지역의 통합방위작전수행이 요구되고, 국민생활에 중대한 영향을 미칠 수 있는 시설

ㅇ “다”급 : 적에 의하여 점령 또는 파괴되거나, 기능 마비시 제한된 지역에서 단기간 통합방위작전수행이 요구되고, 국민생활에 상당한 영향을 미칠 수 있는 시설

국가중요시설 지정 및 방호 훈령에서 지정한 국가중요시설의 유형은 다음과 같다.

ㅇ 주요 국가 및 공공기관시설

ㅇ 철강, 조선, 항공기, 정유, 중화학, 방위산업, 대규모 가스·유류 저장시설 등 주요 산업시설

ㅇ 원자력 발전소, 대용량 발전소 및 변전소 등 주요 전력시설

ㅇ 전국 및 지역권 방송국, 송신·중계소 등 주요 방송시설

ㅇ 국제위성지구국, 해저통신중계국, 국가기간전산망, 전화국 등 주요 정보통신시설

ㅇ 철도 교통관제 센터 및 지하철 종합사령실, 교량, 터널 등 주요 교통시설

ㅇ 주요 국제·국내선 공항

ㅇ 대형 선박의 출·입항이 가능한 항만

ㅇ 대형 취수·정수시설 및 다목적 댐 등 주요 수원시설

ㅇ 종합적인 체계를 갖춘 연구시설, 핵연료 개발 연구시설 등 국가 안보상 중요한 과학연구시설

ㅇ 교정·정착지원 시설

○ 전력, 통신, 상수도, 가스 등을 수용하고 있는 대도시 주요 지하공동구 시설

○ 기타 적에 의해 점령 또는 파괴되거나 기능이 마비될 경우 국가안보 및 국민생활에 심대한 영향을 미치는 시설

해당 훈령은 시설 유형에 따라 각 등급에 해당하는 구체적인 시설을 제시하고 있다. 일부 시설 유형에 대한 등급별 시설은 다음 <표 4-16>과 같다.

<표 4-16> 훈령 - 국가중요시설의 분류 및 지정

시설 유형	등급	국가중요시설
국가 및 공공기관시설	가	• 청와대, 국회의사당, 대법원, 정부중앙청사 • 국방부·국가정보원 청사 • 한국은행 본점
	나	• 중앙행정기관 각 부(部)·처(處) 및 이에 준하는 기관 • 대검찰청·경찰청·기상청 청사 • 한국산업은행·한국수출입은행 본점
	다	• 중앙행정기관의 청사 • 국가정보원 지부 • 한국은행 각 지역본부 • 다수의 정부기관이 입주한 남북출입관리 시설 • 기타 중요 국·공립기관
산업시설	가	• 철강, 조선, 항공기, 정유 등 국가경제에 중대한 영향을 미치는 대규모 산업시설 • 전투기, 전차, 함정, 화포 등 중화기를 생산하는 방위산업시설 중 파괴 또는 기능 마비시 국가안보에 직접적인 영향을 미치는 시설 • 1,000만 배럴 이상의 대규모 저유시설과 LNG, LPG 인수기지 • 연쇄적인 폭발위험성이 있는 대규모 총·포탄, 화약류 생산시설
	나	• 국가경제에 영향을 미치는 중요산업시설로서 파괴시 대체가 곤란한 시설 • “가” 급 이외의 방위산업시설 중 주요 전투장비의 완제품 및 핵심부품 생산시설 • 200만 배럴 이상의 저유시설과 1,000톤 이상의 LPG 저장시설
	다	• 100만 배럴 이상의 저유시설과 500톤 이상의 LPG 저장시설 • 기타 “가”, “나” 급 이외의 특별한 보호가 요구되는 산업시설

자료 : 통합방위법, 국가중요시설 지정 및 방호 훈령

다. 정보통신기반시설 분류

정보통신기반 보호법[95]은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 기준을 제시하고 있는 법으로 정보통신기반시설을 지정하는 기준을 제시하고 있다. 정보통신기반시설은 실질적으로 각 관리기관이 고시를 통하여 지정하고 있다.

정보통신기반 보호법에서는 정보통신기반시설을 지정하기 위한 기준을 다음과 같이 제시하고 있다.

- ㅇ 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
- ㅇ 제1호에 따른 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
- ㅇ 다른 정보통신기반시설과의 상호연계성
- ㅇ 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
- ㅇ 침해사고의 발생가능성 또는 그 복구의 용이성

정보통신기반시설은 해당 관리기관이 고시를 통해 정하고 있다. 각 기관에서 정보통신기반시설로 지정한 예는 다음 <표 4-17>과 같다.

<표 4-17> 정보통신기반시설 지정 예시

기관	관련 고시	정보통신기반시설
행정안전부	주요정보통신기반시설 신규 지정(행정안전부고시)(제2015-12호) 외	공공아이핀시스템, 통합지방세시스템, U-City통합운영시스템, 긴급구조시스템, 경전철종합관제시스템 등
산업통상자원부	산업통상자원부 소관 주요정보통신기반시설 신규 및 변경 지정 고시(산업통상자원부고시)(제2015-40호) 외	발전제어시스템, 천연가스 생산제어시스템, 전력계통운영시스템 등
기획재정부	기획재정부 주요정보통신기반시설 지정 고시(기획재정부고시)(제2014-4호) 외	한은금융망, 카드발급시스템 등
방송통신위원회	방송통신위원회 소관분야 주요정보통신기반시설(방송통신위원회고시)(제2011-17호) 외	인터넷접속망, 이동전화(무선인터넷망), 국가정보통신망, 침해사고대응지원시스템, 초고속국가망 등

자료 : 정보통신기반 보호법

95) [시행 2020. 6. 11.], [법률 제16758호, 2019. 12. 10., 일부개정]

행정안전부 소관 주요정보통신기반시설 보호지침[96]에서는 다음 <표 4-18>와 같이 세부시설 지정 기준을 제시하고 있다.

<표 4-18> 행정안전부 - 주요정보통신기반시설 세부시설 지정기준

분야	지정단위	세부시설 지정기준(필수)	선택 세부시설
도시철도 경전철	철도운영종합관제 시스템 (신호관제 시스템, 전력관제 시스템, 통신관제 시스템)	종합관제소 내 신호관제, 전력관제 및 통신관제를 위해 운영되는 서버, PC, 네트워크, 보안, 제어콘트롤러, 통신설비 등 모든 시스템	Serial통신방식의 설비, 기계설비제어시스템, 현장 역사 내 서버, PC 등
교통신호	교통신호제어 시스템	교통신호제어, 조회, 저장을 위해 운영되는 서버, PC, 네트워크, 보안, 통신설비 등 모든 시스템	교차로 신호제어기 등
긴급구조	긴급구조 시스템	신고접수, 출동지령, 상황관제를 위해 운영되는 서버, PC, 네트워크, 보안장비 등 모든 시스템	소방서, 안전센터 내 지령단말 등
U-City	도시안전통합 시스템 (교통신호제어 시스템)	교통신호제어, 조회, 저장을 위해 운영되는 서버, PC, 네트워크, 보안, 제어콘트롤러 등 모든 시스템	CCTV 관제시스템, 교차로의 신호제어기 등
정수제어	상수도정수제어 시스템	정수센터내 정수처리 관련 정보수집, 감시, 제어조작을 위해 운영되는 서버, PC, 네트워크, 보안, 제어콘트롤러, 통신설비 등 모든 시스템	Serial통신방식의 설비, 원격지의 현장 설비
물재생공정	물재생공정제어 시스템	물재생센터 내 하수처리 관련 정보수집, 감시, 제어조작을 위해 운영되는 서버, PC, 네트워크, 보안, 제어콘트롤러, 통신설비 등 모든 시스템	Serial통신방식의 설비, 원격지의 현장 설비
지역난방	지역난방제어 시스템	발전소내 열공급설비 관련 운전정보 저장, 제어를 위해 운영되는 서버, PC, 네트워크, 보안, 제어콘트롤러, 통신설비 등 모든 시스템	Serial통신방식의 설비, 원격지의 현장 설비
인터넷 및 업무	인터넷 및 업무 시스템	광역시도의 내·외부 백본네트워크시스템, 내·외부 보안시스템, 대표홈페이지, 시도행정, 전자결재시스템	필수 외 시스템

자료 : 행정안전부 소관 주요정보통신기반시설 보호지침

96) 행정안전부훈령 제7호. 2017.09.21. 개정

라. 사회기반시설 분류

사회기반시설에 대한 민간투자법[97]에서는 사회기반시설에 대해 정의하고 있으며, 이를 기반으로 한 사회기반시설사업·지역개발사업의 정보화계획 수립에 관한 지침[98]은 구체적인 사회기반시설의 유형을 제시하고 있다.

사회기반시설에 대한 민간투자법은 사회기반시설을 각종 생산활동의 기반이 되는 시설, 해당 시설의 효용을 증진시키거나 이용자의 편의를 도모하는 시설 및 국민생활의 편익을 증진시키는 시설로 정의하고 있으며 다음과 같은 세부 기준을 제시하고 있다.

ㅇ 각종 생산활동의 기반이 되는 시설, 해당 시설의 효용을 증진시키거나 이용자의 편의를 도모하는 시설 및 국민생활의 편익을 증진시키는 시설로서 다음 항목에 해당하는 시설

- 도로, 철도, 항만, 하수도, 하수·분뇨·폐기물처리시설, 재이용시설 등 경제활동의 기반이 되는 시설
- 유치원, 학교, 도서관, 과학관, 복합문화시설, 공공보건의료시설 등 사회서비스의 제공을 위하여 필요한 시설
- 공공청사, 보훈시설, 방재시설, 병영시설 등 국가 또는 지방자치단체의 업무수행을 위하여 필요한 공용시설 또는 생활체육시설, 휴양시설 등 일반 공중의 이용을 위하여 제공하는 공공용 시설

사회기반시설사업·지역개발사업의 정보화계획 수립에 관한 지침에서 제시하고 있는 사회기반시설의 예시는 다음 <표 4-19>과 같다.

<표 4-19> 사회기반시설사업의 종류 (예시)

1. 도로 및 도로의 부속물(「도로법」 제2조제1호 및 제2호)
2. 철도(「철도사업법」 제2조제1호)
3. 도시철도(「도시철도법」 제2조제2호)
4. 항만시설(「항만법」 제2조제5호)

97) [시행 2020. 10. 1.] [법률 제17148호, 2020. 3. 31., 일부개정]
98) [시행 2017. 10. 17.] [과학기술정보통신부고시 제2017-18호, 2017. 10. 17., 전부개정]

5. 공항시설(「공항시설법」 제2조제7호)
6. 다목적댐(「댐건설 및 주변지역지원 등에 관한 법률」 제2조제2호)
7. 수도(「수도법」 제3조제5호)
8. 중수도(「물의 재이용 촉진 및 지원에 관한 법률」 제2조제4호)
9. 하수도(「하수도법」 제2조제3호)
10. 공공하수처리시설(「하수도법」 제2조제9호)
11. 분뇨처리시설(「하수도법」 제2조제10호)
12. 하·폐수처리수 재이용시설(「물의 재이용 촉진 및 지원에 관한 법률」 제2조제7호)
13. 하천시설(「하천법」 제2조제3호)
14. 어항시설(「어촌·어항법」 제2조제5호)
15. 폐기물처리시설(「폐기물관리법」 제2조제8호)
16. 전기통신시설(「전기통신기본법」 제2조제2호)
17. 전원설비(「전원개발촉진법」 제2조제1호)
18. 가스공급시설(「도시가스사업법」 제2조제5호)
19. 집단에너지시설(「집단에너지사업법」 제2조제5호)
20. 정보통신망(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호)
21. 물류터미널 및 물류단지(「물류시설의 개발 및 운영에 관한 법률」 제2조제2호 및 제6호)
22. 여객자동차터미널(「여객자동차 운수사업법」 제2조제5호)
23. 관광지 및 관광단지(「관광진흥법」 제2조제6호 및 제7호)
24. 노외주차장(「주차장법」 제2조제1호나목)
25. 도시공원(「도시공원 및 녹지 등에 관한 법률」 제2조제3호가목)
26. 공공폐수처리시설(「수질 및 수생태계 보전에 관한 법률」 제2조제17호)
27. 공공처리시설(「가축분뇨의 관리 및 이용에 관한 법률」 제2조제9호)
28. 재활용시설(「자원의 절약과 재활용촉진에 관한 법률」 제2조제10호)
29. 전문체육시설에 따른 생활체육시설(「체육시설의 설치·이용에 관한 법률」 제5조 및 제6조)

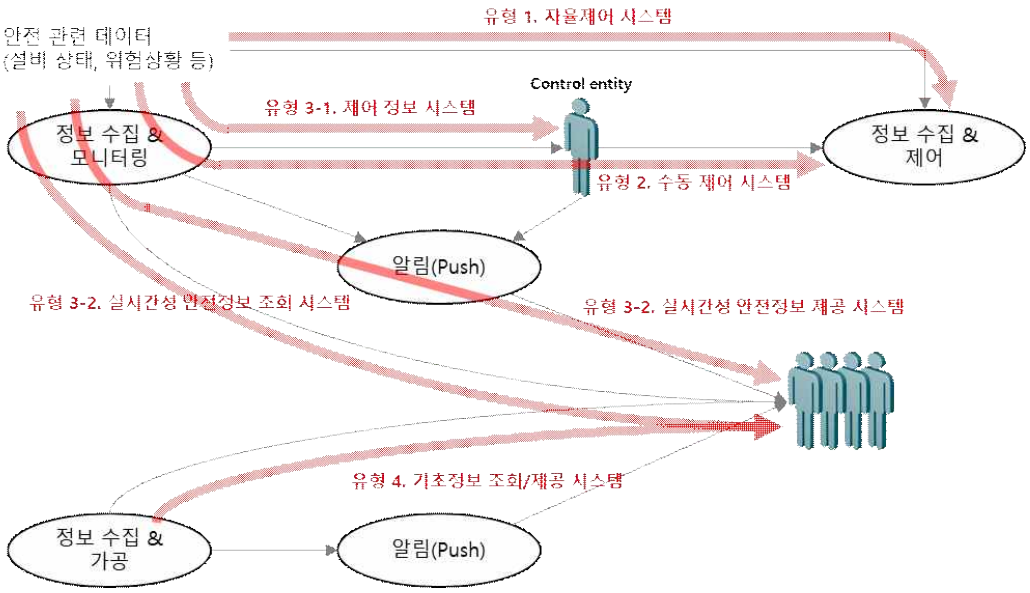
제5장 공공기관 시스템 위험요인 조사

제1절 위험분석 대상 시스템 선정

1. 공공기관 시스템 유형 분류

국가 기간 시스템 안전진단 결과에 기반하여 공공기관 시스템의 위험요인을 조사한다. “제 3장 공공기관 시스템 종류 및 등급제 조사” 의 결과와 같이, 공공기관 시스템은 공공 정보시스템 분류, 기반시설 분류 등, 다양하게 분류 가능하며 그 종류도 매우 많다. 모든 공공기관 시스템의 위험요인을 조사하는 것은 불가능하기에, 본 절에서는 공공기관 시스템의 특성을 분석하여 해당 특성에 따른 유형을 구분하고, 각 시스템 유형에 해당하는 공공기관 시스템을 샘플링하고자 한다.

[그림 5-1] 공공기관 시스템 유형 분류



공공기관 시스템은 크게 제어를 위한 시스템과 정보 제공을 위한 시스템으로 구분 가능하다. 제어 시스템의 경우 사람의 관여 없이 자율적으로 제어하는 시스템과 사람의 개입이 가능한 시스템으로 구분 가능하였다. 정보 시스템의 경우에는, 시스템이 최종적으로 제어 기능까지 수행하지는 않지만 제어 정보를 제공하는 시스템이 존재하였

으며, 제어와 관련없는 안전에 필요한 참조 정보를 제공하는 시스템으로 구분할 수 있었다. 또한, 단순 정보만 제공해주는 시스템과 필요에 따라 국민에게 알람을 제공하는 시스템의 유형을 확인할 수 있다. 따라서, 본 연구에서는 공공기관 시스템의 유형을 다음과 같이 4가지의 유형으로 구분하고, 각 유형에 해당하는 시스템을 샘플링하여 위험분석을 진행한다.

<표 5-1> 시스템 유형 구분

시스템 유형	설명
유형 1	수집된 정보를 기반으로 소프트웨어 판단에 따른 자율 제어 시스템
유형 2	제어자의 판단에 따라 현장 설비를 제어하는 시스템
유형 3	수집된 정보를 모니터링하여 제어자에게 관련 정보를 제공하는 시스템 - 현장 설비를 제어하는데 활용되는 제어 정보 제공 - 모니터링 및 분석을 통해 시설에 대한 특정 안전 상태 정보 제공 . 예) 유독 가스 알람 설비 제어 모니터링및분석을통해자연재해,인재등의재난정보제공
유형 4	수집된 정보를 해당 환경에 노출된 관계자들에게 제공하는 시스템 - 식품, 의약품 등의 안전 관련 정보 제공 - 기후, 기상, 환경, 생활 정보 등의 일반 정보 제공

각 시스템 유형에 해당하는 시스템들은 아래 표와 같이 구분할 수 있다.

<표 5-2> 각 시스템 유형에 해당하는 공공기관 시스템(예)

시스템 유형 구분	시스템 (예)
유형 1. 자율 제어 시스템 유형 2. 수동 제어 시스템	지하철 스크린도어 제어 지하철 화재 차단 방화벽 제어 열차 진로 제어 공항 등화 제어 터널 설비(진입 차단, 환풍기) 제어 전력 시설 제어 하수도 처리 제어
유형 3-1. 제어 정보 시스템 유형 3-2. 실시간성 안전정보 제공 시스템 유형 3-3. 실시간성 안전정보	산불 관제/경보 열차 점유정보 시스템 도로사고 정보 전파(핸드폰, 전광판) 시설물 내 가스누출 인지 및 경고

조회 시스템	가변차선 신호 표시 기상 특보 전파 - 폭우, 폭염, 해상 하수 처리 모니터링 시스템
유형 4. 기초정보 조회 제공 시스템	식품안전 정보 제공 기상 특보 전파 - 폭염 폭우 해상 안전사고 사례, 안전 행동 요령 조회 비행 운행 정보

2. 공공기관 시스템 위험분석

2015 ~2019년 TTA 소프트웨어안전진단 사업을 통해 수행했던 국가 기간 시스템의 안전진단 경험 및 결과를 활용하여, 다수의 공공기관 시스템을 대상으로 시스템 유형을 구분하고, 모든 시스템 유형을 포함할 수 있도록 샘플링한다. 이후 해당 시스템의 위험요인을 조사한다. 분석 대상 공공기관 시스템 및 각 시스템에 대한 위험요인 분석은 다음 표에서 확인 가능하다.

<표 5-3> 분석 대상 공공기관 시스템 및 시스템 유형 식별

도메인	시스템		시스템 유형	
건강	식품안전 시스템	식품에 대한 안전성 관리 및 위해 식품 유통 차단 등의 정보를 제공하는 시스템	정보시스템	유형4
	의약품안전 시스템	의약품의 안전한 유통과 사용을 위한 정보를 제공하는 시스템	정보시스템	유형4
	질병예방 시스템	질병의 감염 및 확산을 방지하기 위한 정보를 제공하는 시스템	정보시스템	유형4
환경	기상 시스템	항공, 해상, 육상에 관련된 기상정보를 관측·예측 및 수집, 관리하기 위한 기초데이터 제공 시스템	정보시스템	유형4
		기상에 따른 재난·재해 사전예방을 위한 기상 예측 및 예보 시스템	정보시스템	유형3
산림	산림자원 시스템	산불상황 관제, 산사태 예보 발령 등 각종 산림재해를 대응하기 위한 시스템	정보시스템	유형3
해양	해상교통 시스템	해상교통과 관련된 시설(항만)의 유지관리 및 선박운행정보 등의 제공 서비스를 위한 정보	정보시스템	유형3
	해양기상 시스템	항로상의 해양기상 정보 제공을 통해 안전한 해양 활동을 지원하기 위한 시스템	정보시스템	유형3

상하수도	상수도 시스템	수처리를 위한 시설에 대하여 원격을 통해 감시 및 제어하는 운영 시스템	제어시스템	유형2 유형3
	하수도 시스템	안정적이고 쾌적한 하수 처리를 위하여 수행되는 서비스의 기반 정보를 제공하는 시스템	정보시스템	유형3
	한강 원격감시 시스템	발전 및 수계 운영을 종합 관리하는 시스템	정보시스템	유형3
도로	터널 시스템	터널 내 설비의 실시간 모니터링 및 원격 제어를 수행하여 원활한 방재업무를 지원하는 시스템	제어시스템	유형2 유형3
	도로교통 시스템	도로의 교통상황과 사고 관련 정보들을 수집 및 가공하여 원활한 교통소통 및 안전관리에 활용하고, 운전자에게 교통정보를 제공하는 시스템	정보시스템	유형3
항공	항공교통 시스템	항공교통과 관련된 시설 운영 및 관리, 항공운항정보 제공 서비스를 위한 정보	정보시스템	유형4
	공항운영 시스템	공항 전역의 단위 시스템 및 자원 상태 정보, 제반 환경 정보 등의 공항 운영 관련 정보를 제공하는 시스템	정보시스템	유형4
		활주로 및 유도로 주변의 항공 설비들을 감시하고 제어하여 항공기 이착륙을 지원하는 시스템	제어시스템	유형2 유형3
철도	철도교통 시스템	철도와 관련된 시설 운영 및 관리, 철도운행정보 제공 서비스를 위한 정보	정보시스템	유형4
	열차진로제어 시스템	철도의 선로상태 정보와 열차 운행상태를 파악하여 열차 스케쥴에 따른 진로를 설정하는 시스템	제어시스템	유형3
	열차점유정보 시스템	열차가 운행되는 선로의 폐색구간에 열차 점유 유무를 검지하는 시스템	정보시스템	유형3

〈표 5-4〉 위험등급

도메인	시스템	최상위 위험원	시스템 위험원
건강	식품안전 시스템	동일 원인에 의한 대규모 식중독 발생	식품안전평가정보 연계 오류 식품안전정보등록오류 식품안전정보표시오류
	의약품 안전 시스템	의약품 등 부작용으로 인한 위해 발생	의약품안전평가정보 연계 오류 의약품안전정보등록오류 의약품안전정보제공및표시오류
	질병예방 시스템	질병 확산 방지 실패로 인한 2~3차 감염	질병(전염병) 발생 예측 오류 질병감염경로분석오류

			질병감염경로전달오류
환경	기상 시스템	기상 문제에 따른 운행 불가 상태 미인지	항공, 해상, 육상 관련 기상정보 수집 및 가공 오류 관측정보제공오류 대민서비스제공오류
		기상에 따른 재난·재해 피해 확산	기상 정보 수집 오류 수집된기상정보기반재난알고리즘오류 재난정보전달오류
산림	산림자원 시스템	산불 피해 확산 산사태피해증가	산불신고정보 수집/제공/전파 오류 산불발생정보전파오류 산불주변정보수집/제공오류 산사태취약지역관련정보의수집/제공오류 산사태예측정보및예보발령정보수집/제공오류 산사태관련정보전파오류(예측,예보발령/해제정보)
해양	해상교통 시스템	위험지역 미인지로 인한 선박 충돌 선박간통신문제로인한 선박충돌	좌초 및 암초 위험 지역 정보 전달 오류 범위내선박정보수집오류 선박정보전달오류
	해양기상 시스템	선박 운항 불가 상태 미인지	실시간 해양기상신호표지 정보 수집 및 배포 오류 실시간해양기상신호표지정보저장및가공오류 관제정보제공오류 대민서비스제공오류
상하수도	상수도 시스템	수질 기준 미달의 수돗물 송/배수 수돗물공급중단 수처리약품및배출수에 의한환경오염	수질 상황 정보 수집 및 제공 오류 설비및공정상태수집및제공오류 설비제어명령전송오류
	하수도 시스템	하수 월류로 인한 수질오염 및 침수피해	하수도 시스템 용량 정보 수집 오류 하수도시스템용량정보모니터링및알람오류
	한강 원격감시 시스템	댐 월류로 인한 발전 설비 및 인명 피해	로컬데이터 수집 및 처리 오류 수집데이터및보고서데이터의저장오류 댐의상태감시오류(저수위,강우량,방수위,방류량등) 서브시스템간데이터동기화수행오류
도로	터널 시스템	터널 내 2차 사고 발생 터널내사고대응지연	터널 현장설비 제어 데이터 생성 오류 터널현장설비제어데이터의전달오류 터널현장설비상태및계측데이터수집오

			류 터널현장설비상태및계측데이터표출오류
	도로교통 시스템	교통혼잡비용 증가 2차교통사고예방지연	실시간 교통정보 수집 및 가공 오류 돌발상황판단및제공오류 교통정보전송및표출오류 CCTV영상정보수집/전송및표출오류 VMS표출정보생성/전송및표출오류
항공	항공교통 시스템	항공기 출/도착 지연	항공기 운항계획 관련 정보 수집/제공 오류 항공기운한스케줄생성오류
	공항운영 시스템	항공기 출/도착 지연	주기장 및 제빙장 배정 관련 정보 수집/제공 오류 항공기지상이동정보수집/제공오류
		항공기 간 충돌 항공기이탈 항공기와다른물체의충돌	항공 설비 상태정보 수신 및 표시 오류 항공설비제어오류 항공설비제어정보전달오류 시스템절체오류
철도	철도교통 시스템	열차 운행 지연	열차 스케줄 생성 오류 열차운행정보수집및제공오류
	열차진로제어 시스템	열차 간 충돌 열차와작업자충돌 열차탈선 열차운행지연	현장설비 상태정보 수집 및 표시 오류 진로제어명령의전송오류 잘못된진로제어명령전송
	열차점유정보 시스템	열차 간 충돌 열차운행지연	주파수 신호(송수신) 처리 오류 궤도계전기의비정상적동작 시스템상태정보전송및표출오류

제2절 위험분석 결과 및 평가 고려사항

공공기관 시스템에 대한 위험분석을 진행해본 결과, 다음과 같은 항목들을 식별할 수 있었으며, 해당 내용을 기반으로 소프트웨어 안전등급 평가 시 고려해야 할 사항들을 도출할 수 있었다.

○ 위험분석을 통한 식별 항목

- 사고에 대한 직접적인 원인을 제공하는 시스템과 사고 피해를 대응하기 위한 목적의 시스템으로 구분할 수 있음

예) 열차 진로 제어 vs. 화재 방화벽 제어

- 발생 가능한 사고의 긴급성, 안전 수단의 중복 여부에 따라 안전등급의 차별 적용이 필요함
  예) 지진 관제/경보 vs. 기상 특보 전파
- 일상적으로 사용되는 시스템과 사고 대응을 위한 시스템의 경우, 위험에 대한 노출도(Occurrence) 차이가 존재함
  예) 지하철 스크린 도어 vs. 지하철 화재 차단 방화벽 제어
- 시스템의 오동작 시, 매번 사고 또는 피해가 발생하는 것은 아님
  예) 매 스크린 도어 고장 시 마다 인명 피해가 발생하지 않음
- 환경 오염. 재산 피해 등이 harm으로 언급됨
- 기구 및 장치를 직접 제어하는 시스템과 제어 또는 조치를 위해 필요한 정보를 제공하는 시스템의 구분이 필요함

이를 통해, 소프트웨어 안전등급 결정 체계를 정의할 시 고려해야 할 사항은 다음과 같다.

ㅇ 소프트웨어 안전등급 결정 체계 정의 시, 고려 사항

- 대상 공공기관 시스템이 사고를 예방하기 위한 성격의 시스템인지, 사고를 유발할 수 있는 성격의 시스템인지, 사고 발생 후 대응을 위한 시스템인지에 따라 소프트웨어 안전등급이 구분될 수 있음
- 해당 공공기관 시스템의 기능이 의도된 기능(intended function)인지, 안전 수단(safety measure)에 해당하는지에 따라 소프트웨어 안전등급이 구분될 수 있음
- 대상 공공기관 시스템 외부에 마련된 별도의 안전대책이 존재하는지, 정보 제공 시 중복되는 정보를 제공하는지 여부에 따라 소프트웨어 안전등급이 구분될 수 있음
- 대상 공공기관 시스템의 기능이 시간에 민감한 기능인지에 따라 소프트웨어 안전등급이 구분될 수 있음
- 대상 공공기관 시스템 기능으로 발생 가능한 위험의 발생가능성(노출도 및 발생

빈도)에 따라 소프트웨어 안전등급이 구분될 수 있음

- 대상 공공기관 시스템 기능의 제어도(또는 위험 관여도)에 따라 소프트웨어 안전등급이 구분될 수 있음
- 위험 영향도에 대한 피해의 범위가 고려되어야 함(인명 피해, 재산 피해, 환경 피해 등)
- 대상 공공기관 시스템이 제어 시스템인지 단순 정보 시스템인지에 따라 소프트웨어 안전등급이 구분될 수 있음
- 대상 공공기관 시스템의 자율 제어도에 따라 소프트웨어 안전등급이 구분될 수 있음

제6장 안전등급에 따른 안전활동 및 기술 조사

제1절 조사 방향

본 장에서는 소프트웨어 안전등급에 따른 안전활동 및 기술을 조사한다. 도메인별 소프트웨어안전활동에 대한 분석은 기존의 소프트웨어안전활동 분석 연구를 통해 많은 부분 진행이 된 상태이다. 하지만 해당 연구에서 고려되지 않은 일부 표준들이 존재하며, 활동 분석의 상세화 수준, 검토 및 검증 활동에 대한 독립성 수준에 대한 분석이 다소 부족한 상태이다. 또한, 일부 소프트웨어안전기법 및 수단에 대한 조사가 수행되었으나, 전반적인 도메인의 안전 표준의 내용을 포함하고 있지는 못하다.

따라서, 본 연구에서는 사회 안전과 관련된 각 분야 별 주요 안전 표준을 선정하고, 선정된 안전 표준에서 정의하고 있는 안전활동 및 기술 등의 관리방안을 조사한다. 조사 대상 분야 및 표준은 다음 표와 같다.

<표 6-1> 조사 대상 분야 및 관련 표준

분야	조사 대상 표준
산업 일반	IEC61508
철도분야	IEC 62279
자동차분야	ISO26262
의료 분야	IEC 62304
항공 분야	DO-178C
항공우주 분야	NASA-STD-8719-13C NASA-GB-8719-13C
국방 분야	MIL-STD-882E Joint-소프트웨어-System-Safety-Engineering-Handbook

제2절 산업일반 안전 표준 (IEC 61508)

1. 개요

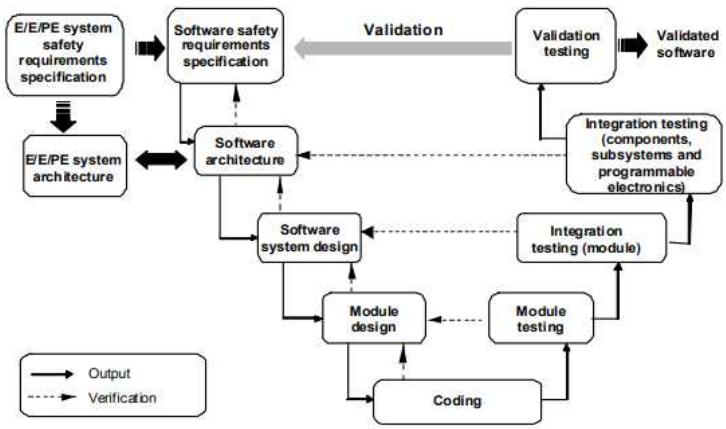
본 절에서는, 산업일반 안전 표준인 IEC 61508[99]을 대상으로 안전등급에 따른 안전 활동 및 기술을 조사하였다. IEC 61508 표준은 모든 종류에 산업에 적용 가능하고, 전기/전자/프로그래밍 가능한 전자 시스템의 기능안전 최상위 표준으로써, 파트 0부터 파트 7까지 총 8개의 파트로 구성되어 있다. 이 중, 소프트웨어 안전과 밀접하게 관련된 부분인 파트 3을 대상으로 조사 및 분석을 수행하였다.

2. 안전활동 및 기술 조사

가. 안전활동 적용 절차

IEC 61508 표준의 안전활동 적용 절차는 [그림 6-1]와 같다. 해당 적용 절차는 V 모델 기반의 절차로써, 각 안전 활동 간 주고받는 정보의 흐름을 간략하게 표현하고 있다. 또한, V 모델의 특성에 따라 각 개발 활동에 대응하는 단계별 검증 활동들이 존재하며, 이에 대한 정보의 흐름을 확인할 수 있다.

[그림 6-1] IEC 61508 안전활동 적용 절차



자료 : IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems, Part 3

99) IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems

나. 안전활동

IEC 61508 표준에서 언급되는 안전활동은 다음 <표 6-2>와 같다. 해당 표준에서는 안전 등급에 따른 활동의 수행 유무를 별도 언급하고 있지 않으며, 소프트웨어 설계 및 개발 단계는 총 5개의 하위 활동으로 상세히 구분하고 있다. 또한, 소프트웨어 요구사항 단계에서의 활동에만 'Safety'가 언급되어 있다. 이후 하위 활동에서는 별도 'Safety'라는 단어가 명시적으로 표현되어 있지 않지만, 정으된 안전 요구사항에 따른 설계 및 검증 활동에 해당하므로 안전에 대한 내용을 포함하고 있다고 볼 수 있다.

<표 6-2> IEC 61508 표준의 안전활동

단계	상위수준 활동	세부 활동
Requirements	Software safety requirements specification	-
	Validation plan for 소프트웨어 aspects of system safety	-
Design	Software design and development	Software architectural design
		Software detailed design and development - 소프트웨어 system design
		Software detailed design and development - Individual 소프트웨어 module design
Implementation		Code implementation
V&V		소프트웨어 module testing
		소프트웨어 integration testing
	Programmable electronics integration (HW and 소프트웨어)	-

자료 : IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems, Part 3

다. 안전기법 및 수단

IEC 61508 표준은 <표 6-3>과 같이 각 개발 단계별로 안전 등급에 따른 기법 및 수

단들을 제공하고 있다. 안전 등급을 기준으로 안전을 위한 세부 기법 및 활동, 방법론 측면에서 설명하고 있다.

<표 6-3> 소프트웨어 안전 등급에 따른 기법 및 수단 - IEC 61508

항목	Technique / Measure	SIL1	SIL2	SIL3	SIL4
Software safety requirements specification	Semi-formal method	R	R	HR	HR
	Formal methods	---	R	R	HR
	Forward traceability between the system safety requirements and the software safety requirements	R	R	HR	HR
	Backward traceability between the safety requirements and the perceived safety needs	R	R	HR	HR
	Computer-aided specification tools to support appropriate techniques/measures above	R	R	HR	HR
Software design and development - Software architecture design	Fault detection	---	R	HR	HR
	Error detecting codes	R	R	R	HR
	Failure assertion programming	R	R	R	HR
	Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer)	---	R	R	---
	Diverse monitor techniques (with separation between the monitor computer and the monitored computer)	---	R	R	HR
	Diverse redundancy, implementing the same software safety requirements specification	---	---	---	R
	Functionally diverse redundancy, implementing different software safety requirements specification	---	---	R	HR
	Backward recovery	R	R	---	HR
	Stateless software design (or limited state design)	---	---	R	HR
	Re-try fault recovery mechanisms	R	R	---	---
	Graceful degradation	R	R	HR	HR
	Artificial intelligence - fault correction	---	NR	NR	NR
	Dynamic reconfiguration	---	NR	NR	NR
	Modular approach	HR	HR	HR	HR
	Use of trusted/verified software elements (if available)	R	HR	HR	HR
	Forward traceability between the software safety requirements	R	R	HR	HR

	specification and software architecture				
	Backward traceability between the software safety requirements specification and software architecture	R	R	HR	HR
	Structured diagrammatic methods **	HR	HR	HR	HR
	Semi-formal methods **	R	R	HR	HR
	Formal design and refinement methods **	---	R	R	HR
	Automatic software generation	R	R	R	R
	Computer-aided specification and design tools	R	R	HR	HR
	Cyclic behaviour, with guaranteed maximum cycle time	R	HR	HR	HR
	Time-triggered architecture	R	HR	HR	HR
	Event-driven, with guaranteed maximum response time	R	HR	HR	-
	Static resource allocation	-	R	HR	HR
	Static synchronisation of access to shared resources	-	-	R	HR
Software design and development - Detailed design	Structured methods **	HR	HR	HR	HR
	Semi-formal methods **	R	HR	HR	HR
	Formal design and refinement methods **	---	R	R	HR
	Computer-aided design tools	R	R	HR	HR
	Defensive programming	---	R	HR	HR
	Modular approach	HR	HR	HR	HR
	Design and coding standards	R	HR	HR	HR
	Structured programming	HR	HR	HR	HR
	Use of trusted/verified software elements (if available)	R	HR	HR	HR
	Forward traceability between the software safety requirements specification and software design	R	R	HR	HR
Software design and development - Software module testing and integration	Probabilistic testing		R	R	R
	Dynamic analysis and testing	R	HR	HR	HR
	Data recording and analysis	HR	HR	HR	HR
	Functional and black box testing	HR	HR	HR	HR
	Performance testing	R	R	HR	HR
	Model based testing	R	R	HR	HR
	Interface testing	R	R	HR	HR
	Test management and automation tools	R	HR	HR	HR
	Forward traceability between the software design specification and the module and integration test specifications	R	R	HR	HR
	Formal verification	---	---	R	R
Programmable	Functional and black box testing	HR	HR	HR	HR

electronics integration (hardware and software)	Performance testing	R	R	HR	HR
	Forward traceability between the system and software design requirements for hardware/software integration and the hardware/software integration test specifications	R	R	HR	HR
Software aspects of system safety validation	Probabilistic testing	---	R	R	HR
	Process simulation	R	R	HR	HR
	Modelling	R	R	HR	HR
	Functional and black box testing	HR	HR	HR	HR
	Forward traceability between the software safety requirements specification and the software safety validation plan	R	R	HR	HR
	Backward traceability between the software safety validation plan and the software safety requirements specification	R	R	HR	HR
Software verification	Formal proof	---	R	R	HR
	Animation of specification and design	R	R	R	R
	Static analysis	R	HR	HR	HR
	Dynamic analysis and testing	R	HR	HR	HR
	Forward traceability between the software design specification and the software verification (including data verification) plan	R	R	HR	HR
	Backward traceability between the software verification (including data verification) plan and the software design specification	R	R	HR	HR
	Offline numerical analysis	R	R	HR	HR
Functional safety assessment	Checklists	R	R	R	R
	Decision/truth tables	R	R	R	R
	Failure analysis	R	R	HR	HR
	Common cause failure analysis of diverse software (if diverse software is actually used)	---	R	HR	HR
	Reliability block diagram	R	R	R	R
	Forward traceability between the requirements of Clause 8 and the plan for software functional safety assessment	R	R	HR	HR
Design and coding standards	Use of coding standard to reduce likelihood of errors	HR	HR	HR	HR
	No dynamic objects	R	HR	HR	HR

	No dynamic variables	---	R	HR	HR
	Online checking of the installation of dynamic variables	---	R	HR	HR
	Limited use of interrupts	R	R	HR	HR
	Limited use of pointers	---	R	HR	HR
	Limited use of recursion	---	R	HR	HR
	No unstructred control flow in programs in higher level languages	R	HR	HR	HR
	No automatic type conversion	R	HR	HR	HR
Dynamic analysis and testing	Test case execution from boundary value analysis	R	HR	HR	HR
	Test case execution from error guessing	R	R	R	R
	Test case execution from error seeding	---	R	R	R
	Test case execution from model-based test case generation	R	R	HR	HR
	Performance modelling	R	R	R	HR
	Equivalence classes and input partition testing	R	R	R	HR
	Structural test coverage (entry points) 100% **	HR	HR	HR	HR
	Structural test coverage (statements) 100% **	R	HR	HR	HR
	Structural test coverage (branches) 100% **	R	R	HR	HR
	Structural test coverage (conditions, MC/DC) 100% **	R	R	R	HR
Functional and black-box testing	Test case execution from cause consequence diagrams	---	---	R	R
	Test case execution from model-based test case generation	R	R	HR	HR
	Prototyping/animation	---	---	R	R
	Equivalence classes and input partition testing, including boundary value analysis	R	HR	HR	HR
	Process simulation	R	R	R	R
Failure analysis	Cuase consequence diagrams	R	R	R	R
	Event tree analysis	R	R	R	R
	Fault tree analysis	R	R	R	R
	Software functional failure analysis	R	R	R	R
Modelling	Data flow diagrams	R	R	R	R
	Finite state machines	---	R	HR	HR
	Formal methods	---	R	R	HR
	Time Petri nets	---	R	HR	HR
	Performance modelling	R	HR	HR	HR
	Prototyping/animation	R	R	R	R
	Structure diagrams	R	R	R	HR

Performance testing	Avalanche/stress testing	R	R	HR	HR
	Response timings and memory constraints	HR	HR	HR	HR
	Performance requirements	HR	HR	HR	HR
Semi-formal methods	Logic/function block diagrams	R	R	HR	HR
	Sequence diagrams	R	R	HR	HR
	Data flow diagrams	R	R	R	R
	Finite state machines/state transition diagrams	R	R	HR	HR
	Time Petri nets	R	R	HR	HR
	Entity-relationship-attribute data models	R	R	R	R
	Message sequence charts	R	R	R	R
	Decision/truth tables	R	R	HR	HR
	UML	R	R	R	R
Static analysis	Boundary value analysis	R	R	HR	HR
	Checklists	R	R	R	R
	Control flow analysis	R	HR	HR	HR
	Data flow analysis	R	HR	HR	HR
	Error guessing	R	R	R	R
	Formal inspections, including specific criteria	R	R	HR	HR
	Walk-through (software)	R	R	R	R
	Symbolic execution	---	---	R	R
	Design review	HR	HR	HR	HR
	Static analysis of run time error behaviour	R	R	R	HR
	Worst-case execution time analysis	R	R	R	R
Modular approach	Software module size limit	HR	HR	HR	HR
	Software complexity control	R	R	HR	HR
	Information hiding/encapsulation	R	HR	HR	HR
	Parameter number limit / fixed number of subprogram parameters	R	R	R	R
	One entry/one exit point in subroutines and functions	HR	HR	HR	HR
	Fully defined interface	HR	HR	HR	HR

자료 : IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems, Part 3

3. 시사점

IEC 61508 표준에서는 소프트웨어 안전등급에 따른 안전활동의 구분이 별도 존재하지 않는다. 소프트웨어 요구사항 정의 단계에서만 'Safety'가 언급되며, 이후 하위 활동에서는 정의된 안전 요구사항에 따른 설계 및 검증 활동을 설명하고 있다. 즉, 일반적인 소프트웨어 개발 활동들은 기본으로 수행된다는 가정 하에 안전 개발을 설명하고 있으며, 안전 특화된 활동들을 개발 단계 별로 구분 지어 설명하고 있지는 않다.

소프트웨어 안전등급에 따라 안전활동이 구분되지는 않으나, 안전 등급에 따른 안전 기법 및 수단의 차등 적용을 제시하고 있다. 다루고 있는 기법 및 수단의 수가 매우 많으며, 안전 등급을 기준으로 세부 기법 및 활동, 방법론 측면에서 설명하고 있다.

제3절 철도 분야 안전 표준 (IEC 62279)

1. 개요

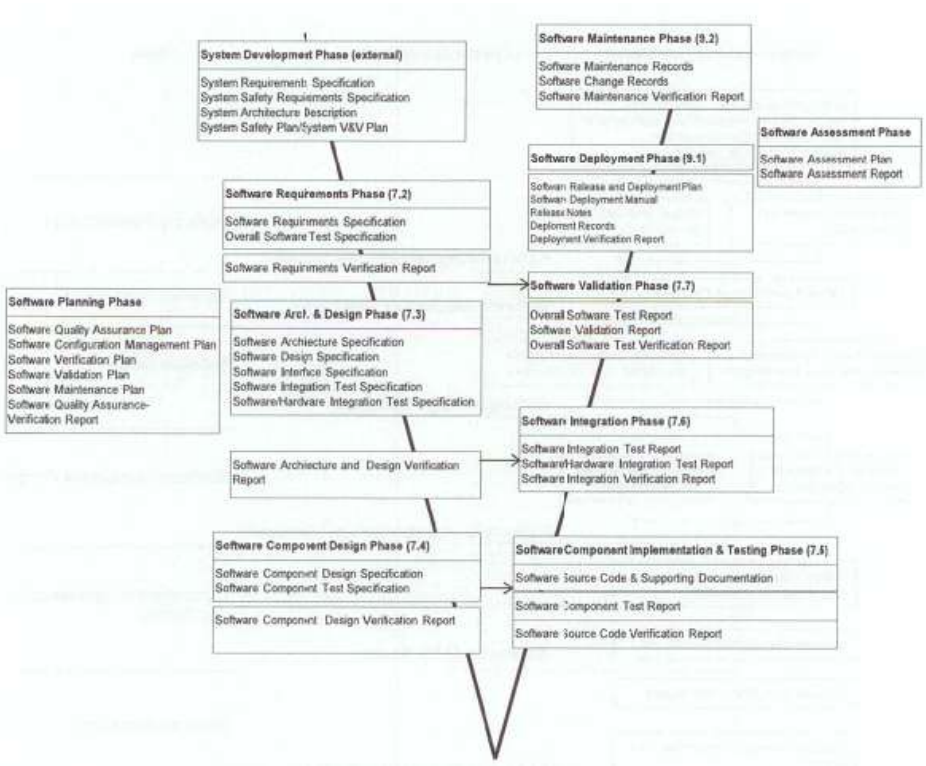
본 절에서는, 철도분야 안전 표준인 IEC 62279를 대상으로 안전등급에 따른 안전활동 및 기술을 조사하였다. IEC 62279 표준은 철도 분야의 안전관련 소프트웨어 개발, 시험, 검증 및 유지보수와 준수해야 할 일련의 요구사항을 제공하는 철도 시스템에 대한 소프트웨어 규격이다. 해당 표준에서는 안전 등급을 0에서 4까지 총 5단계로 구분하여 안전 무결성 등급(Safety Integrity Level: SIL)을 정의하고 있으며, SIL 수준에 따라 활동 및 기술을 설명하고 있다.

2. 안전활동 및 기술 조사

가. 안전활동 적용 절차

IEC 62279 표준의 안전활동 적용 절차는 [그림 6-2]과 같다. 해당 적용 절차는 V 모델 기반의 절차로써, 각 안전 활동 간 주고받는 정보의 흐름을 간략하게 표현하고 있다. 또한, V 모델의 특성에 따라 각 개발 활동에 대응하는 단계별 검증 활동들이 존재하며, 이에 대한 정보의 흐름을 확인할 수 있다.

[그림 6-2] IEC 62279 표준의 안전활동 적용 절차



자료 : IEC 62279, Railway application Software for railway control and protection systems

나. 안전활동

IEC 62279 표준에서 언급되는 안전활동은 다음 <표 6-4>과 같다. 해당 표준에서는 단계별 개발 활동을 제시하고 있으며, 제시하고 있는 활동명에서 일반 및 안전 개발이 명시적으로 구분되어 있지는 않으나 안전 관련 내용을 포함하고 있다. 또한, <표 6-5>와 같이 소프트웨어 안전등급에 따라 각 안전활동에 대한 산출물 작성 여부가 결정되지만 등급에 따른 차등 적용 수준이 매우 미미한 편이다.

<표 6-4> IEC 62279 표준의 안전활동

단계	상위수준 활동	세부 활동
Requirements	Software requirements	Software requirements specification
		Overall software test specification
		Software requirements verification

		report
Design	Software architecture	Software architecture specification
	Software design	Software design specification
		Software interface specification
		Software integration test specification
		Software/Hardware integration test specification
		Software architecture and design verification report
Implementation	Software component design	Software component design specification
		Software component test specification
		Software component design verification report
V&V	Component implementation and testing	Software source code and supporting documentation
		Software Component Test Report
		Software Source Code Verification Report
	Software integration	Software Integration Test Report
		Software/Hardware Integration Test Report
		Software Integration Verification Report
	Software validation	Overall software test report
		Overall software test verification report
		Software validation report
		Tools validation report
		Release note

자료 : IEC 62279, Railway application Software for railway control and protection systems

<표 6-5> 소프트웨어 안전등급에 따른 산출물 작성 - IEC 62279

활동	산출물	SIL0	SIL1	SIL2	SIL3	SIL4
Software Requirements	Software Requirements Specification	HR	HR	HR	HR	HR
	Overall Software Test Specification	HR	HR	HR	HR	HR
	Software Requirements	HR	HR	HR	HR	HR

	Verification Report					
Architecture and Design	Software Architecture Specification	HR	HR	HR	HR	HR
	Software Design Specification	HR	HR	HR	HR	HR
	Software Interface Specification	HR	HR	HR	HR	HR
	Software Integration Test Specification	HR	HR	HR	HR	HR
	Software/Hardware Integration Test Specification	HR	HR	HR	HR	HR
	Software Architecture and Design Verification Report	HR	HR	HR	HR	HR
Component Design	Software Component Design Specification	R	HR	HR	HR	HR
	Software Component Test Specification	R	HR	HR	HR	HR
	Software Component Design Verification Report	R	HR	HR	HR	HR
Component Implementation and Testing	Software Source Code and Supporting Documentation	HR	HR	HR	HR	HR
	Software Component Test Report	R	HR	HR	HR	HR
	Software Source Code Verification Report	HR	HR	HR	HR	HR
Integration	Software Integration Test Report	HR	HR	HR	HR	HR
	Software/Hardware Integration Test Report	HR	HR	HR	HR	HR
	Software Integration Verification Report	HR	HR	HR	HR	HR
Overall Software Testing / Final Validation	Overall Software Test Report	HR	HR	HR	HR	HR
	Overall Software Test Verification Report	HR	HR	HR	HR	HR
	Software Validation Report	HR	HR	HR	HR	HR
	Tools Validation Report	R	HR	HR	HR	HR
	Release Note	HR	HR	HR	HR	HR

자료 : IEC 62279, Railway application Software for railway control and protection systems

다. 안전기법 및 수단

IEC 62279 표준은 <표 6-6>과 같이 각 개발 단계별로 안전 등급에 따른 기법 및 수단들을 제공하고 있다. 안전 등급을 기준으로 안전을 위한 세부 기법 및 활동, 방법론 측면에서 설명하고 있다.

<표 6-6> 소프트웨어 안전 등급에 따른 기법 및 수단 - IEC 62279

항목	Technique / Measure	SIL0	SIL1	SIL2	SIL3	SIL4
Software Reqruiements	Formal Methods	---	R	R	HR	HR
	Modelling	R	R	R	HR	HR
	Structured Methodology	R	R	R	HR	HR
	Decision Tables	R	R	R	HR	HR
Software Architecture	Defensive Programming	---	HR	HR	HR	HR
	Fault Detection & Diagnosis	---	R	R	HR	HR
	Error Correcting Codes	---	---	---	---	---
	Error Detecting Codes	---	R	R	HR	HR
	Failure Assertion Programming	---	R	R	HR	HR
	Safety Bag Techniques	---	R	R	R	R
	Diverse Programming	---	R	R	HR	HR
	Recovery Block	---	R	R	R	R
	Backward Recovery	---	NR	NR	NR	NR
	Forward Recovery	---	NR	NR	NR	NR
	Retry Fault Recovery Mechanisms	---	R	R	R	R
	Memorising Executed Cases	---	R	R	HR	HR
	Artificial Intelligence - Fault Correction	---	NR	NR	NR	NR
	Dynamic Reconfiguraton of Software	---	NR	NR	NR	NR
	Software Error Effect Analysis	---	R	R	HR	HR
	Graceful Degradation	---	R	R	HR	HR
	Information Hiding	---	---	---	---	---
	Information Encapsulation	R	HR	HR	HR	HR
	Fully Defined Interface	HR	HR	HR	M	M
	Formal Methods	---	R	R	HR	HR
	Modelling	R	R	R	HR	HR
	Structured Methodology	R	HR	HR	HR	HR
	Modelling Supported by Computer Aided Design and Specification Tools	R	R	R	HR	HR
Software Design and Implementation	Formal Methods	---	R	R	HR	HR
	Modelling	R	HR	HR	HR	HR
	Structured Methodology	R	HR	HR	HR	HR
	Modular Approach	HR	M	M	M	M
	Components	HR	HR	HR	HR	HR
	Design and Coding Standards	HR	HR	HR	M	M
	Analysable Programs	HR	HR	HR	HR	HR
	Strongly Typed Programming Language	R	HR	HR	HR	HR
	Structured Programming	R	HR	HR	HR	HR
	Programming Language	R	HR	HR	HR	HR
	Language Subset	---	---	---	HR	HR

	Object Oriented Programming	R	R	R	R	R
	Procedural Programming	R	HR	HR	HR	HR
	Metaprogramming	R	R	R	R	R
Verification and Testing	Formal Proof	---	R	R	HR	HR
	Static Analysis	---	HR	HR	HR	HR
	Dynamic Analysis and Testing	---	HR	HR	HR	HR
	Metrics	---	R	R	R	R
	Traceability	R	HR	HR	M	M
	Software Error Effect Analysis	---	R	R	HR	HR
	Test Coverage for Code	R	HR	HR	HR	HR
	Functional / Black-box Testing	HR	HR	HR	M	M
	Performance Testing	---	HR	HR	HR	HR
	Interface Testing	HR	HR	HR	HR	HR
Integration	Functional and Black-box Testing	HR	HR	HR	HR	HR
	Performance Testing	---	R	R	HR	HR
Overall Software Testing	Performance Testing	---	HR	HR	M	M
	Functional and Black-box Testing	HR	HR	HR	M	M
	Modelling	---	R	R	R	R
Software Analysis Techniques	Static Software Analysis	R	HR	HR	HR	HR
	Dynamic Software Analysis	---	R	R	HR	HR
	Cause Consequence Diagrams	R	R	R	R	R
	Evert Tree Analysis	---	R	R	R	R
	Software Error Effect Analysis	---	R	R	HR	HR
Coding Standards	Coding Standard	HR	HR	HR	M	M
	Coding Style Guide	HR	HR	HR	HR	HR
	No Dynamic Objects	---	R	R	HR	HR
	No Dynamic Variables	---	R	R	HR	HR
	Limited Use of Pointers	---	R	R	R	R
	Limited Use of Recursion	---	R	R	HR	HR
	No Unconditional Jumps	---	HR	HR	HR	HR
	Limited size and complexity of Functions, Subroutines and Methods	HR	HR	HR	HR	HR
	Entry/Exit Point strategy for Functions, Subroutines and Methods	R	HR	HR	HR	HR
	Limited number of Subroutines Parameters	R	R	R	R	R
	Limited use of Global Variables	HR	HR	HR	M	M
Dynamic Analysis and Testing	Test Case Execution from Boundary Value Analysis	---	HR	HR	HR	HR
	Test Case Execution from	R	R	R	R	R

	Error Guessing					
	Test Case Execution from Error Seeding	---	R	R	R	R
	Performance Modelling	---	R	R	HR	HR
	Equivelence Classes and Input Partition Testing	R	R	R	HR	HR
	Structure-based Testing	---	R	R	HR	HR
Functional / Black Box Test	Test Case Execution from Cuase Consequence Diagrams	---	---	---	R	R
	Prototyping / Animation	---	---	---	R	R
	Boundary Value Analysis	R	HR	HR	HR	HR
	Equivalence Classes and Input Partition Testing	R	HR	HR	HR	HR
	Process Simulation	R	R	R	R	R
Diagrammatic Language for Application Algorithms	Functional Block Diagrams	R	R	R	R	R
	Sequential Function Charts	---	HR	HR	HR	HR
	Ladder Diagrams	R	R	R	R	R
	State Charts	R	HR	HR	HR	HR
Modeling	Data Modelling	R	R	R	HR	HR
	Data Flow Diagrams	---	R	R	HR	HR
	Control Flow Diagrams	R	R	R	HR	HR
	Finite State Machines or State Transition Diagrams	---	HR	HR	HR	HR
	Time Petri Nets	---	R	R	HR	HR
	Decision / Truth Tables	R	R	R	HR	HR
	Formal Methods	---	R	R	HR	HR
	Performance Modelling	---	R	R	HR	HR
	Prototyping / Animation	---	R	R	R	R
	Structure Diagrams	---	R	R	HR	HR
	Sequence Diagrams	R	HR	HR	HR	HR
Performance Testing	Avalanche / Stress Testing	---	R	R	HR	HR
	Response Timing and Memory Constraints	---	HR	HR	HR	HR
	Performance Requirements	---	HR	HR	HR	HR
Static Analysis	Boundary Value Analysis	---	R	R	HR	HR
	Checklists	---	R	R	R	R
	Control Flow Analysis	---	HR	HR	HR	HR
	Data Flow Analysis	---	HR	HR	HR	HR
	Error Guessing	---	R	R	R	R
	Walkthroughts / Design Reviews	HR	HR	HR	HR	HR
Components	Information Hiding	---	---	---	---	---
	Information Encapsulation	R	HR	HR	HR	HR
	Parameter Number Limit	R	R	R	R	R

	Fully Defined Interface	R	HR	HR	M	M
Test Coverage for Code	Statement	R	HR	HR	HR	HR
	Branch	---	R	R	HR	HR
	Compound Condition	---	R	R	HR	HR
	Data Flow	---	R	R	HR	HR
	Path	---	R	R	HR	HR

자료 : IEC 62279, Railway application Software for railway control and protection systems

3. 시사점

IEC 62279 표준에서는, 소프트웨어 안전등급에 따라 안전활동에 대한 산출물 작성 여부가 구분된다. 명시적으로 활동에 대한 구분을 언급하고 있지는 않지만, 해당 활동의 산출물에 대한 작성 여부를 정의하고 있으므로, 소프트웨어 안전등급에 따른 안전활동의 구분 측면으로 바라볼 수 있다. 하지만 가장 낮은 등급(SIL0)에서 극히 일부 활동 및 산출물이 생략 가능한 것으로, 안전 등급에 따른 차등 적용 수준은 매우 미미한 편이다.

또한, 해당 표준 역시 안전 등급에 따른 안전 기법 및 수단의 차등 적용을 제시하고 있다. IEC 61508 표준을 모 표준으로 하고 있으므로, 개발 단계 별 적용 가능한 안전 기법 및 수단의 종류와 유형이 대부분 동일하다.

제4절 자동차 분야 안전 표준 (ISO 26262)

1. 개요

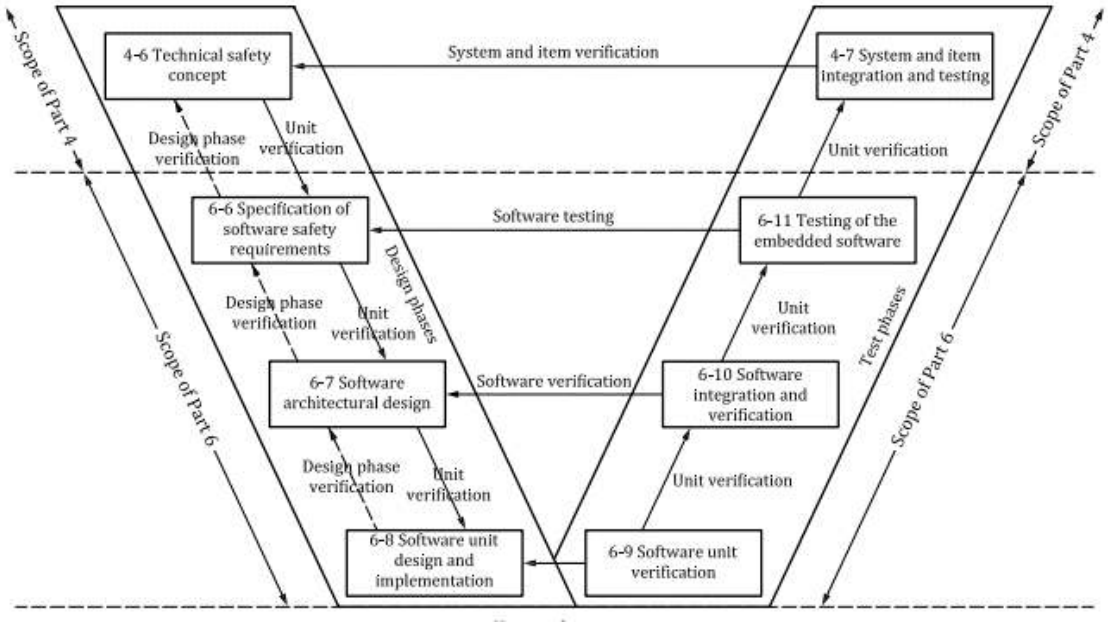
본 절에서는, 자동차 분야 안전 표준인 ISO 26262를 대상으로 안전등급에 따른 안전활동 및 기술을 조사하였다. ISO 26262는 자동차에 내장되는 전기/전자 시스템 안전(Functional Safety)를 위하여, IEC 61508을 근간으로 제정된 표준이다. 해당 표준에서는 위험 상황의 노출 가능성, 위험의 잠재적 심각도, 통제 가능성을 고려하여 차량 무결성 등급(ASIL A ~ D)을 정의하고, 해당 등급에 따라 안전성 목표가 정해지며 활동 및 기술을 설명하고 있다.

2. 안전활동 및 기술 조사

가. 안전활동 적용 절차

ISO 26262 표준의 안전활동 적용 절차는 [그림 6-3]과 같다. 해당 적용 절차는 V 모델 기반의 절차로써, 각 안전 활동 간 주고받는 정보의 흐름을 간략하게 표현하고 있다. 또한, 시스템 개발 프로세스와 소프트웨어 개발 프로세스 사이의 직접적인 관계를 나타내고 있으나, HW 개발 프로세스와의 접점은 독립적으로 구분되어 있다. 마찬가지로 V 모델의 특성에 따라 각 개발 활동에 대응하는 단계별 검증 활동들이 존재하며, 이에 대한 정보의 흐름을 확인할 수 있다.

[그림 6-3] ISO 26262 표준의 안전활동 적용 절차



자료 : ISO 26262, Road vehicles-Functional safety-Part6: Product development as the software level

나. 안전활동

ISO 26262 표준에서 언급되는 안전활동은 다음 <표 6-7>와 같다. 해당 표준에서는 상위 수준의 활동만 언급하고 있으며, 해당 활동의 세부 요구사항에서 세부 활동들을 언급하고 있다. 타 표준에서 언급했던 활동과의 수준을 비슷한 수준으로 유지하기 위하여, 해당 표준에서는 상위 수준 활동의 목표 및 세부 요구사항을 기반으로 하위 활동을 식별하였다. 또한, IEC 61508 표준과 마찬가지로, 소프트웨어 요구사항 단계에서의 활동에만 'Safety'가 언급되어 있다. 이후 하위 활동에서는 별도 'Safety'라는

단어가 명시적으로 표현되어 있지 않지만, 정의된 안전 요구사항에 따른 설계 및 검증 활동에 해당하므로 안전에 대한 내용을 포함하고 있다고 볼 수 있다.

<표 6-7> ISO 26262 표준의 안전활동

단계	상위수준 활동	세부 활동
Requirements	Specification of software safety requirements	Specify or refine the software safety requirements
		Define the safety related functionalities and properties
		Refine the requirements of the hardware software interface
		Verify the software safety requirements
Design & Implement	Software architectural design	Develop the software architectural design
		Verify the software architectural design
		Support the implementation and verification of the software
	Software unit design and implementation	Develop the software unit design
		Implement the software units
V&V	Software Unit Verification	Verify implemented software units
	Software integration and verification	Define integration steps and integrate the softwate elements
		Verify integrated software unit and components
	Testing of the embedded software	Provide evidence that the embedded software fulfiles the safety related requirements

자료 : ISO 26262, Road vehicles-Functional safety-Part6: Product development as the software level

다. 안전기법 및 수단

ISO 26262 표준은 <표 6-8>와 같이 각 개발 단계별로 안전 등급에 따른 기법 및 수

단들을 제공하고 있다. 해당 표준은 IEC 61508 표준과 IEC 62279 표준과는 달리 안전 등급을 기준으로 각 개발 단계별 안전 기법 및 수단을 표기법, 설계 원칙, 방법론 측면으로 구분하여 설명하고 있다.

<표 6-8> 소프트웨어 안전 등급에 따른 표기법 - ISO 26262

항목	Notation	ASIL A	ASIL B	ASIL C	ASIL D
Specification of software safety requirements	Informal notations	++	++	+	+
	Semi-formal notations	+	+	++	++
	Formal notations	+	+	+	+
Software architectural design	Natural language	++	++	++	++
	Informal notations	++	++	+	+
	Semi-formal notations	+	+	++	++
	Formal notations	+	+	+	+
Software unit design and implementation	Natural language	++	++	++	++
	Informal notations	++	++	+	+
	Semi-formal notations	+	+	++	++
	Formal notations	+	+	+	+

자료 : ISO 26262, Road vehicles-Functional safety-Part6: Product development as the software level

<표 6-9> 소프트웨어 안전 등급에 따른 설계원칙 - ISO 26262

항목	Design Principle	ASIL A	ASIL B	ASIL C	ASIL D
Software architectureal design	Appropriate hierarchical structure of the software components	++	++	++	++
	Restricted size and complexity of software components	++	++	++	++
	Restricted size of interfaces	+	+	+	++
	Strong cohesion within each software component	+	++	++	++
	Loose coupling between software components	+	++	++	++
	Appropriate scheduling properties	++	++	++	++
	Restricted use of interrupts	+	+	+	++
	Appropriate spatial isolation of the software components	+	+	+	++
	Appropriate management of shared resources	++	++	++	++
Software unit design and implementation - Design Principle	One entry and one exit point in subprograms and functions	++	++	++	++
	No dynamic objects or variables, or else online test during their creation	+	++	++	++

	Initialization of variables	++	++	++	++
	No multiple use of variable names	++	++	++	++
	Avoid global variables or else justify their usage	+	+	++	++
	Restricted use of pointers	+	++	++	++
	No implicit type conversions	+	++	++	++
	No hidden data flow or control flow	+	++	++	++
	No unconditional jumps	++	++	++	++
	No recursions	+	+	++	++

자료 : ISO 26262, Road vehicles-Functional safety-Part6: Product development as the software level

<표 6-10> 소프트웨어 안전 등급에 따른 방법 - ISO 26262

항목	Methods	ASIL A	ASIL B	ASIL C	ASIL D
Software safety requirements verificaton	Verification by walk-through	++	+	o	o
	Verification by inspection	+	++	++	++
	Semi-formal verification	+	+	++	++
	Formal verification	o	+	+	+
Software architectureal design verification	Walk-through of the design	++	+	o	o
	Inspection of the design	+	++	++	++
	Simulation of dynamic behaviour of the design	+	+	+	++
	Prototype generation	o	o	+	++
	Formal verification	o	o	+	+
	Control flow analysis	+	+	++	++
	Data flow analysis	+	+	++	++
	Scheduling analysis	+	+	++	++
Software unit verification	Walk-through	++	+	o	o
	Pair-programming	+	+	+	+
	Inspection	+	++	++	++
	Semi-formal verification	+	+	++	++
	Formal verification	o	o	+	+
	Control flow analysis	+	+	++	++
	Data flow analysis	+	+	++	++
	Static code analysis	++	++	++	++
	Static analyses based on abstract interpretation	+	+	+	+
	Requirements-based test	++	++	++	++
	Interface test	++	++	++	++
	Fault injection test	+	+	+	++
	Resource usage evaluation	+	+	+	++
	Back-to-back comparison test between model and code, if applicable	+	+	++	++
	Analysis of requirements	++	++	++	++
	Generation and analysis of equivalence classes	+	++	++	++
	Analysis of boundary values	+	++	++	++

	Error guessing based on knowledge or experience	+	+	+	+
	Statement coverage	++	++	+	+
	Branch coverage	+	++	++	++
	MC/DC (Modified Condition/Decision Coverage)	+	+	+	++
Software integration and verification	Requirements-based test	++	++	++	++
	Interface test	++	++	++	++
	Fault injection test	+	+	++	++
	Resource usage test	++	++	++	++
	Back-to-back comparison test between model and code, if applicable	+	+	++	++
	Verification of the control flow and data flow	+	+	++	++
	Static code analysis	++	++	++	++
	Static analyses based on abstract interpretation	+	+	+	+
	Analysis of requirements	++	++	++	++
	Generation and analysis of equivalence classes	+	++	++	++
	Analysis of boundary values	+	++	++	++
	Error guessing based on knowledge or experience	+	+	+	+
	Function coverage	+	+	++	++
	Call coverage	+	+	++	++
Testing of the embedded software	Hardware-in-the-loop	++	++	++	++
	Electronic control unit network environments	++	++	++	++
	Vehicles	+	+	++	++
	Requirements-based test	++	++	++	++
	Fault injection test	+	+	+	++
	Analysis of requirements	++	++	++	++
	Generation and analysis of equivalence classes	+	++	++	++
	Analysis of boundary values	+	+	++	++
	Error guessing based on knowledge or experience	+	+	++	++
	Analysis of functional dependencies	+	+	++	++
	Analysis of operational use cases	+	++	++	++

자료 : ISO 26262, Road vehicles-Functional safety-Part6: Product development as the software level

3. 시사점

ISO 26262 표준은 IEC61508 표준을 모 표준으로 하고 있다. 소프트웨어 안전등급에 따른 안전활동의 구분이 별도 존재하지 않으며, 소프트웨어 요구사항 정의 단계에서만

‘Safety’ 가 언급되고 있다. 이후 하위 활동은 안전 요구사항에 따른 설계 및 검증 활동이며, 이는 해당 표준에서 언급하고 있는 활동은 일반 소프트웨어 개발 활동을 모두 포함하고 있는 형태임을 의미한다.

안전 특화된 활동을 언급하고 있는 것이 아니기에, 등급에 따른 활동의 구분은 없지만 안전등급에 따른 안전기법 및 수단의 차등 적용을 제시하고 있다. IEC 61508 및 IEC 62279 표준에서 언급하고 있는 안전기법 및 수단에 비해 보다 일반적인 기술 측면으로 다루고 있으며, 표기법 및 설계 원칙, 방법론 측면에서 설명하고 있다.

제5절 항공 분야 안전 표준

1. 개요

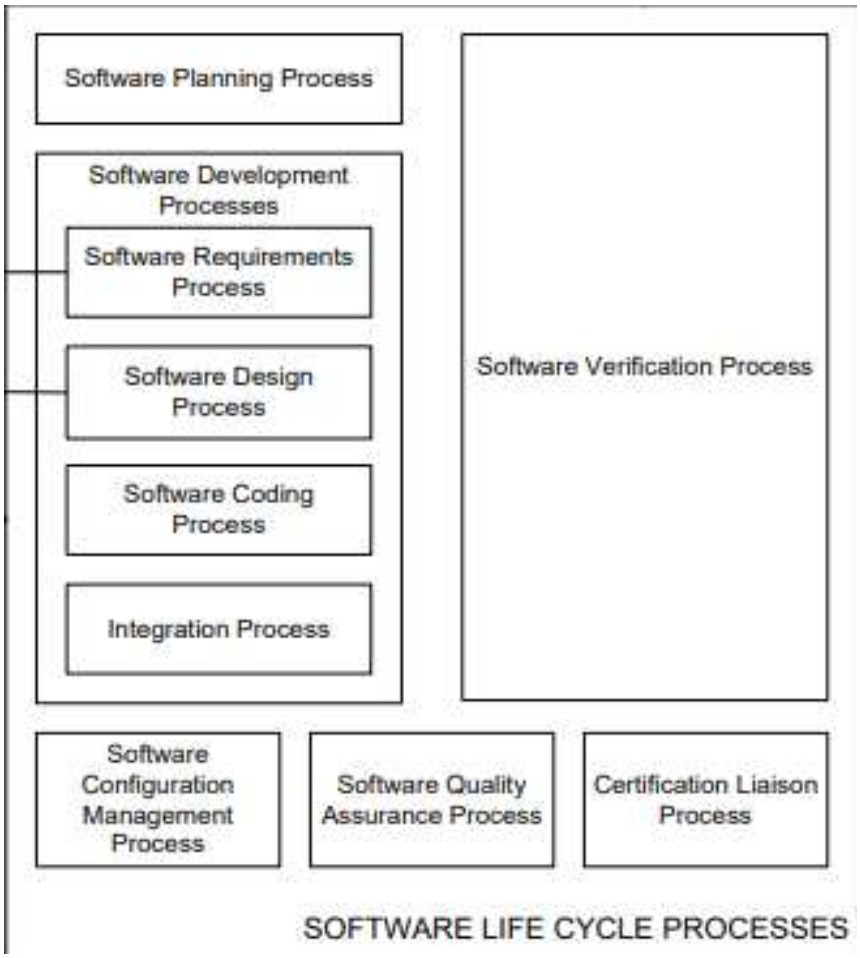
본 절에서는, 항공 분야 안전 표준인 DO-178C를 대상으로 안전등급에 따른 안전활동 및 기술을 조사하였다. DO-178C 표준은 항공기와 항공기 엔진, 보조 파워 장비, 프로펠러 등과 같은 항공용 시스템 및 장비에 활용되는 소프트웨어 인증 표준으로써, 소프트웨어 항공 환경에서 신뢰할 수 있는 수준으로 수행 가능한지 확인하기 위한 가이드이다. 해당 표준에서는 안전등급을 A~D 등급으로 구분하여 정의하고, 각 등급에 따른 소프트웨어 개발 및 안전활동을 설명하고 있다.

2. 안전활동 및 기술 조사

가. 안전활동 적용 절차

DO-178C 표준의 안전활동 적용 절차는 [그림 6-4]과 같다. 타 표준과들과 유사한 수준의 안전활동 적용 절차가 구성되어 있으나, 검증 활동의 경우, 하나의 Software Verification Process에 모두 대응되도록 표현하고 있다.

[그림 6-4] DO-178C 표준의 안전활동 적용 절차



자료 : DO-178C, Software Consideration in Airborne Systems and Equipment Certification

나. 안전활동

DO-178C 표준에서 언급되는 안전활동은 다음 <표 6-11>과 같다. 해당 표준의 안전활동은 타 표준과는 다르게 하나의 태스크 수준으로 활동을 표현하고 있는 것이 아니라, 각 활동을 수행하면서 달성되어야 하는 요건 측면에서 정의하고 있으며, 검토 및 검증 활동의 경우 소프트웨어 verification 활동으로 모두 대응되도록 표현하고 있다.

또한, 해당 표준에서는 소프트웨어 안전등급 별 관리 방안의 차이를 활동의 수행 유무와 검토 및 검증 활동 수행의 독립성 수준 차이로 구분하고 있다. 검토 및 검증 활동의 독립성 수준은 두 가지 유형으로 구분되며, 소프트웨어 안전등급이 높을수록 개발 활동을 수행한 당사자 외 제 3자가 검토 및 검증 활동을 수행하도록 권고하고 있다. <표 6-11>에서, O의 경우 활동 수행의 독립성이 고려되지 않아도 되는 것을 의미

하며, ●의 경우, 활동 수행 시 독립성이 보장되어야 함을 의미하고 있다.

이외, 소프트웨어 안전등급에 따른 안전기법 및 수단은 별도 정리되어 있지 않다.

<표 6-11> 소프트웨어 안전 등급에 따른 활동 - DO-178C

상위수준 활동	세부 활동	A	B	C	D
소프트웨어 Requirements	High-level requirements are developed	○	○	○	○
	Derived high-level requirements and desfined and provided to the system processes, including the system safety assessment process	○	○	○	○
소프트웨어 Design	Software architecture is developed	○	○	○	○
	Low-level requirements are development	○	○	○	
	Derived low-level requirements are defined and provided to the system processes including the system safety assessment process	○	○	○	
소프트웨어 Implement	Source code is developed	○	○	○	
	Executable object code and parameter data item files, if any, are produced and loaded in the target computer	○	○	○	○
소프트웨어 Requirements Verification	High-level requirements comply with system requirements	●	●	○	○
	High-level requirements are accurate and consistent	●	●	○	○
	High-level requirements are compatible with target computer	○	○		
	High-level requirements are verifiable	○	○	○	
	High-level requirements conform to standards	○	○	○	
	High-level requirements traceable to system requirements	○	○	○	○
	Algorithms are accurate	●	●	○	
소프트웨어 Design Verification	Low-level requirements comply with high-level requirements	●	●	○	
	Low-level requirements are accurate and consistent	●	●	○	
	Low-level requirements are compatible with target computer	○	○		
	Low-level requirements are verifiable	○	○		
	Low-level requirements conform to standards	○	○	○	
	Low-level requirements are traceable to high-level requirements	○	○	○	

	Algorithms are accurate	●	●	○	
	Software architecture is compatible with high-level requirements	●	○	○	
	Software architecture is consistent	●	○	○	
	Software architecture is compatible with target computer	○	○		
	Software architecture is verifiable	○	○		
	Software architecture conforms to standards	○	○	○	
	Software partitioning integrity is confirmed	●	○	○	○
소프트웨어 Unit Verification	Source code complies with low-level requirements	●	●	○	
	Source code complies with software architecture	●	○	○	
	Source code is verifiable	○	○		
	Source code conforms to standards	○	○	○	
	Source code is traceable to low-level requirements	○	○	○	
	Source code is accurate and consistent	●	○	○	
	Output of software integration process is complete and correct	○	○	○	
	Parameter data item file is correct and complete	●	●	○	○
	Verification of parameter data item file is achieved	●	●	○	
소프트웨어 Test	Executable object code complies with high-level requirements	○	○	○	○
	Executable object code is robust with high-level requirements	○	○	○	○
	Executable object code complies with low-level requirements	●	●	○	
	Executable object code is robust with low-level requirements	●	○	○	
	Executable object code is compatible with target computer	○	○	○	○
Verification of verificatio process result	Test procedures are correct	●	○	○	
	Test result are correct and discrepancies explained	●	○	○	
	Test coverage of high-level requirements is achieved	●	○	○	○
	Test coverage of low-level requirements is achieved	●	○	○	
	Test coverage of software structure(MC/DC) is achieved	●			

자료 : DO-178C, Software Consideration in Airborne Systems and Equipment Certification

3. 시사점

항공 분야 안전 표준인 DO-178C에서는 소프트웨어 안전등급에 따라 개발 및 검증 활동의 수행 여부에 차이를 두어 관리방안을 적용한다. 개발 활동에 대한 안전등급 별 활동의 차등 적용 수준은 미미한 편이지만, 검토 및 검증 활동에 대한 안전등급 별 활동의 차등 적용 수준은 보다 명확하다. 또한, 검토 및 검증 활동의 독립성 수준을 구분하여 관리방안의 차이를 두고 있다. 기타 많은 표준에서도 안전등급에 따른 활동의 독립성 측면이 많이 거론되고 있으며, 독립성 수준을 어떻게 구분하느냐도 하나의 주요 논의점 중 하나이다.

제6절 의료 분야 안전 표준

1. 개요

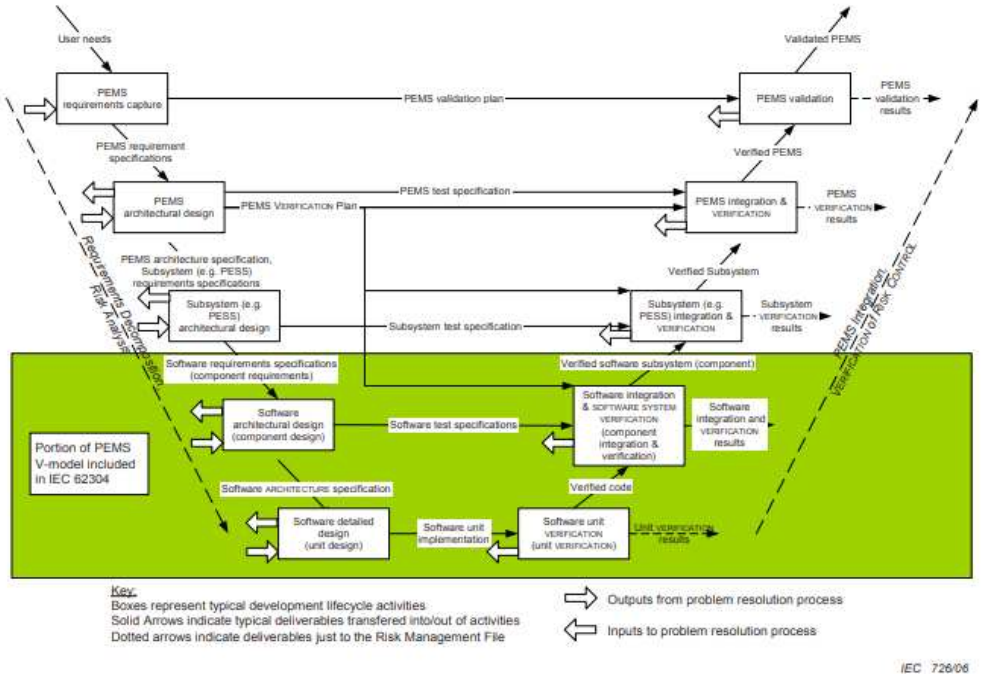
본 절에서는, 의료 분야 안전 표준인 IEC 62304를 대상으로 안전등급에 따른 안전활동 및 기술을 조사하였다. IEC 62304 표준은 의료기기 소프트웨어 개발을 위한 생명주기 프로세스를 정의하고 있는 표준으로써, 의료기기 소프트웨어의 안전 설계 및 유지관리를 위해 수행되어야 하는 활동 및 작업을 포함하고 있다. 해당 표준에서는 안전등급을 Class A ~ C 등급으로 구분하여 정의하고, 각 등급에 따른 소프트웨어 개발 및 안전활동을 설명하고 있다.

2. 안전활동 및 기술 조사

가. 안전활동 적용 절차

IEC 62304 표준의 안전활동 적용 절차는 [그림 6-5]와 같다. 해당 절차는 PEMS 개발을 대상으로 IEC 62304를 적용할 때 사용할 수 있는 절차로써, V 모델을 기반으로 한다. V 모델의 특성에 따라 각 개발 활동에 대응하는 단계별 검증 활동들이 존재하며, 이에 대한 정보의 흐름을 확인할 수 있다.

[그림 6-5] IEC 62304 표준 안전활동 적용 절차



자료 : IEC 62304, Medical device software-Software life-cycle processes

나. 안전활동

IEC 62304 표준에서 언급되는 안전활동은 다음 <표 6-12>와 같다. 해당 표준에서는 소프트웨어 안전만을 고려한 활동이 아닌 일반적인 개발 활동과 구분 없이 설명하고 있다. 또한, 요구사항 및 설계 단계에서 소프트웨어의 위험 기여도를 판단하고, 해당 기여도에 따른 사례에 대하여 위험 관리 조치를 정의하는 안전 활동이 별도 포함되어 있다. 소프트웨어 안전등급에 따라 안전활동의 수행 여부에 차이를 둔 관리방안을 제시하고 있으며, 소프트웨어 안전등급에 따른 안전기법 및 수단은 별도 정리되어 있지 않다.

<표 6-12> 소프트웨어 안전 등급에 따른 활동 - IEC 62304

상위수준 활동	세부 활동	Class A	Class B	Class C
Software requirements analysis	Define and document software requirements from system requirements	O	O	O
	Software requirements content	O	O	O
	Include risk control measures in software		O	O

	requirements			
	Re-evaluate medical device risk analysis	O	O	O
	Update requirements	O	O	O
	Verify software requirements	O	O	O
Software architectural design	Transform software requirements into an architecture		O	O
	Develop an architecture for the interfaces of software items		O	O
	Specify functional and performance requirements of soup item		O	O
	Specify system hardware and software required by soup item		O	O
	Identify segregation necessary for risk control			O
	Verify software architecture		O	O
Software detailed design	Subdivide software into software units		O	O
	Develop detailed design for each software unit			O
	Develop detailed design for interfaces			O
	Verify detailed design			O
Software unit implementation	Implement each software unit	O	O	O
	Establish software unit verification process		O	O
	Software unit acceptance criteria		O	O
	Additional software unit acceptance criteria			O
	Software unit verification		O	O
Software integration and integration testing	Integrate software units		O	O
	Verify software integration		O	O
	Software integration testing		O	O
	Software integration testing content		O	O
	Evaluate software integration test procedures		O	O
	Conduct regression tests		O	O
	Integraiton test record contents		O	O
	Use software problem resolution process		O	O
Software system testing	Establish tests for software requirements	O	O	O
	Use software problem resolution process	O	O	O
	Retest after changes	O	O	O
	Evaluate software system testing	O	O	O
	Software system test record contents	O	O	O

자료 : IEC 62304, Medical device software-Software life-cycle processes

3. 시사점

IEC 62304 표준에서는 소프트웨어 안전등급에 따라 개발활동의 수행 여부에 차이를 두어 관리방안을 적용한다. 타 표준에 비해 소프트웨어 안전등급에 따른 활동의 차등 적용 수준이 명확하게 구분된다.

제7절 항공우주 분야 안전 표준

1. 개요

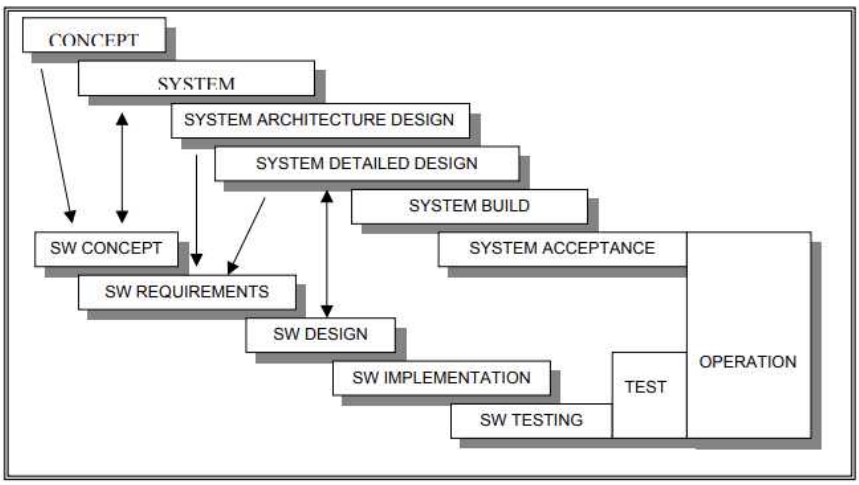
본 절에서는, 항공우주 분야 안전 표준인 NASA-STD-8719-13C와 해당 표준에 대한 가이드 NASA-GB-8719-13C를 대상으로 안전등급에 따른 안전활동 및 기술을 조사하였다. NASA-STD-8719-13C 표준에서는 소프트웨어 개발 시 안전을 고려하여 개발할 수 있도록 고안한 정규 표준으로 소프트웨어 안전분류 도출을 위해 위험 심각도 및 소프트웨어 통제 등급 정보 활용을 제안한다. NASA-GB-8719-13C 가이드는 소프트웨어 안전 분류에 관한 지침 뿐만 아니라 안전 분류에 따라 적절한 수준으로 수행되어야 하는 안전 활동에 대한 내용도 포함하고 있다.

2. 안전활동 및 기술 조사

가. 안전활동 적용 절차

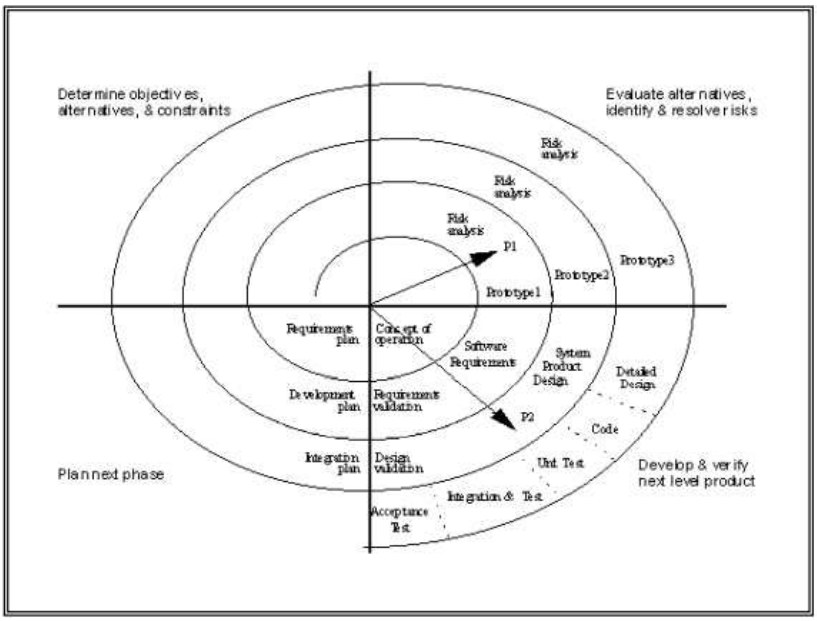
해당 표준에서는 특정 안전활동 적용 절차를 권고하지 않는다. Waterfall Lifecycle Model, Rapid Prototyping, Spiral Model, Incremental Development Lifecycle 등 주요 소프트웨어 개발 모델에 대하여 설명하고 있으며, 개발 특성 및 프로젝트 상황에 따라 적절한 안전활동 적용 절차를 사용할 수 있도록 권고하고 있다.

[그림 6-6] Waterfall Lifecycle Model



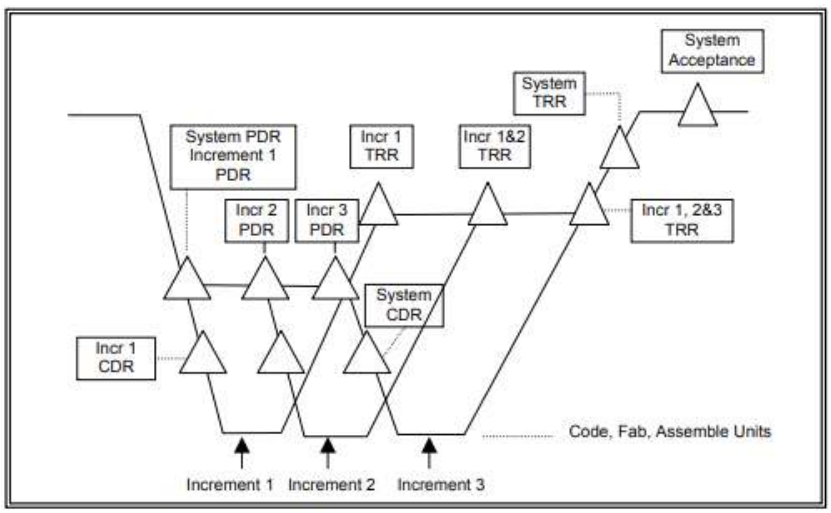
자료 : NASA-GB-8719-13C, NASA Software Safety Guidebook

[그림 6-7] Spiral Lifecycle Model



자료 : NASA-GB-8719-13C, NASA Software Safety Guidebook

[그림 6-8] Incremental Development Lifecycle Model



자료 : NASA-GB-8719-13C, NASA Software Safety Guidebook

나. 안전활동

NASA-STD-8719-13C 표준에서 언급하고 있는 안전활동은 다음 <표 6-13>과 같다. 해당 표준에서는 상위 수준에서의 안전 활동만을 언급하고 있으며, 일반 개발 활동과는 구분된 안전 특화된 활동만을 언급하고 있다.

<표 6-13> 소프트웨어 안전 등급에 따른 활동 - NASA-STD

단계	상위수준 활동	세부 활동
Requirements	Software Safety Requirements Determination and Analysis	Software Safety Requirements Determination
		Software Safety Requirements Analysis
Design	Software Safety Design and Analysis	-
Implementation	Software Safety Implementation and Analysis	-
Overall	Software Safety Verification & Validtion	-
V&V	Verification and Validation by Test	-

자료 : NASA-STD-8719-13C, NASA Software Safety Standard

NASA-GB-8719-13C 가이드에서 언급하고 있는 안전활동은 다음 <표 6-14>과 같다. 해당 가이드북에서는 Software Engineering Task와 System and Software Safety Task, Software Assurance or IV & V Task로 구분하여 일반 소프트웨어 개발 활동 및 안전 활동을 언급하고 있다. Software Assurance or IV & V Task에서는 Independent Verification & Verification 활동을 포함하고 있으며, 해당 표준 및 가이드에서는 안전 등급에 따른 검토 활동의 독립성 수준 보장을 중요시하고 있으나 구체적인 방안을 제시하고 있지는 않다.

<표 6-14> 소프트웨어 안전 등급에 따른 활동 - NASA-GB

단계	Software Engineering Tasks	System and Software Safety Tasks	Software Assurance or IV & V Tasks
Requirements	Software requirements development	Development of software safety requirements	Formal methods for verification
	Requirements management	Safety requirements flowdown analysis	Model checking
	Formal methods for specification	Requirements criticality analysis	Formal inspections of software requirements
	Formal inspections of software requirements	Specification analysis of safety critical requirements	Specification analysis
	System test planning	Software fault tree analysis	Timing, throughput and sizing analysis

	Timing, throughput and sizing considerations	Software failure modes and effects analysis	-
	-	Formal inspections of software requirements	-
	-	Develop safety package for phase 0/1 safety review or other external safety review	-
Design	Create design from requirements, incorporating safety requirements and features	Trace safety-critical requirements into the design	Reviewselection of language, OS, and tools. Passanysafetyconcernst osoftwaresafety.
	Formal inspection of design products	Update criticality analysis	ReviewCOTS and reused software. Passanysafetyconcernst osoftwaresafety.
	Design for reliability and maintainability	Formal inspection of design products	Reviewcoding standards and checklists for inclusion of good practices and exclusion of unsafe functions or practices.
	Select language, operating system and tools	Hazard risk assessment	Reviewcomplexity measurements. Workwithdeveloperiftoo high.
	Select COTS and reusable components	Design safety analysis	Reviewreliability and maintainability metrics.
	Develop language restrictions and coding standards	Software element analysis	Formal inspection of design products
Implementation	Create source code that implements the design, including safety features.	Participate in Source code Formal Inspections of safety-critical code.	Participate in Source code Formal Inspections
	Perform unit testing on individual source units. Prepare and follow test procedures for safety-critical units.	Review Analyses from Software Assurance for any safety implications.	Verify unit tests adequately test the software and are actually performed.
	Maintain source code within a Configuration	Verify that safety-critical software	Witness any formal unit testing.

	Management system, with adequate documentation of changes.	is designated as such, and that it will receive special treatment by theprogrammers.	
	Follow coding standards and checklists.	Review unit test plans and results for safety-critical units.	Review previous analyses and update with new information.
	Participate in Formal Inspections and informal code reviews.	Review previous analyses and update with new information.	Audit software configuration management system to verify proper usage.
	Follow formal change process for changes to baselined system.	Program Slicing for safety-critical variables or data.	Audit software development to verify processes followed and coding standards used.
	Program Slicing for debugging.	Safety Data Package for Phase III Safety Review	Participate in formal change process (change control board)
	Test Coverage Analysis	-	Audit software change process.
	-	-	Code logic analysis
	-	-	Code data analysis
	-	-	Code interface analysis
	-	-	Unused code analysis
	-	-	Program slicing
	-	-	Interrupt analysis
V&V	Integrate individual software units into a complete software system. Test throughout the process.	Participate in Test Plan and Procedures Formal Inspections when safety-critical functions are to be tested.	Participate in Formal Inspections of test plans and procedures.
	Integrate the software with the hardware system and perform testing throughout the process.	Review Analyses from Software Assurance for any safety implications.	Analyze test reports for completeness and requirements coverage.
	Create and follow written test procedures for integration and system testing.*	Verify all safety requirements have been adequately tested (Safety Verification Matrix).	Verify all requirements have been adequately tested.
	Perform regression	Witness testing of	Review problem

	testing after each change to the system.*	safety critical software and special safety tests.	reports
	Participate in Formal Inspections of test plans and procedures.	Review problem reports for safety implications.	Witness all integration tests, or at least those involving safety-critical units.
	Prepare Test Report upon completion of a test.	Reliability Modeling	Witness all system tests.
	Verify COTS software operates as expected.	Review previous analyses and update with new information.	Review previous analyses and update with new information.
	Use formal Configuration Management system for sourcecode,executables, testplansandprocedures, andtestdata.	Safety Verification Tracking Log Closeout	-
	Follow problem reporting and corrective action procedures when defects are detected.	-	-

자료 : NASA-GB-8719-13C, NASA Software Safety Guidebook

다. 안전기법 및 수단

NASA-STD-8719-13C 표준에서는 <표 6-15>와 같이 각 개발 단계별로 안전등급에 따른 기법 및 수단. 해당 표준에서는 타 표준과는 다르게 안전활동도 안전등급에 따른 기법 및 수단을 정의한 테이블에 포함하여 설명하고 있다. 해당 안전활동은 상위수준에 정의된 안전활동을 근간으로 특정 기법 및 수단의 활용 측면으로 정리되어 있다.

<표 6-15> 소프트웨어 안전 등급에 따른 안전기법 및 수단 - NASA-STD-8719-13C

항목	Technique or Analysis	MIN	MOD	FULL
Software Safety	Peliminary Hazard Analysis (PHA)	M	M	M

Effort for Conception Phase	Software Subsystem Hazard Analysis	M	M	M
	Software Safety Requirements	M	M	M
	Checklist and Cross References	HR	HR	M
Software Safety Effort for Requirements Phase	Preliminary Hazard Analysis (PHA) (if not previously performed)	M	M	M
	Software Subsystem Hazard Analysis (if not previously performed)	M	M	M
	Software Safety Requirements Development			
	Generic Requirements	HR	HR	HR
	Fault and Failure Tolerance	HR	HR	M
	Hazardous Commands	M	M	M
	Requirements Management	M	M	M
	Formal Inspections	R	M	M
	Software Safety Requirements Flow-down Analysis	HR	M	M
	Requirements Criticality Analysis	R	HR	M
	Specification Analysis	NR	R	HR
	Formal Methods	NR	HR	HR
	Model Checking	NR	HR	HR
	Timing, Throughput, and Sizing			
	Development Considerations	HR	M	M
	Analysis	HR	M	M
	Software Fault Tree Analysis	R	HR	M
	Software Failure Modes and Effects Analysis	NR	R	HR
Software Safety Effort for Software Design Phase	Language Restrictions and Coding Standards	M	M	M
	Defensive Programming	HR	M	M
	Criticality Analysis	HR	M	M
	Hazard Risk Assessment			
	Design Safety Analysis	HR	M	M
	Independence Analysis	R	HR	M
	Formal Inspections of Design Products	R	HR	M
	Formal Methods and Model Checking	NR	R	HR
	Data Logic Analysis	NR	R	M
	Design Data Analysis	R	HR	M
	Design Interface Analysis	R	HR	M
	Design Traceability Analysis	M	M	M
	Software Element Analysis	R	HR	M
	Rate Monotonic Analysis	NR	R	HR
	Dynamic Flowgraph Analysis	NR	NR	R
	Markov Modeling	NR	R	HR
	Requirements State Machines	NR	R	HR
Software Safety Effort for Implementation Phase	Coding Checklists and Standards	M	M	M
	Unit Testing (Mandatory for safety-critical units)	HR	HR	M
	Safety Critical Unit Test Plans			
	Program Slicing of Safety Critical Data	R	R	HR
	Code Logic Analysis	NR	NR	R
	Code Data Analysis	R	HR	M
	Code Interface Analysis	R	HR	M
	Unused Code Analysis	R	HR	M

	Interrupt Analysis	R	HR	M
	Test Coverage Analysis	R	M	M
	Formal Isnpections of Source Code	HR	M	M
	Final Timing, Throught, and Sizing Analysis	HR	M	M
Software Safety Effort for Testing Phase	Integration Testing	R	HR	M
	System & Functional Testing (Number of tests is tailorable)	M	M	M
	Regression Testing (amount of testing is tailorable)	M	M	M
	Software Safety Testing	M	M	M
	OTS Analyses and Test	R	HR	M
	Test Coverage Analysis	R	HR	M
	Formal Inspections of Test Plan and Procedures	R	HR	M
	Reliability Modeling	NR	R	HR
	Test Results Analysis	M	M	M
Software Safety Effort for Testing Phase - Dynamic Testing(Unit or Integration Level)	Typical sets of sensor inputs	HR	M	M
	Test specific functions	HR	M	M
	Volumetric and statistical tests	NR	R	HR
	Test extreme values of inputs	HR	M	M
	Test all modes of each sensor	HR	M	M
	Every statement executed once	HR	M	M
	Every branch tested at least once	HR	M	M
	Every predicate term tested	R	HR	M
	Every loop executed 0, 1, many, max - 1, max, max + 1 times	HR	M	M
	Every path executed	R	HR	M
	Every assignment to memory tested	NR	R	HR
	Every reference to memory tested	NR	R	HR
	All mappings from inputs checked	NR	R	HR
	All timing constraints verified	R	HR	M
	Test worst case interrupt sequences	R	HR	M
	Test significant chains of interrupts	R	HR	M
	Test Positioning of data in I/O space	R	HR	M
	Check accuracy of arithmetic	NR	R	HR
	All components executed at least once	M	M	M
	All invocations of components tested	HR	M	M
Software Safety Effort for Testing Phase - Dynamic Testing(Software System Testing)	Simulation (Test Environment)	R	HR	M
	Load Testing	HR	M	M
	Stress Testing	HR	M	M
	Boundary Value Tests	R	HR	M
	Test Coverage Analysis	R	HR	M
	Functional Testing	M	M	M
	Performance Monitoring	R	HR	M
	Disaster Testing	R	HR	HR
	Resistance to Failure Testing	R	HR	M
	“Red Team“ Testing	NR	R	HR
	Regression Testing (Tailored to the level of original testing)	M	M	M

자료 : NASA-GB-8719-13C, NASA Software Safety Guidebook

3. 시사점

NASA-STD-8719-13C 표준 및 NASA-GB-8719-13C 가이드에서는 안전등급에 따라 안전활동(분석활동 측면) 수행 여부에 차이를 두었으며, 적용 가능한 안전기법 및 수단을 구분하여 관리방안을 적용한다. 타 표준에 비해 안전등급에 따른 안전활동의 구분이 명확한 편이며, 검토 및 검증 활동에 대한 독립성 수준을 언급하고 있으나 구체적인 방안을 제시하고 있지는 않고 있다.

또한, NASA-STD-8719-13C 표준에서는 각 단계별 'Safety' 활동을 정의하고 있다. 일반적인 소프트웨어 개발활동은 기본으로 수행된다는 가정하에 안전 특화된 활동을 언급하고 있다. NASA-GB-8719-13C 표준에서는 일반적인 소프트웨어 개발 활동과 안전 특화된 활동, 검증 및 검토 관련 활동으로 구분 지어 설명하고 있으며, 타 표준에 비해 보다 상세한 수준의 활동을 제공하고 있다. 상세한 수준의 활동은 기법 및 방법론적인 측면이 강하므로, 타 표준과의 비교를 위해 보다 상위 수준의 활동으로 추상화할 필요가 있다.

제8절 국방 분야 안전 표준

1. 개요

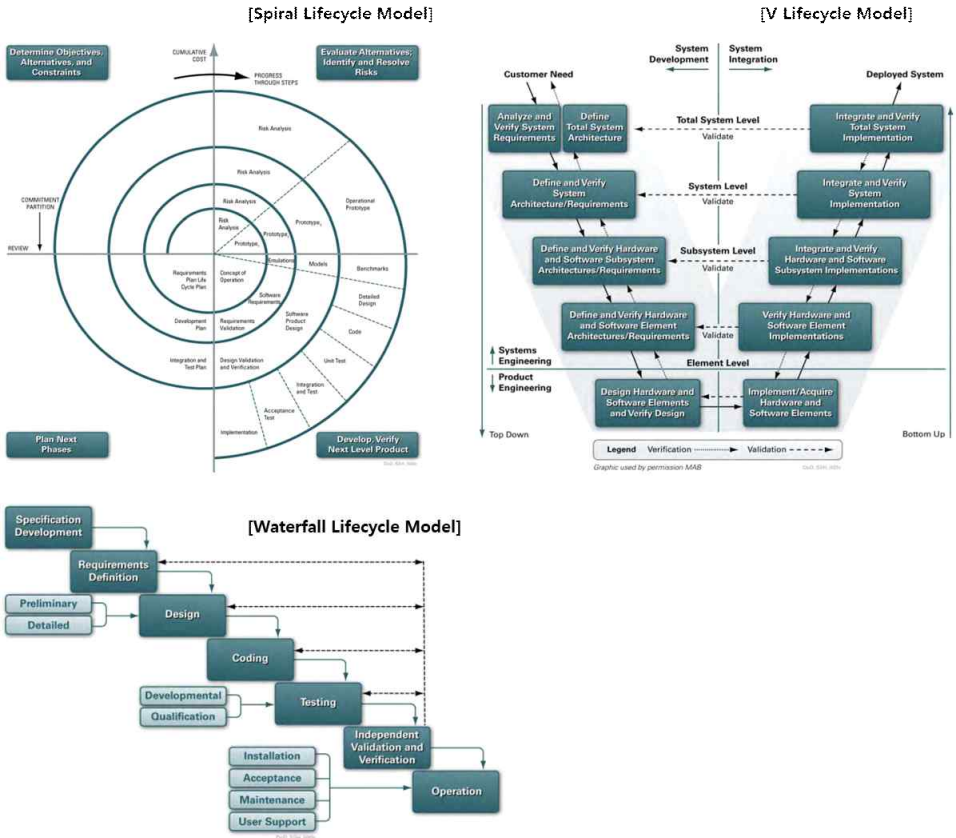
본 절에서는, 국방 분야 안전 표준인 MIL-STD-882E와 해당 표준에 대한 가이드인 Joint 소프트웨어 System-Safety Engineering Handbook을 대상으로 안전등급에 따른 안전활동 및 기술을 조사하였다. MIL-STD-882E는 미국 국방부 사한의 모든 군사부서 및 국방기관에서 사용이 승인된 안전 표준이다. 해당 표준에서는 위험에 대한 식별 및 분류, 회피에 대한 일반적인 방안을 제시하고 있다. MIL-STD-882E 표준에서는 NASA 표준과 동일하게 위험 심각도 및 통제 등급 정보를 활용한 소프트웨어 안전분석 및 안전등급 분류 방안을 주로 제시하고 있다. 안전활동의 경우 Level of Rigor 제공을 통해 최소한의 활동만을 언급하고 있다.

2. 안전활동 및 기술 조사

가. 안전활동 적용 절차

NASA 표준과 마찬가지로, 특정 안전활동 적용 절차를 권하고 있지 않다. Waterfall Model, V Lifecycle Model, Spiral Lifecycle Model, Object-Oriended Analysis and Design, Component-Oriented and Package-Oriented Design 등의 적용 가능한 다양한 모델 및 예시를 제공하고 있으며, 개발 특성 및 프로젝트 상황에 따라 적절한 안전활동 적용 절차를 사용할 수 있도록 권고하고 있다.

[그림 6-9] 다양한 안전활동 적용 절차 예시



자료 : Joint-소프트웨어-Systems-Safety-Engineering-Handbook

나. 안전활동

해당 표준에서는 타 안전 표준과는 달리 필수적으로 수행해야 한다는 의미로 등급별 활동이나 기법 및 수단을 제시하고 있지 않다. 소프트웨어 안전분석 및 안전등급

분류가 초점이 맞추어져 있으며, 이 과정에서 Level of Rigor(이하 LoR)를 제공하여 안전등급에 따른 최소한의 관리방안을 언급하고 있는 정도이다.

Joint 소프트웨어-System Safety Engineering Handbook에서는 MIL-STD-882E 표준에서 언급한 절차 및 방법을 가이드하는 과정에서 수행되어야 하는 안전 활동들을 언급하고 있다. 또한 [그림 6-10]와 [그림 6-11]와 같이, MIL-STD-882E에서 정의된 LoR에 대하여, 적절한 활동을 식별하고, 수행의 정도를 구분할 수 있도록 고려가 필요한 항목과 그에 대한 예시를 제공하고 있다.

[그림 6-10] Level of Rigor 및 예시

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

Design Requirements	Process Tasks	Test Tasks
Fault Tolerant Design	Design Reviews	Safety-Significant Function Testing
Fault Detection	Safety Reviews	Functional Thread Testing
Fault Isolation	Design Walkthroughs	Limited Regression Testing
Fault Annunciation	Code Walkthroughs	100% Regression Testing
Fault Recovery	Independent Reviews	Failure Modes and Effects Testing
Warnings Cautions, and Advisories	Independent Walkthroughs	Safety-Critical Interface Testing
Redundancy	Traceability of Safety-Significant Requirements to Design	COTS, Government Off-the-Shelf Input, Output Test, and Verification
Independence	Traceability of Safety-Significant Requirements to Code	Independent Testing of Prioritized Safety-Related Functions
Functional Partitioning	Traceability of Safety-Significant Requirements to Test	Functional Qualification Testing
Physical Partitioning	Safety Test Results Review	Verification and Validation
Design Safety Standards	Software Quality Assurance Inspections and Audits	Independent Verification and Validation
Design Safety Guidelines	Traceability of Safety-Significant Requirements to Hazards	Full Screening of All COTS Features
Design Safety Lessons Learned	Specific Software Language Requirements	
Full COTS Features Disclosure and Analysis		

자료 : MIL-STD-882E, Joint-소프트웨어-Systems-Safety-Engineering-Handbook

[그림 6-11] LoR Task 예

Level of Rigor	Requirements Tasks	Design Tasks	Implementation Tasks	Test and V&V Tasks	Lifecycle Support Tasks
LOR-1 High Risk	• All LOR-2 and -3 Tasks • Create requirements for a fault tolerant design [Safety and Requirements and Design] • Create requirements to ensure that all interfaces are validated and controlled at all times [Safety and Requirements and Design]	• All LOR-2 and -3 Tasks • Functionally partition all implementations of LOR-3 requirements from lower levels of rigor in the design [Design] • Update design to be stress tolerant [Design] • Update design for SCF (and only SCF) philosophy [Safety and Design] • Update design to control functional, physical, and human interfaces [Design]	• All LOR-2 and -3 Tasks • Create a unit test plan defining the criteria for unit testing of safety-critical code [Safety and Development] • Review unit test results and verify that the unit tests provide the required unit test coverage and were executed in compliance with the unit test plan [Safety and Test] • Perform detailed inspections of code for compliance with safety-critical coding standards and guidelines [Test] • Perform detailed code inspections for fault contributions [Safety, Test, and Development] • Create unit tests with goal of approaching 100% source code branch-point unit testing [Development]	• All LOR-2 and -3 Tasks • Add safety-critical integration test cases to the formal test plan(s) [Safety and someone independent of the developer] • Execute safety-critical integration and test cases [Someone independent of the developer] • Add fault injection safety-critical test cases to the formal test plan(s) [Safety and Test] • Execute fault injection testing [Test] • Add test cases to the Regression Test Plan to support 100% regression testing on all LOR-3 software [Safety, Test, and Development] • Perform 100% regression testing on all LOR-3 software that is changed [Test] • Test to verified and validated interfaces [Test] • Perform code walkthroughs and review all LOR-3 code for safety issues [Safety and Development] • Add safety test cases to verify that all functional, physical, and human interfaces are under continuous control [Safety and Test] • Execute complete decision coverage of the code [Test] • Execute complete modified condition/decision coverage of the code [Test]	• All LOR-2 and -3 Tasks
LOR-2 Med Risk	• All LOR-3 Tasks • Review safety-critical requirements for completeness [Safety]	• All LOR-3 Tasks • Perform a Sub-System Hazard Analysis [Safety] • Functionally partition all implementations of LOR-2 requirements from lower levels of rigor in the design [Design] • Incorporate fault isolation, annunciation, and tolerance into the design [Design]	• All LOR-3 Tasks • Perform high-level reviews of code for compliance with safety-critical coding standards and guidelines [Safety and Development] • Independently witness the execution of unit tests [Safety and Test] • Review unit test plan [Safety]	• All LOR-3 Tasks • Create test cases for safety-critical code to test for [Safety, Test, and Development]: - Stress testing - Stability testing - Disaster testing • Review each LOR-2+ test case [Safety] • Participate in test anomaly resolution [Safety] • Plan, perform, and review failure modes and effects testing (FMET) plans and procedures. • Plan, perform, and review functional and FMET regression test plans and procedures.	• All LOR-3 Tasks • Review defects for safety impact [CM and Safety] • Review and give signature approval on safety-critical Change Requests (CRs) [Safety] • Independently review and check in code changes to CM [someone other than the author of the changes]
LOR-3 Low Risk	• Perform a System Hazard Analysis [Safety] • Create a traceability matrix from safety-critical requirements (contributing or mitigating) to identified hazards (of initial RAC Medium or High) [Safety] • Review safety-critical requirements and prioritize for future builds [Safety and Requirements] • Create requirements to ensure that safety-critical interfaces are validated and controlled at all times [Safety, Requirements, and Design] • Map safety requirements to functions and into views of the system and software architectures, labeling COTS and NDI as they become "make-or-buy" outcomes.	• Continue System Hazard Analysis [Safety] • Follow design guidelines for safety-critical design [Design] • Analyze the design (including functional systems and software architectures and interfaces) for failure modes and hazard contributions [Safety and Design] • Review the design for compliance with the design guidelines and for safety issues [Safety and Design] • Review of the User Interface design for safety issues [Safety and Design] • Create traceability from design components to safety-critical requirements [Requirements and Design]	• Continue System Hazard Analysis [Safety] • Mark safety-critical code with the appropriate LOR [Development] • Follow coding guidelines and comply with coding standards for safety-critical code [Development] • Create traceability from code to safety-critical design requirements [Design and Development] • Execute unit tests [Development] • Participate in acceptance review of safety-critical code [Safety] • Create a safety-critical test report documenting the safety-critical unit testing compliance and execution results [Safety and Test]	• Continue System Hazard Analysis [Safety] • Create test cases for safety-critical code [Safety, Test, and Development] - Exception handling correctness - Fault handling correctness - Interface correctness - Boundary handling correctness • Review safety-critical test results and verify that the safety-critical test cases provide the required test coverage and were executed in compliance with the formal test plans [Safety and Test] • Create traceability between safety-critical test cases and safety-critical requirements [Safety and Test] • Mark safety-critical test cases with the appropriate LOR [Safety and Test] • Create a safety-critical test report documenting the safety-critical formal testing compliance and execution results [Safety and Test] • Calculate and document the residual safety risk (after mitigation) [Safety] • Review all traceability matrices for coverage and completeness [Safety and Design]	• Review proposed CRs for safety impact [Safety and Requirements] • Mark safety-critical items in CM with the appropriate LOR [Development and CM] • Document the results of any Safety Reviews [Safety] • Review problem reporting/defect tracking, change control, and change review activities for safety impact and compliance [CM and Safety] • Perform an Operations and Support Hazard Analysis [Safety]

자료 : Joint-소프트웨어-Systems-Safety-Engineering-Handbook

3. 시사점

MIL-STD-882E 표준에서는 소프트웨어 안전등급에 따른 관리방안으로 안전등급 별 LoR을 정의하고 있다. 하지만 제공되는 LoR은 각 안전등급에 따른 최소한의 활동을 언급하는 정도이며, 구체적인 안전활동, 안전기법 및 수단을 제시하고 있지는 않다. 해당 표준에서는 시스템 소프트웨어의 안전을 달성하기 위해서는 원하는 결과와 목표

달성을 위한 안전활동을 모델에 적절하게 연관시키고 통합해야 한다는 것을 강조하고 있으며, 적용 가능한 다양한 모델 및 예시를 제공하고 있다. 따라서, 해당 정보들을 기반으로 타 표준에서 설명하고 있는 수준의 활동을 식별 및 정리할 필요가 있으며, 이후 타 표준과의 비교 분석을 진행하도록 한다.

제7장 공공기관 시스템 소프트웨어 안전등급 결정방안 도출

본 장에서는, 국내외 안전제도 및 관련 표준 조사를 통한 안전등급 결정방법 및 평가요소 분석 결과, 공공기관 시스템 분류 및 위험분석 결과를 기반으로 공공기관 시스템의 소프트웨어 안전등급 결정방안을 도출한다. 방대한 자료 조사 및 분석 결과를 기반으로 적절한 소프트웨어 안전등급 결정체계를 도출하기 위하여, 전문가 검토를 통한 1) 소프트웨어 안전등급 결정체계 방향성 검증을 수행하고, 2) 소프트웨어 안전등급 결정체계를 구축하도록 한다. 이후, 소프트웨어 안전등급 결정체계에 대한 3) 전문가 검토를 재 수행하여 최종적인 소프트웨어 안전등급 결정방안을 도출한다.

제1절 소프트웨어 안전등급 결정체계 방향성 도출

1. 소프트웨어 안전등급 결정체계 방향성 도출

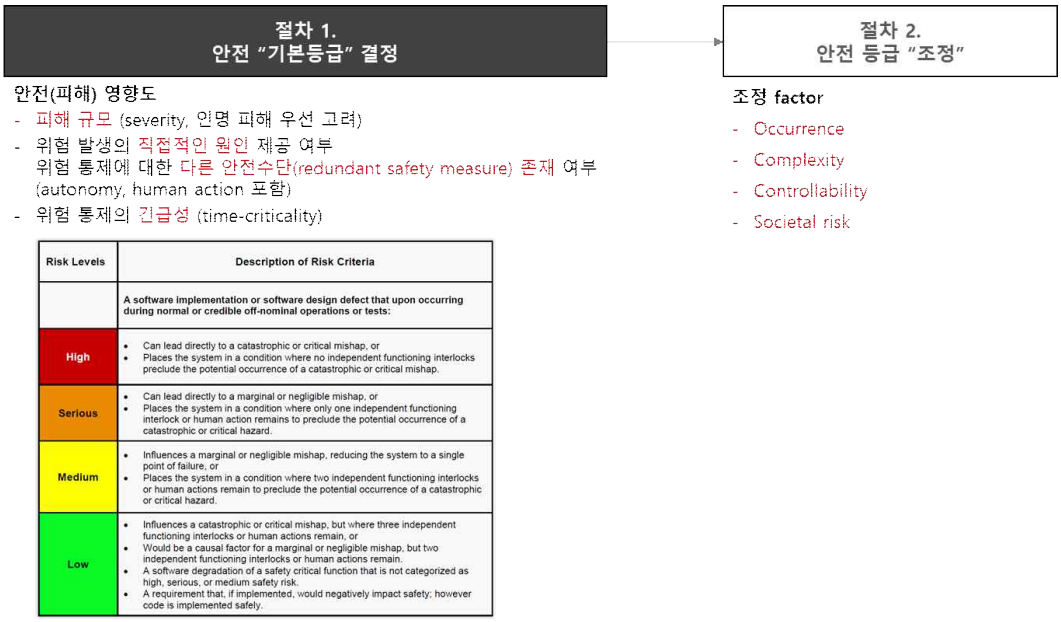
가. 방안 1) 공통 평가기준 정의

방안 1은 미국방 표준(MIL-STD-882E)과 NASA 표준(NASA-STD-8719-13C) 접근방법에 기반한 것으로, 안전에 대한 “기본등급”을 우선 결정한 이후, 여러 조정 요인들을 기반으로 안전등급을 “조정”하는 방안이다.

다음 그림과 같이, 타 안전 표준에서 안전등급에 대한 주요 평가요인으로 식별되었던 항목들을 기반으로 “기본등급”을 결정한다. 해당 평가요인으로는 기능 실패로 인한 피해의 규모, 직접적인 원인 제공 또는 간접적인 원인 제공 여부, 위험 통제를 위한 외부 안전대책 존재 여부 등이 포함될 수 있다.

이후, 조정을 위한 평가요인을 기반으로 “기본등급”을 세부 조정한다. 해당 평가요인은 특정 분야 및 주요 표준에서 언급하고 있는 안전등급에 대한 평가요인으로 구성되며, 주로 위험이 발생 빈도, 시스템의 복잡도, 기능의 통제도 등으로 구성될 수 있다. 조정을 위한 평가요인은 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용할 수 있도록 정의한다.

[그림 7-1] 공통 평가기준 정의



Risk Levels	Description of Risk Criteria
	A software implementation or software design defect that upon occurring during normal or credible off-nominal operations or tests:
High	• Can lead directly to a catastrophic or critical mishap, or • Places the system in a condition where no independent functioning interlocks preclude the potential occurrence of a catastrophic or critical mishap.
Serious	• Can lead directly to a marginal or negligible mishap, or • Places the system in a condition where only one independent functioning interlock or human action remains to preclude the potential occurrence of a catastrophic or critical hazard.
Medium	• Influences a marginal or negligible mishap, reducing the system to a single point of failure, or • Places the system in a condition where two independent functioning interlocks or human actions remain to preclude the potential occurrence of a catastrophic or critical hazard.
Low	• Influences a catastrophic or critical mishap, but where three independent functioning interlocks or human actions remain, or • Would be a causal factor for a marginal or negligible mishap, but two independent functioning interlocks or human actions remain. • A software degradation of a safety critical function that is not categorized as high, serious, or medium safety risk. • A requirement that, if implemented, would negatively impact safety; however code is implemented safely.

해당 방안은 각 도메인 별 판단항목 및 지표가 달라 기준이 구체화되기 어려우며, 판단 기준이 구체화되지 않으면 등급 판정에 혼선 발생할 수 있다. 때문에, 각 도메인에서 수용할 수 있는 공통 평가 기준 도출에 어려움이 있어 공통 기준이 마련되어도 개별 도메인에서 수용되기 어려울 수 있는 단점이 존재한다.

나. 방안 2) 안전보장 등급에 대한 기준 정의

방안 2는 시스템이 충족시켜야 할 안전 요구사항을 정의하고, 특정 안전 요구사항을 만족시켰을 때, 보장되는 안전등급(Safety Assurance Level)을 정의하는 방법이다. 해당 방안은 정보보호제품의 공통평가기준(Common Criteria)의 평가보증등급(EAL)을 부여하는 것과 유사한 방안이다.

많은 도메인에서 이미 안전표준을 가지고 있기 때문에 별도로 만들어진 안전등급 판정 기준이 적용되기 쉽지 않다. 따라서, 안전등급 기준을 직접적으로 정의하지 않고, 적용해야 하는 안전 요구사항을 기반으로 하는 안전보장등급을 정의하고, 각 산업도메인 별 안전등급 기준과 매핑 정보만 제공하도록 한다.(예. SAL 3등급은 ISO26262 ASIL B에 부여되는 안전 요건과 비슷한 수준)

다. 방안 3) 공공기관 시스템 기능 별 잠정등급 정의

방안 3은 공공기관 시스템 기능에 대하여 잠정적인 등급을 사전에 정의하는 방안이다. 먼저 공공기관 시스템 및 기능에 대한 분류를 수행하여 사전에 정의된 카테고리를 제시하고, 이에 따른 잠정등급을 정의하여 제공한다. 이후 소관 분야별 특성에 따라 잠정등급을 조정할 수 있도록 추가적인 평가요인을 정리하여 제공한다.

해당 방안은 정보보안 분야(한국, 미국) 및 원자력 안전 분야에서 유사한 접근방식을 취하고 있다.

2. 전문가 검토 및 소프트웨어 안전등급 결정 방안 선정 (방안 1)

소프트웨어 안전등급 결정체계 방향성에 대하여 다양한 분야(원자력, 철도, 국방, 보안, 항공, 자동차 분야 등)의 전문가를 대상으로 전문가 검토를 수행하였다. 이를 통해 소프트웨어 안전등급 제도의 필요성, 소프트웨어 안전등급 적용 시 문제점 및 고려 필요한 사항, 소프트웨어 안전등급 결정 방향성에 대한 검토 의견을 수렴하여 반영할 수 있었다.

ㅇ 소프트웨어 안전등급 제도의 필요성

- 사람의 안전, 시설의 안전, 환경의 위해 등을 예방하기 위해 등급 제도가 필요함
- 소프트웨어 사용 범위 및 중요도가 증가함에 따라 소프트웨어 안전을 향상시키기 위한 제도가 필요함
- 공공기관 시스템 및 주요 산업 분야별 표준에서 정의하고 있는 소프트웨어 시스템의 안전 관리를 위해 등급 제도가 필요함
- 도메인 별 주요 기능을 제외하고, 안전에 영향이 미미하거나 필수가 아닌 경우 안전 기준의 적용이 미흡한 실정임
- 도메인 별 안전 기준의 적용이 미흡한 부분에 대하여, 각 산업 별 안전

기준을 엄격히 적용하기 전 중간 과정으로 활용하는데 필요할 수 있음

ㅇ 소프트웨어 안전등급 적용 시 고려되어야 할 점

- 장시간의 기간을 두고 점진적으로 준비가 필요하며, 등급을 부여하고, 제대로 개발되었는지 인증 시험을 부여할 경우, 이에 대한 체계도 준비되어야 함
- 분야별 표준과의 관계를 고려하여 관련 표준에서 다루지 못하는 시스템 중심으로 적용하고, 표준에서 다루는 부분은 해당 표준을 따르도록 위임해야 함

ㅇ 소프트웨어 안전등급 결정 방안

- 기존 안전 관련 표준들이 각 도메인에서 기 사용되고 있으므로, 기존의 도메인과 신규(새로운 기능) 도메인을 구분하여 방안을 적용해야 함
- 공공기관 발주자 등이 모호한 기준에 따라 업무를 수행하고 요구사항을 도출하는 것이 쉽지 않을 수 있으므로, 공통 평가 기준을 바탕으로 테일러링 할 수 있는 방안 및 가이드라인을 제시
- 방안 3을 기반으로 안전등급 부여 시, 범위가 광범위할 것으로 판단되며, 잠정등급이 정해지면 변경하기가 쉽지 않을 것 같음(변경이 필요한 경우)

ㅇ 소프트웨어 안전등급 결정에 필요한 평가요인

- 시스템 위험 심각도
- 시스템에 대한 소프트웨어의 영향 범위
- 소프트웨어 특성(제어 또는 정보)
- 위험발생 빈도(HW의 위험발생빈도와 달리 특정할 수 없는 어려움이 있음)

ㅇ 소프트웨어 안전등급 적용이 필요한 공공시스템

- 안전 제어 시스템(SIS, Safety Instrumented System) - 발전, 가스생산,

상수도 등

- 안전에 영향을 미치는 정보시스템
- 국가핵심 기반 시스템(재난 등)
- 사람의 생명과 관련된 경찰/소방 관련 소프트웨어 시스템

제2절 소프트웨어 안전등급 결정체계 구축

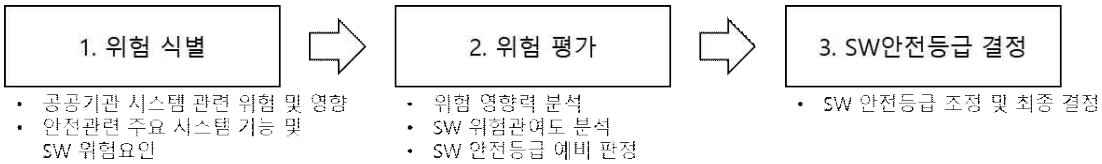
소프트웨어 안전등급 결정체계 방향성을 통해 도출된 3가지 안에 대한 전문가 검토 의견을 기반으로 소프트웨어 안전등급 결정체계를 구축한다.

안전보장 등급의 경우, 소프트웨어 안전등급이 결정되지 않아 본 연구의 원래 취지에 부합하지 않는 문제가 있다. 공공기관 시스템의 광범위한 범위로 인해 시스템 안전에 대한 잠정등급을 부여하는 것은 매우 어려울 것이며, 시스템 개발에 대한 감사 등의 이유로 한번 정해진 잠정등급을 조정하기란 매우 어려울 수 있다. 또한, 신규 시스템의 경우, 사전에 등급을 지정하기 어려울 것이란 의견이 다수 존재하였다.

따라서, 공통 평가기준을 정의하여 소프트웨어 안전등급을 부여하고, 필요에 따라 조정할 수 있는 **방안 1을** 기반으로 소프트웨어 안전등급 결정체계를 구축한다. 해당 방안의 경우, 도메인에 적용하는 공통 기준을 구체적으로 기술하기 힘들고, 구체화하여도 적용하기 쉽지 않을 수 있다. 때문에, 시스템 위험 심각도 및 소프트웨어 특성만을 고려한 보다 러프한 수준의 공통 평가기준을 정의하고, 각 분야 별 특성에 따라 조정할 수 있는 방향으로 소프트웨어 안전등급 결정체계를 도출하였다.

소프트웨어 안전등급 결정은 다음과 같은 절차로 수행된다.

[그림 7-2] 소프트웨어 안전등급 결정 절차



1. 용어 정의

<표 7-1> 용어 정의

용어	설명
수용가능한 위험(Tolerable Risk)	현재 사회의 가치를 고려했을 때 수용할 수 있는 수준의 위험 정도 (ISO/IEC GUIDE 51:2014)
안전(Safety)	수용불가능한 (not tolerable) 위험이 없는 상태 (ISO/IEC GUIDE 51:2014)
안전관련 기능(Safety-Related Function)	이것의 오동작 또는 동작의 실패가 위험요인(Hazard)이 되는 기능 (MIL-STD-882E의 'safety-critical function' 및 'safety-related' 정의 내용 기반으로 내용 정리)
안전상태(Safe State)	안전이 달성된 시스템의 상태 (IEC 61508-4)
안전대책(Risk Reduction Measure or Protective Measure)	위험요인의 발생을 예방하거나 위험을 완화시키기 위한 수단 또는 조치 (ISO/IEC GUIDE 51:2014)
위험(Risk)	피해의 심각도(Severity)와 발생가능성(Probability of Occurrence)의 조합 (ISO/IEC GUIDE 51:2014)
위험영향력(Severity)	위험으로 인한 피해의 정도 (IEC 61508-4)
위험요인(Hazard)	피해를 발생하게 하는 잠재적 원인 (ISO/IEC GUIDE 51:2014)
정보 시스템 또는 정보처리 기능(Information System or Information Processing Function)	정보의 수집, 처리, 저장, 배포하도록 설계된 시스템. 정보를 입력 받아 다른 형태의 정보로 변환하는 기능 (WIKIPEDIA)
제어 기능/시스템(Control Function/System)	프로세스 또는 운영자의 입력 신호에 반응하여 시스템이 의도된 대로 동작하도록 신호를 출력하는 기능/시스템 (IEC 61508-4). 정보 시스템과 다르게 장치나 설비 등 실물을 제어함
피해(Harm)	사람의 부상 또는 건강의 손상, 경제적 손실 및 국가기반시설의 기능 장애 (ISO/IEC GUIDE 51:2014 기반으로 일부 내용 조정)
소프트웨어 안전등급(소프트웨어 Safety Integrity Level)	소프트웨어가 주어진 조건하에서 정해진 시간 내에 안전관련 기능을 성공적으로 수행할 수 있는 가능성에 대한 분류 기준 (IEC 61508-4 기반으로 일부 내용 조정)

소프트웨어 위험관여도(소프트웨어 Control Category)	전체 시스템 상에서 소프트웨어가 수행하는 기능의 제어형태(자율성), 정보의 필수성, 안전대책의 중복성을 기반으로 한 분류 기준 (MIL-STD-882E)

2. 위험 식별

가. 공공기관 시스템과 관련된 위험과 영향

공공기관 시스템과 관련된 위험은 크게 2가지 형태로 구분될 수 있다. 하나는 공공기관 시스템의 고장, 오동작 등으로 인해 유발될 수 있는 위험이고, 다른 하나는 원인과 상관없이 공공기관 시스템이 대응 또는 완화해야 하는 위험이다.

또한, 공공기관 시스템과 관련된 위험은 사회적 위험, 기반 위험, 자연적 위험과 같이 3가지 유형으로 구분할 수 있다. 위의 정보와 시스템 사용 환경을 고려하여 분석 대상 공공기관 시스템으로부터 발생 가능한 최상위 위험원을 식별한다.

<표 7-2> 공공시스템과 관련된 위험

위험 유형	세부위험
사회적 위험	화재(방화)・붕괴・폭발・교통사고(항공사고 및 해상사고를 포함)・화생방사고・환경오염사고・산불・핵심인력손실(유출)・직원사상・테러・핵심정보(기관정보, 고객정보 등) 유출・파업・전쟁 또는 국지전・유괴/인질・유언비어 유포・사업장내 안전사고・외주업체 공급 중단・중요문서 분실 또는 소실 ・감염병・가축질병(구제역) 등
기반 위험	전력공급중단(정전)・통신장애・가스공급중단・에너지 공급제한・상하수도 처리 오류・가스 누출 및 폭발・설비장애(냉난방 등)・누수・수자원시설 훼손・사업장 위험(폐쇄 또는 접근불가, 주변위험)・물류중단(배송 등) 등
자연적 위험	태풍・홍수・호우・강풍・풍랑・해일(지진해일)・대설・낙뢰・가뭄・지진・황사・조류대발생(적조)・조수(潮水)・화산폭발・산사태

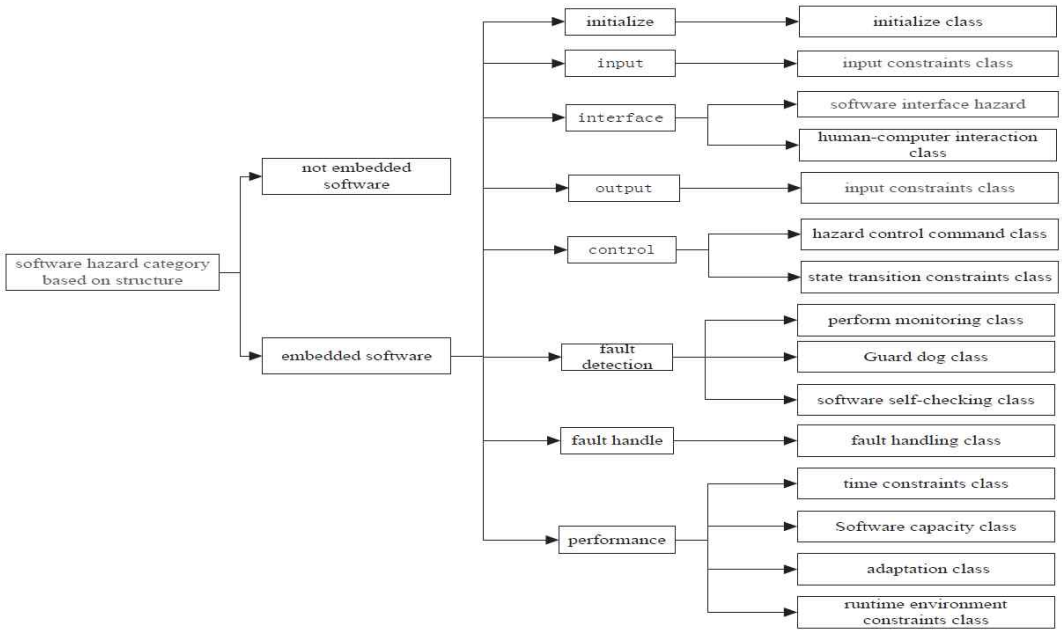
자료 : 해양수산부, 2018.2, 2018년 국가기반시설 보호 계획

나. 소프트웨어 위험 요인

1) 소프트웨어 위험요인 분류

- ㅇ 시스템의 기능에 따라 소프트웨어의 위험요인을 분류할 수 있다. 예를 들면 엔진 제어 시스템 소프트웨어, 브레이크 제어 시스템 소프트웨어, 운행 제어 시스템 소프트웨어 등이다.
- ㅇ 소프트웨어 개발 프로세스 측면에서 위험을 분류할 수 있다.
- ㅇ 소프트웨어의 구조적 측면에서 위험을 분류 할 수 있다.

[그림 7-3] 구조적 측면으로 위험 분류



자료 : Ji Shujuan, Bao Xiaohong a(2013), Research on Software Hazard Classification, ISAA 2013

2) 안전관련 주요 시스템 기능과 소프트웨어 위험 요인

최상위 수준의 위험이 식별되면, 해당 최상위 위험원에 영향을 미칠 수 있는 안전관련 기능을 식별한다. <표 7-3>는 다양한 위험에 영향을 미칠 수 있는 주요 안전관련 기능의 예시를 보여주고 있다. 해당 내용은 하나의 예시이며, 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용 가능하다.

기능(Function)에 대한 정의는 다음과 같다.

- ㅇ 사용자가 볼 수 있는 어플리케이션의 피처(Feature) 또는 능력(Capabilities) (ISO/IEC 20926[100])
- ㅇ 시스템 또는 컴포넌트의 정의된 목적 또는 특징적인 동작(Action) (ISO/IEC/IEEE 24765[101])

<표 7-3> 예시 - 주요 안전관련 기능

위험 유형	세부위험
시설 또는 장치 제어 시스템	• 위험을 직접적으로 유발할 수 있는 하드웨어 제어 관련 기능 또는 이를 위한 정보 제공 기능 - 하드웨어를 제어하는 기능 - 제어와 관련된 일련의 처리과정과 관련된 기능 - 제어를 위한 데이터/트랜드 분석 기능 등 • 위험이 발생될 수 있는 상태나 조건의 검출, 보고, 및 대응 관련 기능 또는 이를 위한 정보 제공 기능 • 이미 위험이 발생한 경우, 피해를 완화시키는 것과 관련된 기능 또는 이를 위한 정보 제공 기능 • 위의 안전관련 기능을 수행하는 소프트웨어와 동일한 프로세서 상에서 구동하는 소프트웨어 • 위의 안전관련 기능을 수행하는 소프트웨어를 검증 및 확인하는 소프트웨어
안전관리 정보시스템	• 재난에 체계적인 예방, 대비, 신속한 대응, 복구 업무를 지원하는 기능

※ 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용

소프트웨어 기능은 소프트웨어의 최종 출력을 기준으로 정의하는 것이 일반적이며, 계층적으로 정의될 수 있다. 위험 평가에 적절한 소프트웨어 기능의 수준은 시스템 특성에 따라 다를 수 있다. 상세한 수준의 소프트웨어 기능에 대해 위험 평가를 하는 경우, 보다 꼼꼼하게 위험평가를 수행할 수 있으나 노력이 많이 들고, 위험 평가 결과가 중복되는 사례가 많을 수 있다. 너무 상위 수준의 소프트웨어기능에 대해 위험 평가를 하는 경우, 기능이 명확하지 않아 위험 평가를 제대로 수행하기 어려울 수 있다.

100) Software and systems engineering — Software measurement — IFPUG functional size measurement method 2009

101) Systems and software engineering — Vocabulary

일반적으로 위험 평가를 위한 소프트웨어기능은 소프트웨어의 사용자가 인지 가능한 수준에서 식별되는 것이 적절하다. 위험 평가가 사람이 인식할 수 있는 수준에서 이루어지기 때문이다. 소프트웨어기능은 시스템의 특성에 따라 위험 평가에 적절한 수준으로 정의되어야 한다.

<표 7-4> 예시 - 항공등화감시제어시스템의 주요 기능

수준 1	수준 2	수준 3
항공등화 감시 및 제어	램프 제어	개별 램프 점/소등
		그룹별 램프 점/소등
		섹션별 램프 점/소등
	수동 제어	경로 생성
		경로 지정
		도로 정지위치 신호등 제어
		차량 정정위치 신호등 제어
		장애구역 설정
	사전설정 제어	등화 밝기 제어
		...

대상 시스템의 주요 소프트웨어 기능을 도출하고, 도출된 기능에 대하여 잠재적인 소프트웨어 위험요인 및 기능 오동작을 분석한다. <표 7-5>에서는 주요 소프트웨어 위험요인과 해당 위험요인으로 인해 발생 가능한 영향에 대한 예시를 보여주고 있다. 해당 내용은 하나의 예시이며, 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용 가능하다.

<표 7-5> 예시 - 소프트웨어 위험요인과 영향

소프트웨어 위험요인	안전관련 영향
오류 정보 제공	안전관련 의사결정 오류로 인해 사회적/기반 위험이 발생하거나 발생된 사회적/기반/자연적 위험의 피해를 증가시킴
정보 제공 지연 또는 미제공	안전관련 의사결정 지연 또는 오류로 인해 사회적/기반 위험이 발생하거나 발생된 사회적/기반/자연적 위험의 피해를 증가시킴
의도하지 않은 장치/시설 동작	장치/시설의 오동작 또는 실패로 인해 사회적/기반 위험이 발생하거나 발생된 사회적/기반/자연적 위험의 피해를 증가시킴
장치/시설 제어 미수행	장치/시설의 오동작 또는 실패로 인해 사회적/기반 위험이 발생하거나 발생된 사회적/기반/자연적 위험의 피해를 증가시킴
장치/시설 제어 시점	장치/시설의 오동작 또는 실패로 인해 사회적/기반 위험이 발생하거나

오류	발생된 사회적/기반/자연적 위험의 피해를 증가시킴
장치/시설 제어량 과소/과다	장치/시설의 오동작 또는 실패로 인해 사회적/기반 위험이 발생하거나 발생된 사회적/기반/자연적 위험의 피해를 증가시킴

※ 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용

3. 위험 평가

위험평가는 소프트웨어의 개별적인 안전관련 기능을 대상으로 수행하며, 이를 기반으로 전체 소프트웨어에 대한 안전등급을 정한다. 위험평가는 “위험영향력”과 “소프트웨어 위험관여도” 관점의 분석을 통해 이루어지며, 이를 기반으로 소프트웨어가 달성해야 할 “소프트웨어 안전등급”을 정한다.

가. 위험영향력 분석

본 연구에서는 국가기반체계보호계획 수립지침 및 해양수산부 국가기반시설 보호 계획(2018)의 위험도 등급 평가 기준 참고하여, 다음 <표 7-6>과 같이 위험영향력 판단 기준을 정의하였다.

위험 영향력은 소프트웨어를 포함한 전체 시스템 수준에서 고려되어야 한다. 제어 시스템의 경우, 소프트웨어의 제어 기능을 통해 물리 세계에 영향을 미치는 영향을 평가하며, 정보 시스템의 경우, 해당 정보를 기반으로 다른 시스템 또는 운영자가 수행하는 안전관련 기능의 영향을 평가한다. 또한, 시스템이 피해에 미치는 연관성의 정도를 고려해서 다음과 같이 영향력 등급을 조정할 수 있다.

- ㅇ 연관성의 정도: 직접 원인(1차 원인), 간접 원인(n차 원인)
- ㅇ 등급 조정 수준: 1 또는 2 등급 하향 조정

예) ‘안전안내문자 발송 시스템’의 경우 예상되는 위험에 대해 정보를 제공하는 시스템으로, 해당 시스템의 고장 또는 오동작이 위험의 피해를 직접적으로 유발한다고 판단하기는 어려움. 자연적/사회적 위험은 사망 사고 등의 피해를 유발할 수 있으나, 해당 시스템이 위험에 직접적인 원인을 제공한다고 보기 어려우므로 위험영향력 등급은 1등급이 아닌 보다 낮은 등급(2등급 또는 3등급)으로 판정하는 것이 합당할 수 있음

마찬가지로, 해당 위험영향력 판단 기준은 하나의 예시이며, 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용 가능하다.

〈표 7-6〉 예시 - 위험영향력 판단 기준

위험영향력	판단 기준
S4	다음 항목 중 하나 이상 해당 인적 피해 - 1명 이상의 사망, 또는 2명 이상의 전치 3개월 ~ 상해자, 또는 10명 이상의 전치 2주 ~ 상해자 발생 경제적 피해 - 10억 이상의 손실 기반시설 피해 - 50% 이상 및 일주일 이상의 국가기반시설 기능 장애 야기
S3	다음 항목 중 하나 이상 해당 인적 피해 - 1명 이상의 전체 3개월 ~ 상해자, 또는 5명 이상의 전치 2주 ~ 상해자 경제적 피해 - 1000만원 이상 ~ 10억원 미만 기반시설 피해 - 30% 이상 및 하루 이상의 국가기반시설 기능 장애 야기
S2	다음 항목 중 하나 이상 해당 인적 피해 - 1명 이상의 전치 2주 ~ 상해자 경제적 피해 - 1000만원 미만 기반시설 피해 - 10% 이상 및 1시간 이상의 국가기반시설 기능 장애 야기
S1	다음 항목 중 하나 이상 해당 인적 피해 - 경미한 상해 경제적 피해 - 경미한 손실 기반시설 피해 - 10% 미만 및 1시간 미만의 국가기반시설 기능 장애 야기
S0	불편함을 느끼거나 피해 없음

※ 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용

나. 소프트웨어 위험관여도 분석

위험 관여도는 전체 시스템 상에서 소프트웨어가 수행하는 기능의 제어형태(자율성), 정보의 필수성, 안전대책의 중복성을 기반으로 한 분류 기준을 의미한다. 본 연구에서는, 미국 항공우주 및 국방 안전 분야 표준(NASA-STD-8719.13C, MIL-STD-882E)를 기반으로 〈표 7-7〉와 같이 소프트웨어 위험관여도 판단 기준을 정의한다. 마찬가지로, 해당 소프트웨어 위험관여도 판단 기준은 하나의 예시이며, 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용 가능하다.

〈표 7-7〉 예시 - 소프트웨어 위험관여도 판단 기준

소프트웨어위험관여도	판단 기준	
	요약	설명
C4	(제어시스템) **자율적으로** 안전관련 **제어기능 수행**	소프트웨어가 자율적으로 안전관련 제어기능 수행 (소프트웨어로 인해 발생가능한 위험에 대해 운영자 개입 또는 다른 안전대책 없음) 해당 제어기능의 오동작(미수행, 오수행, 시점오류, 제어수준오류)으로 인해 위험이 발생하거나 피해가 증가하는 경우에 해당 예) 열차자율주행시스템
C3	(제어시스템) 자율적으로 안전관련 제어기능을 수행하나, **통제가 가능함**	소프트웨어가 자율적으로 안전관련 제어기능을 수행하나, 필요시 다른 수단(예, 운영자, 하드웨어 안전대책 등)으로 위험 통제 가능 해당 제어기능의 오동작(미수행, 오수행, 시점오류, 제어수준오류)으로 인해 위험이 발생하거나 피해가 증가하는 경우에 해당 예) 터널관리시스템 - 제연시설 제어
	(정보시스템) 안전관련 제어기능을 수행하는데 **필수적인 정보 제공**	운영자 또는 다른 시스템이 안전관련 제어기능을 수행하는데 필수적인 정보 제공 (제어 기능을 수행하는데 다른 정보를 참조할 시간적 여유 없음) 해당 정보 제공의 오류(오정보, 지연/미제공)로 인해 위험이 발생하거나 피해가 증가하는 경우에 해당 예) 표준수운영시스템 - 정수공정 감시
C2	(제어시스템) **중복되는 다른 안전대책**이 운영되는 상황 하에서 안전관련 제어 기능 수행	소프트웨어가 안전관련 제어기능을 수행하나, 소프트웨어로 인한 위험을 통제할 수 있는 다른 안전대책이 항상 동작하여 소프트웨어 단독 오류로는 위험 발생하지 않음 해당 제어기능의 오동작(미수행, 오수행, 시점오류, 제어수준오류)으로 인해 위험이 발생하거나 피해가 증가하는 경우에 해당 예) 항공등화관제시스템 - 활주로 및 유도로 등화 제어
	(정보시스템) 안전관련 기능을 수행하는데 필요한 **중복되는 정보 제공**	운영자 또는 다른 시스템이 안전관련 기능을 수행하는데 필요한 중요한 정보 제공하나, 해당 정보가 다른 수단에 의해서도 중복적으로 제공됨 해당 정보 제공의 오류(오정보, 지연/미제공)로 인해 위험이 발생하거나 피해가 증가하는 경우에 해당 예) 산림재해통합관리시스템 - 산불상황관제 및 대응관리
C1	안전관련 의사결정에 도움이 되는 정보 제공	안전관련 기능 수행을 위한 의사결정에 도움이 되는 정보 제공 (반드시 필요한 정보는 아니며, 다양한 대체가능한 정보 중 일부) 해당 정보 제공의 오류(오정보, 지연/미제공)로 인해 위험이 발생하거나 피해가 증가하는 경우에 해당 예) 안전안내문자 발송 시스템
C0	안전과 관련 없는 기능 수행 또는 정보 제공	소프트웨어가 안전관련 기능 또는 정보 제공을 수행하지 않음 해당 정보 제공의 오류(오정보, 지연/미제공)로 인해 위험이 발생하거나 피해가 증가하지 않음

		예) 여객흐름관리시스템 - 자동입국심사

※ 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용

소프트웨어 위험관여도 판단 기준에서 언급된 ‘다른 안전대책’은 대상이 되는 소프트웨어의 외부에 마련된 안전대책을 말한다. 즉 해당 소프트웨어 외부의 하드웨어, 기구 등의 다른 기술로 구현된 안전대책, 해당 소프트웨어가 아닌 다른 소프트웨어의 안전대책, 해당 소프트웨어의 운영자의 안전조치 등이 이에 해당한다. 또한, 해당 소프트웨어 시스템에 포함된 안전대책은 배제하고 안전등급을 평가해야 한다.

<표 7-8> 및 [그림 7-4]에서는 소프트웨어 위험관여도 판단에 대한 기술적 판단 기준과 기능 특성에 따라 소프트웨어 위험관여도를 결정하는 방법에 대하여 제공하고 있다.

<표 7-8> 소프트웨어 위험관여도 판단 기준표 - 기술적 판단 기준(예시)

안전대책/정보 중복성 / 기능유형			상시 중복	필요시 중복	중복성 없음
안전관련성 있음	제어기능	자율제어	X	C3	C4
		수동제어	C2	X	X
	정보처리 기능	안전필수정보	C2	X	C3
		안전참조정보	C1	X	X
안전관련성 없음	-		C0		

X - 적용되지 않음 / 해당사항 없음

※ 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용

○ 안전 관련성: 시스템의 고장, 오동작 등으로 인해 위험이 유발되거나, 위험으로 인한 피해가 증가하면 안전 관련된 시스템으로 판단

○ 제어형태 (제어 기능/시스템에 적용)

- 자율제어: 시스템이 자체적인 판단 또는 외부 시스템의 입력에 반영하여 설비나 장치의 제어를 수행함 (기본적으로는 시스템이 운영자의 개입 없이 제어 기능을 수행함. 경우에 따라 운영자가 제어 통제권을 가져갈 수 있음 - 반자율)

- 수동제어: 시스템이 운영자의 입력에 반응하여 설비나 장치의 제어를 수행함

ㅇ 정보의 필수성 (정보 시스템 또는 정보처리 기능에 적용)

- 안전필수 정보: 안전관련 기능을 수행하는데 필수적인 정보 제공하는 경우
- 안전참조 정보: 안전관련 기능을 위한 의사결정에 도움이 되는 정보

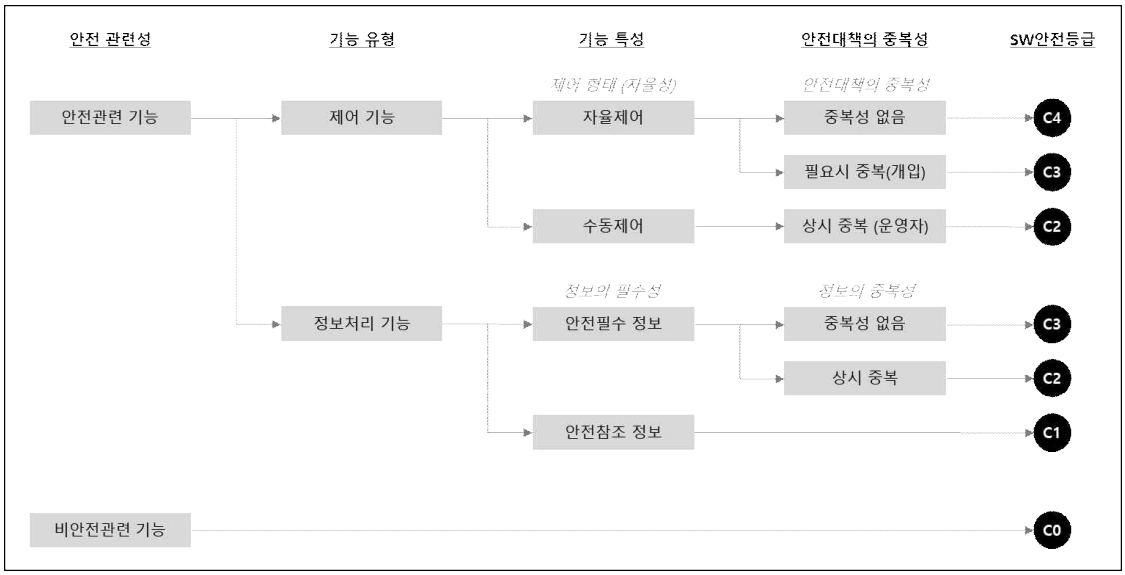
ㅇ 안전대책의 중복성 (제어 기능/시스템의 경우)

- 중복성 없음: 소프트웨어로 인해 발생가능한 위험에 대해 다른 안전대책이 없음
- 필요시 중복: 소프트웨어의 제어기능에 대해 필요시 다른 안전대책(예, 운영자의 조치, 하드웨어 안전장치 등)으로 위험 통제 가능
- 상시 중복: 소프트웨어로 인한 위험을 통제할 수 있는 다른 안전대책이 항상 동작하여 소프트웨어 단독 오류로는 위험 발생하지 않음

ㅇ 안전대책의 중복성 (정보 시스템 또는 정보처리 기능의 경우)

- 중복성 없음: 소프트웨어가 제공하는 정보 외에 참조할 중복된 정보 없음 (다른 정보가 있더라도, 안전대책을 수행하는데 이를 참조할 여유가 없는 경우에도 중복된 정보가 없는 것으로 판단. 예, 실시간 시스템)
- 상시 중복: 소프트웨어가 제공하는 정보 외에 참조할 중복 또는 대체할 정보가 항상 존재

[그림 7-4] 예시 - 기능 특성에 따른 소프트웨어 위험관여도 결정 방법



다. 소프트웨어 안전등급 예비 판정

위험영향력과 소프트웨어 위험관여도가 결정되면, 소프트웨어 안전등급 판단 기준표를 참고하여 소프트웨어 안전등급을 판정한다.

소프트웨어 안전등급 = (위험 영향력) X (소프트웨어 위험관여도)

위험평가는 소프트웨어의 개별적인 안전관련 기능을 대상으로 수행하며, 이를 기반으로 전체 소프트웨어에 대한 안전등급을 정한다.

〈표 7-9〉 예시 - 소프트웨어 안전등급 판단 기준

		위험영향력				
		S4	S3	S2	S1	S0
소프트웨어 위험관여도	C4	VH	VH	H	M	L
	C3	VH	H	H	M	L
	C2	H	H	M	M	L
	C1	M	M	M	M	L
	C0	L	L	L	L	L

VH(Very High, 매우 높음), H(High, 높음), M(Medium, 중간), L(Low, 낮음)

※ 소관 분야별 특성에 따라 자체 실정에 맞게 탄력적으로 적용

ㅇ 소프트웨어 안전등급 예비 판정시 고려 사항

- 위험평가는 1차적으로 소프트웨어의 개별적인 안전관련 기능을 대상으로 수행한다. 즉, 소프트웨어 안전관련 기능별로 위험 영향력, 소프트웨어 위험관여도를 분석하고 이에 기반하여 소프트웨어 안전등급을 결정한다.
- 소프트웨어 전체에 대한 소프트웨어 안전등급은 해당 소프트웨어의 안전관련 기능에 부여된 소프트웨어 안전등급 중 가장 높은 등급이 부여된다.
- 기본적으로 소프트웨어 구성요소(예, 모듈, 컴포넌트, 유닛 등)는 해당 구성요소에 할당된 안전관련 기능의 소프트웨어 안전등급이 부여된다. 소프트웨어 구성요소들에 부여된 소프트웨어 안전등급이 서로 상이한 경우, 이 중 가장 높은 소프트웨어 안전등급이 모든 소프트웨어 구성요소들에 재부여된다. 다만, 소프트웨어 구성요소들 간 독립성이 보장된다면 원래 부여된 상이한 소프트웨어 안전등급을 유지할 수 있다. (구성요소 간 독립성이란 한 구성요소의 오류가 다른 구성요소의 기능에 영향을 미치지 않음을 의미한다)
- 소프트웨어를 포함한 시스템수준에서 안전등급이 결정되는 경우, 소프트웨어의 안전등급은 시스템 수준의 안전등급을 그대로 상속하거나, 별도의 기준을 정하여 소프트웨어 안전등급을 판단할 수 있다.

4. 소프트웨어 안전등급 결정

소프트웨어안전 등급의 평가요소 및 판단기준은 조직의 안전관련 방침 및 시스템의 특성에 따라 다르게 정의되고 적용될 수 있다.

ㅇ [예시] 위험영향력의 경제적 피해 기준은 영역별로 큰 차이가 있을 수 있어, 피해 금액을 조정하여 사용할 수 있음

ㅇ [예시] 특정 영역에서는 안전등급을 결정하는데 방호계층(Layer Of Protection)을 고려함

또한, 위에서 언급된 평가요소(위험 영향력, 소프트웨어 위험관여도) 외에 위험의 “발생가능성(probability of occurrence)”을 추가적으로 고려할 수 있다. 위험발생가능성은 위험에 대한 노출도(exposure), 시스템의 오동작을 포함한 위험을 초래할 수 있는 이벤트 발생빈도(occurrence) 및 위험이 발생한 상황에서 피해를 회피할 수 있는 가능성(possibility of avoiding) 등의 요소를 고려해서 정한다. 위험발생가능성은 소프트웨어를 포함한 시스템 수준에서 평가하고, 위험발생가능성이 낮게 판단되는 경우, 소프트웨어 안전등급을 하향 조정할 수 있다.

다음 표를 통해 소프트웨어 안전등급 판정 예시를 확인할 수 있다.

<표 7-10> 예시 - 소프트웨어 안전등급 판정

시스템	소프트웨어 기능	주요 위험 요인 및 영향력 판단 근거(예시)	영향력	위험 관여도 판단 근거(예시)	관여도	안전 등급
열차자율주행 시스템	자동열차보호(ATP)	[위험요인] 의도하지 않은 감속, 자동 정지 기능 미수행 [영향력] 열차 간 충돌, 열차 탈선 등으로 승객 사상	S4	시스템이 스스로 운행상황을 파악하고, 필요시 감속 및 제어를 자율적으로 수행. 이 시스템으로 인한 위험을 통제할 수 있는 다른 안전장치가 없고, 위험상황에 대한 운영자의 개입이 어려움	C4	VH
신호관제시스템	진로제어	[위험요인] 잘못된 방향으로 진로 제어, 진로 변경 제어 미수행 [영향력] 열차 간 충돌, 작업자 추돌 등으로 승객 또는 작업자 사상	S4	기본적으로 시스템이 자동으로 진로를 제어함. 필요시 운영자가 제어에 개입 가능	C3	VH
	열차추적	[위험요인] 선로에 위치한 열차 정보 미제공 또는 지연 제공으로 진로제어 오류 [영향력] 열차 간 충돌, 작업자 추돌 등으로 승객 또는 작업자 사상	S4	진로제어를 위해 필수적인 열차추적 정보를 제공함. 열차의 위치를 파악하기 위해 다른 방법(예, 열차운행계획, 기관사/역무원 확인 등)을 통해 관련 정보를 확인함.	C2	H
터널관리시스템	제연시설(환풍기) 제어	[위험요인] 제연시설 미작동 [영향력] 터널 내 발생한 유독가스 미배출로 인한 인명사상, 제연 미수행으로 2차사고 발생 및 인명사상	S4	기본적으로 시스템이 자동으로 상황을 인지하여 제연을 수행함. 필요시 운영자(관제)가 수동제어 가능	C3	VH
표준수운영시스템	정수공정감시	[위험요인] 잘못된 수질 측정 또는 공정상태 정보 제공	S2	수질 측정 또는 공정 상태 정보는 상수처리를 위해 필수 정보임. 이 시스템 외에 관련	C3	H

		[영향력] 수질기준에 부적합한 수도물 송.배수로 인명 피해		정보를 제공하는 시스템 없음		
항공등화감시 제어시스템	활주로 등화 감시제어	[위험요인] 잘못된 활주로에 대한 등화 제어, 활주로 점등 미수행 [영향력] 항공기 이탈 또는 항공기 간 충돌로 인명 사상	S4	운영자가 수동 제어 및 확인 (시스템 자동 제어 아님)	C2	H
	유도로 등화 감시제어	[위험요인] 잘못된 유도로에 대한 등화 제어, 유도로 점등 미수행 [영향력] 항공기 이탈 또는 항공기와 다른 물체(이동차량 등) 간 충돌로 인명 사상	S3	운영자가 수동 제어 및 확인 (시스템 자동 제어 아님)	C2	H
댐관리시스템	원격측정 및 감시	[위험요인] 잘못된 수위 정보 제공 [영향력] 댐 수위 관리를 잘못하여, 댐 월류로 인한 발전설비 고장 또는 인명 피해	S4	수문 제어를 수행하는데 판단 근거가 되는 필수적인 정보를 제공함. 다른 방법(예, 영상관제시스템, 운영자 육안 확인 등)을 통해 관련 정보를 중복 확인함	C2	H
산림재해통합 관리시스템	산불상황관제 및 대응	[위험요인] 잘못된 산불발생 장소 정보 제공, 지연된 산불발생 정보 제공 [영향력] 산불 대응 활동을 못하거나, 지연으로 재산 피해 및 인명 피해 증가	S4	산불 대응활동을 하는데 산불상황 정보는 필수적임. 다른 방법(예, 전화통화, 현장확인 등)을 통해 관련 정보를 중복 확인함	C2	H
	산사태 예보 발령	[위험요인] 산사태 예보 정보가 제공되지 않거나 잘못된 정보 제공 [영향력] 미리 대피하지 못해	S4 à S3*	휴대폰을 통한 산사태 예보 정보가 대피를 위해 도움이 되는 정보이기는 하나, 현장에서의 기상상태 확인, 대중매체, 현장방송/통제 등 정보를 전달할 수 있는	C1	M

		인명 피해 발생		다양한 방법이 존재하여 해당 정보의 부재로 인한 피해의 직접적인 연관성이 낮음		
해양기상신호 표지시스템	해양안전정보 수집 및 전파	[위험요인] 해양안전정보가 제공되지 않거나 잘못된 정보 제공 [영향력] 정보부족으로 해양활동 시 안전사고 발생	S4 à S3*	해양안전정보(기상, 항로, 조류 등)가 정보가 안전한 해양활동을 위해 도움이 되는 정보이기는 하나, 현장에서의 기상상태 확인, 대중매체, 현장방송/통제 등 정보를 전달할 수 있는 다양한 방법이 존재하여 해당 정보의 부재로 인한 피해의 직접적인 연관성이 낮음	C1	M
대국민교통정보시스템	교통상황/돌발상황 전파	[위험요인] 교통/돌발상황(사고 등) 정보가 제공되지 않거나 잘못된 정보 제공 [영향력] 교통/돌발상황 정보 부족으로 사고가 발생되지는 않음	S0	교통/돌발상황 정보가 안전운전에 도움이 되는 정보이기는 하나, 안전운전은 대부분 운전자의 현장상황 판단에 의존하며 교통/돌발상황 정보가 사고 회피를 위한 필수 정보는 아님	C1	L
여객흐름관리시스템	자동입국심사 및 검역관리	[위험요인] 입국심사 및 검역관리 처리 지연 또는 기능 미제공 [영향력] 공항 혼잡 또는 항공기 출발 지연 발생 (안전 관련 없음)	S0	안전과 관련된 제어 기능 또는 정보를 제공하지 않음	C0	L

<표 7-11> 예시 - 소프트웨어 안전등급 판정 대상 시스템 정보

시스템 명	기관 및 주무부처	설명
열차자율주행시스템	도시철도공사	이동 폐색 방식 등을 이용하여 기관사가 탑승하지 않고, 열차간 무선통신을 통해 열차의 속도, 운행위치 등을 원격으로 제어하고, 열차의 출입문 개폐와 가/감속을 제어하는 시스템

신호관제시스템	도시철도공사	도시철도의 선로상태 정보와 열차의 운행상태를 파악하여 열차 운행스케줄에 따라 진로를 설정하는 등 열차의 운영관리에 대한 전반적인 업무를 자동으로 수행하기 위해 개발된 시스템
터널관리 시스템	한국도로공사(국토교통부)	전국 각 지 터널 내 설비의 실시간 모니터링 및 제어를 통해 원활한 방재업무를 수행하고, 각 지사별 상황실의 터널설비 운영을 지원하여 업무효율화를 제고하기 위해 개발된 시스템
표준수운영 시스템	수자원공사(환경부)	수처리를 위한 취수장 및 정수장, 가압장 등의 시설에 대하여, 원격지 통합센터에서 감시 및 제어하기 위해 표준화된 수도 통합운영 시스템
항공등화감시제어 시스템	한국공항공사(국토교통부)	활주로 및 유도로 주변에 설치된 항공등화를 제어하여 항공기의 이착륙을 지원하기 위해 개발된 시스템
댐 관리 시스템	한국수력원자력(산업통상자원부)	발전 및 수계 운영을 종합 관리하는 시스템
산림재해통합관리 시스템	산림청	산림 생태 통계, 국가 산림자원 및 산림생물 정보 등 각종 산림 공간정보를 제공하고, 산불상황 관제, 산사태 예보 발령, 병해충 방제 관리 등 각종 산림재해에 대응하고 관리하기 위해 개발된 시스템
해양기상신호표지 시스템	국립해양측위정보원(해양수산부)	항로상의 해양기상 정보를 항행 선박, 조업 선박, 레저 보트 등의 관련 선박 및 사용자들에게 적기에 제공하여 안전한 해양 활동을 지원하기 위해 개발된 시스템
대국민교통정보 시스템	한국도로공사(국토교통부)	고속도로의 교통상황과 돌발상황 관련 정보들을 수집 및 가공하여 원활한 교통소통 및 안전관리 등에 활용하고, 운전자에게 다양한 교통정보를 제공하기 위해 개발된 시스템
여객흐름관리 시스템	인천국제공항공사(국토교통부)	출국장 및 환승장에서 여객의 진입 시 유효성을 확인하는 기능

		과 보안 검색을 위한 기능을 제공하며 여객 흐름 및 혼잡도 정보를 연계 시스템에 전달하여 여객의 편의성 관련 업무를 효율적으로 수행할 수 있도록 하는 시스템

〈표 7-12〉 예시 - 소프트웨어 안전등급 판정 대상 시스템 기능 설명

시스템 명	소프트웨어 기능	설명
열차자율주행시스템	자동열차보호(ATP)	전방열차의 위치에 따라 후방 열차의 속도를 제어하는 장치로 열차 과속 사고를 방지할 수 있는 안전거리 확보 및 선로 이용 효율 증대를 위해 제공하는 기능
신호관제 시스템	진로 제어	열차운행스케줄에 의하여 감시시간에 주어진 진로에 대해 자동으로 제어하는 기능
	열차 추적	궤도상태를 운영자 콘솔에 전송, 화면에 현시하여 열차의 이동 상황을 알리고, 점유와 해제정보를 이용하여 열차를 이동시키며, 현장설비간 정보전송장치를 통해 정거장에서 정보수신 시 열차번호를 점검하여 상이하면 경고 메시시를 출력하고, 차상에 궤도상태로 추적된 열차번호를 전송하는 기능
터널관리 시스템	제연시설(환풍기) 제어	터널 내 제연설비의 상태정보 및 이벤트 정보와 센서를 통한 터널 내 화재 및 공기질 상태 정보를 참고하여 해당 설비의 원격 제어를 진행하는 기능
표준수운영 시스템	정수공정 감시	수처리 공정과정에서의 현장 설비의 데이터를 취득하여 설비상태를 모니터링 하고, 밸브, 펌프 등과 같은 공정 설비에 제어 명령을 제공하는 기능
항공등화감시제어 시스템	활주로 등화 감시제어	항공기 활주로등, 활주로시단등, 활주로종단등, 접지구역대등 등의 활주로 상의 등화 관련 현장 설비의 상태 정보를 취득하여 모니터링하고, 해당 등화를 관제하는 기능
	유도로 등화 감시제어	항공기 유도로중선등, 일시정지 위치등, 유도로등 등의 유도로 상의 등화 관련 현장 설비의 상태 정보를 취득하여 모니터링하고, 해당 등화를 관제하는 기능
댐관리 시스템	원격측정 및 감시	댐 관련 현장 설비에서 계측되는 정보(저수위, 방수위 등) 및 현장 설비의 상태 등에 대한 정보를

		수집하여 운영자에게 제공하는 기능
산림재해통합관리 시스템	산불상황관제 및 대응	GPS 단말기를 통한 산불신고 및 모바일 앱, 119 신고 시스템으로 입수된 산불 신고 정보가 자동으로 연계되어 관계자에게 알림을 제공하는 기능
	산사태 예보 발령	연계 시스템을 통해 산사태 예측정보를 받아 이를 조회하고, 예보 발령 및 문자 메시지를 발송하는 기능, 사방댐, 각종 산사태, 황폐지 통계 등의 대장 및 산사태 취약지역을 관리하는 기능을 제공하는 기능
해양기상신호표지 시스템	해양안전정보 수집 및 전파	해양안전종합정보시스템(GICOMS) 및 각 지방청으로부터 전송된 항로표지, 기상표지, 조류신호표지 등의 해양기상관측정보를 실시간으로 수집, 배포, 모니터링 하는 기능
대국민교통정보 시스템	교통상황/돌발상황 전파	도로 상에 설치된 차량검지시스템(VDS), 구간검지기(AVI) 등의 현장 설비로부터 교통 정보를 수집하고, 해당 정보를 가공하여 교통 상황정보를 제공하며, 민간 정보 및 CCTV 정보를 참고하여 문자 및 도로전광표지(VMS)로 해당 정보를 제공하는 기능
여객흐름관리 시스템	자동입국심사 및 검역관리	출입국 지원 단말들과 연계하여 출국장 및 환승장에 진입하는 여객에 대한 유효성을 확인하고 보안 검색을 수행하는 기능

5. 안전등급 선정 항목 및 지표에 대한 전문가 자문

최종 도출된 소프트웨어 안전등급 결정방안에 대하여, 다수의 소프트웨어안전 전문가들로부터 검토 의견을 청취하였다. 전문가 그룹은 원자력 분야, 항공 분야, 철도 분야, 자동차 분야 등 다양한 분야에서 활발히 활동하고 있는 인원으로 구성되었다.

전문가 검토 결과, 소프트웨어 안전등급의 평가 단위의 명확한 정의, 평가항목 및 지표 개선, 소프트웨어안전수단 중복 적용 시 고려사항, 시스템과 소프트웨어 간 안전등급 관계 등 다양한 검토 의견을 수렴하여 반영할 수 있었다. 전문가 검토 결과에 대한 분석 및 개선 방향, 반영 여부에 대한 내용은 다음 <표 7-13>를 통해 확인할 수 있다.

<표 7-13> 전문가 검토 결과

소프트웨어 안전등급 별 관리방안 주요 검토 의견	확인내용/개선방향	반영
안전등급 평가 단위 • 기능 단위로 안전등급 부여할 시, 소프트웨어 전체에 대한 등급 결정 방법 • 소프트웨어 전체에 대한 안전등급 부여를 위해 파티셔닝에대한 설명 필요	소프트웨어 전체에 대한 안전등급은 기능 단위 평가 중 가장 높은 안전등급으로 부여됨 소프트웨어 기능에 대한 설명과전체 소프트웨어 등급 판단 시 독립성(파티셔닝조건)에 대한 설명을 추가함	O
소프트웨어 고장으로 인해 위험이 유발되는 경우(위험유발 소프트웨어)가 있고, 이미 발생한 위험에 대해 대응하는 소프트웨어(위험대응 소프트웨어)가 모두 고려되어야 함	소프트웨어 위험관여도에서 두 가지 유형을 모두 언급하고 있음 • 소프트웨어 유형에 상관 없이, 해당 상황(피해 직접 유발, 피해 증가)에 대한 관여도를 기반으로 안전등급을 판정함	O
소프트웨어 안전등급을 숫자로 표현할 경우, 낮은 숫자를 고 등급으로 표현해야 할지 낮은 등급으로 표현해야 할지 모호할 수 있음	소프트웨어 안전등급을 영문 표기로 변경하여 직관적으로 확인할 수 있도록 변경 • VH(Very High), H(High), M(Medium), L(Low)	O
‘타안전장치’ 항목을 소프트웨어위험 관여도 판단 시 고려하는 것이 적절한 것인가? 타 안전장치가 존재한다는 것은 고안전제품으로 분류됨	소프트웨어의 안전등급이 높게 결정될 경우, 해당 위험을 완화시키기 위해 ‘타 안전장치’가 구현되거나, 소프트웨어 시스템 자체를 fault tolerant하게 개발하는 것이 올바른 방향으로 여겨짐	X
소프트웨어를 포함한 시스템 자체의 안전등급이 높을 경우, 해당 시스템에 포함되는	현재 평가기준에서 ’위험 영향력’은 시스템 수준에서 평가되는 항목이며, 시스템 수준	O

소프트웨어의 안전등급도 기본적으로 높게 고려되어야 할 것으로 보임	의 평가가 어느 정도 반영되어야 하는 구조임. 상황에 따라, 시스템 등급을 그대로 상속받은 방법과 별도의 소프트웨어 안전등급 기준을 따를 수 있음을 언급함	
‘안전관련 기능’, '위험 영향력’, '위험 관여도' 등 용어의 정의가 필요할 것으로 보임	주요 용어에 대한 정의 추가	O
시스템 수준에서는 사고/위험의 발생가능성을 고려하는 경우가 있으며, 소프트웨어 안전등급 결정 시 해당 발생가능성을 고려할 필요가 있음	시스템 수준의 평가에서 발생 가능성이 낮은 경우, 소프트웨어 안전등급이 조정 가능하도록 보완	O
소프트웨어 안전등급의 판단 주체에 대한 고려 필요 • 판단이 주관적일 수 있으며, 담당자들은 등급을 낮추려 할 것임	해당 사항은 본 과제의 범위를 벗어나며, 제도적인 측면에서 고려되어야 할 필요가 있음	X

제8장 공공기관 시스템 소프트웨어 안전등급별 관리방안 도출

사회 안전과 관련된 각 분야별 주요 안전 표준을 대상으로 조사한 안전등급에 따른 안전활동 및 기술 내용을 기반으로, 공공기관 시스템의 소프트웨어 안전등급별 관리방안을 도출한다. 먼저, 조사 결과로 식별된 대상 표준들의 안전활동을 비교 분석하여 후보 관리방안을 도출한다. 이후, 후보 관리방안으로 정의된 각 안전활동들에 대응하는 산출물 및 안전기법, 수단 등을 정리한다. 해당 내용들에 대하여 전문가 검토를 통해 적절성을 검토받고, 최종 관리방안을 결정하도록 한다.

제1절 소프트웨어 안전등급별 관리방안 도출

1. 도메인별 안전표준들의 세부 안전활동 비교

안전등급에 따른 안전활동 및 기술 조사를 통해 식별한 각 도메인 별 안전활동들을 대상으로 수행, 검토, 분석 측면으로 활동들을 재 구조화하여 비교분석하였다. 수행, 검토, 분석은 다음과 같이 정의된다.

- ㅇ 수행: 각 단계 별 주요 개발 및 검증 활동의 수행
- ㅇ 검토: 수행 활동을 통해 작성된 산출물과 이전 단계산출물과의 일관성 및 완전성 측면에서의 검토
- ㅇ 분석: 각 단계별 활동 수준에서 야기될 수 있는 위험 요소의 존재를 식별하고, 식별된 위험 요소가 시스템 소프트웨어의 전체 안전에 얼마만큼의 영향을 미치는지 분석하는 활동

또한, 각 표준마다 정의하고 있는 안전활동들의 수준이 서로 상이하여 표준들 간의 활동 수준을 조정하였다. 일부 표준의 경우, 세부 요구사항을 기반으로 하위 활동을 재 식별하였고, 일부 표준의 경우, 기법 및 수단으로 표현 가능한 수준의 활동은 제외하였다. 각 표준들의 안전활동 비교 결과는 아래 표와 같다.

<표 8-1> 각 표준 별 안전활동 비교 - 산업일반 및 철도, 자동차 분야

단계	세부 활동	IEC 61508	IEC 62279	ISO 26262
Req.	수행	Software safety requirements specification	Specify software requirements	Specify or refine the software safety requirements Definethesafetyrelatedfunctionalitiesandproperties Refinehardware-softwareinterfacerequirements
	검토	Verification of software safety requirements	Verify software requirements	Verify the software safety requirements
	분석	Common cause failure analysis	Common cause failure analysis	-
Arch. Design	수행	Software architectural design	Specify software archtecture Specifysoftwaredesign Specifysoftwareinterface	Develop the software architectural design Supporttheimplementationandverification ofthesoftware
	검토	Verification of software architecture	Verify software architecture and design	Verify the software architectural design
	분석	세부 요구사항에서 관련 안전 분석 언급	세부 요구사항에서 관련 안전 분석 언급	세부 요구사항에서 관련 안전 분석 언급(Safety-oriented analysis Analyses)
Detailed Design	수행	Software detailed design and development - 소프트웨어 system design Softwaredetaileddesignanddevelopment-Individual소프트웨어moduledesign	Specify software component design	Develop the software unit design
	검토	Verification of software module design	Verify software component design	Verify software units design
	분석	-	-	-
Implement	수행	Code implementation	Implement software source code	Implement the software units

ation	검토	Verification of software source code	Verify software source code	Verify implemented software units
	분석	-	-	-
소프트웨어 Unit Test	수행	소프트웨어 module testing	Test software component	Verify implemented software units
	검토	-	-	Confirmation reivew
소프트웨어 Integration Test	수행	소프트웨어 integration testing	Specify software integration test case Specifysoftware/hardwareintegrationtestcase Testsoftwareintegrationtest Testsoftware/hardwareintegrationtest Verifysoftwareintegration	Define integration steps and integrate the softwate elements Verifyintegratedsoftwareunitandcomponents
	검토	-	-	Confirmation reivew
소프트웨어 Test	수행	Programmable electronics integration (HWand소프트웨어) Validationplanforsoftwareaspectsofsystem safety	Specify overall software test Testoverallsoftware Validatesoftware	Provide evidence that the embedded software fulfiles the safety related requirements
	검토	-	-	Confirmation reivew

<표 8-2> 각 표준 별 안전활동 비교 - 항공우주 및 국방 분야

단계	세부 활동	NASA-STD/GB-8719-13C	MIL-STD-882E
Req.	수행	Software requirements development Development of software safety requirements	Derive system software safety requirements Documentingsoftwaresafetyrequirements
	검토	Formal inspections of software requirements Formalmethodsforverification	-

		Modelchecking	
	분석	Timing, throughput and sizing analysis Safetyrequirementsflowdownanalysis Requirementscriticalityanalysis Specificationanalysisforsafetycriticalrequirements Softwarefaulttreeanalysis Softwarefailuremodesandeffectsanalysis	In-Depth hazard causal analysis
Arch. Design	수행	Create design from requirements, incorporating safety requirements and features Designforreliabilityandmaintainability Selectlanguage,operatingsystemandtools SelectCOTSandreusablecomponents Developlanguagerestrictionsandcodingstandards	Preliminary software design
	검토	Formal inspection of design products Reviewdesign	-
	분석	Update criticality analysis Designsafetyanalysis Softwareelementanalysis Hazardriskassessment	Module safety criticality analysis Programstructureanalysis Traceabilityanalysis
Detailed Design	수행	Create design from requirements, incorporating safety requirements and features Designforreliabilityandmaintainability Selectlanguage,operatingsystemandtools SelectCOTSandreusablecomponents Developlanguagerestrictionsandcodingstandards	Detailed software design
	검토	Formal inspection of design products Reviewdesign	

	분석	Update criticality analysis Designsafetyanalysis Softwareelementanalysis	Safety critical path analysis, thread analysis Code-levelanalysis
Implement ation	수행	Create source code that implements the design, including safety features. MaintainsourcecodewithinaConfigurationManagementsystem,wit hadequatedocumentationofchanges. Followcodingstandardsandchecklists. Followformalchangeprocessforchangestobaselinedsystem.	-
	검토	Participate in Formal Inspections and informal code reviews. ParticipateinSourcecodeFormalInspectionsofsafety-criticalcode. ProgramSlicingfordebugging. Witnessanyformalunittesting. Participateinformalchangeprocess(changecontrolboard)	-
	분석	Review previous analyses and update with new information. Codeanalysis ProgramSlicingforsafety-criticalvariablesordata	-
소프트웨어 Unit Test	수행	Perform unit testing on individual source units. Prepare and follow test procedures for safety-critical units.	Nominal and functional requirements based testing Robustnesstesting
	검토	Review unit test plans and results for safety-critical units. TestCoverageAnalysis Verifyunittestsadequatelytestthesoftwareandareactuallyperform ed.	Demonstrate compliance with all software design(TC) Accomplishedbysoftwarestructuralcoverageanalysis
소프트웨어 Integration Test	수행	Integrate individual software units into a complete software system. Integratethesoftwarewiththehardwaresystemandperformtestingt hroughouttheprocess.	Nominal and functional requirements based testing Robustnesstesting

		Createandfollowwrittentestproceduresforintegrationandsystemtesting.* Performregressiontestingaftereachchangetothesystem.*	
	검토	Participate in Formal Inspections of test plans and procedures. ParticipateinTestPlanandProceduresFormalInspection소프트웨어hensafety-criticalfunctionsaretobetested. Verifyallsafetyrequirementshavebeenadequatelytested(SafetyVerificationMatrix). Analyzetestreportsforcompletenessandrequirementscoverage.	Demonstrate compliance with all software design(TC) Accomplishedbysoftwarestructuralcoverageanalysis
소프트웨어 Test	수행	Integrate individual software units into a complete software system.	Nominal and functional requirements based testing Robustnesstesting
	검토	Participate in Formal Inspections of test plans and procedures. ParticipateinTestPlanandProceduresFormalInspection소프트웨어hensafety-criticalfunctionsaretobetested. Verifyallsafetyrequirementshavebeenadequatelytested(SafetyVerificationMatrix). Analyzetestreportsforcompletenessandrequirementscoverage.	Demonstrate compliance with all software requirements(TC) Accomplishedbysoftwarerequirementscoverageanalysis

<표 8-3> 각 표준 별 안전활동 비교 - 항공 및 의료 분야

단계	세부 활동	DO-178C	IEC 62304
Req.	수행	Develop high-level requirements	Define and document software requirements from system requirements

			Softwarerequirementscontent
	검토	Verify high-level requirements	Verify software requirements
	분석	세부 요구사항에서 소프트웨어 요구사항에 대한 검토 및 분석이 언급됨	Include risk control measures in software requirements Re-evaluatemedicaldeviceriskanalysis
Arch. Design	수행	Develop software architecture Developlow-levelrequirements	Transform software requirements into an architecture Developanarchitecturefortheinterfacesofsoftwareitems Specifyfunctionalandperformancerequirementsofsoupitem Specifysystemhardwareandsoftwarerequiredbysoupitem
	검토	Verify software architecture Verifylow-levelrequirements	Verify software architecture
	분석	세부 요구사항에서 아키텍처 설계에 대한 검토 및 분석이 언급됨	Identify segregation necessary for risk control
Detailed Design	수행	Develop low-level requirements	Subdivide software into software units Developdetaileddesignforeachsoftwareunit Developdetaileddesignforinterfaces
	검토	Verify low-level requirements	Verify detailed design
	분석	세부 요구사항에서 상세 설계에 대한 검토 및 분석이 언급됨	
Implement ation	수행	Develop source code	Implement each software unit
	검토	Verify source code	
	분석	세부 요구사항에서 소스코드에 대한 검토 및 분석이 언급됨	
소프트웨어 Unit Test	수행	Test low-level requirements	Establish software unit verification process Softwareunitacceptancecriteria Additionalsoftwareunitacceptancecriteria Softwareunitverification
	검토	Verify test procedure Analyzetestcoverageacheivement Analyzetestresult	
소프트웨	수행	Test low-level requirements	Integrate software units

어 Integration Test		Testsoftwarearchitecture	Verifysoftwareintegration Softwareintegrationtesting Softwareintegrationtestingcontent Conductregressiontests Integraitontestrecordcontents Usesoftwareproblemresolutionprocess
	검토	Verify test procedure Analyzetestcoverageacheivement Analyzetestresult	Evaluate software integration test procedures
소프트웨 어 Test	수행	Test high-level requirements	Establish tests for software requirements Retestafterchanges Softwaresystemtestrecordcontents Usesoftwareproblemresolutionprocess
	검토	Verify test procedure Analyzetestcoverageacheivement Analyzetestresult	Evaluate software system testing

2. 소프트웨어 안전등급별 활동 비교 분석

분야 별 대상 표준들의 안전활동 비교 내용을 기반으로 소프트웨어 안전등급 관점에서의 활동 비교를 수행한다. 활동의 수준과 마찬가지로, 각 표준들에서 제안하고 있는 소프트웨어 안전등급의 수준도 모두 상이하다. 먼저, 분석 대상인 각 표준에서 정의된 안전등급과 본 연구에서 제안한 소프트웨어 안전등급과의 비교를 통해 소프트웨어 안전등급에 대한 적용방안의 근거를 마련한다.

<표 8-4> 각 표준의 안전등급과 본 연구에서 제안한 안전등급 비교

표준	위험영향력				
SPRi	Very High	High		Medium	Low
NASA-STD-8719-13C	FULL	MOD		MIN	-
MIL-STD-882E	소프트웨어CI 1	소프트웨어CI 2	소프트웨어CI 3	소프트웨어CI 4	소프트웨어CI 5
IEC 61508	SIL 4	SIL 3	SIL 2	SIL 1	-
IEC 62279	SIL 4	SIL 3	SIL 2	SIL 1	SIL 0
ISO 26262	ASIL D	ASIL C	ASIL B	ASIL A	QM
DO-178C	A	B	C	D	E
IEC 62304	Class C	Class B		Class A	

또한, 수행, 검토, 분석 측면의 각 활동에 대한 독립성 수준은 아래와 같은 표기법으로 구분한다.

○ : 대상 활동 수행 시, 독립성이 고려되지 않아도 됨
● : 대상 활동 수행 시, 독립성이 고려되어야 함
I0 : 산출물 작성자가 아닌 사람이 검토 및 검증을 수행해야 함
I1 : 산출물 작성자의 업무와 직접적인 관계가 없는 사람이 검토 및 검증을 수행해야 함
I2 : 산출물 작성자와 서로 다른 팀의 사람이 검토 및 검증을 수행해야 함
(검토자는 프로젝트 관리자에게 검토 결과를 보고하지 않으며, 제품의 출시를 중단할 수 있음)

가. 수행 활동에 대한 분석

소프트웨어 안전등급을 기준으로 각 표준에서 언급하고 있는 안전활동 중 '수행' 측면의 활동에 대하여 분석한다. 아래 그림을 살펴보면, IEC 62279,

IEC 62304 표준은 안전에 영향이 없는 Low 등급에서도 소프트웨어안전요구사항 정의 및 구현, 검증 일부 활동 등의 단계별 주요 활동의 수행을 권고하고 있다. MIL-STD-882E 표준의 경우, 안전 등급에 따른 별도 수행 구분을 특정짓고 있지 않았지만, 모든 등급에서 기본적인 개발 및 검증 활동들을 언급하고 있다. 해당 표준은 안전 달성을 위해 원하는 결과와 목표달성을 위한 안전 활동을 모델에 적절하게 연관시키고 통합해야 한다는 것을 강조하고 있다.

이외의 표준에서는 Medium 등급 이상일 경우에만, 대부분의 기본 개발 및 검증 활동의 수행을 권고하고 있다. IEC 62304, DO-178C 표준의 경우, 안전 등급이 Medium일 때 설계 및 설계검증 활동 일부가 생략될 수 있으며, NASA 표준에서는 High ~ Medium 등급에서 단위 및 통합 테스트 활동의 생략이 가능하다.

또한 IEC 62279 표준과 DO-178C 표준에서는 검증 단계활동에 독립성 수준에 대한 요구사항을 반영하고 있다.

[그림 8-1] 수행 활동 측면에 대한 분석 - 항공우주, 국방, 의료, 항공 분야

단계	NASA-STD				MIL-STD				IEC 62304				DO-178C			
	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low
Requirements	O	O	O	-	O	O	O	O	O	O	O	O	O	O	O	-
Architecture Design	O	O	O	-	O	O	O	O	O	O	-	-	O	O	O	-
Detailed Design	O	O	O	-	O	O	O	O	O	O	-	-	O	O	-	-
Implementation	O	O	O	-	-	-	-	-	O	O	O	O	O	O	O	-
SW Unit Test	O	-	-	-	O	O	O	O	O	O	-	-	●(I1)	●(I0)	-	-
SW Integration Test	O	-	-	-	O	O	O	O	O	O	-	-	●(I1)	●(I0)	-	-
SW Test	O	O	O	-	O	O	O	O	O	O	O	O	O	O	O	-

[그림 8-2] 수행 활동 측면에 대한 분석 - 산업일반, 철도, 자동차 분야

단계	IEC 61508				IEC 62279				ISO 26262			
	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low
Requirements	O	O	O	-	O	O	O	O	O	O	O	-
Architecture Design	O	O	O	-	O	O	O	O	O	O	O	-
Detailed Design	O	O	O	-	O	O	O	-	O	O	O	-
Implementation	O	O	O	-	O	O	O	O	O	O	O	-
SW Unit Test	O	O	O	-	●(I2)	●(I2)	●(I1)	-	O	O	O	-
SW Integration Test	O	O	O	-	●(I2)	●(I2)	●(I1)	O	O	O	O	-
SW Test	O	O	O	-	●(I2)	●(I2)	●(I1)	O	O	O	O	-

해당 분석 결과를 기반으로, 다음과 같은 세부 방안을 도출할 수 있다.

<표 8-5> 수행 활동 측면에서의 세부 관리방안

세부 방안	내용
1안	• Low 등급은 안전에 영향이 없는 등급으로 간주하여, 별도의 안전 활동을 권고하지 않음 • 각 단계 별, 기본 개발 활동 및 검증 활동은 등급과 무관하게 모두 수행 • 검증 활동의 경우, DO-178C 표준 및 IEC 62279 표준을 참고하여 독립성 수준을 구분 - 타 표준에서는 독립성 수준을 언급하지 않았지만, 독립적인 검토 및 검증의 중요성을 언급하고 있음(ISO 26262, NASA 표준 등) - 독립성 수준은 IEC 62279 표준을 참고하여 적용함
2안	• Low 등급은 안전에 영향이 없는 등급으로 간주하여, 별도의 안전 활동을 권고하지 않음 • 안전 등급에 따라, 설계 및 설계에 대한 검증 활동의 수행을 구분함 - IEC 62304 및 DO-178C 표준을 참고하여 Medium 단계에서의 설계 및 설계에 대한 검증 활동을 생략함 • 검증 활동의 경우, DO-178C 표준 및 IEC 62279 표준을 참고하여 독립성 수준을 구분 - 1안과 달리, Medium 등급에서는 일부 검증 활동을 생략하므로 보다 완화된 수준의 DO-178C 표준의 독립성 수준을 참고함

나. 검토 활동에 대한 분석

소프트웨어 안전등급을 기준으로 각 표준에서 언급하고 있는 안전활동 중 ‘검토’ 측면의 활동에 대하여 분석한다. IEC 62279, IEC 62304 표준은 안전에 영향이 없는 Low 등급에서도 일부 검토 활동의 수행을 권고하고 있다. ‘수행’ 활동 측면과 마찬가지로, MIL-STD-882E 표준의 경우 안전 등급에 따른 별도 수행 구분을 특정 짓고 있지 않았지만, 모든 등급에서 기본적인 개발 및 검증 활동들을 언급하고 있다. 해당 표준은 안전 달성을 위해 원하는 결과와 목표달성을 위한 안전활동을 모델에 적절하게 연관시키고 통합해야 한다는 것을 강조하고 있다.

또한, NASA 및 MIL-STD 표준을 제외하면, 등급에 상관 없이(Medium 등급 이상) 개발 단계에서의 산출물에 대한 검토 활동이 대부분 수행되고 있는 것

을 확인할 수 있다. IEC 62405 표준과 DO-178C 표준에서는 등급이 Medium 일 경우, 설계 및 설계 검증 산출물에 대한 검토가 생략 가능하며, NASA 표준의 경우, Very High 등급에서만 모든 검토 활동이 수행되고, 아래 등급에서는 검토 활동이 대부분 생략 가능한 것을 확인할 수 있었다.

단계 별 검증 활동에 대한 산출물의 검토는, IEC 61508, IEC 62279 표준에서만 언급되지 않았으며, NASA 표준의 경우 등급에 따른 기본 검증활동 수행과 일관되게 검토 활동의 수행 여부가 구분됨을 확인할 수 있다. 또한, ISO 26262 및 IEC 62279 표준과 DO-178C 표준에서는 검토 활동에 독립성 수준에 대한 요구사항이 반영되어 있다.

[그림 8-3] 검토 활동 측면에 대한 분석 - 항공우주, 국방, 의료, 항공 분야

단계	NASA-STD				MIL-STD				IEC 62304				DO-178C			
	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low
Requirements	O	O	-	-	-	-	-	-	O	O	O	O	●(I1)	●(I0)	O	-
Architecture Design	O	-	-	-	-	-	-	-	O	O	-	-	●(I1)	●(I0)	-	-
Detailed Design	O	-	-	-	-	-	-	-	O	-	-	-	●(I1)	●(I0)	-	-
Implementation	O	O	-	-	-	-	-	-	O	O	-	-	●(I1)	●(I0)	-	-
SW Unit Test	O	-	-	-	O	O	O	O	O	O	-	-	●(I1)	●(I0)	-	-
SW Integration Test	O	-	-	-	O	O	O	O	O	O	-	-	●(I1)	●(I0)	-	-
SW Test	O	O	O	-	O	O	O	O	O	O	O	O	●(I1)	O	O	-

[그림 8-4] 검토 활동 측면에 대한 분석 - 산업일반, 철도, 자동차 분야

단계	IEC 61508				IEC 62279				ISO 26262			
	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low
Requirements	O	O	O	-	●(I2)	●(I2)	●(I1)	O	O	O	O	-
Architecture Design	O	O	O	-	●(I2)	●(I2)	●(I1)	O	●(I3)	●(I1/I2)	●(I1)	-
Detailed Design	O	O	O	-	●(I2)	●(I2)	●(I1)	-	O	O	O	-
Implementation	O	O	O	-	●(I2)	●(I2)	●(I1)	O	O	O	O	-
SW Unit Test	-	-	-	-	-	-	-	-	●(I2)	●(I1/I2)	●(I0)	-
SW Integration Test	-	-	-	-	-	-	-	-	●(I2)	●(I1/I2)	●(I0)	-
SW Test	-	-	-	-	-	-	-	-	●(I2)	●(I1/I2)	●(I0)	-

해당 분석 결과를 기반으로, 다음과 같은 세부 방안을 도출할 수 있다.

〈표 8-6〉 검토 활동 측면에서의 세부 관리방안

세부 방안	내용
1안	• Low 등급은 안전에 영향이 없는 등급으로 간주하여, 별도의 안전 활

	동을 권고하지 않음 • 각 단계 별, 개발 및 검증 산출물에 대한 검토 활동은 등급과 무관하게 모두 수행 - 개발 활동에 대한 산출물 검토는 ISO 26262, IEC 61508, IEC 62279 표준을 참고하며, 독립성 수준은 IEC 62279 표준을 참고하되 I0부터 순차적으로 수준을 올림 - 검증 활동에 대한 산출물 검토는 ISO 26262 표준을 참고하며, 독립성 수준 또한 해당 표준을 참고함
2안	• Low 등급은 안전에 영향이 없는 등급으로 간주하여, 별도의 안전 활동을 권고하지 않음 • 안전 등급에 따라, 개발 산출물에 대한 검토 활동의 수행을 구분함 - IEC 62304 표준과 DO-178 표준을 참고하여, Medium 등급에서는 설계 및 설계에 대한 검증 단계에서 검토 활동을 수행하지 않음 - 해당 안은 1안에 비해 상대적으로 검토의 중요성을 낮게 판단하므로, 독립성 수준은 DO-178C를 따름

다. 분석 활동에 대한 분석

소프트웨어 안전등급을 기준으로 각 표준에서 언급하고 있는 안전활동 중 '분석' 측면의 활동에 대하여 분석한다. MIL-STD 및 ISO 26262 표준을 제외하고, 대부분의 표준이 안전 등급에 따라 안전 분석 활동의 수행을 구분하고 있다. NASA 및 MIL-STD 표준의 경우, 소프트웨어에 대한 안전 분석에 초점을 맞춘 표준이므로, 타 표준들과 달리 전 단계 별 안전 활동들이 언급되고 있다.

[그림 8-5] 분석 활동 측면에 대한 분석 - 항공우주, 국방, 의료, 항공 분야

단계	NASA-STD				MIL-STD				IEC 62304				DO-178C			
	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low
Requirements	O	O	-	-	O	O	O	O	O	O	-	-	-	-	-	-
Architecture Design	O	O	-	-	O	O	O	O	O	-	-	-	-	-	-	-
Detailed Design	O	O	-	-	O	O	O	O	-	-	-	-	-	-	-	-
Implementation	O	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

[그림 8-6] 분석 활동 측면에 대한 분석 - 산업일반, 철도, 자동차 분야

단계	IEC 61508				IEC 62279				ISO 26262			
	Very High	High	Medium	Low	Very High	High	Medium	Low	Very High	High	Medium	Low
Requirements	○	○	-	-	○	○	-	-	-	-	-	-
Architecture Design	○	○	-	-	○	○			○	○	○	-
Detailed Design	-	-	-	-	-	-	-	-	-	-	-	-
Implementation	-	-	-	-	-	-	-	-	-	-	-	-

해당 분석 결과를 기반으로, 다음과 같은 세부 방안을 도출할 수 있다.

<표 8-7> 분석 활동 측면에서의 세부 관리방안

세부 방안	내용
1안	• Low 등급은 안전에 영향이 없는 등급으로 간주하여, 별도의 안전 활동을 권고하지 않음 • 대부분의 표준과 같이, 안전분석 활동은 등급에 따라 수행을 구분함 - Very High, High 등급에서는 안전분석 활동을 수행 - Medium 등급에서는 안전분석 활동의 수행을 생략함 • NASA 및 MIL-STD 표준을 참고하여, 전 단계 별 세부 활동으로 안전분석 활동을 수행함 - Very High일 경우, 모든 단계에서 수행 - High일 경우, 구현 단계를 제외한 모든 단계에서 수행

3. 소프트웨어 안전등급별 후보 관리방안 도출

수행, 검토, 분석 측면에서의 활동 분석을 통해 도출한 세부 관리방안을 기반으로 후보 관리방안을 도출한다. 후보 관리방안은 수행, 검토, 분석 측면의 각 세부 관리방안의 조합을 통해 도출한다. 수행 측면의 활동, 즉, 단계별 주요 활동이 수행되지 않은 경우에는 검토 활동 또한 수행되지 않으므로, 해당 경우는 제외하고 후보 관리방안을 도출한다. 후보 관리방안은 다음과 같이 총 3개의 유형으로 구분될 수 있다.

ㅇ 소프트웨어 안전등급별 후보 관리방안 1

- 안전 관련 개발 및 검토 활동은 등급에 구분 없이 모두 수행함
- 등급에 따른 관리방안 수준의 차이는 다음과 같음
  . 분석 활동의 수행 유무
  . 검토 활동의 독립성 수준

ㅇ 소프트웨어 안전등급별 후보 관리방안 2
- ‘수행’, ‘검토’, ‘분석’ 활동 모두 안전 등급에 따라 구분하여 수행함
- 등급에 따른 관리방안 수준의 차이
  . 주요 개발 및 검증 활동, 분석 활동, 검토 활동의 수행 유무
  . 검토 활동의 독립성 수준

ㅇ 소프트웨어 안전등급별 후보 관리방안 3
- 단계별 메인 활동은 등급에 구분 없이 모두 수행함
- 등급에 따른 관리방안 수준의 차이
  . 검토 및 분석 활동의 수행 유무
  . 검토 활동의 독립성 수준

[그림 8-7] 소프트웨어 안전등급별 후보 관리방안 1

단계	세부활동	SW안전등급			
		Very High	High	Medium	Low
Requirements	SW 안전 요구사항 정의	○	○	○	별도의 안전관련 활동을 요구하지 않음
	SW 안전 요구사항 검토	●(I2)	●(I1)	●(I0)	
	SW 안전 요구사항 분석	○	○		
Architecture Design	SW 안전 아키텍처 설계	○	○	○	
	SW 안전 아키텍처 검토	●(I2)	●(I1)	●(I0)	
	SW 안전 아키텍처 분석	○	○		
Detailed Design	SW 안전 상세 설계	○	○	○	
	SW 안전 상세 검토	●(I2)	●(I1)	●(I0)	
	SW 안전 상세 분석	○	○		
Implementation	SW 안전 구현	○	○	○	
	SW 안전 구현 검토	●(I2)	●(I1)	●(I0)	
	SW 안전 구현 분석	○			
SW Unit Test	SW 단위 테스트 수행	●(I1)	●(I0)	○	
	SW 단위 테스트 검토	●(I2)	●(I1)	●(I0)	
SW Integration Test	SW 통합 테스트 수행	●(I1)	●(I0)	○	
	SW 통합 테스트 검토	●(I2)	●(I1)	●(I0)	
SW Test	SW 테스트 수행	●(I1)	●(I0)	○	
	SW 테스트 검토	●(I2)	●(I1)	●(I0)	

[그림 8-8] 소프트웨어 안전등급별 후보 관리방안 2

단계	세부활동	SW안전등급			
		Very High	High	Medium	Low
Requirements	SW 안전 요구사항 정의	○	○	○	별도의 안전관련 활동을 요구하지 않음
	SW 안전 요구사항 검토	●(I1)	●(I0)		
	SW 안전 요구사항 분석	○	○		
Architecture Design	SW 안전 아키텍처 설계	○	○		
	SW 안전 아키텍처 검토	●(I1)	●(I0)		
	SW 안전 아키텍처 분석	○	○		
Detailed Design	SW 안전 상세 설계	○	○		
	SW 안전 상세 검토	●(I1)	●(I0)		
	SW 안전 상세 분석	○	○		
Implementation	SW 안전 구현	○	○	○	
	SW 안전 구현 검토	●(I1)	●(I0)		
	SW 안전 구현 분석	○			
SW Unit Test	SW 단위 테스트 수행	●(I1)	●(I0)		
	SW 단위 테스트 검토	●(I1)	●(I0)		
SW Integration Test	SW 통합 테스트 수행	●(I1)	●(I0)		
	SW 통합 테스트 검토	●(I1)	●(I0)		
SW Test	SW 테스트 수행	●(I1)	●(I0)	○	
	SW 테스트 검토	●(I1)	●(I0)	○	

[그림 8-9] 소프트웨어 안전등급별 후보 관리방안 3

단계	세부활동	SW안전등급			
		Very High	High	Medium	Low
Requirements	SW 안전 요구사항 정의	○	○	○	별도의 안전관련 활동을 요구하지 않음
	SW 안전 요구사항 검토	●(I1)	●(I0)		
	SW 안전 요구사항 분석	○	○		
Architecture Design	SW 안전 아키텍처 설계	○	○	○	
	SW 안전 아키텍처 검토	●(I1)	●(I0)		
	SW 안전 아키텍처 분석	○	○		
Detailed Design	SW 안전 상세 설계	○	○	○	
	SW 안전 상세 검토	●(I1)	●(I0)		
	SW 안전 상세 분석	○	○		
Implementation	SW 안전 구현	○	○	○	
	SW 안전 구현 검토	●(I1)	●(I0)		
	SW 안전 구현 분석	○			
SW Unit Test	SW 단위 테스트 수행	●(I1)	●(I0)	○	
	SW 단위 테스트 검토	●(I1)	●(I0)		
SW Integration Test	SW 통합 테스트 수행	●(I1)	●(I0)	○	
	SW 통합 테스트 검토	●(I1)	●(I0)		
SW Test	SW 테스트 수행	●(I1)	●(I0)	○	
	SW 테스트 검토	●(I1)	●(I0)	○	

4. 전문가 검토 및 소프트웨어 안전등급별 관리방안 선정(관리방안 2)

표준별 활동 분석을 통해 도출한 후보 관리방안과 각 안전활동 별로 정리된 산출물 및 안전기법/수단에 대하여, 다수의 소프트웨어안전 전문가들로부터 검토 의견을 청취하였다. 전문가 그룹은 원자력 분야, 항공 분야, 철도 분야, 자동차 분야 등 다양한 분야에서 활발히 활동하고 있는 인원으로 구성되었다.

전문가 검토 결과, 후보 관리방안 2가 현시점에서 다양한 도메인에 공통적으로 적용하기에 적절할 것이라는 의견이 나왔으며, 이 외에도 식별된 각 안전활동의 정의에 대한 의견, 독립성 수준에 대한 고찰, 관리적인 부분에서의 이슈 등 다양한 검토 의견을 수렴하여 반영할 수 있었다. 전문가 검토 결과에 대한 분석 및 개선 방향, 반영 여부에 대한 내용은 다음 <표 8-8> 전문가 검토 결과를 통해 확인할 수 있다.

<표 8-8> 전문가 검토 결과

소프트웨어 안전등급 별 관리방안 주요 검토 의견	확인내용/개선방향	반영
식별된 안전 활동의 명확한 정의 필요 • 일반적인 소프트웨어 개발 활동이 포함되는 것인지 • 안전에 특화된 활동들인지 • 기존의 요구사항 정의, 설계, 구현 및 검토, 시험과 안전 요구사항 활동과의 차이 • 안전 요구사항의 검토와 분석의 차이	각 개별 안전활동에 대한 세부 정의 수행 • 식별된 안전활동은 안전에 특화된 활동을 의미함 • 기본적인 소프트웨어 개발 활동을 수행하는 것으로 가정 • 개별 안전활동에 대한 정의 이전에 수행/검토/분석 측면의 상위 수준 설명 추가 • 개별 안전활동 세부 정의 시, 기존 활동과의 차이점 설명	O
검토의 독립성 수준에 대한 고찰 • 개발사 외부 독립된 조직에서, 안전등급이 높은 시스템 소프트웨어의 검토 가능성 • Assessment 관점에서 고려되어야 하는 사항이 아닐까?	ISO 26262, IEC 62279 표준 등 독립성 수준의 필요성을 언급하고 있는 표준을 참고하면, 핵심은 안전등급에 따른 검토 결과의 보고라인이 개발과 독립적이어야 한다는 것임 • 독립성 레벨 구분에 대한 명확한 설명 보완(단순 내/외부 조직의 수행 관점이 아닌 보고라인의 차별화 관점으로 수정)	O
관리방안 1이 가장 엄격하나, 실무 적용 용이성을 고려하여 관리방안 2로 결정하는 것이 타당할 것으로 보임	과반수 전문가 의견에 따라 관리방안 2를 최종 안으로 결정	O
적용 방안에 대한 근거 마련 • 각 표준의 안전등급과 본 연구에서 정의한 안전등급과의 비교 • 정리된 안전등급 기반으로 안전 활동 비교 분석	각 표준의 안전등급과 본 연구에서 정의한 안전등급 비교분석 수행 • 안전등급 기준 비교 테이블 제공•해당 내용 기반으로 각 표준의 안전활동 취합 및 비교/분석	O
산출물 개수의 증가에 대한 우려 • 안전 특화된 활동인 경우, 기존에 작성하는 기본 개발 산출물 별도로 추가 작성해야 하는 산출물이 증가할 수 있음.	개별 안전활동에 대한 정의 시, 산출물 작성 유형에 대해 언급 • 별도 산출물로 작성 필요한 유형 • 기본 개발 산출물 내 포함 가능한 유형	O
사업의 특수성 혹은 사업별 추가 요구사항이 있을 경우, 다른 기법을 허용할 수 있도록 언급할 필요가 있음	개별 안전활동에 대한 정의 시, 기법 및 수단 항목에 관련 내용 보완	O
소프트웨어 개발 활동 뿐만 아니라, 관리 지원 활동(최소한 프로젝트 계획 및 형상 관리)이 반영될 필요가 있어 보임	본 과제의 범위는 아님. 향후 고도화 시 고려될 필요가 있음	X
입출력물의 필요 내용 정의, R&R 등이 정의되면 좋을 것 같음	본 과제의 범위는 아님. 향후 고도화 시 고려될 필요가 있음	X

제2절 안전활동에 대응하는 산출물 및 안전기법, 수단 정리

1. 각 표준별 산출물 비교

본 절에서는 분석 대상 표준들에서 정의하고 있는 안전활동 별 산출물, 안전기법 및 수단을 비교 정리하였다. 대부분의 표준에서는 비슷한 수준의 기본 개발 및 검증 활동에 대한 산출물을 요구하고 있었으며, 일부 표준(NASA-STD/GB-8719-13C, ISO 26262, IEC 62279)에서는 인터페이스 관련 산출물에 대하여 보다 상세한 수준을 요구하고 있었다. 또한, 일부 표준에서는 개발 단계에서 검증 계획 및 Test spec.을 언급하고 있기도 하였다.

반면에, IEC 61508, ISO26262 표준의 일부 활동에에서는, 세부 요구사항에서 검토 활동을 명시하고 있으나, 별도의 검토 산출물을 언급하고 있지 않고 있다. 또한, IEC 61508, IEC 62279 표준은 세부 요구사항에서 안전분석 활동을 명시하고 있으나, 별도의 분석 관련 산출물을 언급하고 있지 않는다.

따라서, 본 연구에서는 기본 개발 및 검증 관련 산출물, 검토 산출물은 대부분의 표준에서 언급하고 있는 산출물의 수준과 동일하게 정의한다. 또한 인터페이스 등의 세부 항목에 대한 산출물은 별도 구분짓지 않으며, 기본 개발 및 검증 활동 산출물 내부에 포함하도록 한다.

개발 단계에서 검증 계획 및 테스트 Spec. 등이 언급되는 이유는 V 모델의 개발 라이프사이클을 적용하기 때문이다. 본 연구에서는 테스트 계획 및 Spec.은 검증 단계의 산출물로 구분하며, 대응하는 개발 단계에서 선 진행 가능한 개념으로 정의한다. 안전분석 산출물에 대해서는, 각 단계구분 없이 Safety Analysis Report로 명명하고, 상세 내용은 특정 기법 및 분석 방법을 따르는 방향으로 정의한다.

다음 표는, 분석 대상 표준별 산출물을 비교 정리한 것이다.

〈표 8-9〉 표준별 산출물 비교 - 항공우주, 국방, 항공, 의료 분야

단계	세부 활동	NASA-STD/GB-8719-13C	MIL-STD-882E	DO-178C	IEC 62304
Requirements	소프트웨어안전요구사항정의	Software requirements document Software interface specification Acceptance test plan System test plan Requirements traceability matrix	Software safety requirements	Software requirements data Tracedata	Software requirements
	소프트웨어안전요구사항검토	Formal inspection of requirements report	-	Software veirfication results	Software requirements verification report
	소프트웨어안전요구사항분석	Analysis reports	Analysis reports	-	Risk analysis report
Architecture Desig n	소프트웨어안전아키텍처설계	Software design specification and other design documents Codingstandards Integrationtestplan Traceabilitymatrix	Preliminary software design	Design description Tracedata	Software architecture design
	소프트웨어안전아	Formal inspection reports	-	Software veirfication results	Software architecture design verification report

	키 텍 처 검토				
	소프트웨어안전아키 텍 처 분석	Analysis reports	Analysis reports	-	Risk analysis report
Detailed Design	소프트웨어안전상세 설계	Software design specification and other design documents Codingstandards Traceabilitymatrix	Detailed software design	Design description	Software detailed design Softwaredetaileddesignforinterface
	소프트웨어안전상세 설계 검토	Formal inspection reports	-	Software veirfication results	Software detailed design verification report
	소프트웨어안전상세설계분석	Analysis reports	Analysis reports	-	-
Implementation	소프트웨어안전구현	Source code Traceabilitymatrix	Source code	Source code Tracedata Executableobjectcode	Source code for each software unit
	소프트웨어안전구현 검토	Formal inspection reports	-	Software veirfication results	Software unit verification report
	소프트웨어안전구현 분석	Analysis reports	-	-	-

소프트웨어 Unit Test	소프트웨어단위테스트 수행	Unit test plan and procedures Unittestreport	Software test report	Software verification cases and procedures Softwareverificaitonresults Tracedata	Software unit verification report
	소프트웨어단위테스트 검토	-	-	-	-
소프트웨어 Integration Test	소프트웨어통합테스트 수행	Test report Traceabilitymatrix	Software test report	Software verification cases and procedures Softwareverificaitonresults Tracedata	Software integration test result
	소프트웨어통합테스트 검토	-	-	-	-
소프트웨어 Test	소프트웨어테스트 수행	Test report Traceabilitymatrix	Software test report	Software verification cases and procedures Softwareverificaitonresults Tracedata	Software system test result
	소프트웨어테스트 검토	-	-	-	-

<표 8-10> 표준별 산출물 비교 - 산업일반, 철도, 자동차 분야

단계	세부 활동	IEC 61508	IEC 62279	ISO 26262
Requirements	소프트웨어안전요구사항정의	Software safety requirements	Software requirements spec. Overallsoftwaretestspec.	Software safety requirements specification Hardware-softwareinterface(HSI)specification(refined)
	소프트웨어안전요구사항검토	-	Software requirements verification report	Software verification report
	소프트웨어안전요구사항분석	-	-	-
Architecture Design	소프트웨어안전아키텍처설계	Software architecture design Softwarearchitectureintegrationtestspec.	Software architecture spec. SoftwareDesignSpec. SoftwareInterfaceSpec. SoftwareIntegrationTestSpec. Software/HardwareIntegrationTestSpec.	Software architectural design specification
	소프트웨어안전아키텍처검토	-	Software Architecture and Design Verification Report	Software verification report
	소프트웨어안전아	-	-	Safety analysis report Dependentfailureanalysisreport

	키 텍 처 분석			
Detailed Design	소프트웨어안전상세 설계	Software system design Softwaremoduledesign Softwaresystemintegrationtestspec. Softwaremoduletestspec.	Software Component Design Spec. SoftwareComponentTestSpec.	Software unit design specification
	소프트웨어안전상세 설계 검토	-	Software Component Design Verification Report	-
	소프트웨어안전상세설계분석	-	-	-
Implementation	소프트웨어안전구현	Source code listing	Source code	Software unit implementation
	소프트웨어안전구현 검토	Code review report	Software Source Code Verification Report	Software verification specification Softwareverificationreport
	소프트웨어안전구현 분석	-	-	-
소프트웨어 Unit	소프트웨어단위테스트 수행	Software module test result Verifiedandtestedsoftwaremodules	Software Source Code and Supporting Doc. SoftwareComponentTestReport	Software verification specification Softwareverificationreport

Test	소프트웨어단위테스트 검토	-	-	Confirmation review result
소프트웨어 Integration Test	소프트웨어통합테스트 수행	Software system integration test results Verifiedandtestedsoftwaresystem	Software Integration Test Report Software/HardwareIntegrationTestReport SoftwareIntegrationVerificationReport	Software verification specification Embeddedsoftware Softwareverificationreport
	소프트웨어통합테스트 검토	-	-	Confirmation review result
소프트웨어 Test	소프트웨어테스트 수행	Software architecture integration test result Programmableelectronicsintegrationtestresult Verifiedandtestedintegratedprogrammableelectornics	Overall Software Test Report OverallSoftwareTestVerificationReport SoftwareValidationReport ReleaseNote	Software verification specification Softwareverificationreport
	소프트웨어테스트 검토	-	-	Confirmation review result

2. 각 표준별 안전기법 및 수단 비교

각 표준마다 단계별 활동을 지원하는 기법 및 수단의 종류, 수준, 유형이 서로 상이하다. 동일한 기법 및 방법이 어떤 표준에서는 방법론으로 구분되기도 하며, 또 다른 표준에서는 기법 및 수단으로 구분되기도 한다. 방법론은 기법의 상위 수준의 표현으로 구분 상에는 문제가 없으나, 각 표준에서 언급하고 있는 안전기술들을 취합하기 위하여 다음과 같이 공통적인 기준을 부여하여 구분한다.

- ㅇ Notation: 활동 수행을 지원하는 다수의 표기법들로 구성(ISO 26262에서만 언급되고 있음)
- ㅇ Design Principle: 설계 활동에 대한 원칙들로 구성(ISO 26262를 제외한 타 표준에서는 별도 원칙을 구분짓지 않았으나, 내용 상 특정 방법 및 절차를 따르는 것이 아닐 경우 원칙으로 구분함)
- ㅇ Technique & Measure: 표기법 및 설계 원칙을 제외한 나머지 기술들을 대상으로 구성

<표 8-11> 분석 활동 측면에서의 세부 관리 방안

단계	세부 활동	유형	기법 및 방법	출처
Requirements	소프트웨어안전요구사항정의	Notation	Informal notations Semi-formalnotations Formalnotations	ISO 26262
		Technique & Measrue	Formal Methods Semi-formalmethods DecisionTables	NASA-GB IEC 61508 IEC 62279
	소프트웨어안전요구사항검토	Technique & Measrue	Walk-through Inspection Semi-formalverification Formalverification	ISO 26262 NASA-GB
	소프트웨어안전요구사항분석	Technique & Measrue	Preliminary Hazard Analysis (PHA) (if not previously performed) SoftwareSubsystemHazardAnalysis(ifnotpreviously performed) SoftwareSafetyRequirementsFlow-downAnalysis RequirementsCriticalityAnalysis SpecificationAnalysis Timing,Throughput,andSizingAnalysis	NASA-GB

			SoftwareFaultTreeAnalysis SoftwareFailureModesandEffectsAnalysis	
Architecture Design	소프트웨어안전아키텍처설계	Notation	Natural language Informalnotations Semi-formalnotations Formalnotations	ISO 26262
		Design Principle	Appropriate hierarchical structure of the software components Restrictedsizeandcomplexityofsoftwarecomponents Restrictedsizeofinterfaces Strongcohesionwithineachsoftwarecomponent Loosecouplingbetweensoftwarecomponents Appropriateschedulingproperties Restricteduseofinterrupts Appropriatespatialisolationofthesoftwarecomponents Appropriatemanagementofsharedresources Statelesssoftwaredesign(orlimitedstatedesign) FullyDefinedInterface InformationHiding InformationEncapsulation	ISO 26262 IEC 61508 IEC 62279
		Techniqueue & Measrue	Requirements State Machines Markov Modeling Use of trusted/verified software elements (if available) Static resource allocation Static synchronisation of access to shared resources Fault Detection & Diagnosis Error Correcting Codes Error Detecting Codes Failure Assertion Programming Safety Bag Techniques Diverse Programming Recovery Block Backward Recovery Forward Recovery Retry Fault Recovery Mechanisms Artificial Intelligence - Fault Correction Dynamic Reconfiguraton of Software Graceful Degradation	NASA-GB IEC 61508 IEC 62279

			Defensive Programming Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer) Diverse monitor techniques (with separation between the monitor computer and the monitored computer) Diverse redundancy, implementing the same software safety requirements specification Functionally diverse redundancy, implementing different software safety requirements specification Automatic software generation Time-triggered architecture Event-driven, with guaranteed maximum response time Memorising Executed Cases	
	소프트웨어안전아키텍처 검토	Techniq ue & Measrue	Walk-through of the design Inspectionofthedesign Simulationofdynamicbehaviourofthedesign Prototypegeneration Formalverification FormalInspectionsofDesignProducts FormalMethodsandModelChecking Controlflowanalysis Dataflowanalysis Schedulinganalysis	ISO 26262 NASA-GB
	소프트웨어안전아키텍처 분석	Techniq ue & Measrue	Defendant failure analysis CriticalityAnalysis DesignSafetyAnalysis IndependenceAnalysis DesignInterfaceAnalysis DesignTraceabilityAnalysis SoftwareElementAnalysis RateMonotonicAnalysis DynamicFlowgraphAnalysis HazardRiskAssessment Cyclicbehaviour,withguaranteedmaximumcycletime Event-driven,withguaranteedmaximumresponsetime	ISO 26262 NASA-GB IEC 61508 IEC 62279

			SoftwareErrorEffectAnalysis	
Detailed Design	소프트웨어안전상세설계	Notation	Natural language Informalnotations Semi-formalnotations Formalnotations	ISO 26262
		Design Principle	One entry and one exit point in subprograms and functions Nodynamicobjectsorvariables,orelseonlinetestdurin gtheircreation Initializationofvariables Nomultipleuseofvariablenames Avoidglobalvariablesorelsejustifytheirusage Restricteduseofpointers Noimplicittypeconversions Nohiddendatafloworcontrolflow Nounconditionaljumps Norecursions Modularapproach Designandcodingstandards	ISO 26262 IEC 61508 IEC 62279
		Techniq ue & Measrue	Markov Modeling RequirementsStateMachines Structuredmethods** Semi-formalmethods** Formaldesignandrefinementmethods** ObjectOrientedProgramming ProceduralProgramming Metaprogramming AnalysablePrograms Useoftrusted/verifiedsoftwareelements(ifavailable) Defensive programming	NASA-GB IEC 61508 IEC 62279
	소프트웨어안전상세설계검토	Techniq ue & Measrue	Walk-through Inspection FormalInspections ModelChecking Staticanalysesbasedonabstractinterpretation Resourceusageevaluation Back-to-backcomparisontestbetweenmodelandcod e,ifapplicable	ISO 26262 NASA-GB
	소프트웨어안전상세설계분석	Techniq ue & Measrue	Data Logic Analysis DesignDataAnalysis DesignInterfaceAnalysis DesignTraceabilityAnalysis	NASA-GB

Implementation	소프트웨어안전구현	Techniqueue & Measrue	Program Slicing of Safety Critical Data	NASA-GB
	소프트웨어안전구현 검토	Techniqueue & Measrue	Pair-programming Semi-formalverification Formalverification Controlflowanalysis Dataflowanalysis Staticcodeanalysis FormalIsnpectionsofSourceCode	ISO 26262 NASA-GB
	소프트웨어안전구현 분석	Techniqueue & Measrue	Code Logic Analysis CodeDataAnalysis CodeInterfaceAnalysis UnusedCodeAnalysis InterruptAnalysis TestCoverageAnalysis FinalTiming,Throught,andSizingAnalysis	NASA-GB
소프트웨어 Unit Test	소프트웨어단위테스트 수행	Techniqueue & Measrue	Requirements-based test Interfacetest Faultinjectiontest Probabilistictesting Analysisofrequirements Generationandanalysisofequivalenceclasses Analysisofboundaryvalues Errorguessingbasedonknowledgeorexperience Statementcoverage Branchcoverage MC/DC(ModifiedCondition/DecisionCoverage)	ISO 26262 NASA-GB IEC 61508 IEC 62279
소프트웨어 Integration Test	소프트웨어통합테스트 수행	Techniqueue & Measrue	Requirements-based test Interfacetest Faultinjectiontest Resourceusagetest Back-to-backcomparisontestbetweenmodelandcode,ifapplicable Checkaccuracyofarithmetic Probabilistictesting Dynamicanalysisandtesting Datarecordingandanalysis Performancetesting Modelbasedtesting Verificationofthecontrolflowanddataflow	ISO 26262 NASA-GB IEC 61508 IEC 62279

			Staticcodeanalysis Analysisofrequirements Generationandanalysisofequivalenceclasses Analysisofboundaryvalues Errorguessingbasedonknowledgeorexperience Functioncoverage Callcoverage Datarecordingandanalysis	
소프트웨어 Test	소프트웨어테스트 수행	Techniq ue & Measrue	Requirements-based test Faultinjectiontest LoadTesting StressTesting BoundaryValueTests FunctionalTesting PerformanceMonitoring DisasterTesting ResistancetoFailureTesting “RedTeam“Testing RegressionTesting(Tailoredtotheleveloforiginaltesting) Probabilistictesting Processsimulation Analysisofrequirements Generationandanalysisofequivalenceclasses Analysisofboundaryvalues Errorguessingbasedonknowledgeorexperience Analysisoffunctionaldependencies Analysisofoperationalusecases TestCoverageAnalysis	ISO 26262 NASA-GB IEC 61508 IEC 62279

3. 안전활동 세부 정의

각 표준 별 비교 분석을 통해 식별된 안전 활동과 안전 산출물, 안전기법 및 수단들을 기반으로, 각 안전활동에 대한 세부 내용을 정의한다. 본 연구에서 정의한 소프트웨어안전활동에 대한 세부 내용에서는, 2019년도 진행되었던 “소프트웨어안전기준 검증과 소프트웨어안전 관련 활동 및 절차 조사” 연구에서 다루지 못했던 소프트웨어 안전활동 별 소프트웨어안전기법이 추가 정리되었으며, 소프트웨어안전활동을 수행, 검토, 분석 활동으로 세분화하여 정의하였다.

안전활동의 세부 정의는, 각 안전활동의 목적, 입/출력 산출물, 설명, 관련 기법 및 수단으로 구성된다.

ㅇ 소프트웨어안전요구사항 정의

시스템 정보를 입력받아 시스템의 안전 기능와 관련된 내용을 식별한다. 이후, 식별된 내용 중 소프트웨어로 할당된 부분을 확인하고, 해당 정보를 바탕으로 안전 기능을 수행하기 위해 소프트웨어가 어떻게 동작할 것인지 정의하는 활동을 의미한다.

<표 8-12> 소프트웨어안전요구사항 정의 활동 구성

목적	안전 기능 구현을 위한 소프트웨어안전요구사항을 정의한다.
입력	System Reqruiements SystemDesign
출력	소프트웨어 Safety Requirements
관련기법 및 수단	
Notation	Informal notations Semi-formal notations Formal notations
Technique and Measure	Formal Methods Semi-formal methods Decision Tables

ㅇ 소프트웨어안전요구사항 검토

시스템 정보 및 분석 결과를 기반으로 소프트웨어안전요구사항이 적절하고 적합하며, 일관되게 정의되었는지 검토하는 활동을 의미한다. 소프트웨어안전요구사항의 검토는 다양한 기법 및 수단을 활용하여 수행할 수 있으며, 검토 중 식별된 결함은 지속적으로 관리하여 조치해야 한다.

<표 8-13> 소프트웨어안전요구사항 검토 활동 구성

목적	소프트웨어안전요구사항이 시스템 정보 및 분석 결과를 기반으로 적절하게 정의되었는지 검토한다.
입력	소프트웨어 Safety Requirements
출력	소프트웨어 Safety Requirements Verification Report

관련기법 및 수단	
Technique and Measure	Walk-through Inspection Semi-formal verification Formal verification

○ 소프트웨어안전요구사항 분석

소프트웨어안전요구사항 수준에서 야기될 수 있는 위험 요소의 존재를 확인한다. 식별된 위험 요소가 시스템 소프트웨어의 전체 안전에 얼마만큼의 영향을 미치는지 확인하고, 위험을 낮출 수 있도록 방안을 모색하는 활동을 의미한다.

<표 8-14> 소프트웨어안전요구사항 분석 활동 구성

목적	시스템 안전에 소프트웨어안전요구사항이 미칠 수 있는 영향도를 확인한다.
입력	소프트웨어 Safety Requirements
출력	Safety Analysis Report
관련기법 및 수단	
Technique and Measure	Preliminary Hazard Analysis (PHA) (if not previously performed) Software Subsystem Hazard Analysis (if not previously performed) Software Safety Requirements Flow-down Analysis Requirements Criticality Analysis Specification Analysis Timing, Throughput, and Sizing Analysis Software Fault Tree Analysis Software Failure Modes and Effects Analysis

○ 소프트웨어안전아키텍처 설계

소프트웨어안전요구사항의 구현을 위하여 소프트웨어 엘리먼트를 식별하고, 구체화하는 활동을 의미한다. 소프트웨어안전아키텍처 설계를 위해 별도의 요구되는 설계 및 개발 방법론, 설계 지침이 존재할 경우 이를 준수하여 수행해야 하며, 이를 위한 다양한 기법 및 수단을 활용할 수 있다.

<표 8-15> 소프트웨어안전아키텍처 설계 활동 구성

목적	소프트웨어 안전 요구사항을 만족하는 소프트웨어 안전 아키텍처 설계를 수행한다.
입력	소프트웨어 Safety Requirements
출력	소프트웨어 Architecture Design
관련기법 및 수단	
Notation	Natural language Informal notations Semi-formal notations Formal notations
Design Principle	Appropriate hierarchical structure of the software components Restricted size and complexity of software components Restricted size of interfaces Strong cohesion within each software component Loose coupling between software components Appropriate scheduling properties Restricted use of interrupts Appropriate spatial isolation of the software components Appropriate management of shared resources Stateless software design (or limited state design) Fully Defined Interface Information Hiding Information Encapsulation Language Restrictions and Coding Standards
Technique and Measure	Requirements State Machines Markov Modeling Use of trusted/verified software elements (if available) Static resource allocation Static synchronisation of access to shared resources Fault Detection & Diagnosis Error Correcting Codes Error Detecting Codes Failure Assertion Programming Safety Bag Techniques Diverse Programming Recovery Block Backward Recovery Forward Recovery Retry Fault Recovery Mechanisms Artificial Intelligence - Fault Correction Dynamic Reconfiguraton of Software

	Graceful Degradation Defensive Programming Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer) Diverse monitor techniques (with separation between the monitor computer and the monitored computer) Diverse redundancy, implementing the same software safety requirements specification Functionally diverse redundancy, implementing different software safety requirements specification Automatic software generation Time-triggered architecture Event-driven, with guaranteed maximum response time Memorising Executed Cases

○ 소프트웨어안전아키텍처 검토

소프트웨어안전아키텍처가 소프트웨어안전요구사항 또는 상위 수준의 설계 정보를 기반으로 적절하고 적합하며, 일관되게 정의되었는지 검토하는 활동을 의미한다. 소프트웨어안전아키텍처의 검토는 다양한 기법 및 수단을 활용하여 수행할 수 있으며, 검토 중 식별된 결함은 지속적으로 관리하여 조치해야 한다.

<표 8-16> 소프트웨어안전아키텍처 검토 활동 구성

목적	소프트웨어 안전 아키텍처가 소프트웨어 안전 요구사항을 기반으로 적절하게 도출되었는지 검토한다.
입력	소프트웨어 Architecture Design
출력	소프트웨어 Architecture Design Verification Report
관련기법 및 수단	
Technique and Measure	Walk-through of the design Inspection of the design Simulation of dynamic behaviour of the design Prototype generation Formal verification Formal Inspections of Design Products Formal Methods and Model Checking Control flow analysis

	Data flow analysis Scheduling analysis

o 소프트웨어안전아키텍처 분석

소프트웨어안전아키텍처 설계 수준에서 야기될 수 있는 위험 요소의 존재를 확인한다. 소프트웨어안전아키텍처를 기반으로 소프트웨어 엘리먼트 별 발생 가능한 위험 요소를 식별하고, 식별된 위험 요소가 시스템 소프트웨어의 전체 안전에 얼마만큼의 영향을 미치는지 확인한다. 또한 해당 위험을 낮출 수 있도록 방안을 모색하는 활동을 의미한다.

<표 8-17> 소프트웨어안전아키텍처 분석 활동 구성

목적	시스템 안전에 소프트웨어 안전 아키텍처 설계가 미칠 수 있는 영향도를 확인한다.
입력	소프트웨어 Architecture Design
출력	Safety Analysis Report
관련기법 및 수단	
Technique and Measure	Defendant failure analysis Criticality Analysis Design Safety Analysis Independence Analysis Design Interface Analysis Design Traceability Analysis Software Element Analysis Rate Monotonic Analysis Dynamic Flowgraph Analysis Hazard Risk Assessment Cyclic behaviour, with guaranteed maximum cycle time Event-driven, with guaranteed maximum response time Software Error Effect Analysis

o 소프트웨어안전상세설계

소프트웨어안전아키텍처에서 식별된 소프트웨어 엘리먼트에 대하여, 포함되어야 하는 소프트웨어 단위를 식별 및 정의하고 해당 엘리먼트가 가질 수 있는 상태 및 단위간 인터페이스를 정의하는 활동을 의미한다. 또한 소프트웨어 엘리먼트 내 동적 행위로 상태 천이, 단위간 동적 행위(제어 및 호출 관계 등)를 설계한다. 소프트웨어안전상

세설계를 위해 별도의 요구되는 설계 및 개발 방법론, 설계 지침이 존재할 경우 이를 준수하여 수행해야 하며, 이를 위한 다양한 기법 및 수단을 활용할 수 있다.

<표 8-18> 소프트웨어안전상세설계 활동 구성

목적	소프트웨어 안전 요구사항 및 아키텍처를 만족하는 소프트웨어 안전 상세 설계를 수행한다.
입력	소프트웨어 Architecture Design
출력	소프트웨어 Detailed Design
관련기법 및 수단	
Notation	Natural language Informal notations Semi-formal notations Formal notations
Design Principle	One entry and one exit point in subprograms and functions No dynamic objects or variables, or else online test during their creation Initialization of variables No multiple use of variable names Avoid global variables or else justify their usage Restricted use of pointers No implicit type conversions No hidden data flow or control flow No unconditional jumps No recursions Modular approach Design and coding standards
Technique and Measure	Markov Modeling Requirements State Machines Structured methods ** Semi-formal methods ** Formal design and refinement methods ** Object Oriented Programming Procedural Programming Metaprogramming Analysable Programs Use of trusted/verified software elements (if available) Defensive programming

○ 소프트웨어안전상세설계 검토

소프트웨어 안전 설계 및 세부 모델이 소프트웨어안전아키텍처 및 요구사항에 따라 적절하고 적합하며, 일관되게 정의되었는지 검토하는 활동을 의미한다. 소프트웨어안전상세설계의 검토는 다양한 기법 및 수단을 활용하여 수행할 수 있으며, 검토 중 식별된 결함은 지속적으로 관리하여 조치해야 한다.

<표 8-19> 소프트웨어안전상세설계 검토 활동 구성

목적	소프트웨어 안전 상세 설계가 소프트웨어 안전 요구사항 및 아키텍처를 기반으로 적절하게 도출되었는지 검토한다.
입력	소프트웨어 Detailed Design
출력	소프트웨어 Detailed Design Verification Report
관련기법 및 수단	
Technique and Measure	Walk-through Inspection Formal Inspections Model Checking Static analyses based on abstract interpretation Resource usage evaluation Back-to-back comparison test between model and code, if applicable

ㅇ 소프트웨어안전상세설계 분석

소프트웨어안전상세설계 수준에서 야기될 수 있는 위험 요소의 존재를 확인한다. 식별된 위험 요소가 시스템 소프트웨어의 전체 안전에 얼마만큼의 영향을 미치는지 확인하고, 해당 위험을 낮출 수 있도록 방안을 모색하는 활동을 의미한다.

<표 8-20> 소프트웨어안전상세설계 분석 활동 구성

목적	시스템 안전에 소프트웨어 안전 상세 설계가 미칠 수 있는 영향도를 확인한다.
입력	소프트웨어 Detailed Design
출력	Safety Analysis Report
관련기법 및 수단	
Technique and Measure	Data Logic Analysis Design Data Analysis Design Interface Analysis Design Traceability Analysis

ㅇ 소프트웨어안전구현

소프트웨어안전상세설계서를 기반으로 소프트웨어를 구현하는 활동을 의미한다. 소프트웨어안전구현을 위한 별도의 구현 지침이 존재할 경우, 이를 준수하여 수행해야 하며, 이를 위한 다양한 기법 및 수단을 활용할 수 있다.

<표 8-21> 소프트웨어안전구현 활동 구성

목적	소프트웨어 안전 상세 설계를 만족하는 소프트웨어 안전 구현을 수행한다.
입력	소프트웨어 Detailed Design
출력	Source Code
관련기법 및 수단	
Technique and Measure	Program Slicing of Safety Critical Data

○ 소프트웨어안전구현 검토

소프트웨어안전구현 결과물이 소프트웨어안전상세설계에 따라 적절하고 적합하며, 일관되게 구현되었는지 검토하는 활동을 의미한다. 소프트웨어안전구현의 검토는 다양한 기법 및 수단을 활용하여 수행할 수 있으며, 검토 중 식별된 결함은 지속적으로 관리하여 조치해야 한다.

<표 8-22> 소프트웨어안전구현 검토 활동 구성

목적	소프트웨어 안전 구현 결과물이 소프트웨어 안전 상세 설계를 기반으로 적절하게 구현되었는지 검토한다.
입력	Source Code
출력	Source Code Verification Report
관련기법 및 수단	
Technique and Measure	Pair-programming Semi-formal verification Formal verification Control flow analysis Data flow analysis Static code analysis Formal Isnpections of Source Code Coding Checklists and Standards

ㅇ 소프트웨어안전구현 분석

소프트웨어안전구현 수준에서 야기될 수 있는 위험 요소의 존재를 확인한다. 식별된 위험 요소가 시스템 소프트웨어의 전체 안전에 얼마만큼의 영향을 미치는지 확인하고, 해당 위험을 낮출 수 있도록 방안을 모색하는 활동을 의미한다.

<표 8-23> 소프트웨어안전구현 분석 활동 구성

목적	시스템 안전에 소프트웨어 구현이 미칠 수 있는 영향도를 확인한다.
입력	Source Code
출력	Safety Analysis Report
관련기법 및 수단	
Technique and Measure	Code Logic Analysis Code Data Analysis Code Interface Analysis Unused Code Analysis Interrupt Analysis Test Coverage Analysis Final Timing, Throught, and Sizing Analysis

ㅇ 소프트웨어단위테스트 수행

소프트웨어단위테스트 수행 전략 및 계획을 수립하고, 해당 계획에 명시된 목표 및 범위, 전략 및 기법에 따라 소프트웨어단위테스트 케이스를 설계한다. 이후, 테스트 대상인 소프트웨어안전구현 결과물(소스코드)의 단위에 대한 테스트를 수행하는 활동을 의미한다.

<표 8-24> 소프트웨어단위테스트 수행 활동 구성

목적	소프트웨어 안전 구현 결과물인 소스코드의 각 단위 별 테스트를 수행한다.
입력	소프트웨어 Detailed Design SourceCode
출력	소프트웨어 Unit Test Specification 소프트웨어UnitTestResult
관련기법 및 수단	
Technique and Measure	Requirements-based test Interface test Fault injection test

	Probabilistic testing Analysis of requirements Generation and analysis of equivalence classes Analysis of boundary values Error guessing based on knowledge or experience Statement coverage Branch coverage MC/DC (Modified Condition/Decision Coverage)

ㅇ 소프트웨어단위테스트 검토

소프트웨어단위테스트 케이스가 소프트웨어안전상세설계 대비, 모델 또는 소스 코드를 검증하기에 적절하고 적합한지 검토하는 활동을 의미한다. 또한, 소프트웨어단위테스트 결과가 계획된 목표 및 범위(커버리지 등)를 적절하게 달성하였는지 검토한다. 검토 중 식별된 결함은 지속적으로 관리하여 조치해야 한다.

<표 8-25> 소프트웨어단위테스트 검토 활동 구성

목적	소프트웨어 단위 테스트 케이스 도출 및 테스트가 적절하게 수행되었는지 검토한다.
입력	소프트웨어 Unit Test Specification 소프트웨어UnitTestResult
출력	소프트웨어 Unit Test Specification & Result Verification Rerport
관련기법 및 수단	
-	-

ㅇ 소프트웨어통합테스트 수행

소프트웨어 통합 및 통합 테스트 수행 전략, 계획을 수립하고, 해당 계획에 명시된 목표 및 범위, 전략 및 기법에 따라 소프트웨어통합테스트 케이스를 설계한다. 이후, 통합 전략에 따라 소프트웨어 단위 및 엘리먼트를 통합하고, 통합 시험 범위에 해당하는 테이스 케이스를 선정하여 테스트를 수행하는 활동을 의미한다.

<표 8-26> 소프트웨어통합테스트 수행 활동 구성

목적	소프트웨어 안전 기능과 관련된 소프트웨어 단위 및 엘리먼트를 통합하고, 요구되는 기능을 만족하는지 검증한다.

입력	소프트웨어 Architecture Design
출력	소프트웨어 Integration Test Specification 소프트웨어IntegrationTestResult
관련기법 및 수단	
Technique and Measure	Requirements-based test Interface test Fault injection test Resource usage test Back-to-back comparison test between model and code, if applicable Check accuracy of arithmetic Probabilistic testing Dynamic analysis and testing Data recording and analysis Performance testing Model based testing Verification of the control flow and data flow Static code analysis Analysis of requirements Generation and analysis of equivalence classes Analysis of boundary values Error guessing based on knowledge or experience Function coverage Call coverage

o 소프트웨어통합테스트 검토

소프트웨어통합테스트 케이스가 소프트웨어안전아키텍처 설계를 검증하기에 적절하고 적합한지 검토하는 활동을 의미한다. 또한, 소프트웨어통합테스트 결과가 계획된 목표 및 범위(커버리지 등)를 적절하게 달성하였는지 검토한다. 검토 중 식별된 결함은 지속적으로 관리하여 조치해야 한다.

<표 8-27> 소프트웨어통합테스트 검토 활동 구성

목적	소프트웨어 통합 테스트 케이스 도출 및 테스트가 적절하게 수행되었는지 검토한다.
입력	소프트웨어 Integration Test Specification 소프트웨어IntegrationTestResult
출력	소프트웨어 Integration Test Specification & Result Verification Rerport

관련기법 및 수단	
-	-

○ 소프트웨어테스트 수행

소프트웨어테스트 수행 전략 및 계획을 수립하고, 해당 계획에 명시된 목표 및 범위, 전략 및 기법에 따라 소프트웨어테스트 케이스를 설계한다. 이후, 소프트웨어테스트 범위에 해당하는 테스트 케이스를 선정하여 테스트를 수행하는 활동을 의미한다.

<표 8-28> 소프트웨어테스트 수행 활동 구성

목적	소프트웨어 시스템 수준에서 요구되는 안전 기능이 올바르게 작동하는지 검증한다.
입력	소프트웨어 Safety Requirements
출력	소프트웨어 Test Specification 소프트웨어TestResult
관련기법 및 수단	
Technique and Measure	Requirements-based test Fault injection test Load Testing Stress Testing Boundary Value Tests Functional Testing Performance Monitoring Disaster Testing Resistance to Failure Testing Red Team Testing Regression Testing (Tailored to the level of original testing) Probabilistic testing Process simulation Analysis of requirements Generation and analysis of equivalence classes Analysis of boundary values Error guessing based on knowledge or experience Analysis of functional dependencies Analysis of operational use cases Test Coverage Analysis

ㅇ 소프트웨어테스트 검토

소프트웨어테스트 케이스가 소프트웨어안전요구사항을 검증하기에 적절하고 적합한지 검토하는 활동을 의미한다. 또한, 소프트웨어테스트 결과가 계획된 목표 및 범위(커버리지 등)를 적절하게 달성하였는지 검토한다. 검토 중 식별된 결함은 지속적으로 관리하여 조치해야 한다.

<표 8-29> 소프트웨어테스트 검토 활동 구성

목적	소프트웨어 테스트 케이스 도출 및 테스트가 적절하게 수행되었는지 검토한다.
입력	소프트웨어 Test Specification 소프트웨어TestResult
출력	소프트웨어 Test Specification & Result Verification Report
관련기법 및 수단	
-	-

제9장 결론

제1절 연구의 요약

본 연구는 공공기관 시스템과 국가핵심기반에 대해 소프트웨어 안전등급 선정방안 및 소프트웨어 안전등급별 안전관리방안의 도출 과정을 다루고 있다. 공통적 소프트웨어 안전등급이 필요한 이유는 하드웨어 안전관리 중심의 안전 중요 시스템의 소프트웨어 안전을 확보하고, 소프트웨어 개발자와 도메인 전문가들에게 소프트웨어 안전 활동과 안전관리에 필요한 기술을 제공하기 위해서이다.

또한 소프트웨어 안전을 확보하는데 걸림돌인 안전확보 비용과 시간을 효율적으로 책정하기 위함이다. 안전확보를 위한 활동이 규제로 인식되는 것은 안전확보를 위한 비용과 시간이 많이 들기 때문이다. 그러므로 최소한의 규제로 최대한의 안전 확보를 위해서는 요구되는 안전수준에 따라 안전 등급을 선정하고 이에 기반하여 안전관리를 해야 한다. 위험 심각성과 시스템 위험에 영향을 미치는 요소들을 파악하여 요구되는 안전 수준에 따라 소프트웨어 안전등급을 선정하고, 안전등급에 따라 안전활동을 정함으로써 안전 확보와 규제(시간과 비용)의 조화를 달성할 수 있다.

본 연구는 안전 등급을 공공기관 시스템에 적용하기 위한 기준과 안전관리 활동을 도출하는 것이다. 이를 위해서 주요 산업 도메인과 공공기관 안전관리 제도에서 안전등급을 결정하는 방법에 대한 조사를 수행하고, 안전등급의 평가요소, 판단항목 및 관련 지표에 관한 조사를 수행한다. 안전관리 활동은 주요산업 도메인의 안전관리 활동을 비교, 분석하고 전문가의 자문을 통하여 결정한다.

먼저, 소프트웨어 안전등급 결정 방안 구축을 위하여 전통적으로 안전을 중요하게 다루는 항공, 원자력, 철도 등의 도메인을 선정하여, 관련 제도 및 안전기준을 조사하였다. 조사 내용은 크게 소프트웨어 안전등급을 결정하는 다양한 유형 및 방법, 소프트웨어 안전등급 평가항목과 지표로 구성되어 있다.

대부분의 산업 도메인에서 위험의 심각도를 평가항목으로 사용하는 것을 확인할 수 있었으며, 세부 항목으로는 인명피해, 금전/환경적 손실, 시스템 기능/성능 손실 등이 많이 사용되는 것을 파악할 수 있었다. 시스템 등급 결정에

사용되는 사고발생도의 경우는 소프트웨어에는 측정이 용이하지 않아 사용되지 않았다. 이 외에도, 소프트웨어 특성을 고려한 평가항목으로 위험 관여도 및 하드웨어와 융영자를 통한 중복 안전장치의 제공 여부가 공통적으로 사용되고 있음을 확인할 수 있었다.

본 연구의 소프트웨어 안전등급은 소프트웨어 진흥법의 고시인 ‘소프트웨어안전 확보를 위한 지침’의 대상이 되는 공공기관 안전 소프트웨어에 적용하는 것을 목표로 한다. 공공기관 시스템에 적용되는 안전기준의 특성을 도출하기 위하여 공공기관 시스템의 종류 및 등급제 사례를 조사하였다. 공공기관 시스템에 적용된 소프트웨어 관련 등급 결정방법, 등급 결정을 위한 평가항목 및 세부 지표에 대하여 조사를 수행하였다. 공공기관 시스템의 평가 기준, 관리체계, 평가/인증 제도에서는 공공시스템 특성을 반영하여 국가 및 사회적 피해 측면의 평가항목이 고려되고 있음을 확인할 수 있었다.

특히. 공공기관 시스템과 관련된 위험요인을 조사하기 위하여, 공공기관 시스템의 특성을 분석하여 해당 특성에 따른 유형을 구분하였다. 이는 제어의 자동/수동 여부와 정보의 특성에 따라 유형을 구분하였으며, 유형별 공공기관 시스템의 사례를 제시하였다. 공공기관 시스템 사례에서 시스템의 위험과 소프트웨어 안전등급 선정 시 고려사항을 도출하였다.

마지막으로, 해당 조사 및 분석 결과를 기반으로 공공기관 시스템의 소프트웨어 안전등급 결정방안 및 소프트웨어 안전등급에 따른 관리방안을 도출하였다. 도출된 결과는 분야별 소프트웨어안전 전문가 검토를 통해 타당성 및 객관성을 확보하였다.

본 연구를 통해, 소프트웨어 안전등급제 및 안전등급에 따른 관리방안을 개발함으로써, 소프트웨어 안전관리를 위한 기본적인 체계를 마련하고, 4차 산업 혁명에 발맞춰 다양한 산업 분야에서 소프트웨어의 안전성 향성에 기여할 것으로 기대한다.

제2절 향후 연구

본 연구에서는 공공기관 시스템에 공통적으로 사용 가능한 소프트웨어 안전등급 선정을 위한 방법, 항목, 지표를 도출하기 위해 문헌조사와 분석을 통한 연구결과의 신뢰성을 위하여 전문가 검증을 수행하였다. 그러나 소프트웨어 안전등급 제도를 시행하기 위해서는 공공기관 시스템에 적용하여 소프트웨어 안전기준의 적합성을 검증을 위한 실증연구를 한다. 또한 환경, 해양, 상하수도, 도로 등의 공공기관 시스템에도 철도, 항공, 자동차 등의 안전표준을 분석하여 도출한 안전기준을 활용가능한 지 여부도 검증이 필요하다.

본 연구는 공공기관 시스템 및 기반시설을 소프트웨어 안전등급 공통 결정 방안을 제시했으며, 철도, 항공, 자동차 등 각 안전 도메인에 적합한 기준은 각 관리기관이 취사선택하도록 안내되어 있다. 향후 각 도메인에 맞는 소프트웨어 안전등급 결정방안에 대한 연구도 필요하겠다.

제3절 연구의 한계

본 연구에서는 소프트웨어 위험발생도는 측정하기도 어렵도 사고 데이터도 없어 등급 결정 요소에서 제외하여 예비 등급을 도출하도록 하였다. 등급 도출 후에 고려사항으로 위험발생도를 검토하도록 하였다. 이는 전문가의 의견도 동일하다. 시스템 위험등급 산출 시에는 중요한 요소의 하나로 사고 위험발생도가 포함되어 있다. 향후 소프트웨어 안전이 더 중요해 지고 사고 사례가 많아지면, 안전등급 결정 시 위험발생도가 중요한 요소가 되어할 것이다. 왜나하면 안전이 중요한 시스템일 지라도 사고가 거의 나지 않는 시스템에 대해서는 안전활동에 많은 노력을 투자하는 것은 낭비일 수 있기 때문이다.

안전선진국의 대학 및 연구기관에서도 소프트웨어 위험발생도에 대한 연구의 진전은 없다. 그러나 향후에 위험발생도 측정에 관한 연구가 진행되어야 할 것이다.

참 고 문 헌

국내 문헌

KEPCO & KHNP(2014), 『Software Program Manual for APR 1400』

KEPCO & KHNP(2014), 『Software Program Manual for APR 1400』

과학기술정보통신부(2020), 『정보통신기반 보호법』

과학기술정보통신부(2017), 『사회기반시설사업·지역개발사업의 정보화계획 수립에 관한 지침』

국가기술표준원(2017), 『KC 62619, 전기용품안전기준-산업용 리튬이차전지 안전』

국가기술표준원(2015), 『전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 기능안전성(KS C IEC61508-1)』

국가기술표준원(2007), 『KS C IEC 60730-1, 전기용품안전기준 - 가정용 및 이와 유사한 자동 제어장치』

국가정보원·미래창조과학부(2014), 주요정보통신기반시설 지정평가기준 가이드라인

국방부(2017), 『통합방위법』

국토교통부(2020), 『시설물의 안전 및 유지관리에 관한 특별법 시행령』

국토교통부(2017), 제4차 시설물의 안전 및 유지관리 기본계획(2018 ~ 2022)

국토교통부(2017), 『철도차량 기술기준』

기획재정부(2020), 『사회기반시설에 대한 민간투자법』

애스앰애이(2019), 위해관리계획서 이행등급 산정 세부기준 마련 연구

원자력안전위원회(2018), 『원자로시설의 안전등급과 등급별 규격에 관한 규정』

소프트웨어정책연구소(2015), 소프트웨어안전 산업동향조사

송지환 외(2018), 소프트웨어안전 분야 선정기준 및 소프트웨어안전공통기준 도출 연구, 소프트웨어정책연구소

진회승 외(2018), 소프트웨어 안전 산업 동향조사

한국원자력안전기술원(2016), 『경수로형 원전 규제기준 및 규제지침』

한국철도기술연구원(2008), 『철도 소프트웨어 안전기준 및 체계 구축 연구보고서』

행정안전부(2020), 『재난 및 안전관리 기본법』

환경부(2020), 화학물질관리법

행정안전부(2019), 『행안부, '정보시스템 등급별 보안관리' 제도 확산 나선다.』

행정안전부(2019.8.23.), 『행정기관 및 공공기관 정보시스템 구축·운영 지침』

행정안전부(2017), 『자체단체 정보시스템 장애 예방 및 대응 지침』

행정안전부(2017), 『주요정보통신기반시설 보호지침』

행정안전부(2012), 『범정부 서비스참조모형 2.2』

홍성수 외 (2019.10), 소프트웨어가 주도하는 차량 안전 기술, 오토저널 41(10)

해외 문헌

B. Gallina, I. Sljivo, O. Jaradat(2012), Towards a safety-oriented process line for enabling reuse in safety critical systems development and certification, in: Proc. 2012 IEEE 35th Software Eng. Work. SEW 2012

DoD(2020), DOD INSTRUCTION 5000.02, "Operation of the Adaptive Acquisition Framework, Department of Defense"

DoD(2012), MIL-STD-882E, “Department of Defense Standard Practice: System Safety, Department of Defense”

Department of Defense(2010), “Joint Software Systems Safety Engineering Handbook”

W. Eric Wong et al.(2014), Evaluating Software Safety Standards: A Systematic Review and Comparison, 2014 Eighth International Conference on Software Security and Reliability

IEC(2020), IEC 61226, “Nuclear power plants - Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems”

IEC(2010) IEC 61508, Electrical/Electronic/Programmable Electronic Safety-related Systems

IEC(2015), IEC 62279, , “Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems”

IEC(2014), IEC 62280, “Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems”

IEC(2006), IEC 62304, “Medical device software — Software life cycle processes”

IIEE(2017), EEE 1012, “IEEE Standard for System, Software, and Hardware Verification and Validation”

IEEE(1974), IEEE 323/323a-1974, “IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations”

International Atomic Energy Agency(2002), “Instrumentation and Control Systems Important to Safety in Nuclear Power Plants”, IAEA Safety Standard Series No. NS-G-1.3

International Atomic Energy Agency(2014), “Safety Classification of Structure, System and Components in Nuclear Power Plants”, IAEA Safety Standards Series No. SSG-30

International Atomic Energy Agency(2016), “Safety of Nuclear Power Plants: Design”, IAEA Safety Standards Series No. SSR-1/2

ISO(2019), ISO 14971, “Medical Devices - Application Of Risk Management To Medical Devices”

ISO(2012), ISO 26262, Road vehicle Functional safety

ISO/IEC(2012), ISO/IEC Guide 65, “General requirements for bodies operating product certification systems”

J. Gapper(2016), Software is steering auto industry - FT.com, Financ. Times

Jean-Paul Blanquart et al.(2011), Criticality categories across safety standards in different domains

John A McDermid(2001), Software Safety: Why is there no Consensus?, 21th ISSC(International System Safety Conference)

Ji Shujuan, Bao Xiaohong a(2013), Research on Software Hazard Classification, ISAA 2013

Kelly D. Moses and Roy W. Malone(2004), “Development of risk assessment matrix for NASA engineering and safety center”, Rouse WP (eds). Handbook of System Engineering and Management. New York: Wiley, pp.1 ~ 22.

Matthew John Squair(2006), Issues in the Application of Software Safety Standards, the 10th Australian Workshop on Safety Related Programmable Systems (SCS’05)

Lucas Layman et al.(2010), The Role and Quality of Software Safety in the NASA Constellation Program

NIST(2004), FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems”

NIST(2008), Special Publication 800-60 Rev. 1, “Guide for Mapping Types of Information and Information Systems to Security Categories”

OSMA(2020), NASA-STD-8719.13C, “Nasa Software Safety Standard”

OSMA(2020), NASA-STD-8739.8, “Software Assurance and Software Safety Standard”

RTCA(2012), DO-178C, “Software Considerations in Airborne Systems and Equipment Certification”

UK Ministry of Defence(1997), DEF STAN 00-55 REQUIREMENTS FOR SAFETY RELATED SOFTWARE IN DEFENCE EQUIPMENT PART 2: GUIDANCE

US Army Communications/Electronics Command(1992), “Software system safety guide (CECOM-TR-92-2)”

W.Eric Wong(2014), Evaluating Software Safety Standards: A Systematic Review and Comparison, 2014 Eighth International Conference on Software Security and Reliability

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.

비매품/무료
95060
9 791197 090486
ISBN 979-11-970904-8-6 (PDF)

OPEN 출처표시 상업용금지 변경금지 공공누리 공공저작물 자유이용허락

[소프트웨어정책연구소]에 의해 작성된 **[SPRI 보고서]**는 공공저작물 자유이용허락 표시기준 제 4유형**(출처표시-상업적이용금지-변경금지)**에 따라 이용할 수 있습니다.
(출처를 밝히면 자유로운 이용이 가능하지만, 영리목적으로 이용할 수 없고, 변경 없이 그대로 이용해야 합니다.)