



SOFTWARE SAFETY INTEGRITY AND SOFTWARE SYSTEMATIC CAPABILITY IN PROCESS INDUSTRY

Honeywell

SPRi Software Safety Conference

November 23, 2017 | Seoul, Republic of Korea

Presenter: Amir Moutameni
Lead Engineer Safety Systems

- MS in Electrical Engineering
- Functional Safety Engineer by TUV Rheinland
- Professional engineer (P.Eng.)
- Project Management Professional (PMP)
- Honeywell Certified Safety Engineer
- 20 Years in Automation

Honeywell
THE POWER OF CONNECTED

AGENDA

- Overview of Failure Types
- IEC 61508 / IEC 61511 Standards
- Safety Integrity
- Systematic Capability
- Management of Software Safety Integrity
- System Safety Lifecycle
- Software Safety Lifecycle
- Software Systematic Capability
- Management of Functional Safety

Honeywell
THE POWER OF CONNECTED

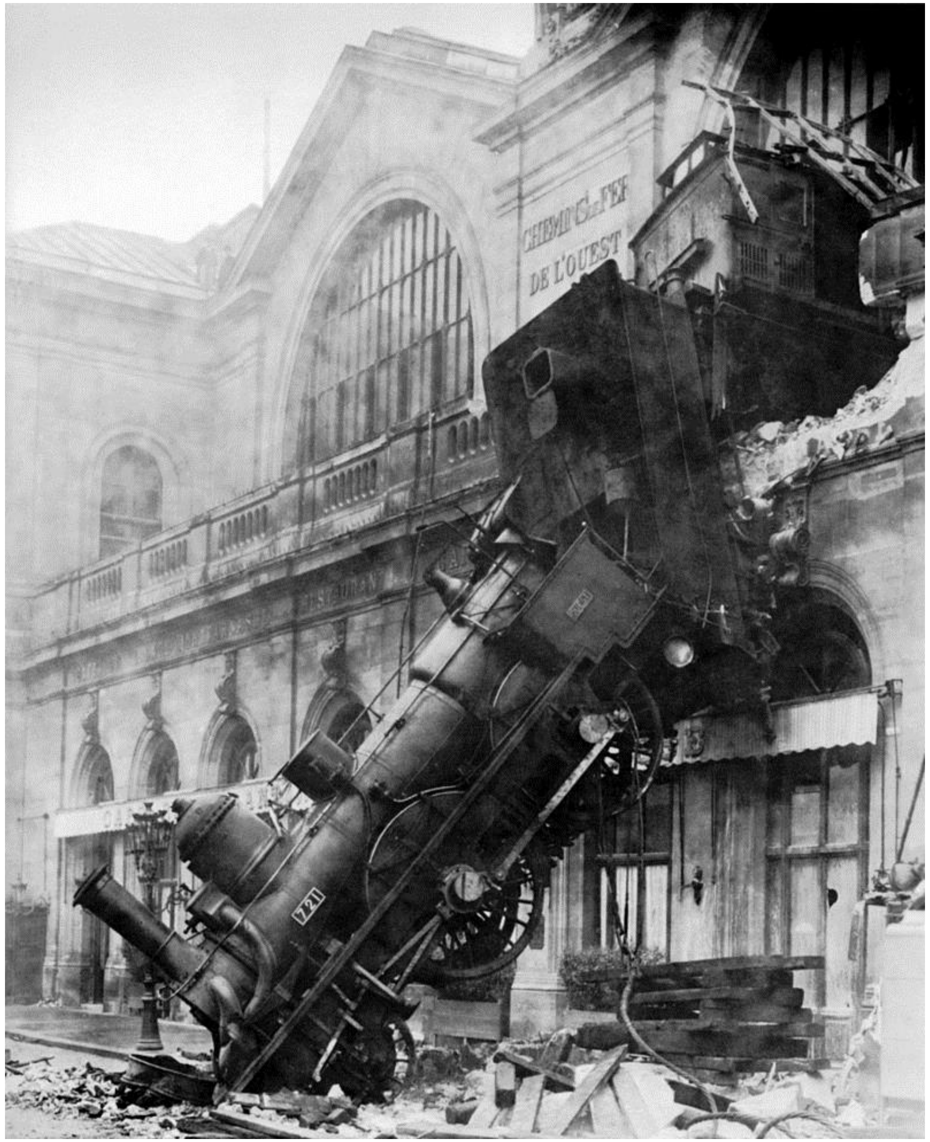
Introduction

Failure
and
Overview of Failure Types

Honeywell
THE POWER OF CONNECTED

Failure

FAILURE IS THE STATE OR CONDITION OF NOT MEETING A DESIRABLE OR INTENDED FUNCTION



Honeywell
THE POWER OF CONNECTED

Failure Types

A SYSTEM MAY FAIL TO FUNCTION AS REQUESTED DUE TO:

- **RANDOM FAILURE**

OR

- **SYSTEMATIC FAILURE**

Honeywell
THE POWER OF CONNECTED

Random Failure

- RELATED TO THE HARDWARE COMPONENTS
- DUE TO PHYSICAL CAUSE

ALSO OCCURS DUE TO VARIOUS RANDOM EVENTS SUCH AS:

- ABNORMAL PROCESS CONDITIONS
- CORROSION, THERMAL STRESSING, …
- WEAR-OUT / TIRE-OUT
- LOW FREQUENCY ATMOSPHERIC EVENT (SNOW IN DESERT)
- NO PATTERN
- IS RANDOM!

QUANTIFIED

Honeywell
THE POWER OF CONNECTED

Random Failure

Systematic Failure

- DUE TO A DETERMINISTIC WAY TO A ROOT CAUSE
- CAUSED BY HUMAN ERROR DURING:
  - DESIGN
  - SPECIFICATION
  - DEVELOPMENT
  - MANUFACTURE
  - INSTALLATION
  - OPERATION
  - MAINTENANCE
  - DECOMMISSIONING

Honeywell

THE POWER OF CONNECTED

Systematic Failure

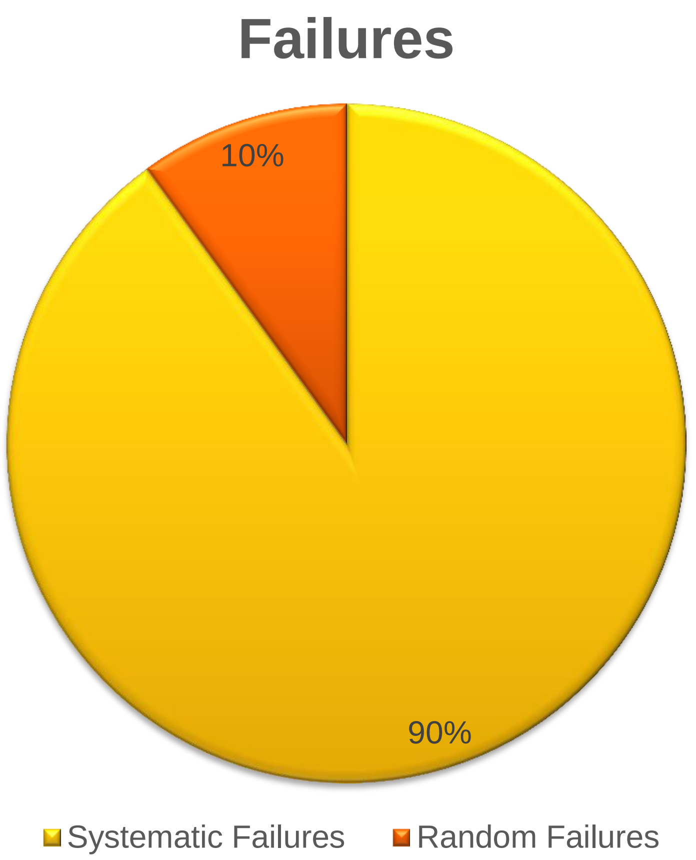
- PATTERN
- IMPOSSIBLE TO ANALYZE IN A PROBABILISTIC MANNER
- IS NOT CONSIDERED IN THE VERIFICATION CALCULATION (NOT PART OF PFD)

CANNOT BE QUANTIFIED

Honeywell
THE POWER OF CONNECTED

Systematic Failure

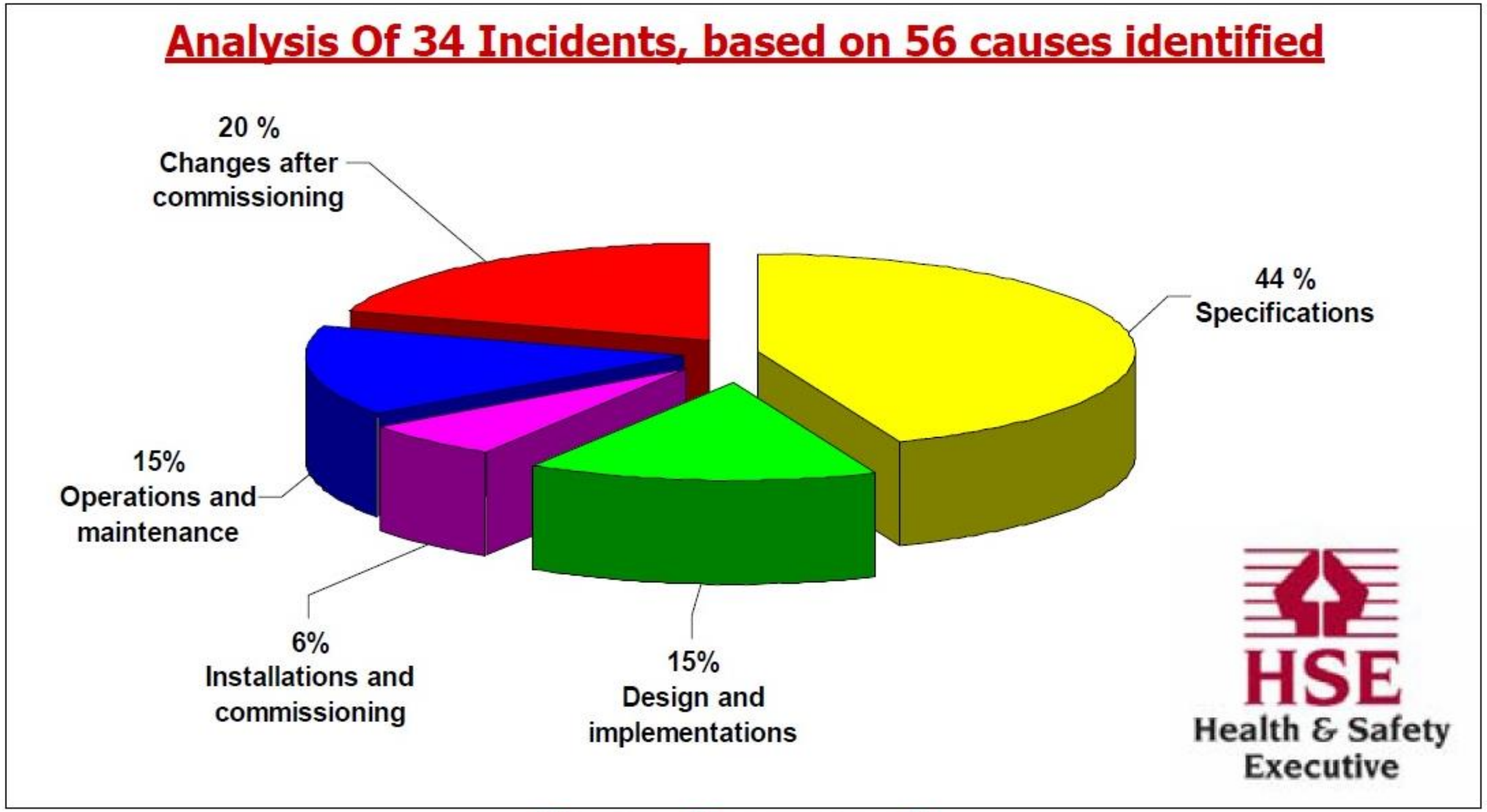
Systematic vs. Random



35 MAJOR INCIDENTS BETWEEN 1987 AND 2012

ANGEL CASAL. 2011, *'SIS PITFALLS, MAJOR ACCIDENTS AND LESSONS LEARNED'*

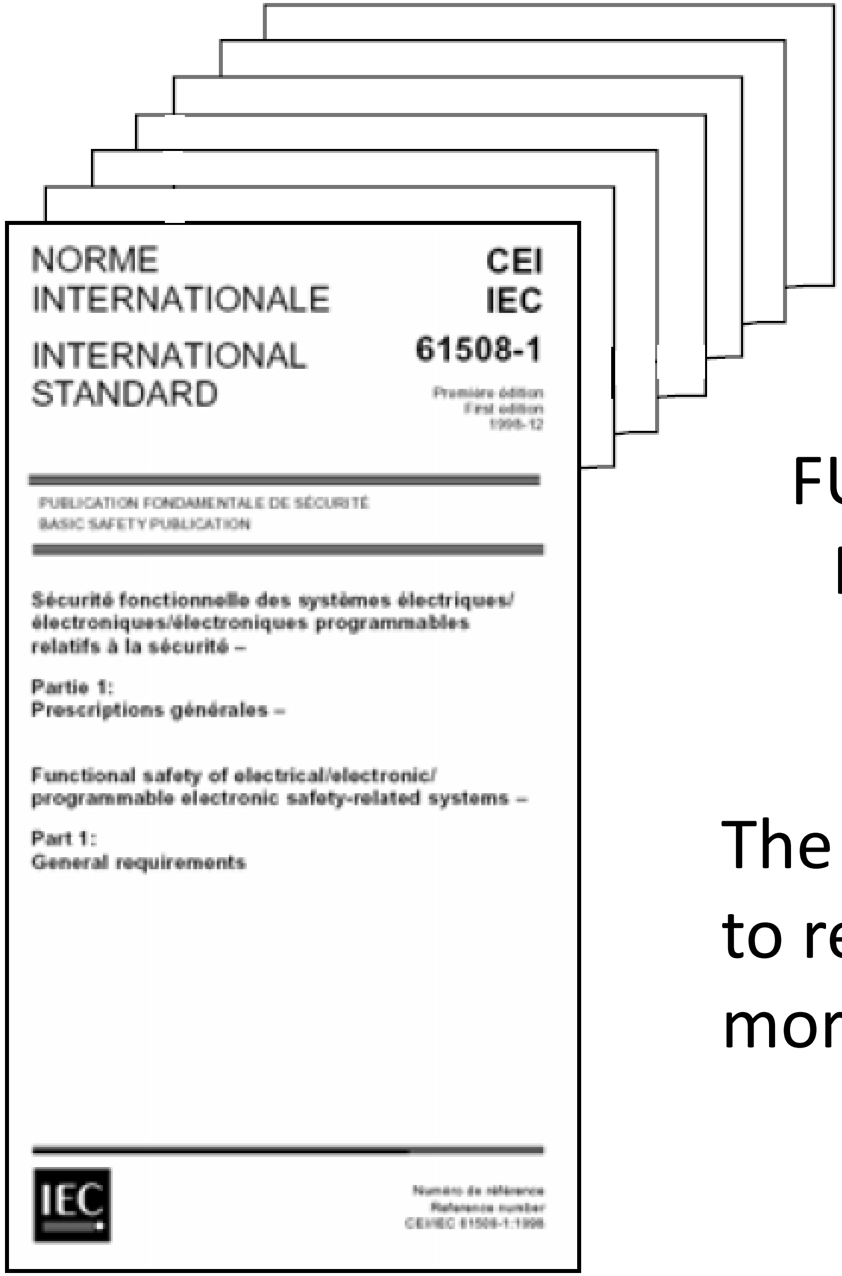
Systematic vs. Random



Out of control

Why control systems go wrong and how to prevent failure?

(2nd edition, source: © Health & Safety Executive HSE – UK)


NORME INTERNATIONALE
INTERNATIONAL STANDARD

CEI
IEC
61508-1

Première édition
First edition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ
BASIC SAFETY PUBLICATION

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –

Partie 1:
Prescriptions générales –

Functional safety of electrical/electronic/programmable electronic safety-related systems –

Part 1:
General requirements

IEC

Numéro de référence
Reference number
CEI/IEC 61508-1:1998

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC)

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS (IEC-61508)

The standards were a natural evolution for the need to reduce process risk and improve safety through a more formalized and quantifiable methodology.

GM

Honeywell
THE POWER OF CONNECTED

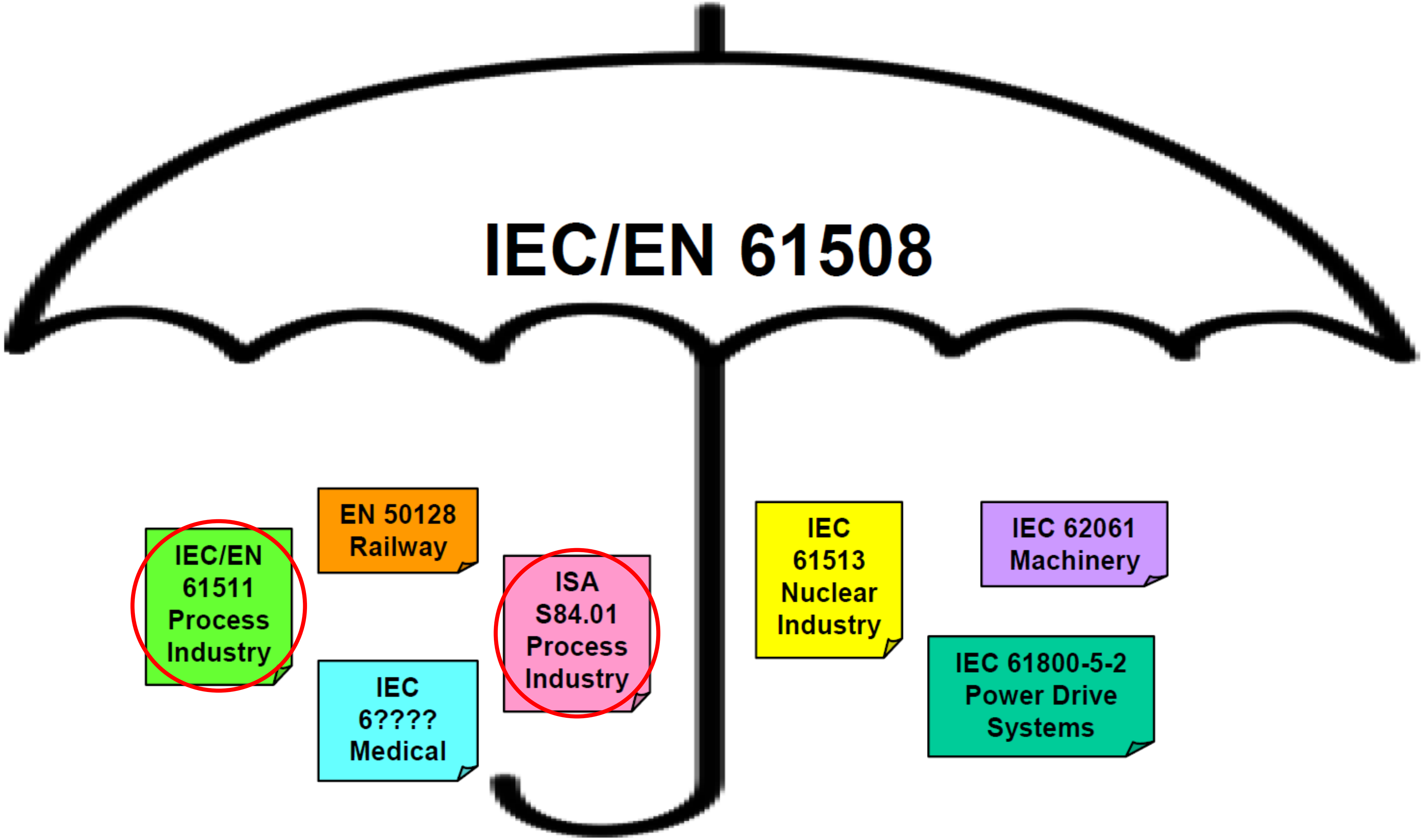
IEC 61508 Standards

SPECIFICALLY FOR IEC 61508, AS THE APPLICATION AND USAGE OF SOFTWARE HAS EVOLVED AND PROLIFERATED, THERE WAS AN INCREASED NEED TO DEVELOP A STANDARD TO GUIDE SYSTEM / PRODUCT DESIGNERS AND DEVELOPERS IN WHAT THEY NEEDED TO DO TO ENSURE AND "CLAIM" THAT THEIR SYSTEMS / PRODUCTS WERE ACCEPTABLY SAFE FOR THEIR INTENDED USES.

GM

Honeywell
THE POWER OF CONNECTED

IEC 61508 STANDARDS



Safety Integrity

ACHIEVEMENT SAFETY INTEGRITY → TARGET RISK REDUCTION

IEC 61511.1—2016:
AVERAGE PROBABILITY OF A SAFETY INSTRUMENTED SYSTEM SATISFACTORILY PERFORMING THE REQUIRED SAFETY INSTRUMENTED FUNCTIONS UNDER ALL THE STATED CONDITIONS WITHIN A STATED PERIOD OF TIME

SAFETY INTEGRITY COMPRISES:

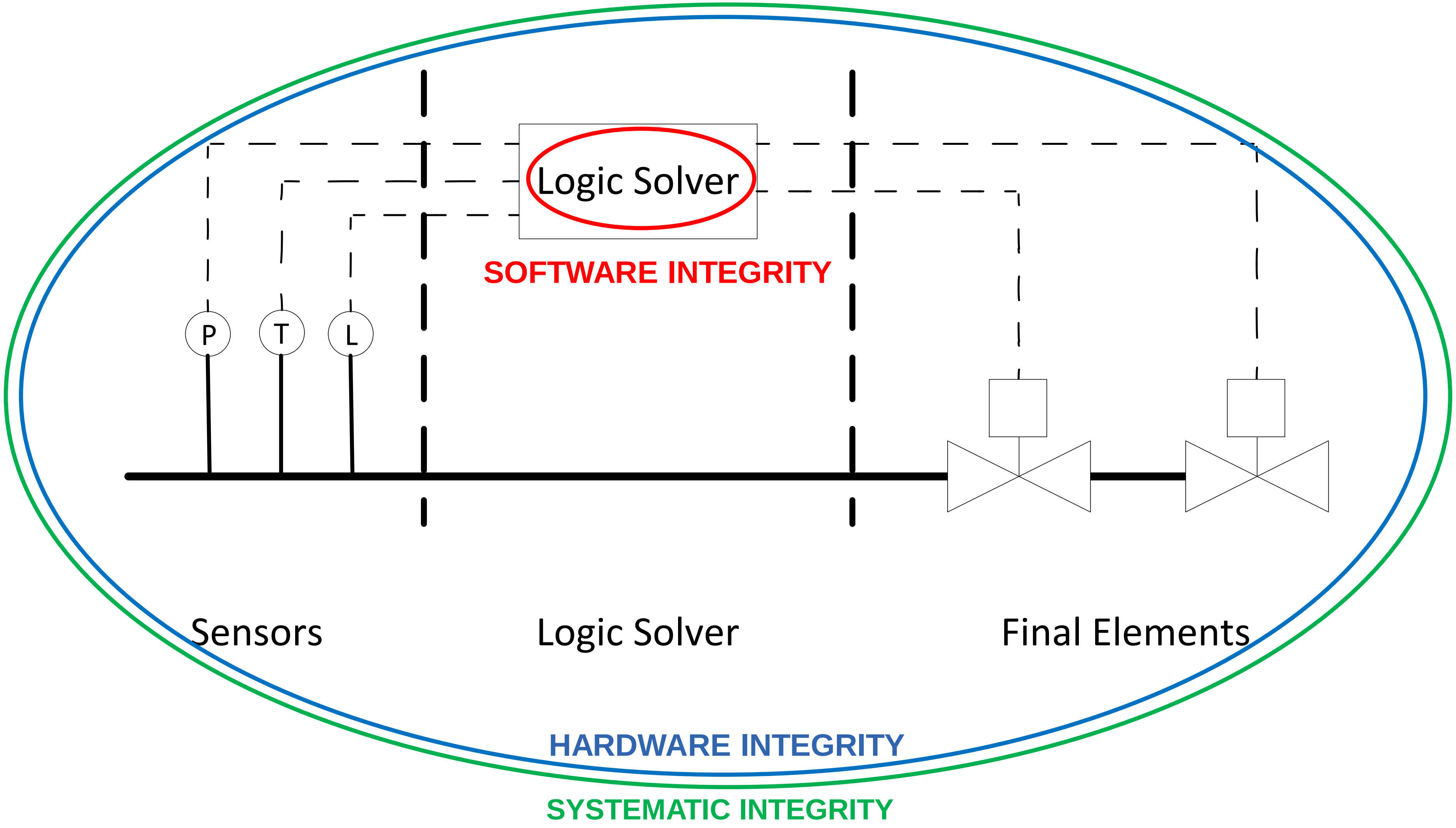
***HARDWARE SAFETY INTEGRITY* (RELATED TO RANDOM FAILURE)**

AND

SYSTEMATIC SAFETY INTEGRITY – INCLUDING SOFTWARE SAFETY INTEGRITY- (RELATED TO SYSTEMATIC FAILURE)

Honeywell
THE POWER OF CONNECTED

Safety Integrity



Systematic Safety Integrity

SYSTEMATIC SAFETY INTEGRITY (AND SOFTWARE SAFETY INTEGRITY) IS TO DO WITH THE MANAGEMENT OF SYSTEMATIC FAILURES:

IEC 61511.1—2016:

3.5.5 SOFTWARE SAFETY INTEGRITY

PART OF SAFETY INTEGRITY OF A SAFETY-RELATED SYSTEM RELATING TO SYSTEMATIC FAILURE IN A DANGEROUS MODE OF FAILURE THAT ARE ATTRIBUTABLE TO SOFTWARE

3.5.6 SYSTEMATIC SAFETY INTEGRITY

PART OF THE SAFETY INTEGRITY OF A SAFETY-RELATED SYSTEM RELATING TO SYSTEMATIC FAILURES IN A DANGEROUS MODE OF FAILURE

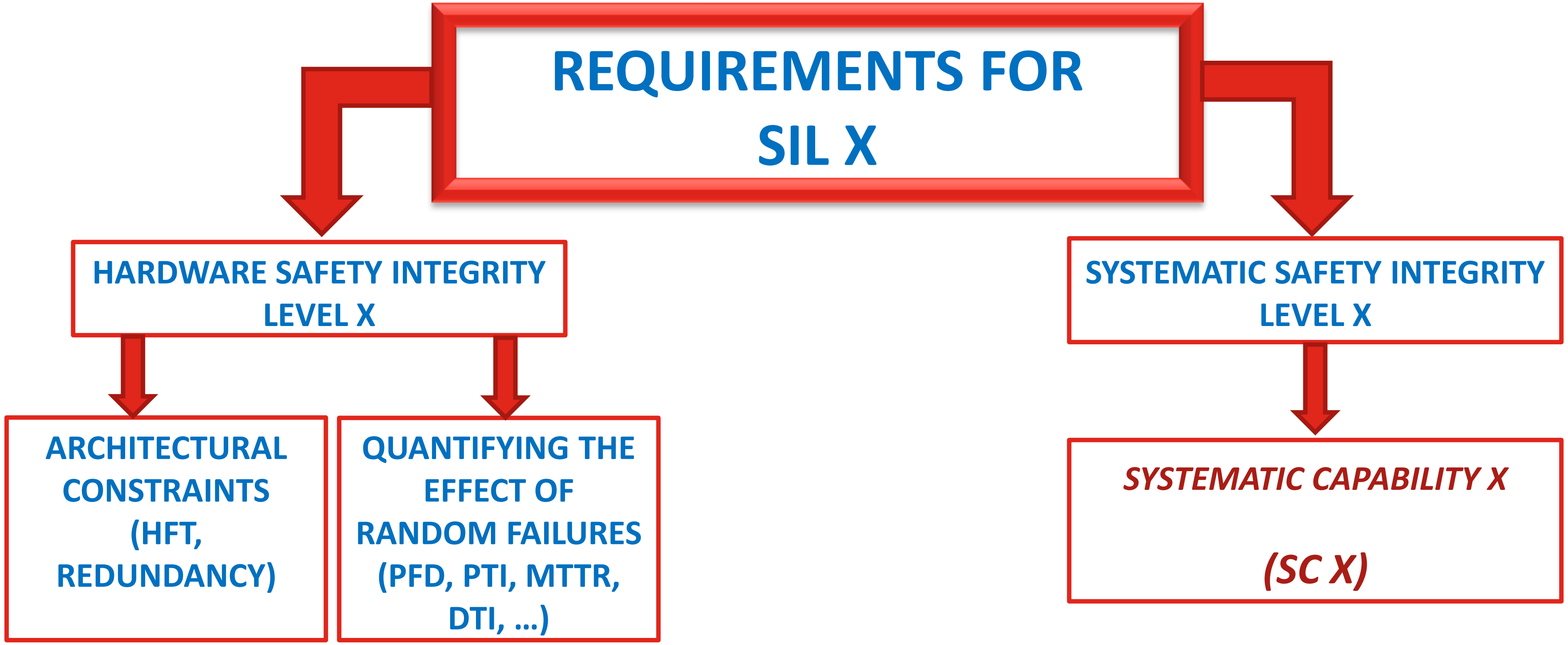
Honeywell

THE POWER OF CONNECTED

Safety Integrity Level (SIL)

HOW MUCH RISK REDUCTION REQUIRED?

4 LEVEL OF SAFETY INTEGRITY DEFINED BY IEC 61508-2010 : SIL 1 TO SIL 4



Honeywell
THE POWER OF CONNECTED

Systematic Capability (SC)

- THE SYSTEMATIC SAFETY INTEGRITY OF AN ELEMENT MEETS THE REQUIREMENTS OF THE SPECIFIED SIL
- IS DETERMINED WITH REFERENCE TO THE REQUIREMENTS FOR THE AVOIDANCE AND CONTROL OF SYSTEMATIC FAULTS
- MEASURE ON A SCALE OF SC 1 TO SC 4

SIL X REQUIRES SC X

FOR A SIL N SIF WE NEED SC N SYSTEMATIC CAPABILITY IN OUR ENGINEERING AND IN OUR SOFTWARE.

Honeywell
THE POWER OF CONNECTED

Achieving Systematic Capability

- **ROUTE 1_S: COMPLIANCE WITH THE REQUIREMENTS FOR THE AVOIDANCE OF SYSTEMATIC FAULTS AND THE REQUIREMENTS FOR THE CONTROL OF SYSTEMATIC FAULTS**

- **ROUTE 2_S: COMPLIANCE WITH THE REQUIREMENTS FOR EVIDENCE THAT THE EQUIPMENT IS PROVEN IN USE**

- **ROUTE 3_S: COMPLIANCE WITH THE REQUIREMENTS OF IEC 61508.3-2010, 7.4.2.12 (PRE-EXISTING SOFTWARE ELEMENTS ONLY)**

Honeywell
THE POWER OF CONNECTED

Route 1_S

1. AVOIDANCE OF SYSTEMATIC FAULTS (IEC 61508.2-2010 ANNEX B)
   a) TABLE B.1 – TECHNIQUES AND MEASURES TO AVOID MISTAKES DURING SPECIFICATION OF SYSTEM DESIGN REQUIREMENTS
   b) TABLE B.2 – TECHNIQUES AND MEASURES TO AVOID INTRODUCING FAULTS DURING SYSTEM DESIGN AND DEVELOPMENT
   c) TABLE B.3 – TECHNIQUES AND MEASURES TO AVOID FAULTS DURING SYSTEM INTEGRATION
   d) TABLE B.4 – TECHNIQUES AND MEASURES TO AVOID FAULTS AND FAILURES DURING SYSTEM OPERATION AND MAINTENANCE
   e) TABLE B.5 – TECHNIQUES AND MEASURES TO AVOID FAULTS DURING SYSTEM SAFETY VALIDATION

2. CONTROL OF SYSTEMATIC FAULTS (IEC 61508.2-2010- ANNEX A)
   a) TABLE A.15 – TECHNIQUES AND MEASURES TO CONTROL SYSTEMATIC FAILURES CAUSED BY HARDWARE DESIGN
   b) TABLE A.16 – TECHNIQUES AND MEASURES TO CONTROL SYSTEMATIC FAILURES CAUSED BY ENVIRONMENTAL STRESS OR INFLUENCES
   c) TABLE A.17 – TECHNIQUES AND MEASURES TO CONTROL SYSTEMATIC OPERATIONAL FAILURES

Honeywell
THE POWER OF CONNECTED

Table B.6 – Effectiveness of techniques and measures to avoid systematic failures

Tat dures

Table B.6 *(continued)*

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Dynamic analysis	B.6.5	Based on block diagrams; highlighting weak points; specifying test cases	Based on detailed diagrams; predicting expected behaviour during test cases; using testing tools
Failure analysis	B.6.6	At module level, including boundary data of the peripheral units	At component level, including boundary data
Worst-case analysis	B.6.7	Performed on safety functions; derived using boundary value combinations for real operating conditions	Performed on non-safety functions; derived using boundary value combinations for real operating conditions
Expanded functional testing	B.6.8	Test that all safety functions are maintained in the case of static input states caused by faulty process or operating conditions	Test that all safety functions are maintained in the case of static input states and/or unusual input changes, caused by faulty process or operating conditions (including those that may be very rare)
Worst-case testing	B.6.9	Test that safety functions are maintained for a combination of boundary values found in real operating conditions	Test that non-safety functions are maintained for a combination of the boundary values found in real operating conditions
Fault insertion testing	B.6.10	At subunit level including boundary data or the peripheral units	At component level including boundary data
NOTE In the cases of the techniques with references B.1.1, B.1.2, B.3.3, B.3.4, B.4.4, B.4.6, B.5.2, B.5.3, B.5.4, B.6.7 and B.6.9, for high effectiveness of the technique or measure, it is assumed that the low effectiveness approaches are also used.			

Honeywell
THE POWER OF CONNECTED

Table A.18 – Effectiveness of techniques and measures to control systematic failures

Technique/measure	See IEC 61508-7	Low effectiveness	High effectiveness
Failure detection by on-line monitoring (see Note)	A.1.1	Trigger signals from the EUC and its control system are used to check the proper operation of the E/E/PE safety-related systems (only time behaviour with an upper time limit)	E/E/PE safety-related systems are retriggered by temporal and logical signals from the EUC and its control system (time window for temporal watch-dog function)
Tests by redundant hardware (see Note)	A.2.1	Additional hardware tests the trigger signals of the E/E/PE safety-related systems (only time behaviour with an upper time limit), this hardware switches a secondary final element	Additional hardware is retriggered by temporal and logical signals of the E/E/PE safety-related systems (time window for temporal watch-dog); voting between multiple channels
Standard test access port and boundary-scan architecture	A.2.3	Testing the used solid-state logic, during the proof test, through defined boundary scan tests	Diagnostic test of solid-state logic, according to the functional specification of the E/E/PE safety-related systems; all functions are checked for all integrated circuits
Code protection	A.6.2	Failure detection via time redundancy of signal transmission	Failure detection via time and information redundancy of signal transmission
Measures against voltage breakdown, voltage variations, overvoltage and low voltage	A.8	Overvoltage protection with safety shut-off or switch-over to secondary power unit	Voltage control (secondary) with safety shut-off or switch-over to secondary power unit; or power-down with safety shut-off or switch-over to secondary power unit
Program sequence monitoring	A.9	Temporal or logical monitoring of the program sequence	Temporal and logical monitoring of the program sequence at very many checking points in the program
Measures against temperature increase	A.10	Detecting over-temperature	Actuation of the safety shut-off via thermal fuse; or several levels of over-temperature sensing and alarms; or connection of forced-air cooling and status indication
Increase of interference immunity (see Note)	A.11.3	Noise filter at power supply and critical inputs and outputs; shielding, if necessary	Filter against electromagnetic injection that is normally not expected; shielding
Measures against physical environment	A.14	Generally accepted practice according to the application	Techniques referred to in standards for a particular application
Diverse hardware	B.1.4	Two or more items carrying out the same function but being different in design	Two or more items carrying out different functions
Modification protection	B.4.8	Modification requires specific tools	Modification requires use of key lock or dedicated tool with password
Input acknowledgement	B.4.9	Echoing of input actions back to the operator	Checking strict rules for the input of data by the operator, rejecting incorrect inputs

NOTE In the cases of the techniques with references A.1.1, A.2.1, A.11.3, and A.14 for high effectiveness of the technique or measure it is assumed that the low effectiveness approaches are also used.

Honeywell
THE POWER OF CONNECTED

IEC 61508.7-2010 B.1.1 Project management

Aim: To avoid failures by adoption of an organizational model and rules and measures for development and testing of safety-related systems.

Description: The most important and best measures are
– The creation of an organizational model, especially for quality assurance which is set down in a quality assurance handbook; and
– The establishment of regulations and measures for the creation and validation of safety related systems in cross-project and project-specific guidelines.

A number of important basic principles are set down in the following:
– Definition of a design organization:

- tasks and responsibilities of the organizational units,
- authority of the quality assurance departments,
- independence of quality assurance (internal inspection) from development;

– Definition of a sequence plan (activity models):

- determination of all activities which are relevant during execution of the project including internal inspections and their scheduling,
- project update;

– Definition of a standardized sequence for an internal inspection:

- planning, execution and checking of the inspection (inspection theory),
- releasing mechanisms for sub-products,
- the safekeeping of repeat inspections;

– Configuration management:

- administration and checking of versions,
- detection of the effects of modifications,
- consistency inspections after modifications;

– Introduction of a quantitative assessment of quality assurance measures:

- requirement acquisition,
- failure statistics;

– Introduction of computer-aided universal methods, tools and training of personnel.

Honeywell
THE POWER OF CONNECTED

MANAGEMENT OF SOFTWARE INTEGRITY TECHNIQUES AND MEASURES

61508.3-2010 ANNEX A

- TABLE A.1 – SOFTWARE SAFETY REQUIREMENTS SPECIFICATION
- TABLE A.2 – SOFTWARE ARCHITECTURE DESIGN
- TABLE A.3 – SUPPORT TOOLS & PROGRAMMING LANGUAGE
- TABLE A.4 – SOFTWARE DETAILED DESIGN
- TABLE A.5 – SOFTWARE MODULE TESTING & INTEGRATION
- TABLE A.6 – HARDWARE AND SOFTWARE INTEGRATION
- TABLE A.7 – SYSTEM SAFETY VALIDATION
- TABLE A.8 – MODIFICATION
- TABLE A.9 – SOFTWARE VERIFICATION
- TABLE A.10 – FUNCTIONAL SAFETY ASSESSMENT

Honeywell
THE POWER OF CONNECTED

MANAGEMENT OF SOFTWARE INTEGRITY
DETAILED TABLES

61508.3-2010 ANNEX B

- TABLE B.1 – DESIGN AND CODING STANDARDS
- TABLE B.2 – DYNAMIC ANALYSIS AND TESTING
- TABLE B.3 – FUNCTIONAL AND BLACK-BOX TESTING
- TABLE B.4 – FAILURE ANALYSIS
- TABLE B.5 – MODELLING
- TABLE B.6 – PERFORMANCE TESTING
- TABLE B.7 – SEMI-FORMAL METHODS
- TABLE B.8 – STATIC ANALYSIS
- TABLE B.9 – MODULAR APPROACH

Honeywell
THE POWER OF CONNECTED

GUIDE TO THE SELECTION OF TECHNIQUES AND MEASURES

Table A.9 – Software verification

Table A.10 – Functional safety assessment

Assessment/Technique *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1	Checklists	B.2.5	R	R	R	R
2	Decision/truth tables	C.6.1	R	R	R	R
3	Failure analysis	Table B.4	R	R	HR	HR
4	Common cause failure analysis of diverse software (if diverse software is actually used)	C.6.3	---	R	HR	HR
5	Reliability block diagram	C.6.4	R	R	R	R
6	Forward traceability between the requirements of Clause 8 and the plan for software functional safety assessment	C.2.11	R	R	HR	HR

Programmable electronics integration testing	See Table A.6
Software system testing (validation)	See Table A.7

specification

8	Forward traceability between the software safety requirements specification and software design	C.2.11	R	R	HR	HR

Honeywell
THE POWER OF CONNECTED

Detailed Tables

Table B.8 – Static analysis

(Referenced by Table A.9)

Table B.9 – Modular approach

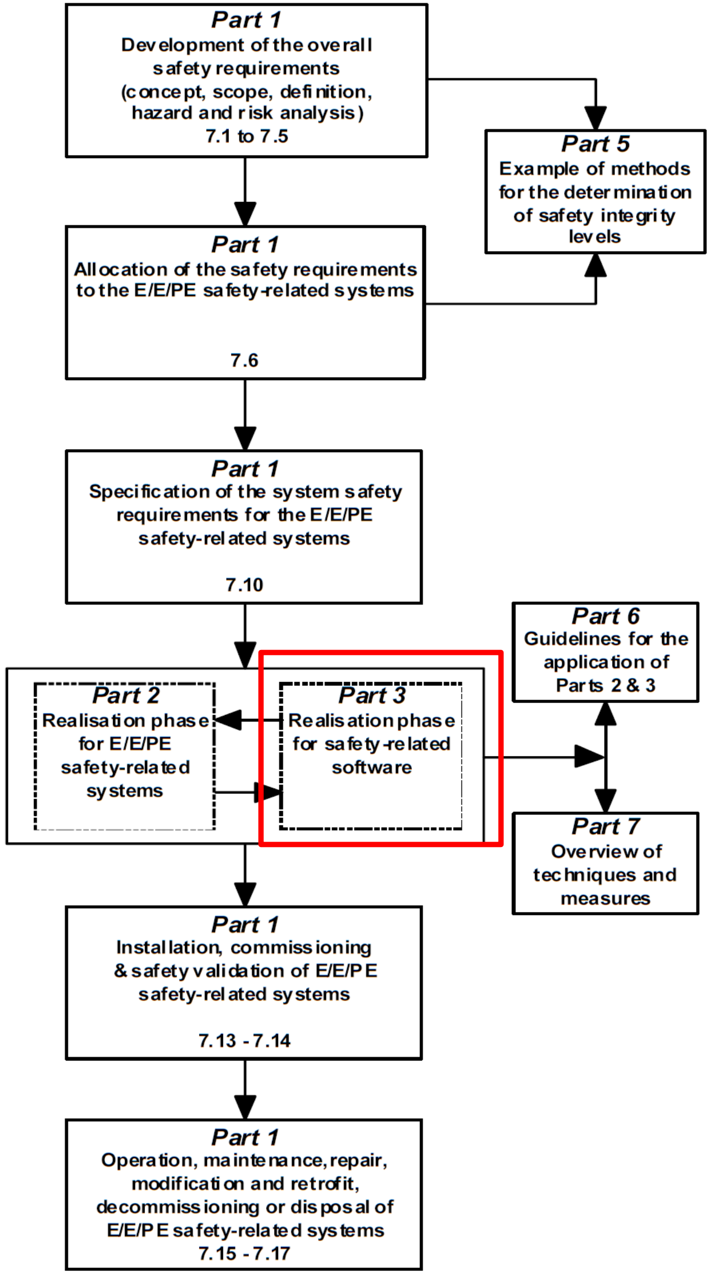
(Referenced by Table A.4)

Technique/Measure *		Ref	SIL 1	SIL 2	SIL 3	SIL 4
1	Software module size limit	C.2.9	HR	HR	HR	HR
2	Software complexity control	C.5.13	R	R	HR	HR
3	Information hiding/encapsulation	C.2.8	R	HR	HR	HR
4	Parameter number limit / fixed number of subprogram parameters	C.2.9	R	R	R	R
5	One entry/one exit point in subroutines and functions	C.2.9	HR	HR	HR	HR
6	Fully defined interface	C.2.9	HR	HR	HR	HR
10	Worst-case execution time analysis	C.5.20	R	R	R	R

Honeywell

THE POWER OF **CONNECTED**

IEC 61508 PART 3 : SOFTWARE REQUIREMENTS

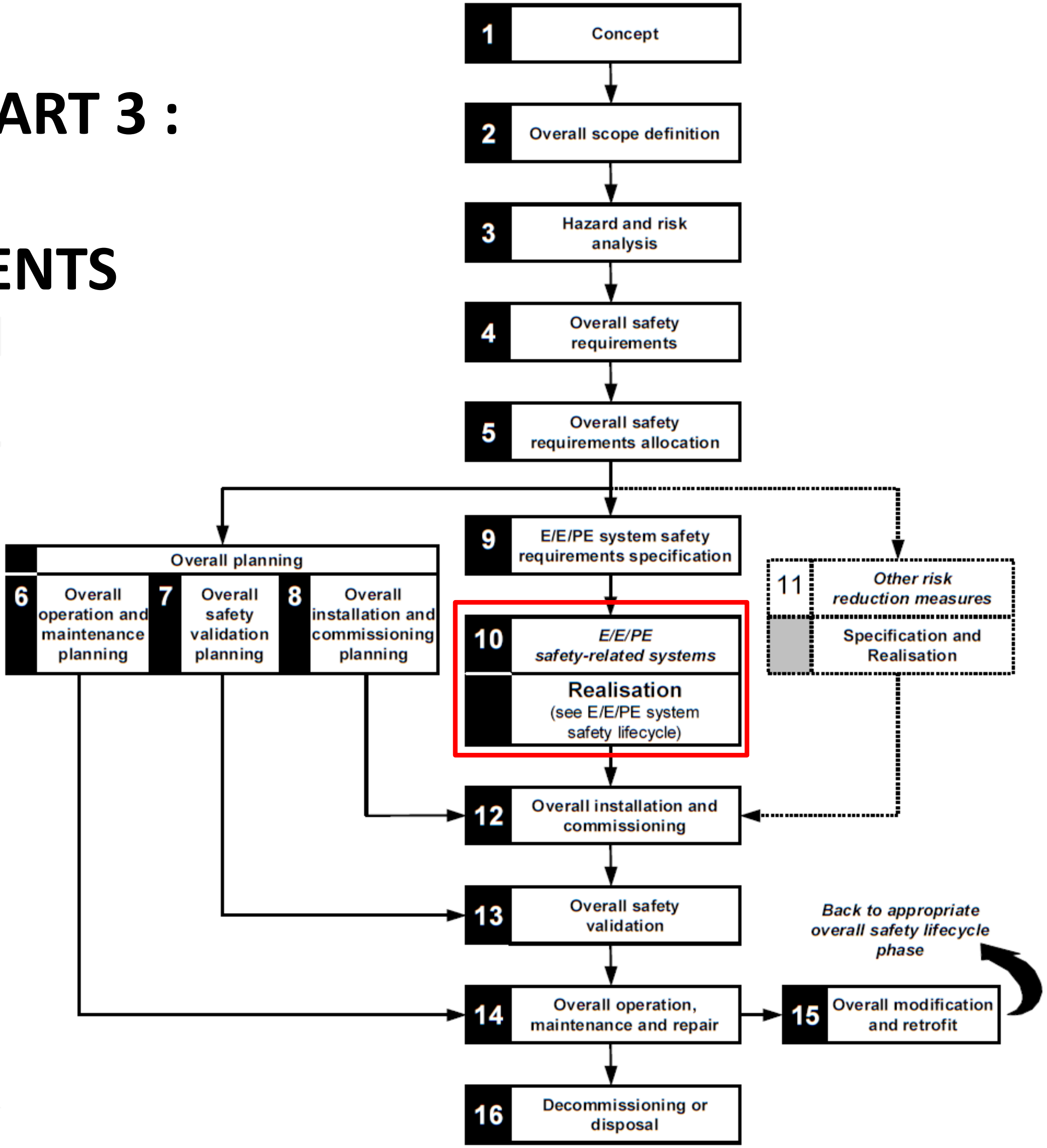


TECHNICAL REQUIREMENTS

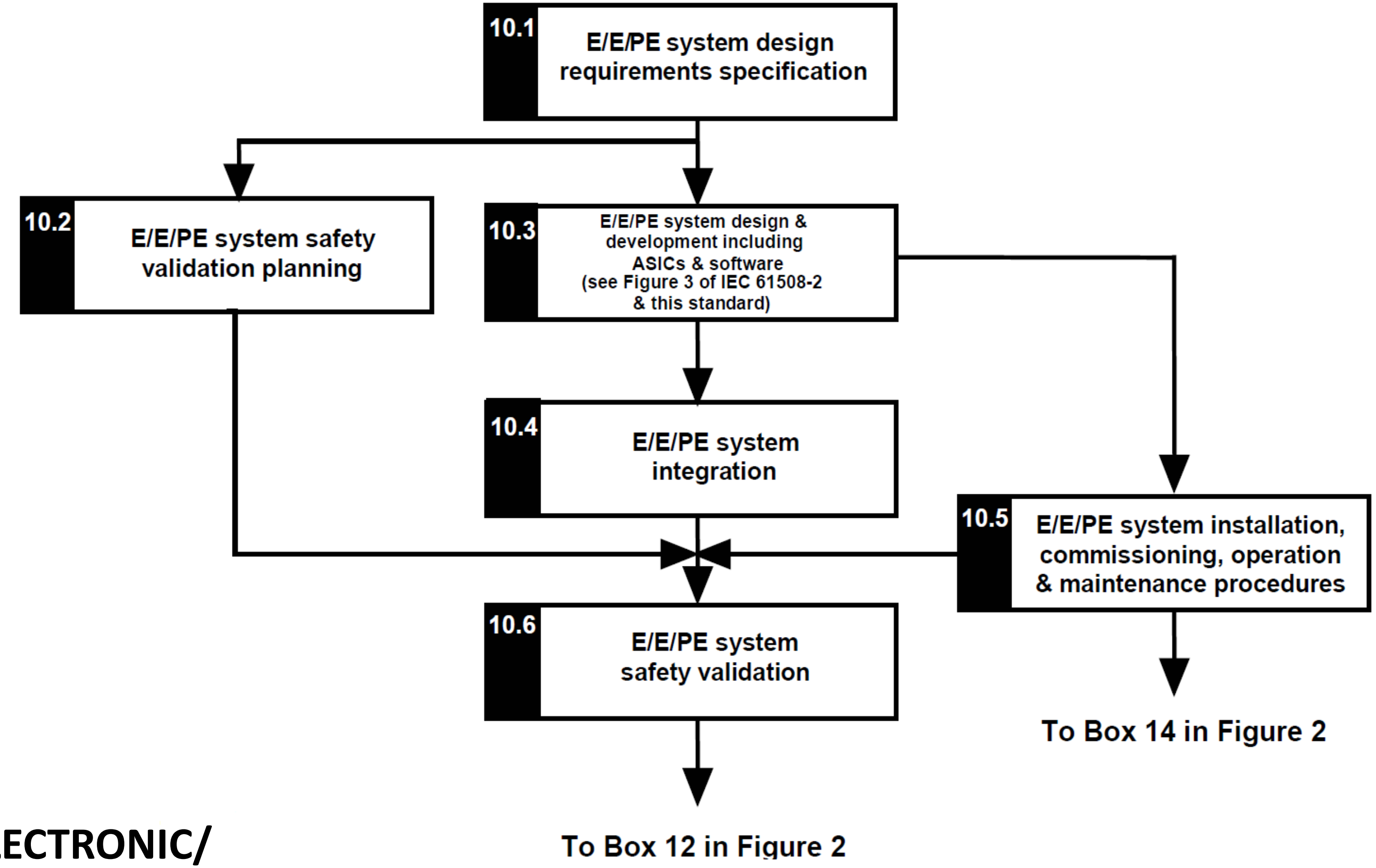
Honeywell
THE POWER OF CONNECTED

IEC 61508 PART 3 : SOFTWARE REQUIREMENTS

OVERALL SAFETY LIFECYCLE



E/E/PE SYSTEM SAFETY LIFECYCLE

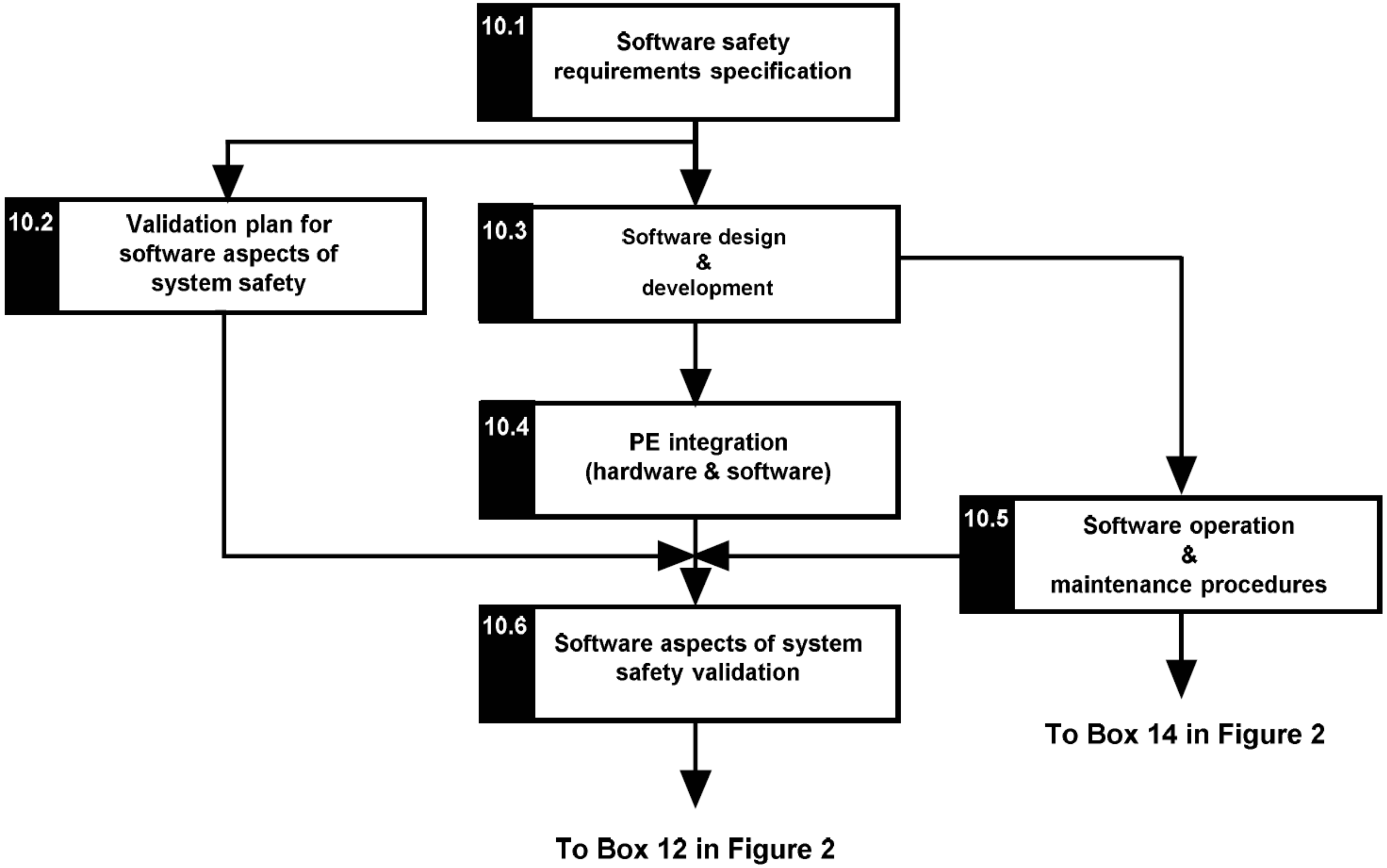


E/E/PE:

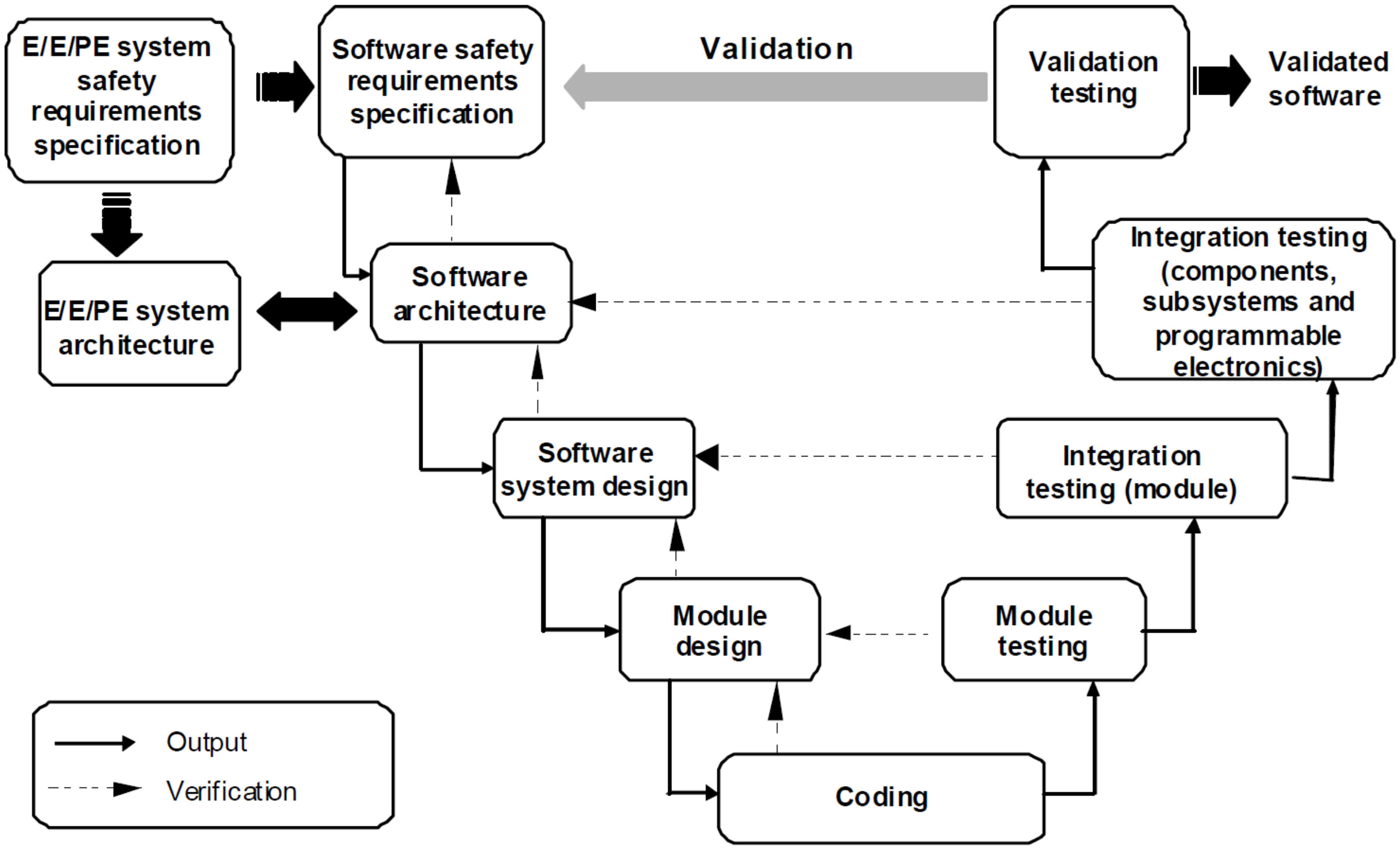
ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC

Honeywell
THE POWER OF CONNECTED

SOFTWARE SAFETY LIFECYCLE



SOFTWARE SYSTEMATIC CAPABILITY AND THE DEVELOPMENT LIFECYCLE (THE V-MODEL)



AVOIDANCE AND CONTROL OF SYSTEMATIC FAULTS ARE SIGNIFICANTLY MORE DIFFICULT IN COMPARE TO RANDOM FAULTS

SAFETY LIFECYCLE

FUNCTIONAL SAFETY PLANNING

<u>MANAGEMENT OF FUNCTIONAL SAFETY</u>

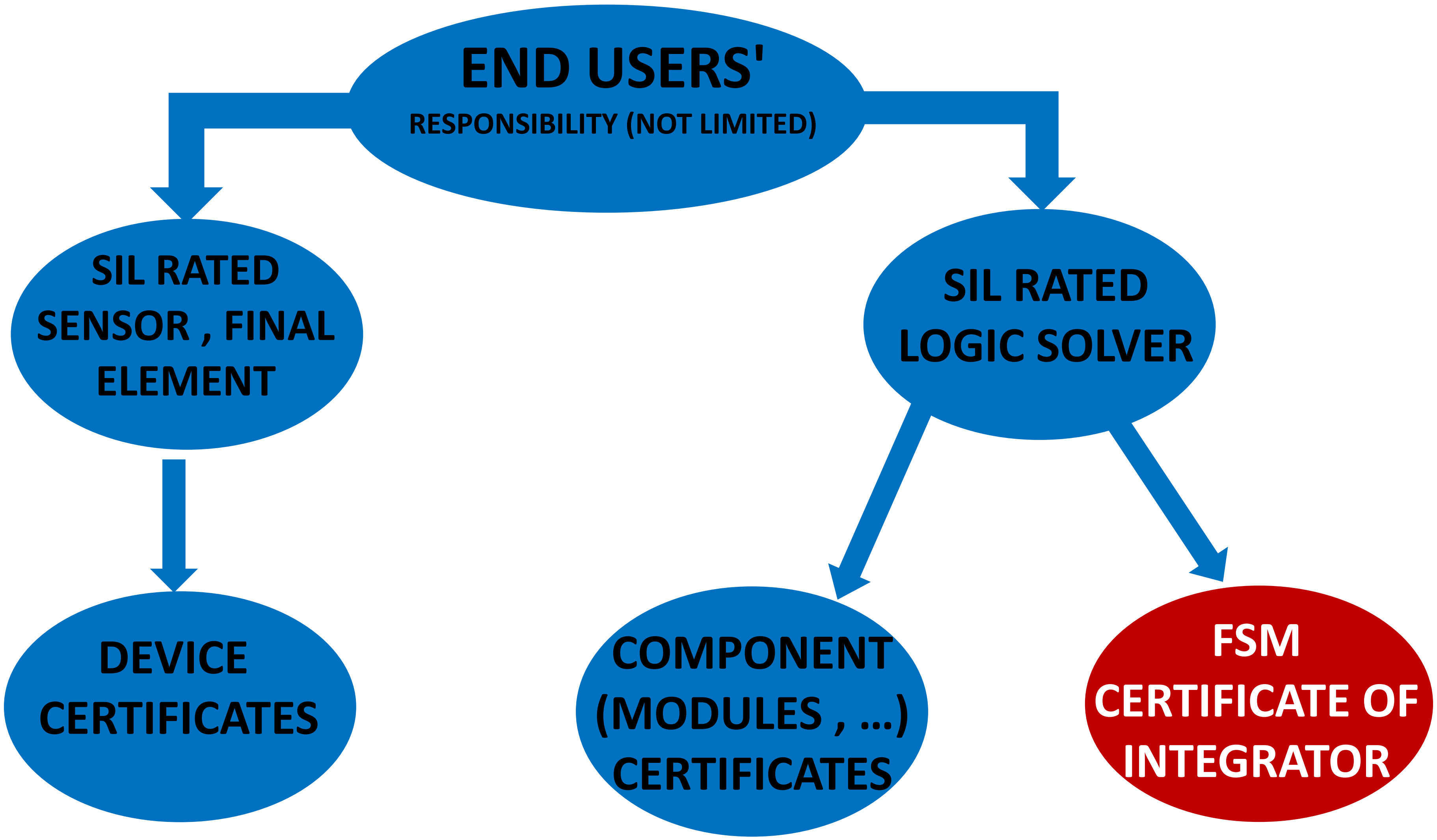
Honeywell
THE POWER OF CONNECTED

AT DIFFERENT PARTS OF THE SAFETY LIFE CYCLE, DIFFERENT PARTIES ARE RESPONSIBLE FOR THE FSM

OVERALL IS ALWAYS END USER

Honeywell
THE POWER OF CONNECTED

EXAMPLE: SELECTION OF SIS ELEMENTS



Honeywell
THE POWER OF CONNECTED

exida

The manufacturer may use the mark:

CERTIFIED • IEC 61508 • SIL 3 CAPABLE • exida

Revision 2.0 June 15, 2016
Surveillance Audit Due
July 1, 2019

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat
Zertifikat / 合格証

exida hereby confirms that the:

Level Transmitter

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:
The Eclipse 706GWR Level Transmitter will measure level and transmit a corresponding signal within the stated safety accuracy.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

exida Certification

Evaluating Assessor

Certifying Assessor

Honeywell
THE POWER OF CONNECTED

TÜV NORD

Certificate

has implemented a

-Functional Safety Management System-

in accordance with

IEC 61511 and IEC 61508

for project engineering of microprocessor-based safety systems including application software.

IEC 61511:2003
Safety Instrumented Systems for the Process Industry Sector

IEC 61508:2010
Functional safety of electrical/electronic programmable safety related systems

---

The certification is based on the assessment report SEBS-A.174646/12FSM and the certificate addendum SEBS-A.174646/12Area1 in the valid versions. It does not replace any specific certification required for safety related E/E/PES or EUC.

Expiry date: 2016-09-24
Reference No.: 8110032699

Gerhard M. Rieger
Branch Manager

Augsburg, 2013-09-24

TÜV NORD
TÜV NORD Systems GmbH & Co. KG
FSM
FSM – Area 1
IEC 61511:2003
IEC61508:2010
SEBS-A.174646/12

TÜV NORD Systems GmbH & Co. KG, Branch South, Halderstr. 27, 86150 Augsburg, Germany

Honeywell
THE POWER OF CONNECTED

QUESTIONS?

Honeywell

THE POWER OF CONNECTED