A Practical Perspective on Software Safety

David N. Card

Research Associate

Experimental Software Engineering Group

Universidade Federal do Rio de Janeiro

Objectives

- Introduce system developers to a comprehensive approach to ensuring software quality and safety
- Help researchers identify useful topics for further research

Safety

- The condition of being protected from or unlikely to cause danger, risk, or injury

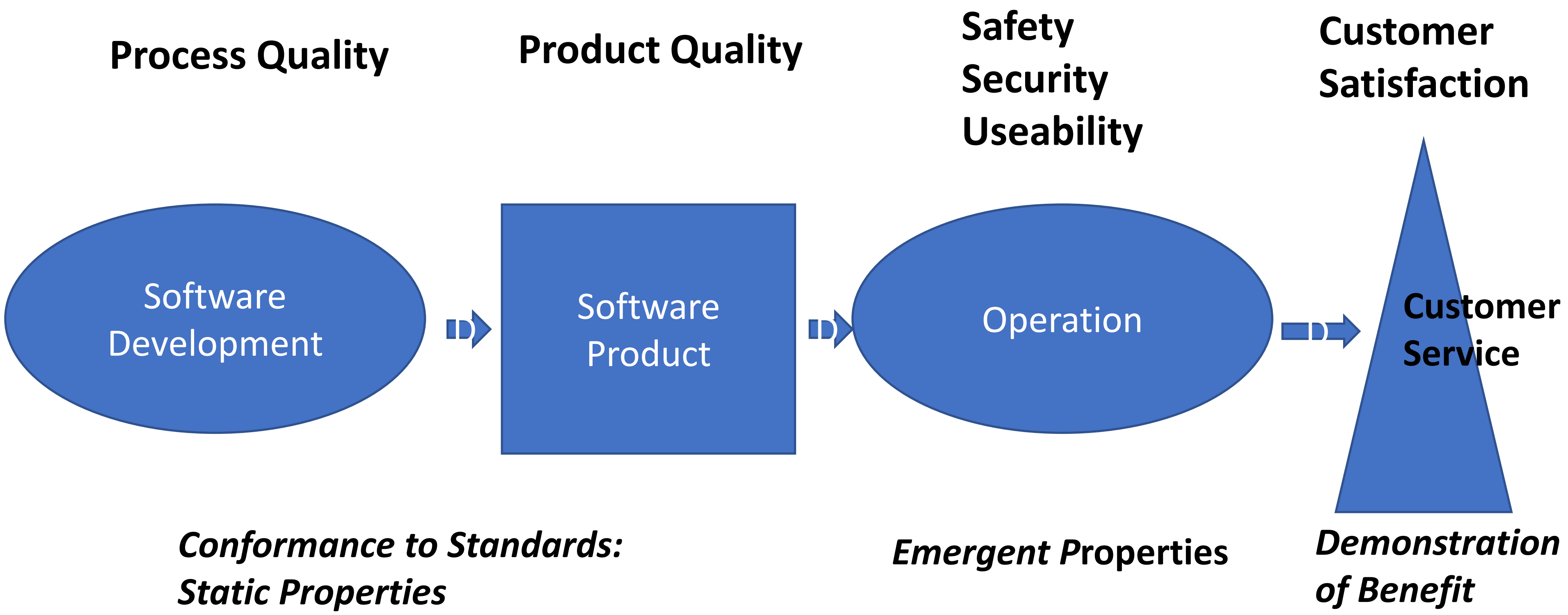
  Merriam Webster

- Typical types of dangers and injuries
  1. Financial
  2. Physical
  3. Reputational

Software Safety

- Software, by itself is safe (except some financial applications)
- Systems (software interacting with hardware) may be safe or unsafe, due to
    - Failure to take intended action
    - Unintended action
    - Action not timely
- Safety cannot be proven in advance
- Software does not wear out – it is delivered with defects
- Software safety is dependent on quality and reliability

Software Quality Model



Process Quality

Product Quality

Safety
Security
Useability

Customer
Satisfaction

Conformance to Standards:
Static Properties

Emergent Properties

Demonstration
of Benefit

Emergent Property

- Not observable in static software
- Cannot be proven or tested to certainty
- Depends on environment and usage

Management of Emergent Property (Safety)

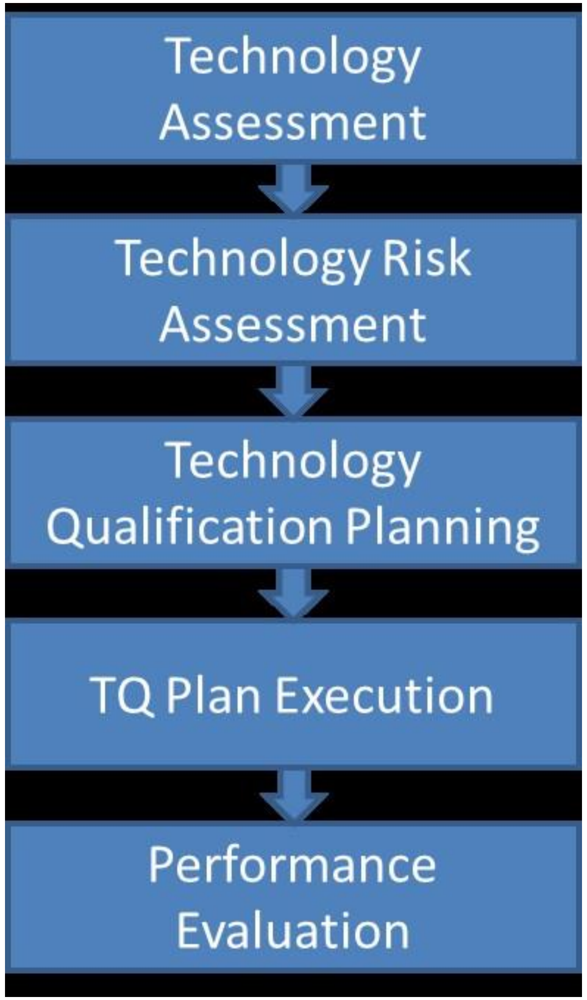
- Understand the operational context
- Perform technical risk analysis (not just management risks)
- Maximize static software quality
- Perform usage-based testing (not use case testing)
- Software redundancy is difficult/expensive to achieve (e.g., STS)
- Consider user/operator behavior (BOP, 737 Max)
- Adopt a system-level comprehensive approach (e.g., Technology Qualification

Technology Qualification

- A process for ensuring that a complex system meets quality, reliability, and safety requirements
- Multiple documented approaches
- Our approach will focus on new (innovative) technology
- Objectives must be defined based on project intent (often specific users/customers are not identified)

Technology Qualification Process

- Based on DNVRP-A203



Technology Assessment

Technology Risk Assessment

Technology Qualification Planning

TQ Plan Execution

Performance Evaluation

Identify Software Innovations
Identify and/or Tailor
Applicable Standards

Risk Analysis (FMEA/FMECA),
Critical Parameters

Test Plan
Data collection Plan
Risk Mitigation

Testing
Data collection
Assess Conformance to
Standards

Meets Critical Parameters
Reliability Analysis

Technology Assessment for Software

Novelty Level	Criteria	Example
1	Existing code previously used for this application	Ballast trim, Robotics framework
2	Existing Code used in other application	Pattern Recognition
3	New code, Existing Algorithm	Communications protocol
4	New code, New Algorithm	Pipeline Following

- Example from Autonomous Undersea Vehicle
- Focuses qualification attention on innovative parts

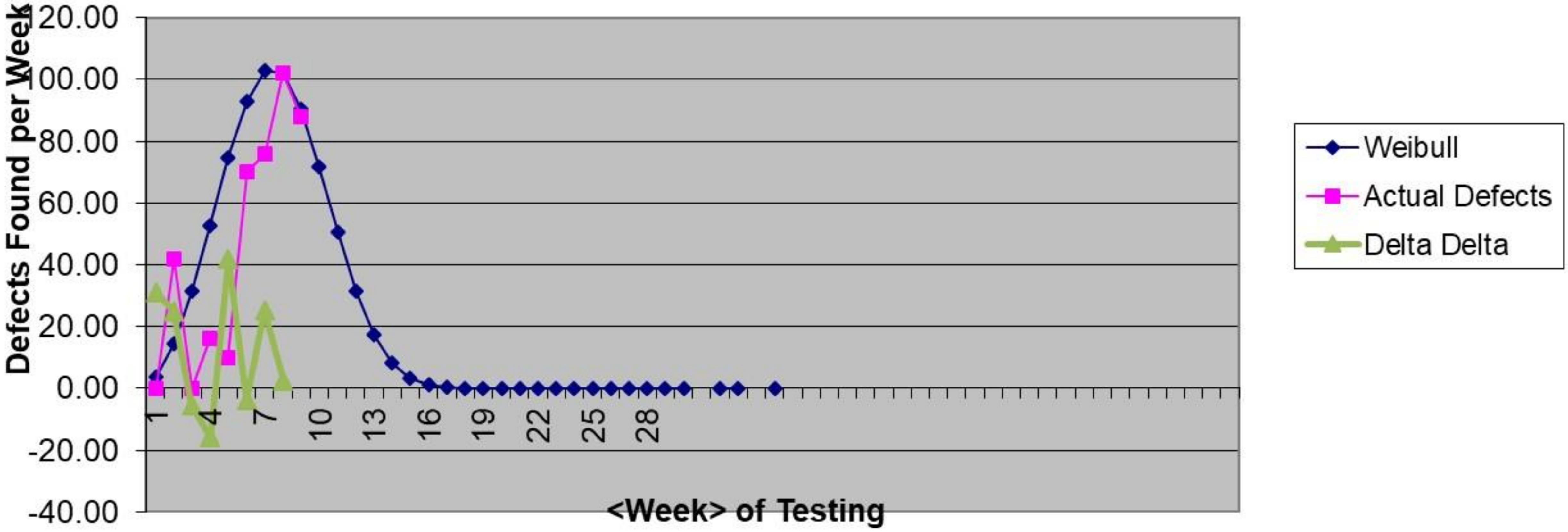
Technical Risk Analysis

- For each (novel) component, determine
  - How component can fail
  - Consequence of failure
  - Probability of failure
  - Magnitude of consequences
- Mitigation actions for critical failures
- Typically generates lots of data

Assess Conformance to Standards

- In-process audits using, e.g.,
  - CMMI
  - ISO/IEC 15288/12207
- Code reviews/inspections
  - Correctness relative to specifications
  - Protocols (e.g, communication, security)
- Static analysis (e.g., check for memory leaks)

Reliability Analysis (Performance Frontier)



Possible Further Research Topics

- Definition of Operational Scenarios to support safety analysis
- Improved Technical Risk Analysis Approaches
- Alternative Reliability Modelling Approaches

Summary

- Safety must be viewed from a system perspective
- Understanding operations is key
- Probe broadly for risks
- Monitor and update as operating environment changes

References

- D.N.Card and M.E. Novaes-Card, *Technology Qualification*, in Perspectives on Systems Engineering, edited by S. Tilley, 2020
- American Petroleum Institute, Recommended Practice 17Q, *Subsea Equipment Qualification*, 2010-2018
- Det Norske Veritas, Recommended Practice A203, *Technology Qualification*, July 2013

Thanks for the Experience

- Det Norske Veritas
- Hyundai Heavy Industries
- Daewoo Shipbuilding and Marine Engineering
- Samsung Heavy Industies
- National Aeronautics and Space Administration
- Carnegie Mellon University Software Engineering Institute