

Why Safety-critical Software needs more than Software Quality Assurance to Manage Safety Risk

Dr. Jeffrey Joyce
Critical Systems Labs Inc.

jeffj@criticalsystemsllabs.com



High Quality → Safety?

“Our company has invested a great deal of effort to ensure that our software development process will develop high quality software, e.g., ISO 9001, CMM.

Isn't this enough to be confident about the safety of the software that we deliver?”



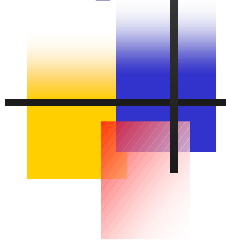
More Thorough Testing

- Software professionals often believe that the main difference in developing safety critical software is simply the thoroughness of testing

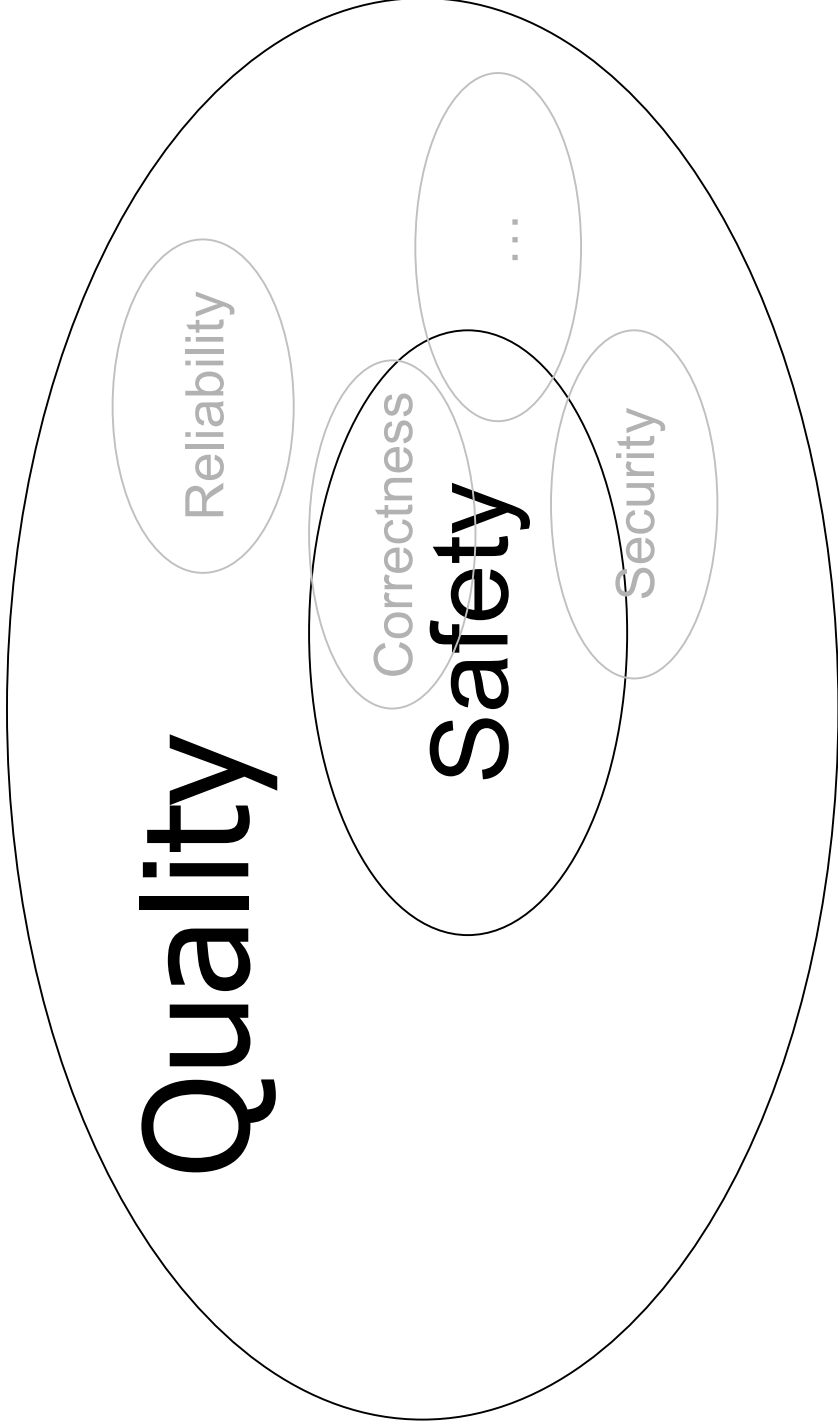


Safety Requirements

- A common strategy is to mitigate all hazards by specifying safety requirements, and then rely on standard requirements-based verification.
- This is intended to transform the safety task into a quality assurance task.

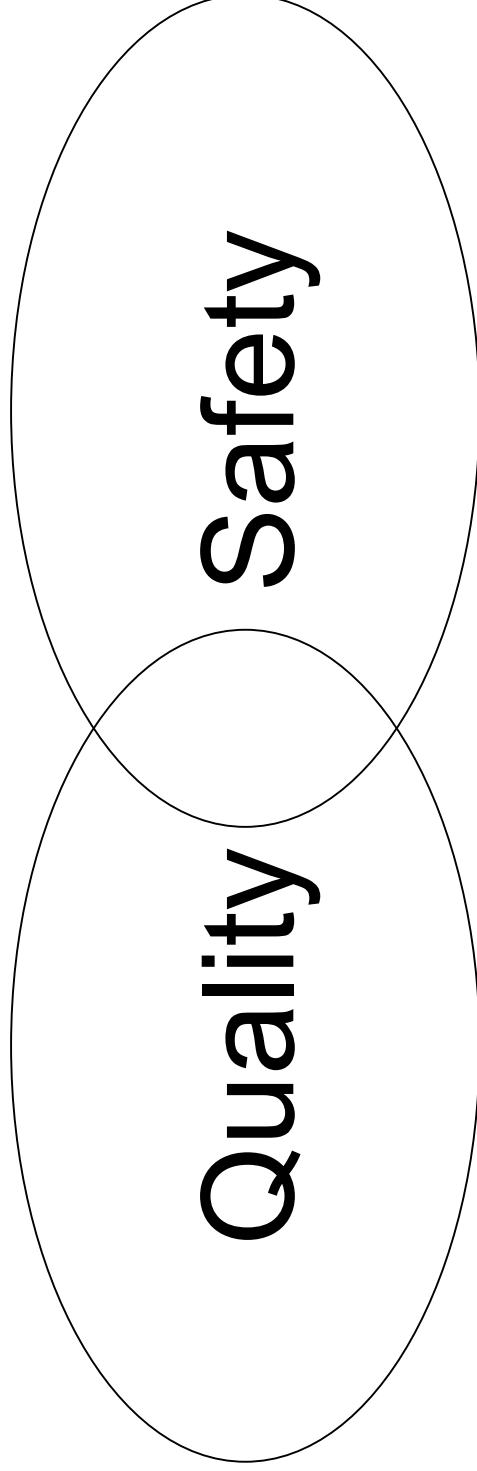


Subset of Quality?



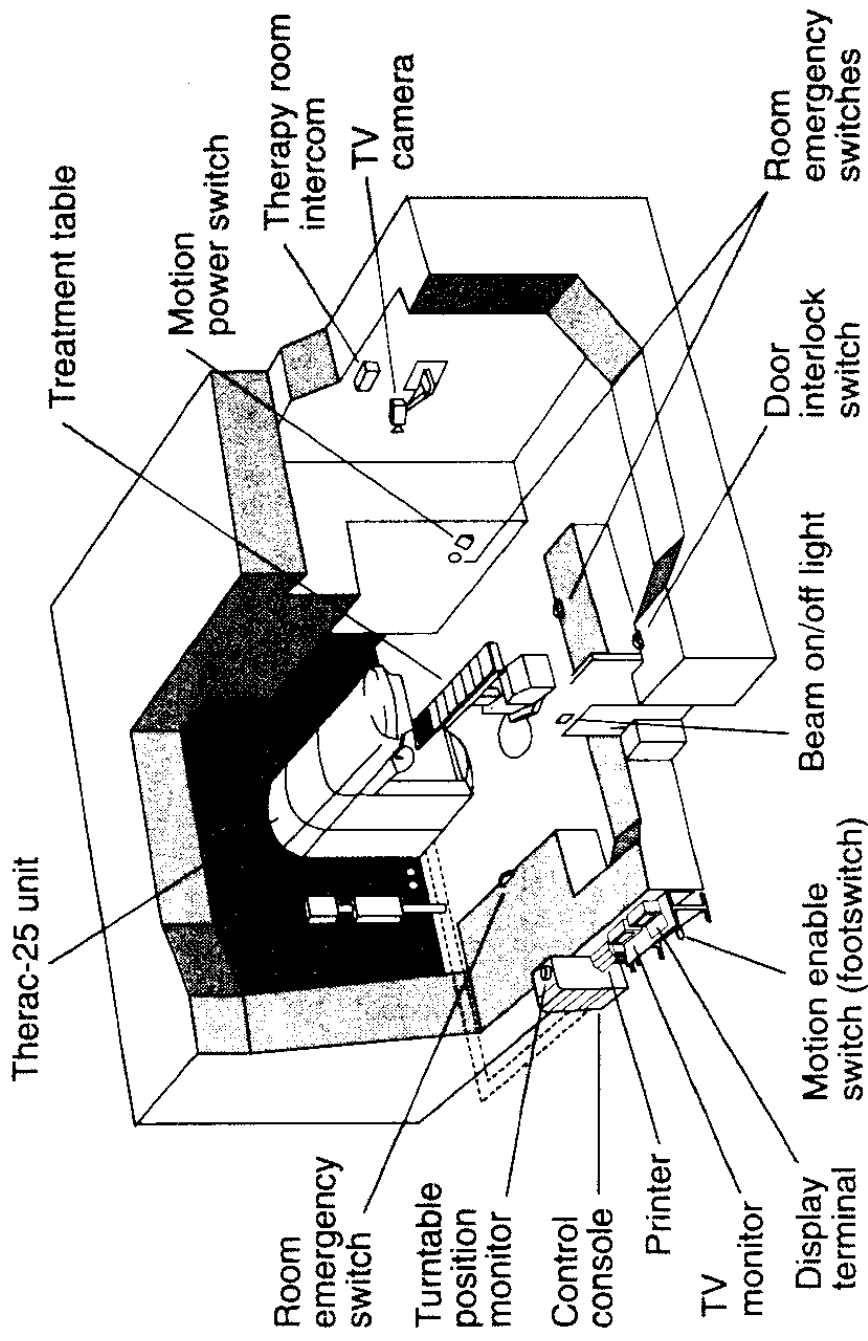


Overlapping?



Therac-25

June 1985 – January 1987



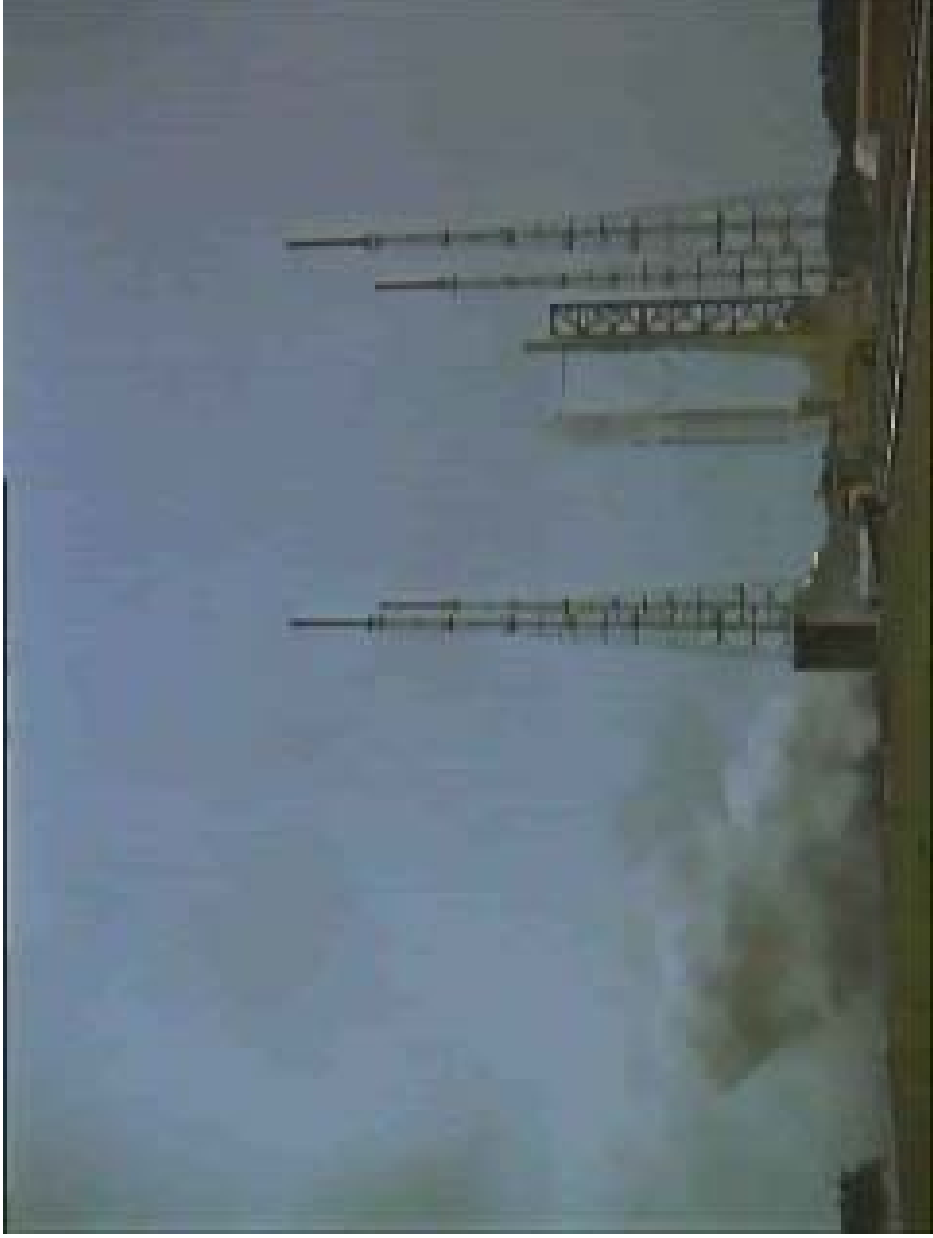
Therac-25

June 1985 – January 1987

- Massive overdose of radiation to 6 cancer patients
- 2 known defects: race condition and a logic error
- Defect #1 was very difficult to reproduce, even with knowledge of the defect
- Re-used S/W from earlier products, but without some of the independent safety mechanisms

Ariane 5

June 4, 1996



Ariane 5

June 4, 1996

- Integer overflow exception occurred in software inherited from earlier generation, Ariane 4
- Value was much higher than expected because the early part of the trajectory of Ariane 5 differs from that of Ariane 4 and results in considerably higher horizontal velocity values
- This inherited software was not needed for Ariane 5, and is only useful during pre-launch sequence; no useful purpose during flight

Panama

August - December 2000




Panama

August - December 2000

- Planning system requires that the spatial coordinates for shielding blocks used to protect healthy tissues during treatment be entered into the system in a specific manner
- Physicists changed their procedure and entered the coordinates of all blocks as a single block, which resulted in incorrect dose calculations and treatment time
- 28 patients affected, including at least 3 deaths

Ueberlingen, Germany, July 1 2002

1. Both aircraft at 36,000 feet
2. TCAS issues traffic warning 
3. 15 seconds later, TCAS issues resolution advisories to both crews:
 - “Climb, climb, now” => Tupolev
 - “Descend, descend, now” => DHL
4. 1 second later, Swiss controller told the Russian crew to "descend Flight Level 350 [35,000 feet], expedite, I have crossing traffic."
5. 14 seconds later, Swiss controller urges Russian crew to "descend Level 350, expedite descent."

Bashkirian Airlines
Tupolev TU-154 jet



DHL Transport
Boeing 757

Ueberlingen, Germany

July 1, 2002



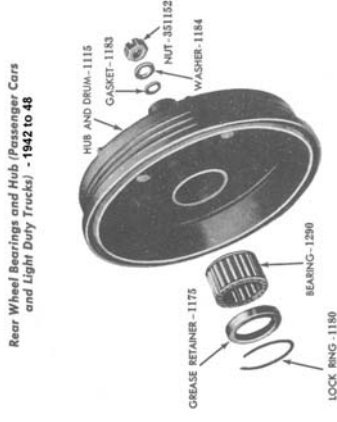


Definitions

- **Quality Assurance** - A planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures
- **Safety** – freedom from accidents, e.g., human harm, loss of property, environment damage

System Safety

- Traditionally, safety was often a matter of avoiding component failures.
- In turn, the avoidance of component failures was largely reduced to a problem of ensuring the quality of the components.





System Safety

- However, this traditional paradigm is less and less applicable as systems become increasingly complex and integrated





Differences

- Quality is an intrinsic property of a software system
- However, its safety inherently depends on the system context



Broad vs. Focused

- In general, quality assurance applies broadly to the entire system
- In contrast, the safety analysis of a complex system usually focuses on very specific details



Conflicting Objectives

- Some quality objectives may conflict with safety objectives, e.g., security, availability, real-time performance



Parallels In Health Care

“Quality improvement can enhance a patient’s experience with clinical care and improve patient outcomes, but does not necessarily protect against harm. This distinction is critical as too often the two are conflated, which serves neither very well. An important aspect of a learning culture is enabling staff to understand what the differences between quality of care and safety are, and to emphasize both at all clinical and other areas of service provision (food preparation, cleaning staff, etc). A clear message from senior management that quality and safety are distinct and that both are highly valued is critically important.”

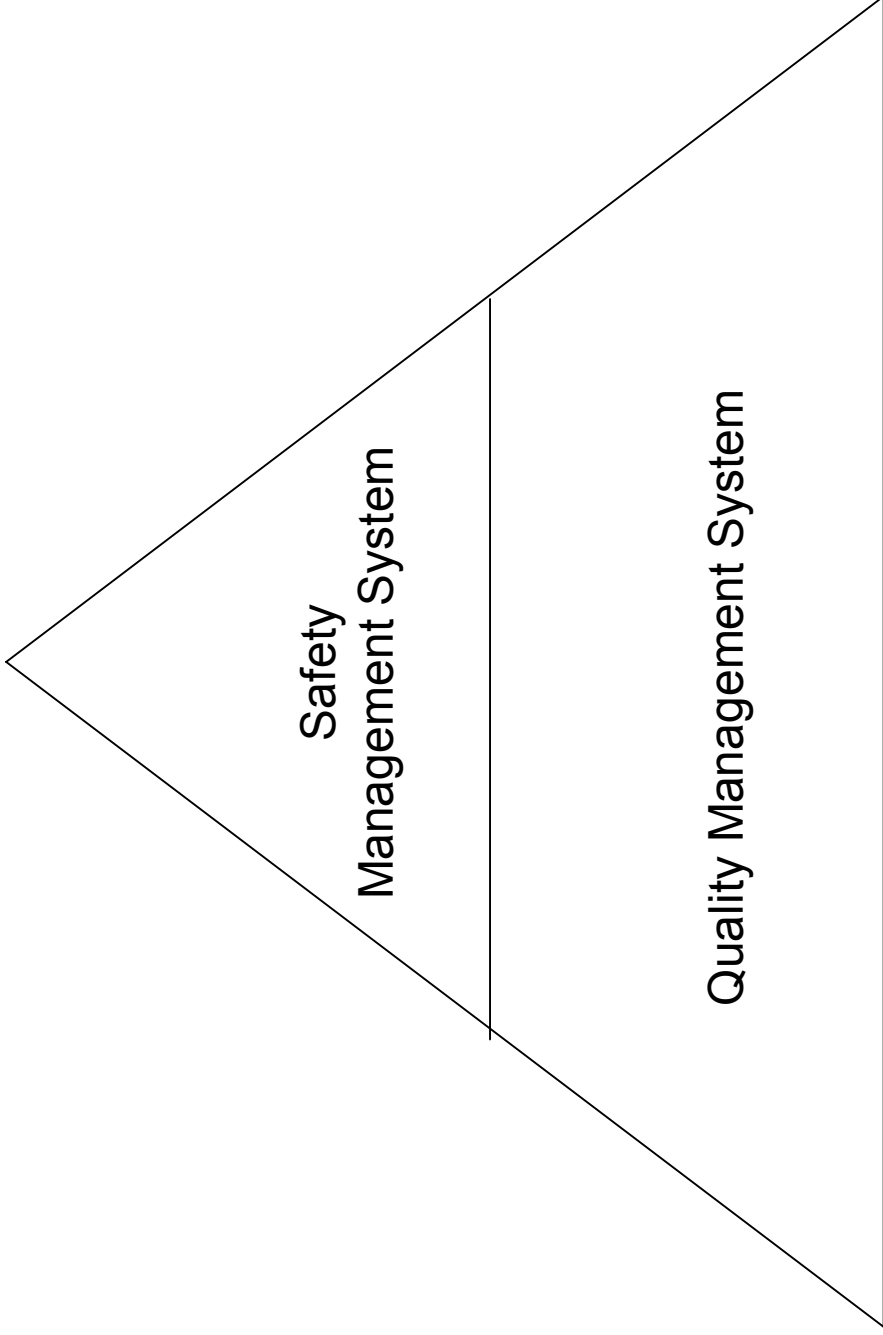
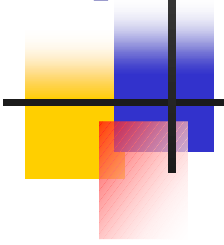
Governance for patient safety: Lessons from non-health risk-critical high-reliability industries , Samuel Sheps, MD, MSc, Karen Cardiff, BScN, MHSc



What More is Needed?

- Hazard Analysis
- Exploratory Hazard-driven Testing
- Traceability Analysis

Quality is a Foundation for Safety





Summary

- Quality and Safety are distinct properties
- Software-related accidents are not necessarily the result of quality problems
- Quality is a foundation for an effective approach to system safety