GRC EDUCATORS Online Training Hub
Axons Technology and Solutions

Webinar on

Identifying Usual 60% Missing Requirements in Specifications

Date : July 22, 2021

Areas Covered

- Good and bad specification examples
- Good team requirements, Active safety requirements,
  Reliability requirements, Installation requirements
- Safe defaults for sudden malfunctions,
  Output interface requirements,
  Serviceability/maintainability requirements
- Human interface requirements, Management participation requirements
- Logistics requirements (software changes, maintenance) & Input interface requirements,
- Engineering change requirements

GRC Online Training Hub EDUCATORS
Axons Technology and Solutions

In this webinar Process software causes problems that are familiar to anyone who has ever used a computer: bugs, crashes, and vulnerability to digital attacks.

PRESENTED BY:

Dev Raheja, MS, CSP, author of the books Design for Reliability", Preventing Medical Device Recalls, and Safer Hospital Care, is international risk management, reliability, durability, and system safety consultant for the government, commercial, and aerospace industry for over 30 years. His clients include Army, Navy, Air Force, NASA, Siemens, Eaton, Boeing, Lockheed, Northrup Grumman, General Motors.

GRC Online Training Hub EDUCATORS
Axons Technology and Solutions

Date : July 22, 2021

Time : 01: 00 PM EST

Duration : 90 Minutes

Price: $149

Webinar Description

Design reviews are supposed to identify all the requirements. The reviews must include three types of risks: the risk of the known, the risk of known unknowns, and the risk of unknown unknowns. But such analyses are often ignored or done too late. Developing good system specifications has become a worldwide goal, regardless of the industry and market. The best organizations around the world have become increasingly intent on harvesting the value proposition for competing globally while significantly lowering life cycle costs. This thinking provides guidance for the best specifications. Many companies attempt to make use of lessons learned, but most do not have formal and verifiable protocols. Some known risks can be identified through tools such as Failure Mode and Effects Analysis, Fault Tree Analysis, Operations & Support Hazard Analysis, and Event Tree Analysis. Some progress is being made in handling the known risks. The other two risks are significant, but there needs to have knowledge captured over the years. This webinar will cover what needs to be done.

GRC EDUCATORS
Online Training Hub
Axons Technology and Solutions

The “known-unknown” risks are unknown to the specification writers but are known to users of similar devices. The author, while working with the Baltimore Mass Transit System, could not come up with more than 200 requirements in the specification with the engineers. He interviewed train drivers, technicians, and passengers in San Francisco’s BART system, and discovered a list of over 1000 concerns. At least 500 of them were added to the Baltimore requirements.

The “unknown-unknowns” are special risks. They mostly apply to smart devices such as smart infusion pumps, MRIs, patient monitoring systems, and smart alarms that depend on trustworthy interoperability. The faults are usually unpredictable with the tools we have today. The reason is that the systems are too complex. No longer are we dealing with one mechanical system which can perform and stand alone. The software in a pacemaker may require over 80,000 lines of code, a drug-infusion pump 170,000 lines, and an MRI (magnetic-resonance imaging) scanner with more than 7million lines. This growing reliance on software causes problems that are familiar to anyone who has ever used a computer: bugs, crashes, and vulnerability to digital attacks. The key point is that we are dealing with a system made up of several systems. The software typically interacts with several systems, resulting in hundreds of possible interactions called system-of-systems. The interactions are unbounded. We cannot know how the system-of-systems will behave by knowing only the behavior of individual systems. Tweaking one system without the knowledge of inter-system behavior is doomed to failure. The unknown -unknown risks are the result of a lack of knowledge of the interactions and associated behavior of the system-of-systems. Altering the behavior of any part affects other parts and connecting systems.

Topic Background

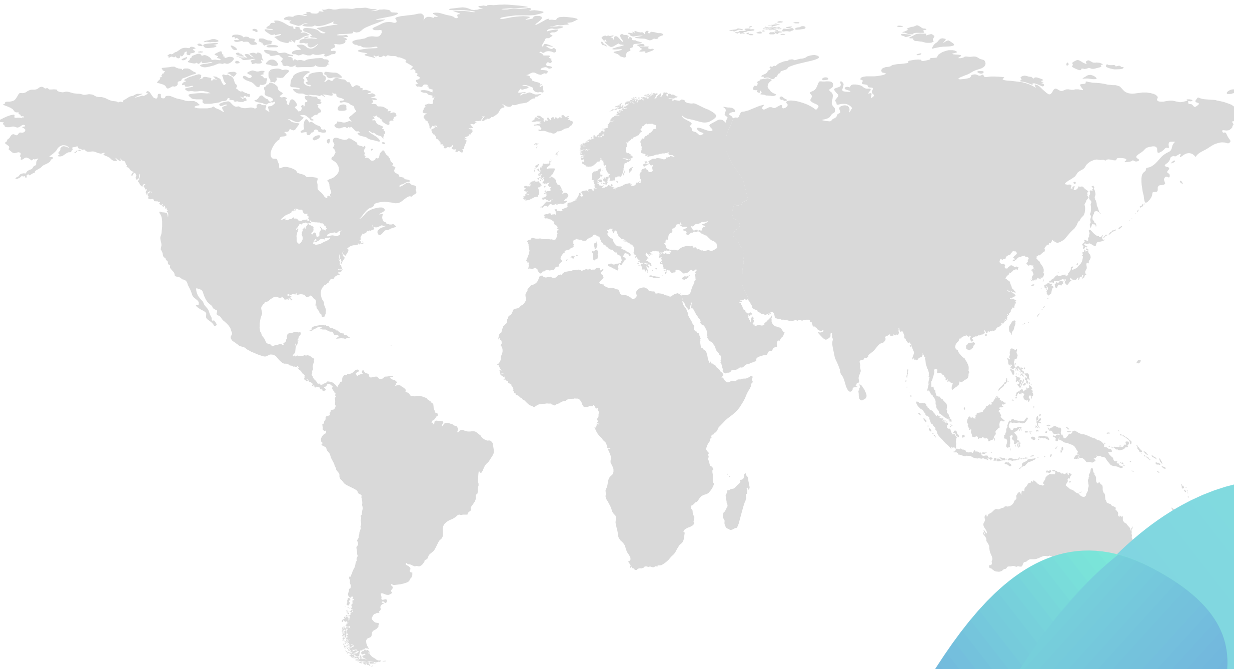
Usually, 60% of requirements are missing in most specifications. This creates unmanageable systems in real use. Architecture and “principled engineering practices” therefore become highly flawed. It affects a wide range of systems and services, with potentially life-threatening consequences. In other words, designs cannot be controlled. The device would accept unsigned, counterfeit software updates and ignore security.

Who Should Attend ?

- *Senior management*
- *Software managers and engineers*
- *Hardware managers and engineer*
- *System engineers*
- *Quality assurance staff*
- *Safety staff*
- *Security staff*
- *Marketing managers*

Why Should You Attend ?

Complexity control in most systems is a function of several systems working together to produce properties and behavior different than those of components. The disciplines of gathering such intelligence are often missing. This is one reason for many missing requirements. Most manufacturers have not applied rigors of hardware risk analysis to software designs. The same methods apply to software even though there are differences in software and hardware. Specification Requirements Analysis, PHA, FMEA, FTA, and HAZOP are great tools for controlling complexity. Approximately 80% of the dollars that go into system development are spent on finding and fixing failures. This is very inefficient. For a robust design, the opposite is required, that is, 80% of dollars should be spent on preventing failures so that the chance of mishaps are dramatically reduced.



GRC EDUCATORS Online Training Hub
Axons Technology and Solutions

To register please visit:

www.grceducators.com
support@grceducators.com
740 870 0321