ADELARD

Achieving Safety and Security: Integrating Engineering within Assurance Cases

Session TH35 "Safety Assurance in Digital Safety Systems"

Sofia Guerra
12 March 2015

PT/294/309/34

Exmouth House 3–11 Pine Street London EC1R 0JH
T +44 20 7832 5850 F +44 20 7832 5853 E office@adelard.com W www.adelard.com

Outline

- Safety principles – why?
- Engineering the safety demonstration
  - Hazard analysis
  - How to consider security?
- Structured assurance cases
  - Communicating and reasoning

IAEA SF-1

2. SAFETY OBJECTIVE

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.

Hazard analysis

- Hazard analysis one of the most important and challenging tasks
- Review of case studies indicate that identifying 85-86% hazards early in a project is reasonable
  - Importance of derived requirements during development
- Efficiency of hazard analysis depends on several factors, including
  - Complexity of the system
  - Competence
  - Effort
  - Technique used

If it's not secure, it's not safe

- Our primary goal is to show that a system is safe:
  - If the system is not secure, it is not safe
- What impact does security have on the safety of a nuclear safety system?

German Steel Mill Cyber Attack

- Phishing email to gain access to the corporate network and then into the plant network
- "Highly likely that the email contained a document such as a PDF that when opened executed malicious code on the computer"
- Steel Mill lost control of its blast furnace

Systems that were known to have been impacted:

- Individual control system components
- Furnace (uncertain on type based on translated report)

Components that were also possibly impacted given the scenario:

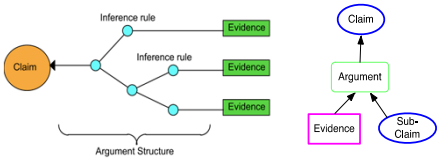
- Centralized controls based on a Programmable Logic Controller (PLC)
- Alarm systems
- Safety Instrumented Systems (SIS)
- Human Machine Interface (HMI)
- The individual control system functions could have been one or more:[3]
  - Burden control
  - Burden distribution
  - Mass and energy balances
  - Kinetic process models
  - Hot-blast system

ICS Defense Use Case (DUC) Dec 30, 2014

Vulnerabilities and hazards

- Vulnerabilities taken into account from both safety and security perspective
  - System vulnerabilities are sources of hazards
  - Credible exploit of vulnerabilities very different from safety perspective
- Similar hazard analysis techniques may be used, but with different interpretations
  - Hazops useful technique
  - Guidewords –"other than" for security

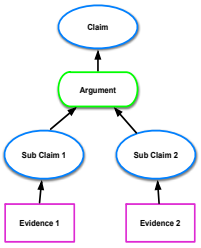
Structured Assurance Case – Claims, Argument, Evidence



- "a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment"

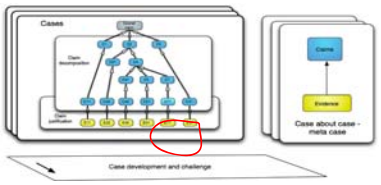
Examples of claims

- Claim are assertions put forward for general acceptance, usually a proposition about a property of the system, e.g.,
  - functions (shut down when T> 500)
  - invariants (water level in reactor pressure vessel always between A and B)



Evidence

- Basis of the justification of the claim
- Sources may include
  - Prior operational data
  - Testing
  - Results of verification



Arguments differ in strength

- Stronger - Deterministic or analytical application of predetermined rules to derive a true/false claim, e.g. formal proof (compliance to specification, safety property), execution time analysis, exhaustive test, single fault criterion
- Weaker - Qualitative compliance with prescriptions indirectly related to the desired attributes, e.g. compliance with QMS and safety standards, staff skills and experience

Making arguments explicit a key idea
Separating evidence from information

Communication and reasoning

- Structured assurance case has two roles:
  - communication is an essential function of the case
    - boundary objects that record the shared understanding between the different stakeholders
  - a method for reasoning about safety-security
- Both are required for assurance of safety-security

Summary

- Important to understand systems –compliance with standards is not enough
  - Specially important for software and COTS
- Assurance cases as a way to support
  - Understanding
  - Reasoning
  - Communication