ADVANCED REACTOR SAFEGUARDS & SECURITY

Security-Inclusive MBSE Tools for Nuclear Reactor Development

PRESENTED BY

Joseph Mahanes

April 30, 2024

INL/CON-24-77646

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

Outline

NOTE: Early phase research with schedule impacted by CR

This presentation assumes familiarity with MBSE

- Nuclear industry questionnaire results
- Identified gaps (from digital I&C perspective)
- Why does this matter?
- Planned R&D approach

Understanding the Current Landscape

- 5 of 9 reactor vendors and digital I&C vendors responded
- 3 of 5 responders used MBSE (it was too soon for the others)
- No standard MBSE methodology is used
- Reactor vendors modeled the entire generic NPP
  - Each plant site will have a separate instance based on generic model.
- Multiple disciplines are incorporated (e.g., nuclear, mechanical, I&C engineering, regulatory compliance, safety, etc.)
  - Both automatic & manual requirements generation and MBSE input are used
  - Various modeling & simulation tools are integrated
  - Functionality, safety, and performance are considered in the methodology

Gaps in MBSE Implementations for Digital I&C

- Risk management is typically NOT included in MBSE
  - Non-adversarial risks are evaluated using various methods (e.g., PRA, SPAR-H, STPA, FMEA, various testing, etc.) but not integrated into MBSE
  - Only one vendor evaluates cyber risk using NEI, NIST, and EPRI guidance
- Currently ZERO vendors polled integrate digital I&C risk or cybersecurity evaluations into their existing MBSE methodology
  - Some vendors are planning to integrate; others are not
  - One vendor would like to integrate, but does not know how

Why include Digital I&C Risk & Security into MBSE?

- What is digital I&C risk?

  Adversarial and non-adversarial threats that exploit a vulnerability on a digital system or asset that adversely impacts a <critical> function and <successfully> results in an adverse consequence.

  – Adversarial threat: Cyber-attack
  – Non-adversarial threat: human performance error, equipment degradation/failure, environmental exposure

It is not just Cyber-Informed Engineering (CIE) and Security-by-Design

IT IS ALSO

Ensuring our single authoritative truth in MBSE includes ALL digital I&C risks and risk treatments

Why include Digital I&C Risk & Security into MBSE?

- We have design requirements digital I&C used for safety functions:
  - Diversity, redundancy, independence, separation, and reliability
  - Forward & backward traceability of requirements
  - Verification and validation requirements

- Document and reconcile discrepancies with requirements and continuously evaluate risk throughout lifecycle
  - Will a safety requirement create a vulnerability in a digital asset?
  - Will physical controls for a digital asset impact construction?
  - If cannot eliminate or mitigate risk, is the residual risk understood and accepted?

We need to stop throwing the ball over the wall!

How to integrate? Path Forward…

- MBSE tools are designed to allow inclusion of any requirement
- We need to demonstrate use cases for integrating digital risk and cybersecurity into an MBSE toolchain
- Preferences:
  - Open-source tools
  - Initial focus on early systems engineering lifecycle phases
  - Short term integration of requirements, documentation, P&IDs, risk analysis
  - Longer term integration of digital twins, validation & verification, product lifecycle management, CAD, physical security, et al.

Open-Source MBSE Tool Options (1)

- MBSE
  - Eclipse Papyrus (UML, SysML)
  - Gaphor (UML, SysML)
  - Eclipse Capella (Arcadia method)
  - Innoslate (not open-source, but INL is using it)
- Separate requirements engineering tool?
  - NASA FRET (Formal Requirements Elicitation Tool)
  - Eclipse: ProR (for ReqIF files)
  - IBM Rational DOORS (not open-source, but INL is using it); also PTC Integrity
- Document creation
  - Sphinx; included also as an extension in Gaphor
  - Model2doc (for Papyrus)
- Data warehouse
  - DeepLynx

Open-Source MBSE Tool Options (2)

- Digital Twin / Simulators
  - OpenModelica (or Modelica)
  - Matlab/Simulink
- Risk analysis
  - RAAML (risk analysis and assessment modeling language standard) is partially implemented in Gaphor
  - Eclipse Safety Framework is an additional safety tool
  - STPA or HAZOP integration
  - Raven + RELAP5D (can be linked to SysML) but these don’t really include security

BUT… will first use tools INL has in-house

- Innoslate
- IBM Rational DOORS
- Additional tools TBD

Initial Case Study Options

- NRC/Galois Reactor Trip System (https://github.com/GaloisInc/HARDENS/tree/develop)
- Existing INL nuclear reactor projects?
  - MARVEL
  - MAGNET
  - Other?
- New homegrown system/SoS

QUESTIONS?