Recent and Ongoing Collaborations on Risk Informed Assessment of Digital I&C systems: VCU and LWRS

Dr. Carl Elks

Associate Professor of ECE
Virginia Commonwealth University
Department of ECE
Richmond VA
crelks@vcu.edu
The Dependable Cyber Physical Systems Lab at VCU

- The VCU Dependable Cyber-Physical Systems (DeCyPS) Lab focuses on the research, design, and verification of highly reliable and secure Cyber-Physical Computing Systems.
- [https://rampages.us/elks-decyps/](https://rampages.us/elks-decyps/)
- Focus on Innovative solutions toward ensuring systems safety and security
- Our lab has a strong focus on experimental methods and practices, that are applied to real-world systems.

(DeCyPS) Lab

- Autonomous Systems
- NASA - Urban Air Mobility Safety Systems
- Medical Devices and Systems
- Nuclear Safety Systems

Model Based Safety Assurance
• LWRS - Nuclear Power Plant Modernization via digital I&C upgrading - one of the more critical activities for US nuclear energy.

• Historically, safety system upgrades exceedingly expensive¹.
  – Regulatory – delays caused by regulatory issues that have to be resolved.
  – Verification and Testing - The “unexpected” costs for V&V, certification, and licensing.

• If large scale NPP modernization is the future, we need a scalable and systematic approaches to digital I&C automation upgrading.

• How do we move from regulatory driven design to risk informed approaches where cost uncertainty is bounded (useful = tight bounds).

The Challenge of Cost Effective Safety Critical DI&C

- Testing, V&V of critical systems is costly and trending more expensive.
  - Happening across multiple sectors - Nuclear, Aerospace, Medical, Defense.
  - Nuclear is lagging, most vulnerable, but also could learn from other sectors.
  - Installed cost is trending toward the 10:1 ratio in safety critical systems.
  - The uncertainty of cost is what kills projects.

- Why?
- Partly due to:
  - Design and testing of safety systems is an additive cost to begin with
  - Utility and regulatory-entity interactions (inefficient and poor scalability)
  - **Systems and technology becoming more complex.** Complexity that manifests in systems without full awareness of it = uncertainty.
  - All together these are contributing factors to cost burden.

---


---

VCU College of Engineering
What are we doing about it and what are others doing?

- **Systems Engineering and Risk Informed Assessment** – Basic Idea, You can’t assess high coupled safety and security problems in isolation. Must have a inclusive or systems interaction perspective so tradeoffs and decision can be assessed in terms of hazards and consequences. New methods and tools are enabling accessibility.

- **Highly Systematic and Integrative Methodologies**
  - VCU: Complexity Awareness Design
  - EPRI: DEG, HAZCADs, TAM
  - INL: Platform for Risk Assessment of Digital I&C systems (PRADIC)
  - General: Model Based Safety and Design Assurance, STAMP, STPA, Accessible Formal Methods.

- **Dependable DevOps** – Current Practice: “assurance of safety and security” is mostly a design time activity.
  - Emerging new practice: Methods where a continuum exists between design-time and run-time assurance creating a shared responsibility for reducing the risk.
    - Gaining wide acceptance in aerospace and automotive.
  - Do any of these have the potential to reduce cost?
  - Yes, and some have proven to reduce LC costs in other domains – e.g., Systems Engineering, Risk Informed, Model based Design Engineering and Testing.
• All well-formed “Systematic” and “Risk Informed” methodologies follow the conceptual model to the right.

• Evidence = credible, defensible data or information to support(refute) a claim.

• Standards or Regulations help “guide” repeatable objective quality (safety, security, reliability, etc.)
  • By demonstrating that sufficient checks have been made along the way
  • By having supporting evidence to show that due diligence has been achieved.

Processes like PRADIC, HAZCAD, etc., are strategies that produce “evidence” wrt risk informed decisions.

Different processes produce different evidence, but all processes should comply to the “triangle” concept.

Adapted from Sofia Guerra, Real-life experiences with “reasoning-structure safety assurance” Halden-NRC presentation March, 2017.
Value Proposition for LWRS-PRADIC

- **Platform for Risk Assessment of Digital I&C systems (PRADIC)** aims to provide a modularized platform for I&C designers, software developers, plant engineers, and risk analysts to efficiently predict and prevent risk by:
  - Identifying all potential crucial failure modes (including CCFs) and system vulnerabilities
  - Effectively quantifying the reliability of digital I&C systems with the identified digital failures
  - Evaluating the impact of consequences of digital failures on the plant responses.

We need methods that indicate good designs or inform a design before using PRADIC. Poor design = no cost saving. Much work needed here... Complexity Aware design is a first step.
VCU Project 1: A Pseudo Exhaustive Software Testing Framework for Embedded Digital Devices in Nuclear Power


- **Background**: Smart Embedded Digital Devices are expected to be an important part of I&C upgrading for safety functions (RPS, ESFAS).
  
  - Example: Smart Sensors capable of auto-calibration, onboard diagnostics, health monitoring and digitally connecting to the control room.

- Commercial Safety Grade devices have varying degrees of SW complexity (footprints). But not much known about them due to proprietary IP protections.

- **Research Proposition and value**: Can we adapt advanced SW testing methods from the aerospace and process control community to address SW testability concerns wrt Nuclear Regulatory guidelines - BTP 7-19?

  - 1.5 year effort, sprint to get data and determine efficacy.
Real-time DI&C Software

- Most EDD are **real time** or **in-time** (demand systems) systems.
- RT systems follow the **reactive** computational model – Correctness is a function of value and time.
- Together, both of these “temporal” abstractions can create complex interactions and orderings that are difficult test and verify.
  - Bohrbugs - A deterministic manifestation that is repeatable.
  - Heisenbugs - Anomalies that seem to disappear or alter their behavior when investigated.
  - Mandelbugs - Underlying causes of an anomaly are so complex and obscure that the anomaly appears to be nondeterministic.
- For all of these reasons, it’s important to test on the actual device!!
Embedded Target: VCU Smart Sensor

- Barometric pressure and temperature sensing device
- Derived from UAV autopilot developed at VCU
- Uses a lightweight RTOS
- Very typical RT processing software stack
- STM32F4 uC ARM Cortex based architecture

| Flash Usage | 102 KB |
| RAM Usage | 81 KB |
| Serial Modem Thread | Barometer Thread | Communication Thread |
| Cyclomatic Complexity | 102 | 33 | 101 |
| Thread Priority | 2 | 4 | 3 |
| Allocated Stack size | 256 | 256 | 2048 |

Academic and Industry Impact of LWRS-VCU Collaboration

• **Goal of ORCAS along with the overall PRADIC:** Demonstrate highly systematic design assurance methods (like pseudo exhaustive SW testing and others) can be coupled to graded assessment approaches to address the issues below. DI&C software CCF events can be potentially identified and quantified to help with mitigation/resiliency strategies.

1. **Lack of industry consensus on effective software testing for single and CCF elimination**
   a). Existing guidance suggest 100% exhaustive testing as requirement to screen against CCF

```
<table>
<thead>
<tr>
<th>Category</th>
<th>Method Name and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eliminate</td>
<td>Internal Diversity</td>
</tr>
<tr>
<td></td>
<td>If sufficient diversity exists within the protection system, then vulnerabilities to Common Cause Failure (CCF) can be considered to be appropriately addressed without further action.</td>
</tr>
<tr>
<td></td>
<td>Simple Design</td>
</tr>
<tr>
<td></td>
<td>A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case.</td>
</tr>
</tbody>
</table>
```

Table. Recommended screening approaches for reliability in DI&C systems [SRM-SECY-93-87]

b). 100% testability is for all practicable purposes impossible to achieve for SW based systems. Industry has indicated 100% testability criteria, [that] “the lack of a graded approach based on safety significance places a high burden for demonstrating that adequate digital I&C system development processes have been employed - especially for systems containing localized embedded digital I&C components”…. [SECY-16-0070]

2. **Identification and quantification of failure events is difficult in complex DI&C systems**
   a). Requirement for “applicants and licenses (1) identify potential hazards unique to the specific DI&C technology and associated impacts to the intended safety functions and (2) evaluate the ability of the design to sufficiently perform its intended safety functions assuming a CCF in the DI&C system.” [SECY-18-0090]
Pseudo Exhaustive Testing Methodology

- Think IEC 61508 SIL 3 and 4 or DO-178c – REALLY rigourous testing requirements
- Our test methodology follows White box testing principles
- Bounded Exhaustive test methodology is organized around the following well-accepted methods:
  - Equivalence Partitioning
  - Boundary Value Analysis
  - T-way combinatorial testing
  - Structural Path Analysis
  - Function Interaction Verification
- These methods when used systematically reduce the testable state space while preserving the interaction relations of the original software.

Hierarchical Test Strategy
- Unit testing: Tests the T-way software parameter or variable interactions.
- Integration Testing: Tests the Function Interactions
- System Testing: Tests the SW Thread Interactions
Big Picture of VCU and LWRS Collaboration

VCU Conducted Experiments on Pseudo Exhaustive Testing approach - Failure Data of VCU Smart Sensor

Natural and extendable Collaboration

- Feedback on Testing Evidence Completeness and Sufficiency
- Better scenario and system level coverage

PRADIC-ORCAS Methodology requires SW defect or failure data from testing/operation

Provide experiment results, documentation, and testing to ORCAS
The variables values from equivalence partitioning and BVA varies from variable to variable, but the average is around 5 values/variable.

The time to execute tests was reasonable for real time testing on a physical device – about 1 test was executed, checked and saved every 400ms.

The automated testing efficiency was ~150K tests/day.
ORCAS Assessment Results (how VCU/software system designers can make benefits from PRADIC-ORCAS?)

Demonstration on VCU smart sensor software and device yielded:

- Areas of testing deficiency via qualitative metrics derived from the requirements traceability matrix and trigger coverage assessment
  - NIST T-way combinatorial testing used to emulate exhaustive testing but PRADIC-ORCAS demonstrates wholistic software defect triggers must be considered for comprehensive considerations

<table>
<thead>
<tr>
<th>Level of Testing</th>
<th>Defect Trigger conditions required for test comprehension</th>
<th>Implemented method by VCU Team</th>
<th>Qualitative Completion Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Startup/Restart</td>
<td>Missing</td>
<td>Indirect</td>
<td>0.5/1</td>
</tr>
<tr>
<td>Configuration Workload/Stress</td>
<td>Missing</td>
<td>Missing</td>
<td>0/2</td>
</tr>
</tbody>
</table>

Table. Abridged trigger coverage assessment matrix indicating areas of inadequate testing

- Identification and quantification of software failure modes in VCU’s digital instrumentation sensor system using proven industry quality assurance metrics and methods
  - Previously, software on peripheral non-control systems was not assessed, PRADIC-ORCAS changes that paradigm and allows fault tree tracing of all types software systems with quantification
Potential collaborations in FY-23

- Digital/software CCF modeling and analysis;
- Integration of PRADIC and VCU-SymPLE design method to optimize the design process of digital/software safety systems;
- Further methodology improvement and demonstration of ORCAS based on VCU facility and data.
Thank you!