Critical Issues and Lessons Learned in the Deployment of FPGA Based Systems in NPPs

Steven Arndt

U.S. Nuclear Regulatory Commission

12th International Workshop on Application of Field Programable Gate Arrays in NPPs

14 October, 2019

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Outline

- Background
- Significant Issues
- Licensing Process
- Licensing Challenges
- Lessons Learned
- Questions

Background

- Much has been accomplished in recent years
  - Twelve annual FPGA workshops
  - Publication of IEC standards
  - Publications of EPRI guides
  - Publication of International guides
    - IAEA NP-T-3.17
    - MDEP DICWG-5
- Development of nuclear specific vendor base
- Acceptance of many FPGA-based platforms for use in NPPs

Licensing and Topical Reports in the US that included FPGAs or CPLDs

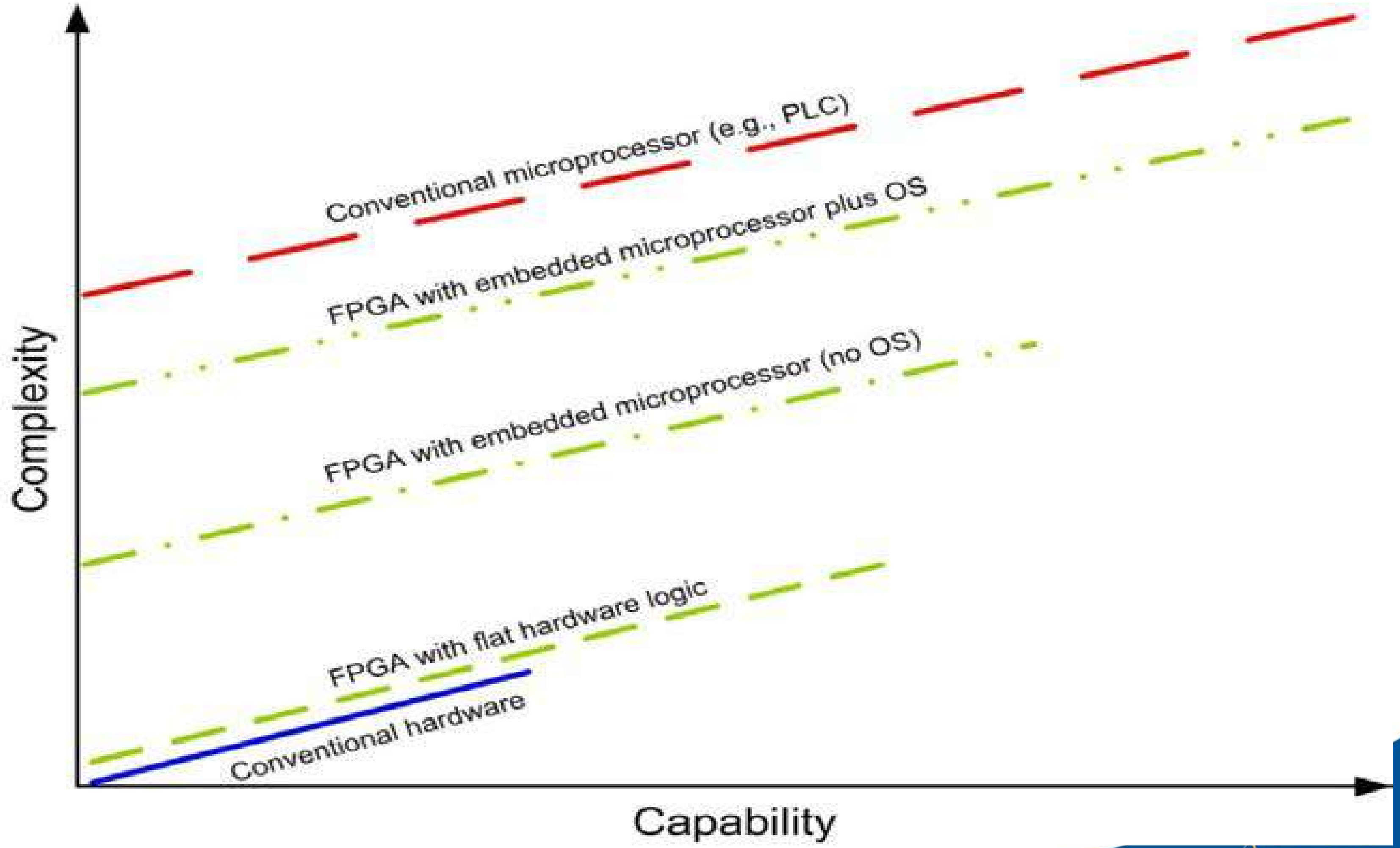
- Westinghouse - ALS Platform
- Westinghouse - SSPS
- Lockheed Martin - NuPAC platform
- NuScale - HIPS
- Radiy - RadIC platform
- Toshiba Power Range Monitoring (in review)

Significant Issues

- Lack of understanding of the key advantages of the technology
  - FPGAs (and CPLDs) can be designed to simplify safety demonstration
  - More resistant to cybersecurity issues
  - FPGAs appear to be more resilient to hardware obsolescence due to portability of HDL to new chips
  - Hardware based fault detection and isolation

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Significant Issues



Significant Issues

- Limitation of the standards and guidelines
  - Although this is quickly becoming a non-issue, new guidelines are slow to be implemented
  - Many systems not developed to nuclear standards
- Less access to internal signals for monitoring, testing and analysis/troubleshooting
- Understanding that tools are a critical part of the safety case/demonstration
  - Insufficient understanding of roles of software tools
- Insufficient guidance for FPGA use in embedded digital technologies including smart devices

Licensing Process

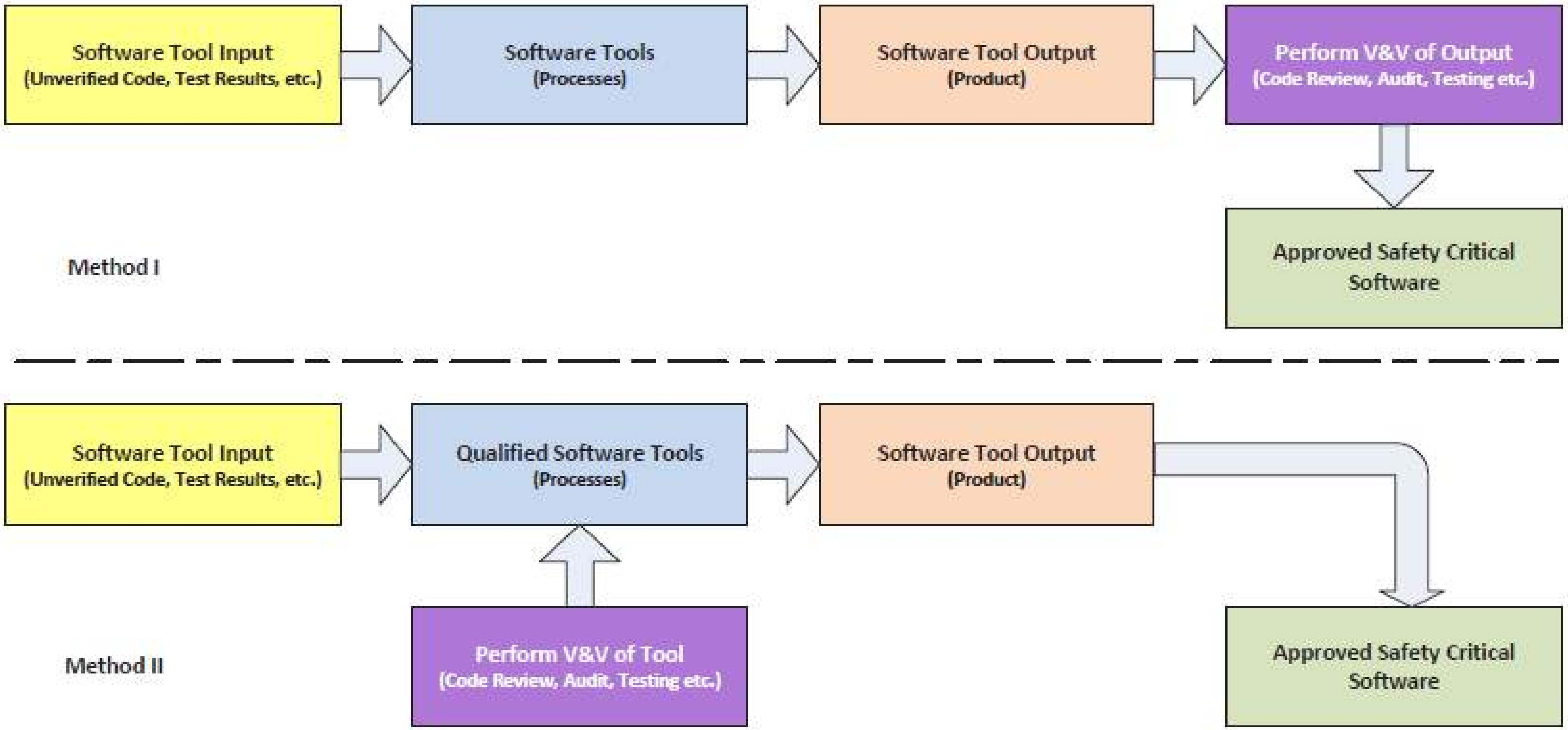
- There are several different general methods for review and approval of FPGA-based systems
  - RG 1.152 (IEEE 7-4.3.2) and RG 1.168 (IEEE 1012) based reviews
  - IEC 62566 and IEC 62566-2 based reviews
  - Other review processes (including the use of Formal Methods)
- Key differences in these approaches include
  - Life cycle requirements including verification and validation
  - Level of detail in requirements
  - Credit for testing and fault tolerance features

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Licensing Challenges

- Evaluating predeveloped blocks (PDBs) or IP cores can be frequently challenging
  - Information from vendors not always available
  - Commercial qualification no always available
- Testing completeness
- Software tools
  - Configuration control of tools
  - Validation of tools
  - Documentation

Licensing Challenges



Two possible methods that the NRC considers to be acceptable for approval of tools. V&V — verification and validation

Lessons Learned

- Common Cause Failure
  - Most regulators required protection from CCF for digital safety systems
  - FPGA-based systems provide opportunities to address CCF
    - Use of FPGA technology as a diverse actuation systems (DAS)
    - Use of FPGA and CPLD as devise from each other
    - Use of different vendors or different tools to make FPGAs diverse from each other

Lessons Learned

- Examples of FPGA-based methods used to address CCF
  - Two channels of computer based processors coupled with two other channels of diverse FPGAs with common requirements
  - Two diverse FPGA chip technologies with common requirements
  - Single FPGA to implement the required safety functions with diverse CPLD device to monitor and identify FPGA faults
- Other FPGA-based methods that are used to address CCF include extensive testing and analysis

FPGAs (and CPLD) based systems provide an alternative for addressing CCF concerns

Lessons Learned

- NRC has conducted a number of reviews of FPGA based systems using IEEE 1012
  - SIL Level - Graded Approach to V&V
  - Software Criticality Emphasis
  - Hardware and System Processes Introduced in Later Revisions
- NRC has had adapted software tasks to FPGA equivalent tasks
  - HDL Code = Software Instructions / code
  - Development Tool / Environment is software based and is similar
  - Audit / CM / Test Coverage / Traceability / Criticality / Risk / Hazard analyses Tasks, etc.
- IEC 62566 may be a better choice for FPGAs in the new revision of NRC regulatory guidance

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Conclusion

- Various vendors and regulators are quickly getting to the point where they can and do treat FPGA-based systems as routine
- Although some issues remain, vendors and regulators have accepted FPGA-based systems, to address CCF issues
- Updating guidance and experience are the largest remaining challenges

Questions ?

United States Nuclear Regulatory Commission

Protecting People and the Environment