U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Regulatory Guidance on the Use of Field Programmable Gate Arrays in the U.S.

October 13, 2015

Steven A. Arndt, Ph.D., P.E.
Office of Nuclear Reactor Regulation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

The views expressed in this presentation are solely those of the author and do not necessarily represent those of the U.S. Nuclear Regulatory Commission.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Agenda

- Introduction
- Key Technical Challenges
- Key Regulatory issues
- Experience in the U.S.
- Future Efforts
- Conclusions

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NRC Mission

License and regulate the Nation's civilian use of source, byproduct, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Introduction

- Increase their use of FPGAs and CPLDs in both safety and non-safety applications in the U.S.
- New digital platforms manufactures that have requested reviews by the NRC
- At the same time there have been several examples of the use of FPGA's and CPLDs being used in nuclear power plants in the U.S. without prior review
- This situation has resulted in a number of efforts within the U.S. to improve technical guidance on the use of these devices

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Introduction

- Internationally the use of FPGAs and CPLD is also increasing
- IAEA has held eight workshop on the applicatio n FPGAs in NPPs, most recently in Shanghai, China in October 2015
- 19 countries attend the workshop, including utilities, regulatory bodies, equipment vendors, and technical support organizations
- As a result of these efforts additional guidance will soon be available from IAEA on the development and use of these devices

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Introduction

- It has become apparent that even with the current information (EPRI documents, IAEA document, IEC standard) that is available more regulatory guidance in the U.S. is needed
- Current U.S. guidance for FPGAs is to use general safety system requirements that do not specially address the unique aspects of FPGAs

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Key Technical Challenges

- Even the definition of what FPGAs and CPLDs are is not particular well established
- Lack of consistency in design with established practices
- Lack of consistency in current NRC regulations and guidance with national and international standards
- Diversity (FPGA-FPGA, FPGA-microprocessor) requirements for systems with FPGA not well defined
- Cyber security

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Key Technical Challenges

- Similarity to software
  - Robust design practices
  - independent verification and validation efforts
- Differences from PLCs and similar devices
  - Complex support functions that have not been specifically developed for nuclear power plant applications
- Complexity of the device (e.g., number of gates, number of inputs/outputs, device-specific features, etc.) can be an issue

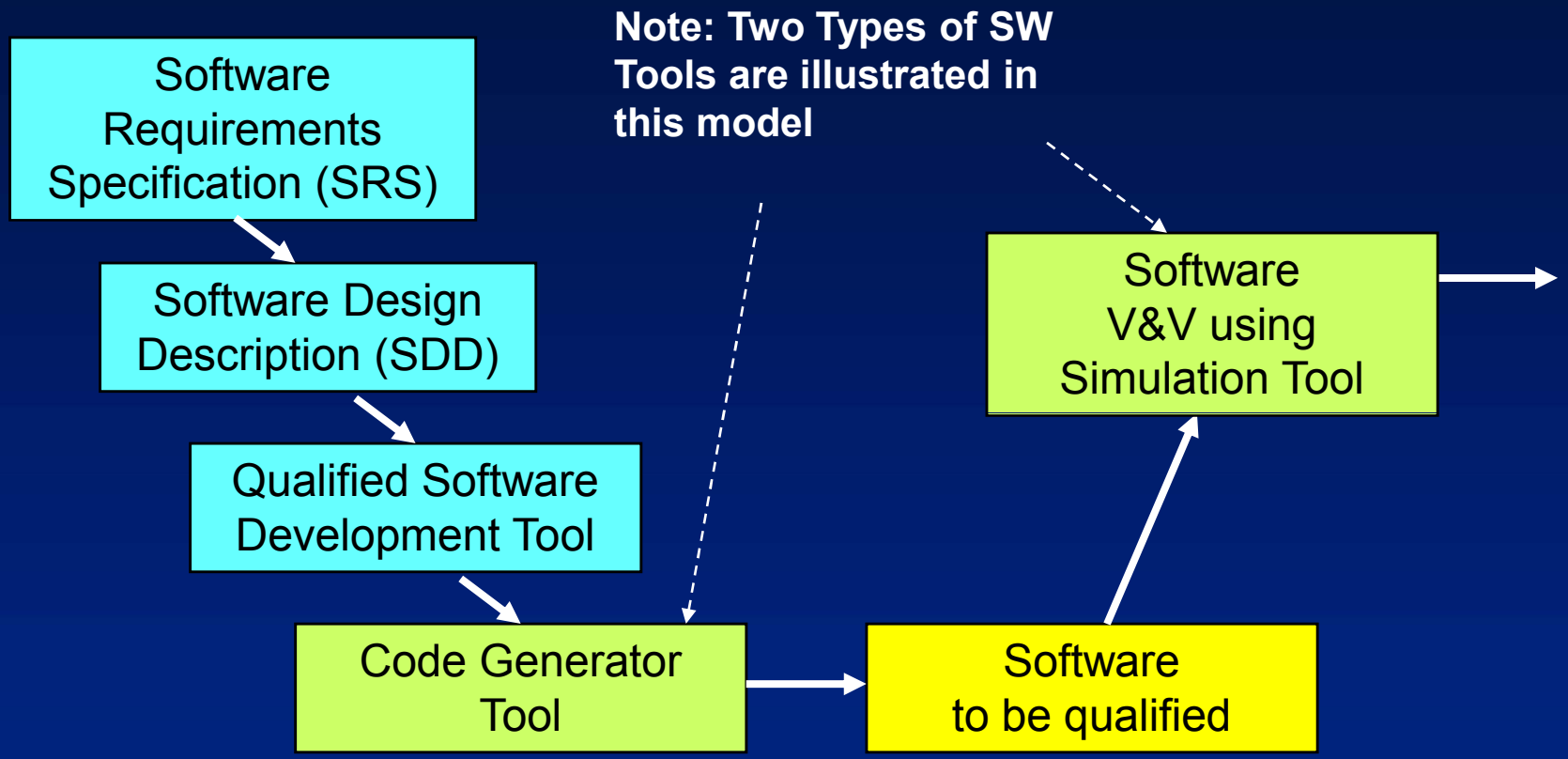
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Key Regulatory Issues

- Qualification of Tools
- Currently done using requirements in IEEE 7-4.3.2 section 5.3.2 “Software Tools
  - Tool usage for V&V activities
  - Qualification requirements for Tool itself
  - Degree of V&V required for output of tool

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

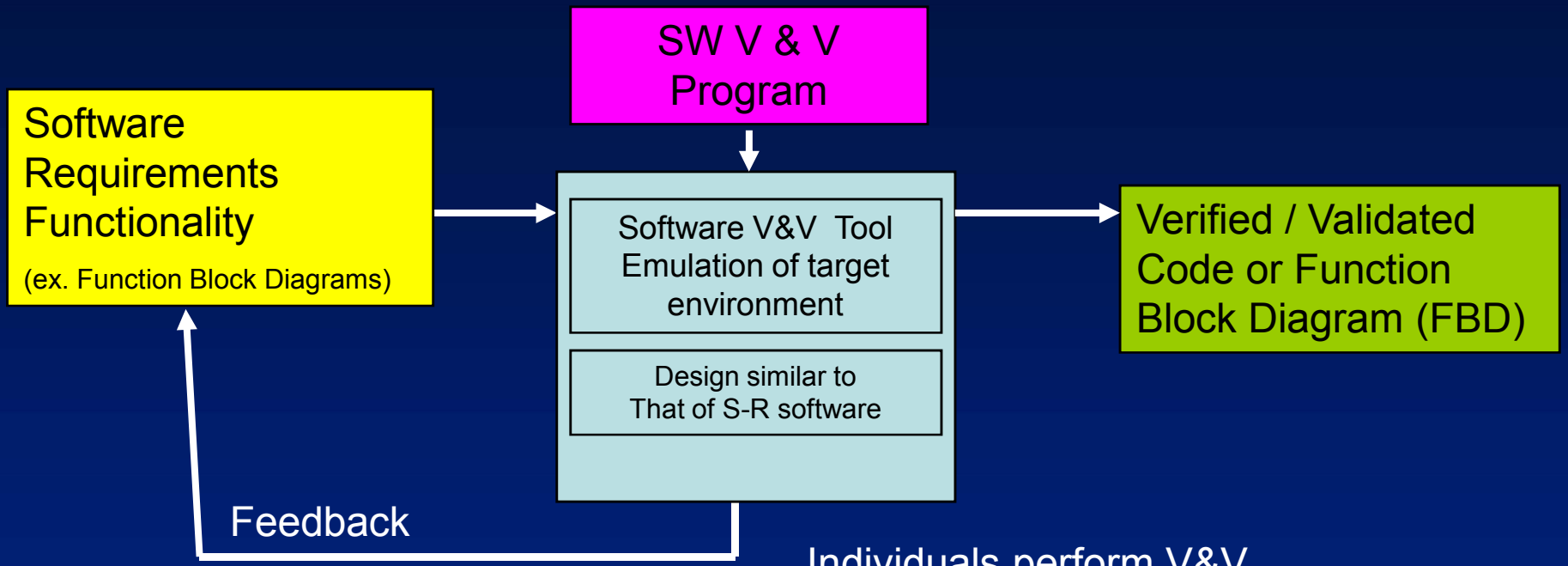
Fully Qualified Software Tool Usage Model Requirements Traceability



The software requirements traceability model defines the process of converting high level system requirements into design detail requirements and then into the verifiable code which will meet those requirements. The next step is to perform V&V on that code.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Fully Qualified Software V&V Tool Usage Model



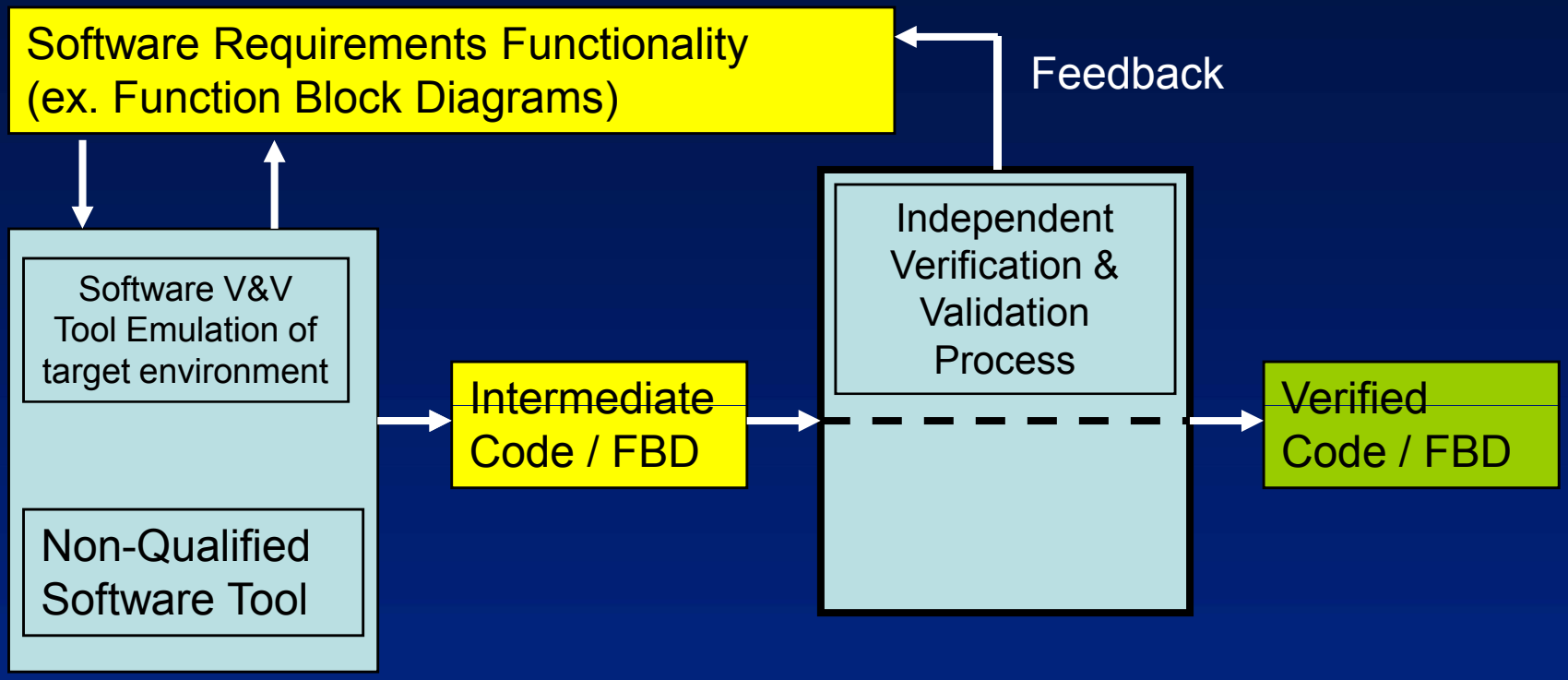
Individuals perform V&V function by using the qualified tool to examine the SW product

The use of a fully qualified V&V tool would allow the IVVT to use the results to formulate a reasonable assurance position.

The feedback loop is used to correct deficiencies discovered during the V&V processes.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Non - Qualified V&V Software Tool Usage Model



The Output of the Tool must undergo full V&V
This is done to ensure that defects that are not detected by the tool will be detected by the downstream V&V activity.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Diversity of FPGAs

- Degree and nature of diversity (FPGA-FPGA, FPGA-microprocessor) that are adequate when using FPGAs
- How do common cause programming failures and other commonalities effect FPGA diversity
- Current diversity guidance, such as NUREG/CR-6303 and NUREG/CR-7007 does not address
- Issue to be address include
  - Identification of the properties sufficient to credit FPGAs as diverse within the same technology,
  - The level of susceptibility that FPGAs have to common cause programming failures

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cyber Security

- FPGAs can provide advantages over more general purpose computer-based implementations
  - FPGA-based system designs can eliminate opportunities for device programming to be altered
  - For some FPGA technology, cannot be read back or can be protected from being read
- Software tool security is more important, because some tools have no diverse counterpart and their outputs cannot be efficiently verified
- Maintenance and operational issues should be easier to address

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Standards

- New IEC standard (for complex programmable devices) however, this standard does not directly address “very simple” FPGAs or CPLDs
- IEEE or other standards’ bodies are encouraged to become involved
- Of particular concern is the absence of available standards and guidance for commercially available software-based FPGA tools, which includes design tools, analysis tools and verification tools

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Regulatory Examples

- In the U.S. we are seeing more and more digital systems using FPGA's and CPLD's
- This includes both platforms that uses FPGA's as there main processor and embedded technology
  - Westinghouse SSPS cards
  - Allan Bradly Relays

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Regulatory Examples

- Toshiba PRM system
- Spinline 3 system (some modules included FPGAs, but not the main processor)
- Westinghouse's ALS system
- Westinghouse SSPS cards
- Lockheed Martin NuPac
- Doosan HF-6000 system
- Radiy FPGA system

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Regulatory Lessons

- The lifecycle process for FPGA-based systems usually incorporates disciplined specification and implementation of design requirements following a logic design approach similar to CPU-based systems
- Establishment of VHDL coding guidance, so the logic produced includes common design attributes
- Development of Design Specification for the FPGA that consists of a combination of hardware and software detailed design description necessary to define the FPGAs

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Regulatory Lessons

- FPGA testing requires testing of the VHDL code (i.e., simulation) and then testing in a programmed FPGA
- Design should be synchronous and deterministic to favor correctness and testability
- Design should explicitly handle all possible cases of logic and timing
- 100% testability of FPGA-based systems require clear definitions of what is being tested

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Future Efforts

- The U.S. Nuclear Regulatory Commission has decided to develop a Regulatory Guide on the use of FPGA and similar devices
- NRC will be using IEC 62566 as the basis for the Regulatory Guide
- However this is proving to be challenging
  - Need to reference IEEE instead of IEC standards for areas where FPGAs are not unique
  - Need to supplement IEC 62566 with some additional positions, including NRC position on diversity

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Conclusions

- FPGA's continue to be used in an increasing number of digital platforms and embedded devices
- Vendors continue to look at how best to use FPGAs in nuclear safety systems
- This technology is being effectively reviewed but better guidance should be developed
- NRC is working to update its guidance

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Questions ?