Providing Cyber Security
for FPGA-based Applications

Kostiantyn Leontiiev, Technical Director

10th International Workshop On the Application of FPGA in NPPs

December 4–6, 2017, Gyeongju, Korea
Agenda

→ Introduction
→ Standards Analysis
→ Secure Development Environment Establishment
→ RadICS Platform specific security features
→ Summary
RPC Radiy is a vendor of FPGA-based I&C Platform/Systems for NPPs

- Main product is RadICS Platform
- RadICS Platform is SIL-3 (single channel) certified as per IEC 61508:2010
- Topical Report for the Platform is under US NRC review
Introduction (2)

- Increasing number of security attacks on industrial safety-critical I&Cs
- COTS- components (FPGA, HW, Development Tools, SW) may have vulnerabilities
- Human factor (human errors/risks of insider attacks)
- Open systems issues (unified protocols)
Inevitable consideration of process-product approach

→ Life cycle of I&C Platform/Application shall consider cyber security risks during design and operation phases

→ I&C Platform/Application design shall provide features to minimize cyber risks

→ Different technologies used to implement I&C Platform/Applications have different properties with respect to cyber security
Standards analysis
Standards Analysis and Requirements Profile

Ukrainian Normative Documents (1)

→ Ukrainian normative document NP 306.2.202 "Nuclear and Radiation Safety Requirements for I&C Systems Important to NPP Safety", issued in 2015, contains umbrella requirements to establishment of secure environment

→ In particular, Section 6 of Chapter IV contains requirements to protection from unauthorized access during operation

→ Section 4 of Chapter VIII contains relevant requirements to software
Standards Analysis and Requirements Profile

Ukrainian Normative Documents (2)

Recommended measures from NP 306.2.202:

→ Physical protection

→ Protection from unauthorized software, databases and archives modification
Standards Analysis and Requirements Profile

Ukrainian Normative Documents (3)

Recommended measures from NP 306.2.202 (cont’d):

→ Protection from unauthorized commands from control rooms

→ Immediate personnel notification on any unauthorized access attempts
Standards Analysis and Requirements Profile

Ukrainian Normative Documents (4)

- Requirements in NP 306.2.202 are quite generic and can be used only as umbrella requirements to be fulfilled in quality management system
- Also, secure development environment issues aren’t covered
- Therefore, relevant NRC and IEC standards were used as guidance during the process of secure development environment establishment:
  - RG 1.152-2011, “Criteria for use of computers in safety systems of Nuclear Power Plants”;
  - RG 5.71-2010, “Cyber security programs for nuclear facilities”
  - IEC 62645, “Nuclear power plants - Instrumentation and control systems - Requirements for security programs for computer-based systems”
Secure Development Environment (SDE) Establishment
With respect to cyber security issues our QMS includes:

- procedures and guidelines on cybersecurity ensuring (who, how, when-stages). It defines approach for creation of secure development environment and its further operation. It provides guidance for designing digital systems (both hardware and software) to ensure that they are free from vulnerabilities that could affect the reliability of the system;
- company policy, aimed at development of secure applications;
- staff training program.
Main elements of cybersecurity ensuring (2). Who ensures security

<table>
<thead>
<tr>
<th>Lifecycle phase (RG 1.152)</th>
<th>System design process stage</th>
<th>Responsibility in this procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concepts</td>
<td>Pre-Development and Planning</td>
<td>End-user, IT manager, Application Design Bureaus and Independent V&amp;V Department</td>
</tr>
<tr>
<td>Requirements</td>
<td>Requirements Specification (SW/HW/HMI)</td>
<td>Design Bureaus, Independent V&amp;V Department and QAPM</td>
</tr>
<tr>
<td>Design</td>
<td>HW, SW Design</td>
<td>Design Bureaus, Independent V&amp;V Department and QAPM</td>
</tr>
<tr>
<td>Implementation</td>
<td>Implementation</td>
<td>Design Bureaus, Independent V&amp;V Department and QAPM</td>
</tr>
<tr>
<td>Test</td>
<td>Integration; Validation and FAT</td>
<td>Independent V&amp;V Department and QAPM</td>
</tr>
<tr>
<td>Installation, checkout, and acceptance testing</td>
<td>Installation</td>
<td>Technical Support and Maintenance Group and QAPM with turnover to the system user</td>
</tr>
<tr>
<td>Operation</td>
<td>Operation and Maintenance</td>
<td>End-user</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Not Applicable</td>
<td>End-user</td>
</tr>
<tr>
<td>Retirement</td>
<td>Not Applicable</td>
<td>End-user</td>
</tr>
</tbody>
</table>
The general scheme of the process approach to the implementation of secure design and operation environment

**Development Stages**

- **Concept Phase**
- **Requirements Phase**
- **Design Phase**
- **Implementation Phase**
- **Test Phase**

### Development Environment Vulnerabilities Analysis
- (customer & radiy)

### Digital I&C Operational Environment Vulnerabilities Analysis
- (customer & radiy)

### Actions to assure secure operational environment:
- System security requirements tracing
- System security design features verification
- System security features verification

### Actions to assure secure development environment:
- Measures to ensure that the requirements development processes and documentation are secure such that the system does not contain unnecessary or extraneous requirements
- Measures to ensure that system design does not contain unnecessary design features or functions
- Measures to minimize and mitigate any inadvertent or inappropriate alterations of the developed system (transformation of the design into code is correct, accurate, and complete)

### Implementation of security measures for development environment and LAN

### LAN security audit & development environment physical security audit

### Actions to assure secure operational environment:
- System security requirements tracing
- System security design features verification
- System security features verification

### Actions to assure secure development environment:
- Measures to ensure that the requirements development processes and documentation are secure such that the system does not contain unnecessary or extraneous requirements
- Measures to ensure that system design does not contain unnecessary design features or functions
- Measures to minimize and mitigate any inadvertent or inappropriate alterations of the developed system (transformation of the design into code is correct, accurate, and complete)

### Implementation of security measures for development environment and LAN

### LAN security audit & development environment physical security audit

### Security audit of measures, which prevent the introduction of unnecessary or extraneous requirements

### Security audit of measures, which prevent the introduction of unnecessary design features or functions

### Measures to validate that system possesses all intended security features

### Concept Phase
- **PPC Radiy**

### Requirements Phase

### Design Phase

### Implementation Phase

### Test Phase
SDE at Concept Phase

- **SDE activities:**
  - Vulnerabilities analysis for development environment (DE).
  - Implementation and audit of security measures related to DE:
    1) Network security hardening (isolated network);
    2) Physical Access Control;
    3) System and Communications Protection;
    4) Identification and Authentication;
    5) Document and Software storage security;
    6) Removable Media usage control;
  - Personnel training
SDE at Requirements Phase

• **SDE task:**
  - Measures to ensure that the requirements defined during this phase do not contain unnecessary or extraneous requirements. Cyber Security requirements shall be considered also.

• **SDE activities:**
  - Implementation and audit of phase-specific security measures to prevent the introduction of unnecessary or extraneous requirements (*configuration management, access control, tracing, review and comments, security audit*)
SDE at Design Phase

• SDE task:
  - Measures to ensure that system design does not contain unnecessary design features or functions which might compromise cyber security

• SDE activities:
  - Implementation and audit of phase-specific security measures to prevent the introduction of unnecessary design features or functions (tracing, configuration management, access control, review and comments, security audit)
SDE at Implementation Phase

- **SDE task:**
  - Measures to minimize and mitigate any inadvertent or inappropriate alterations of the developed system (transformation of the design into code is correct, accurate, complete and doesn’t contain unnecessary functionality)

- **SDE activities:**
  - Implementation and audit of phase-specific security measures to prevent appearance of undocumented codes or functions (*static code analysis and review, positive and negative functional testing, configuration management, access control, etc.*)
SDE at Test Phase

• SDE task:
  - To validate that system possesses all intended security features

• SDE activities:
  - System security features validation
  (validation testing, configuration management, access control)
Structure of SDE Report

Contains description for more than 60 security controls:

• System design features for security
  ➔ Physical Access Controls
  ➔ Electronic Access Controls
  ➔ Software Alteration Controls
  ➔ Deterministic Performance Controls

• Development processes for security
RadICS Platform specific cyber security features
FPGA technology advantages

- There are no known viruses and malware designed to attack HDL coded configurations; FPGA-based platforms have a simple and structured design, therefore the corresponding V&V processes performed at each stage of design are more likely detect the presence of potential threats and malicious design;

- FPGAs do not use operating systems which could be the target of potential cyber attacks

- FPGA programming and reprogramming can be done only through a special interface. It is impossible to connect common storage media or communication devices that could infect the control logic code, as was the case in the Stuxnet attack.

- FPGA chips itself may contain vulnerabilities. So it’s extremely recommended to use chips which presents on the market more then 3 years without changing their revision (e.g. floorplan)
FPGA technology vulnerabilities

- Configuration cloning;
- Reverse Engineering;
- Tampering;
- Spoofing;
- Attack from the field;
Some of security controls implemented in I&C systems based on the RadICS Platform (1)

- Physical locks on equipment cabinets
- It’s not possible to reconfigure modules during operation (remotely or locally - need to extract module(s) from chassis)
- It’s not possible to reconfigure modules (EPCS, EEPROM(s), CPLD Flash) using standard vendor programmer (special converter needed)
- Watchdog (based on diverse technology) checks FPGA configuration process and all FPGA supply voltages levels (switch-off FPGA power supply)
- Partial configuration is not allowed by the platform design
Some of security controls implemented in I&C systems based on the RadICS Platform (2)

- FGPA’s configuration integrity fully (using chip’s vendor and proprietary techniques) checked during module startup period and continuously during operation
- FGPA’s configuration UID easily verifiable (local display, MATS display)
- Only point-to-point safety communications (no rings, no broadcast) with Proprietary protocol
- Self-diagnostic of interfaces helps to detect intrusion (data corruption\modification will be detected)
- One-way communication interfaces to external systems
Some of security controls implemented in I&C systems based on the RadICS Platform (3)

- Interfaces used for the modification of the set-points are de-energized during normal operation. Requires two-steps authorization.
- Local indication provides all information to check that plant data and diagnostic monitoring system provide correct data for operator.
- Full control of design. Home-made source code. No 3-rd party IP cores in the Platform Level. Source code available for audit by independent entities.
- Manuals are issued with supplied I&C systems to encourage operation and maintenance personnel to implement security measures.
Summary

• Providing cyber security is an important business process of the company. It takes into account the specifics of the company, its resources and technologies.

• The process of cybersecurity is implemented within the QMS. Secure development environment is a must.

• Secure I&C system development is a joint responsibility of developer/manufacturer and customer. It should be based on the process-product approach.
Thank you for your attention!

Public Company «Research and Production Corporation «Radiy»
29 Geroyiv Stalingrada Street, Kirovograd, Ukraine, 25009
e-mail: ksleontiev@radiy.com
http://www.radiy.com