COMPUTER SECURITY APPROACH FOR ROLLS-ROYCE SPINLINE® SAFETY PLATFORM

Julien BACH, Arnaud DUTHOU & Pierre MONTEIL
Rolls-Royce Civil Nuclear
23, Chemin du Vieux Chêne
Meylan 38240, France
Julien.Bach.cn@Rolls-Royce.com; Arnaud.Duthou.cn@Rolls-Royce.com; Pierre.Monteil.cn@Rolls-Royce.com

Mark BURZYNSKI
Rolls-Royce Instrumentation & Controls
5959 Shallowford Road, Suite 511
Chattanooga, Tennessee 37421, USA
Mark.Burzynski@rolls-roycenuclear.com

ABSTRACT

The number of digital assets at commercial nuclear power plants is significant and will likely continue to increase with time. As a consequence, these plants have become potential targets for cyber-attacks. Around the world, nuclear safety authorities and national Computer and Information Security Agencies are implementing stricter regulations and inspections for critical systems in nuclear plants. There is a particular focus on instrumentation and control systems as they implement key nuclear safety functions.

Rolls-Royce follows a strict computer and information security program based on general and nuclear specific norms, Rolls-Royce group processes, and proven technologies. The Spinline digital safety platform has been designed specifically for nuclear applications and features a secure development and operational environment that provides barriers against unauthorized modifications and implements design requirements promoting integrity and reliability during operation and maintenance. The Rolls-Royce secure development environment provides layers of protection utilizing physical and environmental security, human resource security, and information technology systems access control.

The Spinline platform strengthens security functions by providing protection against unauthorized, unintended, and unsafe modifications to the system. The Spinline platform has design features promote integrity and reliability during operation and maintenance in the event of inadvertent operator actions or undesirable behavior of connected equipment.

The Spinline technology and these computer security processes are based in a wide spectrum of international standards that were accepted as providing a secure development and operating environment by the United States Nuclear Regulatory Commission in 2014.

Key Words: I&C, Cyber Security, Spinline, Safety, Rolls-Royce

1 INTRODUCTION

The number of digital assets at commercial nuclear power plants (NPPs) is significant and will likely continue to increase with time. As a consequence, these plants have become potential targets for cyber-attacks. Around the world, nuclear safety authorities and national computer and information security agencies are implementing stricter regulations and inspections for critical systems in NPPs. There is a particular focus on instrumentation and control (I&C) systems as they implement key nuclear safety functions.

Rolls-Royce I&C follows a strict computer and information security program based on general and nuclear specific norms, Rolls-Royce group processes, and proven technologies. Spinline, Rolls-Royce's digital safety platform, has been designed specifically for nuclear applications and features a secure development and operational environment that provides barriers against unauthorized modifications and implements design requirements promoting integrity and reliability during operation and maintenance.

Rolls-Royce development environment is protected thanks to general security principles:

- Physical and environmental security: physical access restrictions and monitoring
- Human resource security: employee and contractor references are checked and non-disclosure agreements must be signed
- Information technology (IT) systems access control: use of networks, applications and IT systems are restricted and monitored

Special care has been taken in the development of Spinline, Rolls-Royce's safety digital platform, which is used to implement the key nuclear safety functions. Spinline-specific procedures are in place during development, testing, and installation phases.

Specific procedures are also implemented during operations, testing, and maintenance, specific procedures are also implemented to control access to the Spinline equipment during operation, prevent remote access, and control local access for maintenance.

Rolls-Royce's I&C computer and information security program is based on International Organization for Standardization (ISO) 27001 [1], ISO 27002 [2], and nuclear specific guides such as International Electrotechnical Commission (IEC) 62645 [3], IEC 62859 [4], International Atomic Energy Agency (IAEA) NSS-17 [5], and United States (U.S.) Nuclear Regulatory Commission (NRC) Regulatory Guides (RGs) 1.152 [6] and 5.71 [7]. Moreover, continuous training programs have been put in place to increase the expertise and the number of specialists able to provide a specific approach adapted to our customers.

2 BACKGROUND

The number of digital assets at commercial NPPs is significant and will likely continue to increase with time. As a consequence, these plants have become potential targets for cyber-attacks and "digital sabotage." This risk was highlighted by the IAEA during its 57th general conference and has become the subject of a specific effort. Similarly, nuclear safety authorities around the world, as well as national computer and information security agencies, are implementing stricter regulations and inspections for critical systems in NPPs.

There is a particular focus on I&C systems because they implement key nuclear safety functions.

Threats:

Figure 1 illustrates the main types of attacks according to their likelihood, author motivation, and potential consequences:

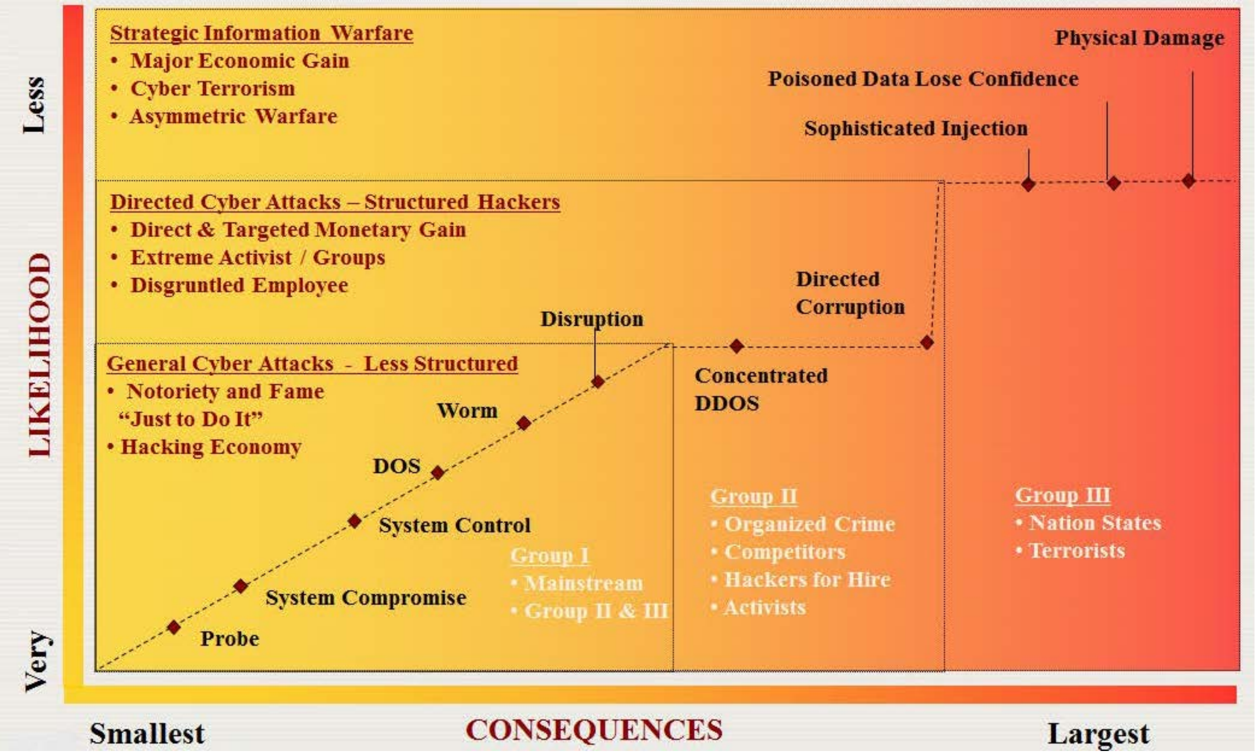

Figure 1. Illustration of Cyber Attack Types

More specifically, I&C operations face several types of disruption:

- Delaying or blocking the information flow in control networks
- Unauthorized modification of the controller (e.g., programmable logic controller (PLC) or distributed control system) instructions
- False data and information sent to operators
- Malicious software (e.g., virus, Trojan horse, etc.) introduced into the systems

These disruptions can result in damage to equipment, control of safety or shutdown systems and, ultimately, to employees and the general population.

Detected Incidents in Nuclear Facilities:

- Davis-Besse NPP, U.S., 2003: a computer worm infected the Safety systems of the plant: completely shutting down parts of the Safety Parameter Display System and Plant Process Computer
- Hatch NPP, U.S., 2008: a software update caused a plant shutdown
- Natanz Nuclear facility, Iran, 2010 Stuxnet worm, Siemens PLCs infected causing centrifuges failures
- Undisclosed South Korean NPP (probably Gori-2 and Wolseong-1), December 2014: worm infection, resulting in stolen data stolen. The hacker's threats to shut down the reactor were published in the international press
- See "A Survey of SCADA and Critical Infrastructure Incidents," for a list of incidents in other industries with high safety requirements [8]

3 ROLLS-ROYCE I&C CYBER SECURITY PROGRAM

The Rolls-Royce I&C group follows a strict computer and information security program that is based on general and nuclear-specific norms, the Rolls-Royce group processes, and state-of-the-art technologies. Special care has been given to the development of Spinline, Rolls-Royce's digital safety platform. This platform is used to implement the key nuclear safety functions. Moreover, continuous training programs have been put in place in order to increase both the level of expertise and the number of our specialists. Doing so will allow us to be able to provide a specific approach adapted to our customers. In particular, the creation of procedures and system specifications that have taken into account the cyber security issue through organization plans and monitoring of technical requirements during the designs phases.

3.1 General Security

Access to the Rolls-Royce development environment in Meylan, France is protected. Access to the factory, the factory local area network (LAN), the development environment, the quality records, and the configuration management system is restricted in accordance with internal procedures. The development environment is connected to the factory LAN and is protected in accordance with Rolls-Royce IT procedures, particularly:

Physical and Environmental Security

- Physical access to facilities is monitored and restricted
- Secure areas access is authorized only to a specific list of people
- Photography and/or video recording is only allowed with authorization
- Video surveillance is in place at strategic points
- Access cards permitting time-limited access to general and/or specific areas may be provided to trainees, vendors, consultants, third parties and other personnel who have been identified, authenticated, and authorized to access those areas
- Visitors are escorted at all times by an employee while on the premises
- The date and time of visitor entry and departure are recorded
- Everyone on site must wear and display their pass at all times
- The access control systems themselves are secured

Human Resource Security

- An applicant's identity, references are verified before employment
- All employees must formally accept confidentiality and non-disclosure agreements
- Employee access rights are updated accordingly after all situation changes

Access Control

- Users of corporate IT systems, networks, applications and information are individually identified and authenticated
- Login attempts are controlled and passwords must be strong
- Privileged access rights are reviewed periodically
- Users must either log off or password-lock their sessions before leaving them unattended
- Password-protected screen savers with an inactivity timeout of no more than 10 minutes is enabled on all workstations/personal computers
- Write access to removable media (universal serial bus drives, compact disc/digital video disc writers etc.) is restricted

3.2 Spinline Specific Measures

The Spinline platform has been designed as the foundation for digital safety I&C systems that implement nuclear safety functions. The design of the platform and the application software life cycle processes applied through the factory test phase also establish a secure development and operational environment that strengthens security functions by:

- Providing protection against unauthorized, unintended, and unsafe modifications to the system
- Implementing design requirements that promote integrity and reliability during operation and maintenance in the event of inadvertent operator actions or undesirable behavior of connected equipment

The main Spinline features ensuring a secure development and operational environment are summarized below.

3.2.1 During Development, Tests and Original Installation

Integrity control procedures are in place during all the production phases. Moreover, each executable has its own signature that can be checked at all times even after install on site.

The Spinline hardware platform is a highly-reliable foundation for a digital safety I&C system that has a proven high reliability record. Board/device-level failure mode and effects analyses and reliability analyses have been performed to demonstrate high reliability. Operational experience demonstrates high reliability from installed Spinline systems and earlier generations of Rolls-Royce digital safety I&C systems. The Spinline hardware incorporates extensive failure detection mechanisms.

Software life cycle processes are in place at the Rolls-Royce factory to ensure production of high integrity, high reliability software for Spinline systems. Strict software design control processes are in place and followed throughout the development lifecycle. Writing guides are used for software life cycle documentation to ensure the systematic production of the comprehensive documentation required for safety system software. The configuration management system is well defined with rights granted individual by individual and project by project. The configuration management system and records provide the framework for implementing requirements traceability.

The configuration management and requirements traceability processes define the approved software baseline and provide the means to detect authorized and unauthorized modifications to that baseline. V&V activities provide an independent capability to detect unauthorized modification of software components and baselines. Testing activities provide the means to demonstrate that design requirements, including security requirements, have been implemented in the plant-specific system.

Spinline software does not include unwanted functions. The Spinline OSS performs only limited functions; primarily those associated with initialization, self-diagnostic tests, and management of interfaces with input/output boards and networks and the application software. The OSS is configured for a plant-specific application, but does not require any change to the OSS baseline. The plant-specific application software is a simple software module that receives data, performs specific calculations, and returns results to the OSS. The communication network uses the Rolls-Royce proprietary NERVIA network technology.

The integrity of the executable code in a Spinline system is checked upon initialization and continuously during the unit processing. The platform software and application software are loaded on flash memory chips as executable code on the UC25+ processor boards. Checksums are calculated and regularly checked by the OSS during the processing unit operation, which verifies that the checksum generated for the executable code in memory is correct. The checksum verification covers the application specific code, the OSS code, and the configuration parameters.

Independent V&V and testing for software is performed at a system level to detect unauthorized modifications.

3.2.2 During Operation, Onsite Tests, and Maintenance

The production code cannot be changed in the field without replacing the flash memory chips holding the code. Updating this software requires replacing the flash memory chips. A UC25+ processor board must be removed from its rack to replace the flash memory chip on the board. The processor boards are not hot-swappable, so the rack must be powered off. Access to Spinline systems to remove a UC25+ processor board is limited to one channel at a time by administrative controls. Access to a cabinet (i.e., door open) causes an alarm. The Spinline platform does not include the capability for remote access to a Spinline system

The NERVIA digital communications network is used to implement data communication within the safety system and with other systems outside the safety system. It implements a proprietary protocol that does not allow for any dynamic modification of the communication scheme established and validated during design. The NERVIA network is deterministic. The network topology is stored on all UC25+ so if the network is modified (e.g., attempt to add a machine to modify data or remove/disable one of the network nodes) it is immediately detected.

NERVIA software can enforce one-way communication via fiber optic cabling to other divisions or external systems. One-way communications will be implemented with a hardware solution. These features are major contributors in making the system secure and preventing external systems from influencing the behavior of a Spinline safety system.

Only local access is available for maintenance and testing of a Spinline system.

The front-panel UC25+ connection used for maintenance and testing by means of the Local Display Unit (LDU) implement proprietary protocols with control access and require physical access to the Spinline cabinets

The potential for operator error during maintenance and testing is reduced by limiting the allowable actions that can be taken locally and including controls over those actions. For example:

- Setpoints that can be modified on-site by the operator and the changes are restricted to ranges defined and fixed during the design of the I&C system
- Access for setpoint modifications using the Spinline LDU is protected by a password
- LDU connection is detected and signaled
- Access to the systems to make setpoint changes is limited to one channel at a time by administrative controls
- Access to a cabinet causes an alarm

3.2.3 Standards and Norms

Rolls-Royce I&C computer and information security program is based on ISO 27001, ISO 27002, and the Rolls-Royce group processes:

- ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements
- ISO/IEC 27002 — Information technology - Security Techniques - Code of practice for information security management

For example, Loviisa I&C modernization project computer security plan was built on ISO 27001 and local YVL norms [9].

Moreover, the following guides and documents are used:

- IEC 62645:2014 — Nuclear power plants – Instrumentation and control systems – Requirements for security programs for computer-based systems
- IEC 62859:2016 — Nuclear power plants - Instrumentation and control systems – Requirements for coordinating safety and cybersecurity
- IAEA guide NSS-17 — Technical Guidance: Computer Security at Nuclear Facilities

The regulatory authorities have published many regulatory documents such as U.S. NRC RGs 1.152 and 5.71, IEEE Standard 7-4.3.2 [10], and Korea Institute of Nuclear Safety Regulatory Guide 8.22 [11].

4 CONCLUSION

Rolls-Royce has put measures in place to fight the increasing cyber threats in the nuclear sector. These measures encompass both general security principles and processes and specific measures dedicated to its products, in particular its digital safety platform Spinline. Rolls-Royce's development environment is protected thanks to the following general security principles:

- Physical and Environmental Security: physical access restrictions and monitoring,
- Human Resource Security: employees and contractors references are checked and non-disclosure agreements s must be signed,
- IT Systems Access Control: uses of networks, applications, and IT systems are restricted and monitored.

Rolls-Royce digital safety platform has been designed specifically for nuclear applications and features a secure development and operational environment that provides protection against unauthorized modifications and implements design requirements promoting integrity and reliability during operation and maintenance.

Spinline specific procedures are in place during development, testing, and installation phases:

- Software life cycle processes in place with:
  - Strict design control process,
  - Configuration management system with rights granted individual by individual and project by project,
  - Configuration management system with traceability to detect unauthorized modifications.
- Spinline software does not include unwanted functions:
  - Proprietary OSS performs only limited functions,
  - The specific application software cannot modify the OSS,
  - The communication network is Rolls-Royce proprietary NERVIA network.
- Integrity of Spinline code is checked upon initialization and continuously during the unit processing:
  - Processing Unit Software loaded on flash memory,
  - Checksum regularly verified.
- Spinline hardware incorporates failure detection and has a proven high reliability record,
- Independent V&V and testing (software and system) to detect unauthorized modifications.

Specific procedures are also implemented during operations, testing, and maintenance:

- Executable code alteration would require physical access to the main processor board of a rack, which is limited by administrative control; moreover, access to a cabinet causes an alarm.
- There is no way for remote access to a Spinline system:
  - NERVIA protocol does not allow dynamic modification,
    - Adding a machine to modify data or remove one node is immediately detected,
    - One way communication to external system is implemented with hardware.
- Only local access is available for maintenance and testing of a Spinline system;

- Physical access is required,
- Allowed actions are pre-defined and limited.

Rolls-Royce I&C computer and information security program is based on ISO 27001, 27002 and nuclear specific guides such as IEC 62645, 62859, IAEA NSS-17, and U.S. NRC RGs 1.152 and 5.71. Moreover, continuous training programs have been put in place to increase both the expertise and the number of our specialists in order to be able to provide a specific approach adapted to our customers.

5 REFERENCES

1. ISO/IEC 27001:2013, "Information security management," International Organization for Standardization.
2. ISO/IEC 27002:2013, "Information technology -- Security techniques -- Code of practice for information security controls," International Organization for Standardization.
3. IEC 62645:2014, "Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems," International Electrotechnical Commission.
4. IEC 62859:2016, "Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity," International Electrotechnical Commission.
5. IAEA Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," International Atomic Energy Agency.
6. Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," July 2011, U.S. Nuclear Regulatory Commission.
7. Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," January 2010, U.S. Nuclear Regulatory Commission.
8. Miller, B. and Rowe, D. 2012. A survey SCADA of and critical infrastructure incidents. In Proceedings of the Proceedings of the 1st Annual Conference on Research in Information Technology (RITI'12) (Calgary, Alberta, Canada, October 11-13, 2012). ACM, New York, NY, 5156. DOI=http://dx.doi.org/10.1145/2380790.2380805.
9. YVL A.11, "Security of A Nuclear Facility," November 2013, Finnish Radiation and Nuclear Safety Authority (STUK).
10. IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
11. Regulatory Guideline 8.22, "Cyber Security of I&C System," Korea Institute of Nuclear Safety.