Secure Enterprise Integration for Multipurpose Research Reactors

N. Howarth[1], with M. Hewes[1], C. Hunt[1], & A. Noonan[1]

1) Australian Nuclear Science and Technology Organisation (ANSTO)
New Illawarra Road, Lucas Heights, NSW 2234 Australia

Corresponding author: nick.howarth@ansto.gov.au

Abstract. The OPAL research reactor operated by the Australian Nuclear Science and Technology Organisation (ANSTO) is a multi-purpose scientific and manufacturing facility. Information produced by the reactor's operational technology (OT) systems is relied upon by engineering, scientific, and manufacturing information systems.

We present an overview of the requirements for, and the techniques applied to achieve secure enterprise integration between the OPAL Research Reactor's Operational Technology (OT) and associated these information systems, while conforming to international and national guidance including:

1. Minimising what "information system" functionality is present on reactor OT systems;
2. Providing a controlled, uni-directional security gateway for data flows from the OT systems to the ERP; and
3. Limiting data entry to reactor OT systems to operator controlled barcoded paper forms using strictly defined data formats.

1. Introduction

The OPAL research reactor operated by the Australian Nuclear Science and Technology Organisation (ANSTO) is a multi-purpose scientific and manufacturing facility. Information produced by the reactor's operational technology (OT) systems is relied upon by engineering, scientific, and manufacturing information systems, including:

- Engineering, operations and maintenance information systems;
- Neutron beamline data acquisition systems; and
- ANSTO's Enterprise Resource Planning (ERP) system for the scheduling of:
  - Silicon Neutron Transmutation Doping (NTD) irradiations, and
  - Irradiation of materials for scientific analysis and for the production of radiopharmaceuticals.

Each consumer of information produced by the OPAL research reactor has its own computer security model ranging from the collaborative network operated by the Australian Centre for Neutron Scattering (ACNS), to the secure network requirements of the ANSTO ERP platform. The differing requirements of each area were taken into account with one fundamental security control from the reactor itself, the physical isolation of the OT network from inward network communication.

Through the application of international guidance from the International Atomic Energy Agency (IAEA), national frameworks and procedures from the Australian Signals Directorate (ASD), and local expertise, ANSTO has formed a security architecture that meets the requirement of all users of the OPAL research reactor while protecting the key OT systems that ensure safe, secure, and sustainable operation.

The techniques applied to achieve this secure enterprise integration while conforming to international and national guidance included:

1. Minimising what "information system" functionality is present on reactor OT systems;
2. Providing a controlled, uni-directional security gateway for data flows from the OT systems to the ERP; and
3. Limiting data entry to reactor OT systems to operator controlled barcoded paper forms using strictly defined data formats.

2. Data Generation and Integration Requirements

Generally, individual users of reactor OT systems generate data when performing engineering, operational, and maintenance activities. This data is then required to be exported from these systems for use in an appropriate enterprise information system for further analysis or storage. Additional to this ad-hoc data generated by users may be data generated automatically by reactor OT systems for the same purpose, generally at a low frequency e.g. daily or weekly, and is not required for use by users or other information systems in real time. Neutron beamline telemetry is acquired by reactor OT systems for use in scientific analysis by the ACNS. This data is comprised of measurements of key neutron beam related reactor plant systems, including temperatures, flows, neutron flux and other reactor plant state information. This data is collected at a comparatively high frequency (multiple samples per minute), and is generally required for use by ACNS scientific analysis systems in near real-time.

For manufacturing purposes, manufacturing job data is first required to be loaded into the reactor OT systems. This data is used to control various aspects of the manufacturing process, executed by the reactor OT system. During the manufacturing processes, data is collected by the reactor OT system for use by ERP systems. This data is used to track the progress of the manufacturing process, and to record data such as irradiation duration, received neutron flux etc. This data is then used for further manufacturing or other supply chain activities within the ERP system in near-real time.

A summary of the data generation and integration requirements is presented below.

Table 1 - Summary of Data Generation Requirements

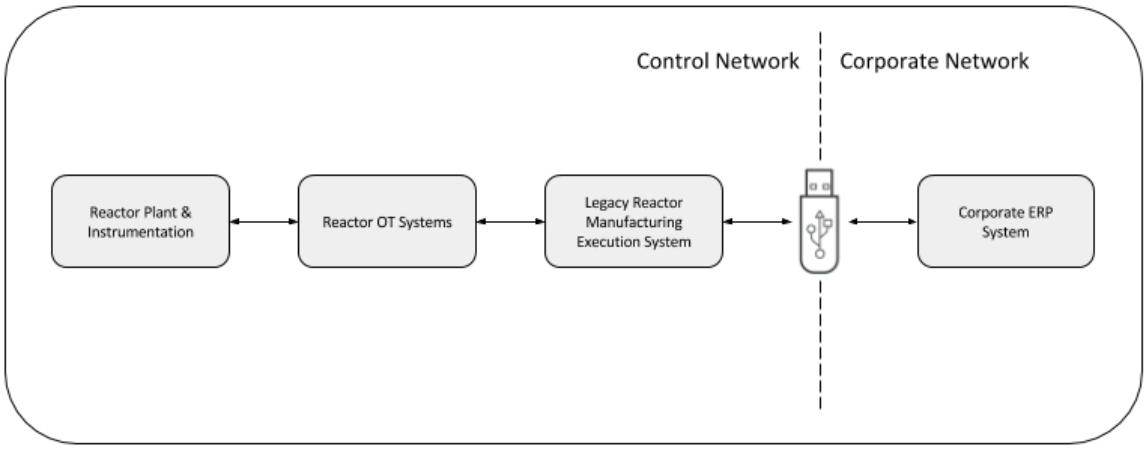
Data Type	Generation Method	Generation Freq.	Usage Req.
Engineering, Operations, Maintenance	User generated	Daily or Weekly	Ad-hoc, non-real-time
Neutron Beam Line Telemetry	System generated	Multiple samples per minute	Automated real-time analysis
Manufacturing execution data	User and System generated	Hourly	Corporate ERP system, near real-time

3. Legacy MEX System

Previously, a discrete manufacturing execution system (MEX) was operated on the reactor OT network. Scheduling staff used this MEX to schedule the manufacturing activities described previously. Manufacturing operations staff then used the MEX to execute the manufacturing activities. The MEX passed data to and from the reactor OT systems in real-time during manufacturing execution using the reactor OT network. Data was then passed between the MEX and the ERP system using USB storage media. Due to the volume and pace of these manufacturing activities, data was required to be passed between the MEX and ERP systems up to several times per day.

A high level data flow across this legacy architecture is presented below

Figure 1 – Legacy Data Flow



4. Cyber Security Requirements

Through the application of international guidance from the IAEA [1], national frameworks and procedures from the ASD [2], and local expertise, ANSTO has formed a security architecture that meets the requirement of all users of the OPAL research reactor while protecting the key OT systems that ensure safe, secure, and sustainable operation. The techniques applied to achieve this secure enterprise integration while conforming to international and national guidance included:

1. Minimising what “information system” functionality is present on reactor OT systems;

2. Providing a controlled, uni-directional security gateway for data flows from the OT systems to the ERP; and

3. Limiting data entry to reactor OT systems to operator controlled barcoded paper forms using strictly defined data formats.

Due to upgrades required to the reactor's OT systems that would render the legacy MEX system obsolete, the opportunity to remove the legacy MEX was realised. The scheduling functionality used in the legacy MEX system was replaced by supply chain wide scheduling functionality in the corporate ERP system, and manufacturing execution functionality was implemented directly in the reactors primary control system. This allowed the removal of the legacy MEX system entirely, reducing the overall "information system" functionality of the reactor OT environment, and reducing the volume and frequency of data transfers required to and from the OT environment.

In addition to the removal of the legacy MEX system, other "information system" functionality present on the OT environment was reduced or removed, such as:

- Word processing, spreadsheet and other desktop productivity software;
- Reporting and analytics systems;
- Printing facilities; and
- Data storage for conventional files.

To facilitate the access to data generated by the reactor's OT systems, a uni-directional security gateway (data diode) is utilised, providing secure data transfer from the OT systems to the corporate IT systems, while simultaneously providing a physical barrier to incoming connectivity. The specific data diode system employed for this purpose uses a single, transmit-only optical fibre connection, without a corresponding receive optical fibre. Due to the physical nature of the barrier, there is no risk of the gateway being compromised by a remote attacker in software only.

The data diode system allows for the real-time transmission of OT system and user generated data from the OT network to the corporate IT network. The specific data diode system employed supports the capacity and reliability requirements of the OT systems and users previously described, without need to reduce or otherwise modify existing processes, with significant additional capacity available for future expansion.

When removing the legacy MEX system, the requirement to be able to efficiently and accurately input manufacturing work order data remained. To facilitate this requirement, barcoded paper forms, generated by the corporate ERP system are employed. The input data requirements for manufacturing work orders are sufficiently low that an industry standard two-dimensional barcode provides adequate capacity for encoding this data, while conserving physical space on the paper form. The small size and fixed format nature of this barcode data allows for thorough validation processes to be performed when the data is read into the control system, for manufacturing execution. The use of barcodes additionally removes the need for work order data to be keyed in manually by operators, preventing keying errors.
A high level data flow across this legacy architecture is presented below

5. Enhanced Manufacturing Process Data Flow

The lifecycle of a manufacturing work order using this enhanced data flow is as follows:

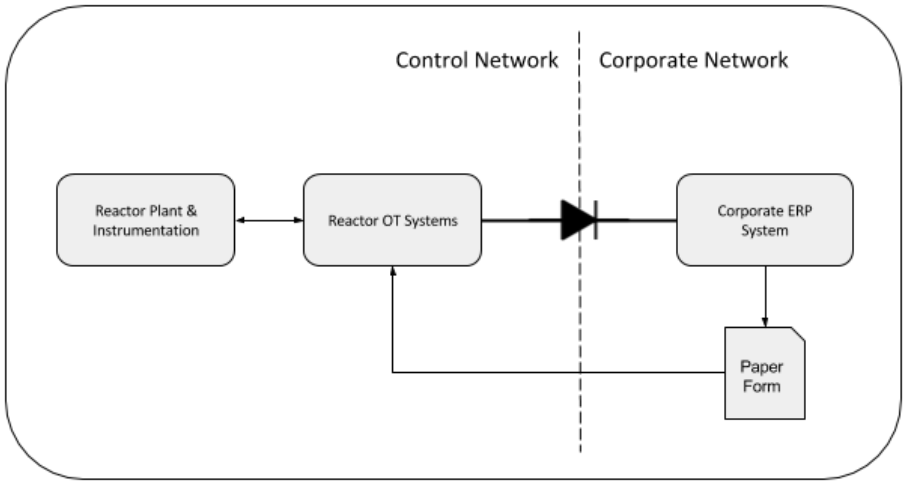
1. Scheduling of manufacturing activities occurs in the corporate ERP system, integrated with the complete supply chain. Ongoing changes to scheduling data are simplified as there is no need to continually transfer data between the corporate ERP system and the legacy MEX.

2. Immediately prior to manufacturing activities commencing, a paper work order form is generated from the corporate ERP containing manufacturing data encoded on a two-dimensional barcode.

3. The work order data is scanned into the control system using a barcode reader. This data is then available for use by the control system when executing manufacturing activities.

4. As manufacturing activities are executed, data is generated by the control system, and is securely transmitted to the corporate ERP system via the data diode on the OT network, in real-time. The corporate ERP system can then report this data to supply chain managers and other stakeholders.

Figure 2 – Enhanced Data Flow



6. Other Data Flows

The data diode system is also utilised for transmitting data generated by other reactor OT systems for integration into other corporate information systems in real-time, including data for scientific, engineering, operations and maintenance information systems. By removing or reducing "information system" functionality from the OT environment, and by consolidating "engineering system" functionality into the OT environment, the need for bi-directional network connectivity between the OT and corporate networks is significantly reduced.

7. Limitations

By implementing a data diode in this security architecture, the restriction on incoming connectivity poses two main limitations:

1. The inability for users to transmit data to the OT environment from the corporate environment for legitimate purposes; and

2. The inability to receive confirmations that data transmitted over the data diode system has been received and processed correctly.

The inability for users to transmit legitimate data to the OT environment from the corporate environment for legitimate purposes is mitigated by incorporating the needs of all stakeholders into the overall design of the OT environment. By consolidating "engineering system" functionality into the OT environment, the need to transmit data into the environment is greatly reduced. This also has the added benefit of allowing greater technical and administrative controls to be applied to the engineering systems together with other systems on the OT environment.

The inability to receive confirmations is mitigated to an extent by including sequencing information within data sent across the data diode system. This sequencing information is then used by corporate information systems to detect if data received from the OT environment is in-order, and used to detect if data has been missed.

8. Summary

As described above, by detailed consideration of data flow, "information system" and "engineering system" requirements, it is possible to design a security architecture that supports the scientific, engineering, operations and maintenance enterprise integration needs of a research reactor, while maintaining very high levels of cyber security assurance.

Reducing "information system" functionality and consolidating "engineering system" functionality on the OT environment greatly simplifies data flow requirements. Implementing a controlled, uni-directional security gateway for data flows from the OT systems to the ERP provides a high level of cyber security control, while still allowing enterprise integration to continue. Finally, where regular data entry to the OT environment is required, limiting this data entry to operator controlled barcoded paper forms allows for semi-automation of data entry, while still maintaining a high level of cyber security assurance.

9. References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, ISBN 978–92–0–120110–2, Vienna (2011) from http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

[2] AUSTRALIAN SIGNALS DIRECTORATE, Information Security Manual, Canberra (2017) from https://www.asd.gov.au/infosec/ism/