Interactive Content Presentation

for the

International Conference on Nuclear Security 2020

IAEA-NSNS (ICONS2020@iaea.org)

The Nuclear SIEM

R. ALTSCHAFFEL

Otto-von-Guericke University

C. NEAL

Polytechnique Montreal

T. HOLCZER

BME Crysys

M. HILDEBRANDT

Otto-von-Guericke University

Next

Start | IT in NPPs | Security in NPP IT | SIEM | Concept for an OT SIEM | Example for an OT SIEM | Summary

NPP Structure

In an NPP, many processes are supported or controlled by the use of computational systems.

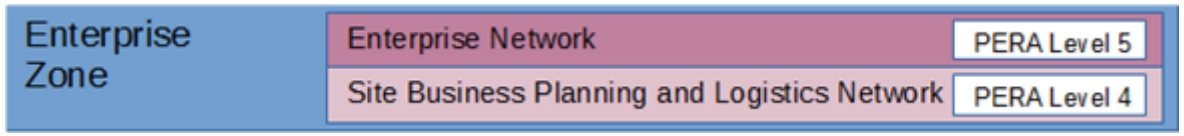
Computational systems come as classical computers as well as embedded systems.

Next

NPP Structure - IT

Computational system are used in plant administration. This business systems are referred to as IT (Information Technology).

They contain office workstations with access to emails, office software or more plant-specific work management systems.



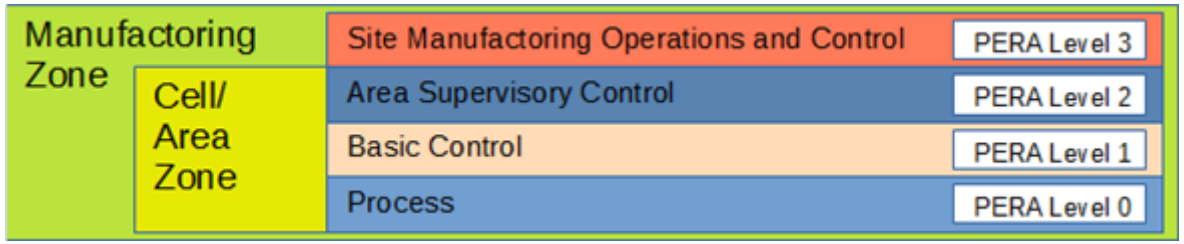
Control Hierarchy of ICS according to WILLIAMS, T. J., " The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation", Research Triangle Park, NC: Instrument Society of America, 1992

Next

Start | IT in NPPs | Security in NPP IT | SIEM | Concept for an OT SIEM | Example for an OT SIEM | Summary

NPP Structure - OT

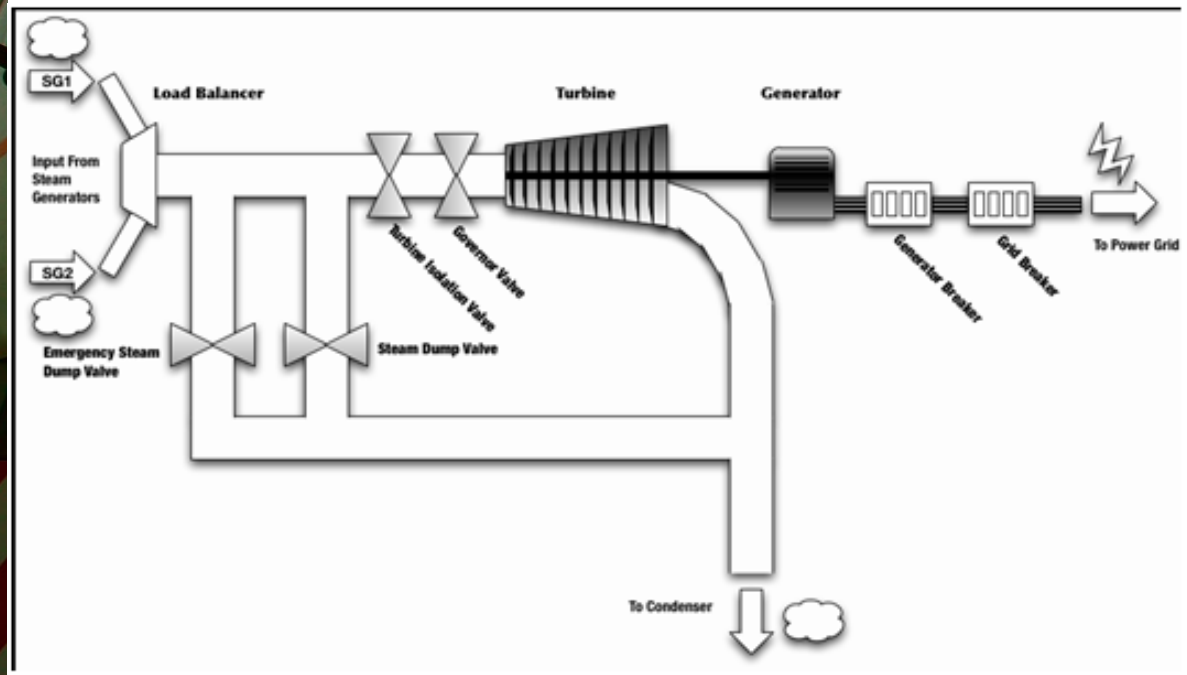
Computational system are also used to control physical processes in the plant. These Instrumentation and Control (I&C) systems are referred to as OT (Operational Technology).



Control Hierarchy of ICS according to WILLIAMS, T. J., " The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation", Research Triangle Park, NC: Instrument Society of America, 1992

Next

NPP Structure – OT Example



For example, computation systems control the valves inside the Steam Turbine Generator.

They consist of:

Sensors gather information about the physical process.

Computational units process this information.

Actors influence the physical process by implementing signals from the computation units

Next

NPP Structure – OT Example

Sensors measure physical properties

For example:
- temperature
- pressure
- water level

Sensors generate a signal from the measurement which is then send to a computing unit.
The signal might be analog or digital.

NPP Structure – OT Example

Computing Units process the data gathered by sensors and order actors to implement changes

Computing Units are called PLCs (programmable logic controllers) or SPS (speicherprogrammierbare Steuerung)

These are small computers with specialized input and output interfaces to communicate with sensors and actors

NPP Structure – OT Example

Actors manipulate the physical process

For example:

- heaters
- pumps
- valves

They receive signals from the computing units to implement these actions.

NPP Computer Security

Nuclear facilities have been the target of cyber-attacks. Cyber-attacks focus on Information Technology as well as Operational Technology. This section gives a brief overview on security mechanics implemented in NPP environments in order to protect from cyber-attacks.

Next

NPP Computer Security – Threats to IT

There are different threats of IT.

One constant treat are untargeted spam mails.

A greater concern are targeted spam mails (Spear-phishing) which try to obtain information from within the IT network or to inject malicious software (Malware) into the IT network. These attacks are performed by more sophisticated actors.

Attacks on IT aim at obtaining information or disrupting business processes.

Next

NPP Computer Security – Threats to OT

OT is a more specialized domain and not the focus of untargeted attacks.

However, control systems are of high interest to sophisticated attackers (e.g. nation state actors) which have the resources and capabilities to tailor attacks to specific systems.

Attacks on OT aim at obtaining information or disrupting physical processes.

Next

NPP Computer Security - DCSA

The IAEA proposed a DCSA (Defensive Computer Security Architecture) in order to support network segregation and security in NST047.

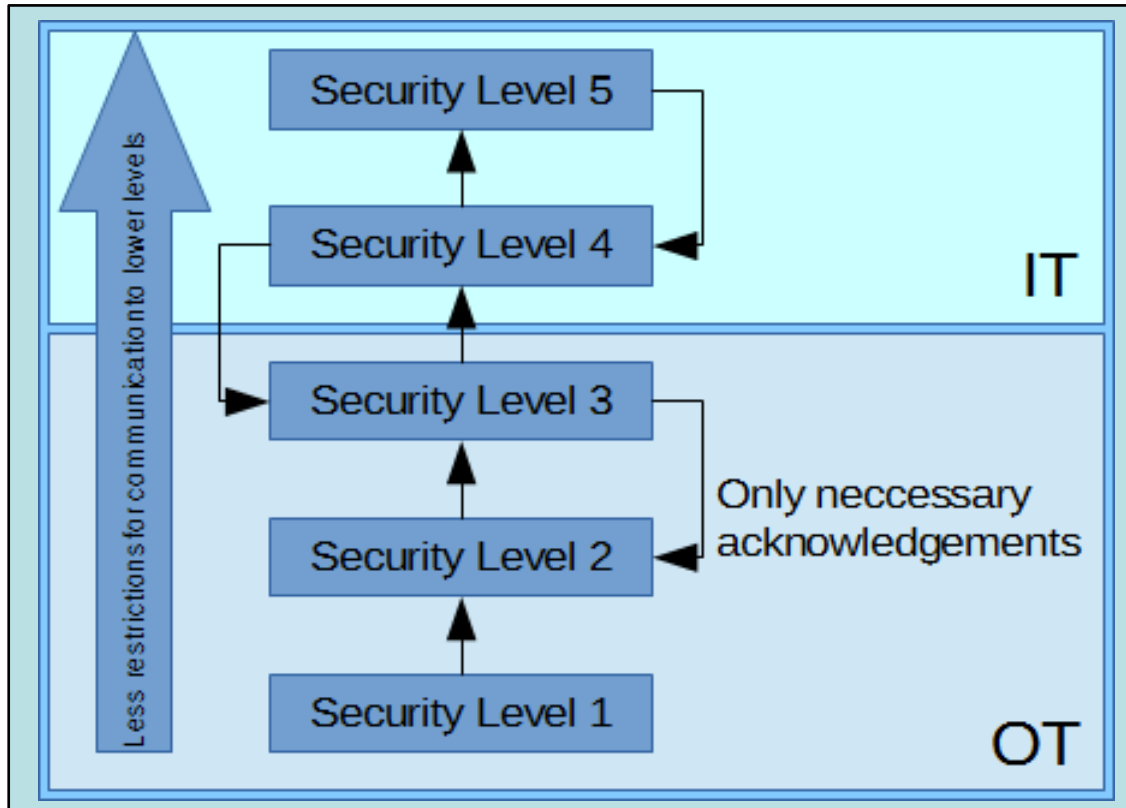
This model limits the flow of data between various components in IT and OT.

The computational devices within the NPP are grouped into Security Levels based on their criticality for the physical process. Devices are furthermore grouped into Security Zones based on physical location or subsystem they serve.

Security Level 1	Protection systems	
Security Level 2	Operational control systems	IT
Security Level 3	supervision real time systems	
Security Level 4	technical data management systems	OT
Security Level 5	Other Systems	

Next

NPP Computer Security - DCSA



Security Level 1	Protection systems	
Security Level 2	Operational control systems	IT
Security Level 3	supervision real time systems	
Security Level 4	technical data management systems	OT
Security Level 5	Other Systems	

Next

NPP Computer Security - Firewalls

Firewalls are used to segregate network from each other. They control the flow of data and hence are important to implement a DCSA.

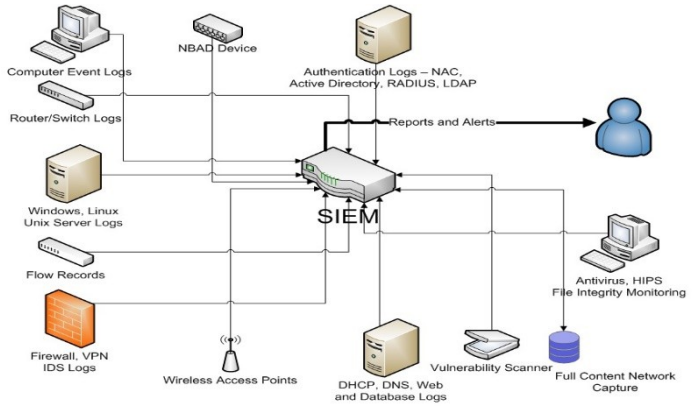
Firewalls are placed at the borders between different networks. In a DCSA, they are placed between Security Zones and Security Levels.

All communication should pass through firewalls when propagating into another Security Zone or Security Level.

Next

NPP Computer Security - SIEM

- Tasks (it is all about logs…)
  - Collect
  - Store
  - Analyze
  - Report



- Sources of information (the more the merrier…)
  - Full packet capture
  - Network devices: firewalls, routers, switches, vpn terminators …
  - Servers: web, email, domain controller, file, dhcp …
  - Security devices: AV, IPS…
  - Other: host event logs, PPS, NAS, SAN …

Next

NPP Computer Security – an OT SIEM?

- **Benefits**
  - **Know what is happening in the OT side from a cyber view**
  - **IT and OT data and anomalies can be correlated**

- **Drawbacks**
  - **Requires special knowledge (IT&OT) to operate**
  - **New connections may be required**
  - **Attack against IT or SIEM can influence OT part**

Next

NPP OT SIEM - Overview

A SIEM is used to help in the detection and response of cyber-threats.

It aggregates network logs and alerts in a centralized location. Events from different sources can be correlated to detect potential intrusions. Can be used in forensic analysis.

SIEM deployments are generally commercial products each with their own advantages and disadvantages. SIEMs are generally built for IT systems, however new OT SIEM products are starting to be developed.

An OT SIEM will incorporate data collect from industrial process networks to gain a more holistic view of the security in an Industrial Control System (ICS).

Next

NPP OT SIEM – Data sources

There are two major categories of data:

Data about the physical process and data about the control components.

Data about the physical process contains set points, sensor readings and the state of actors.

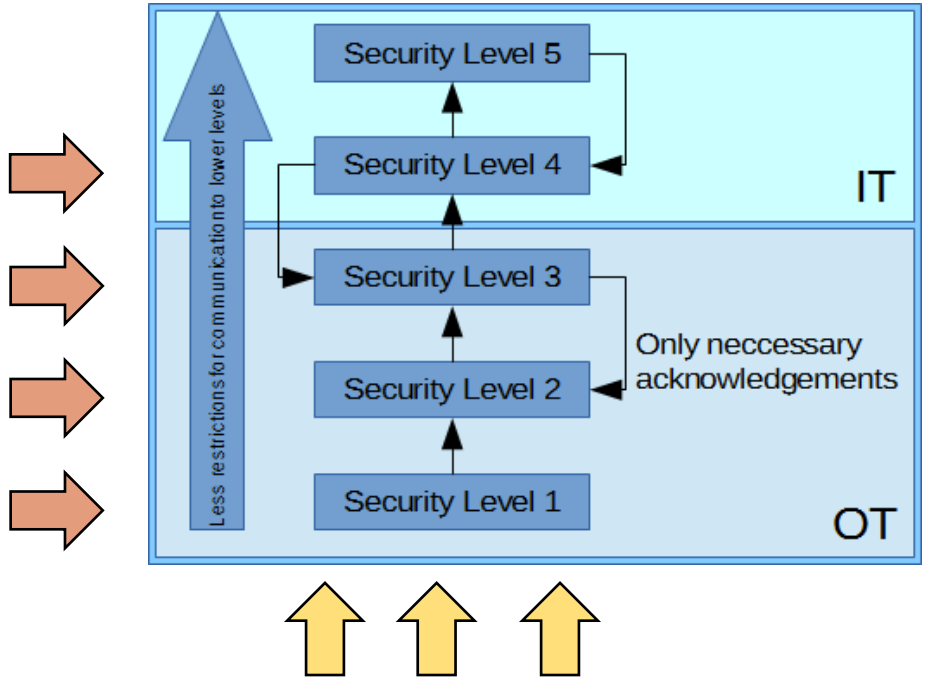
Data about the control components contains data which is similarly found in IT (such as log messages from components, firewall and switch logs) and and new traces including industrial communication protocols (Industrial Ethernet-Based: Modbus/TCP, OPC UA, OPC DA, S7comm, …; Field Bus-Based: Modbus, Profibus, CAN, …)

Next

NPP OT SIEM – Data sources

How to place sensors

On Vital Systems and Protocol Converters – e.g. Historians



Between Security Levels

Between Zones on the same Security Level

Next

NPP OT SIEM – Data sources

An OT SIEM would ideally reside within a Security Operations Center (SOC) dedicated to the OT network in an ICS

An OT SIEM is connected to the controllers and sensors in the OT operations network. After tuning the OT SIEM for the operations environments, anomalous OT traffic and events will signal alerts.

The OT network is ideally isolated from traditional IT networks behind firewalls and data diodes

Next

NPP OT SIEM – Data storage

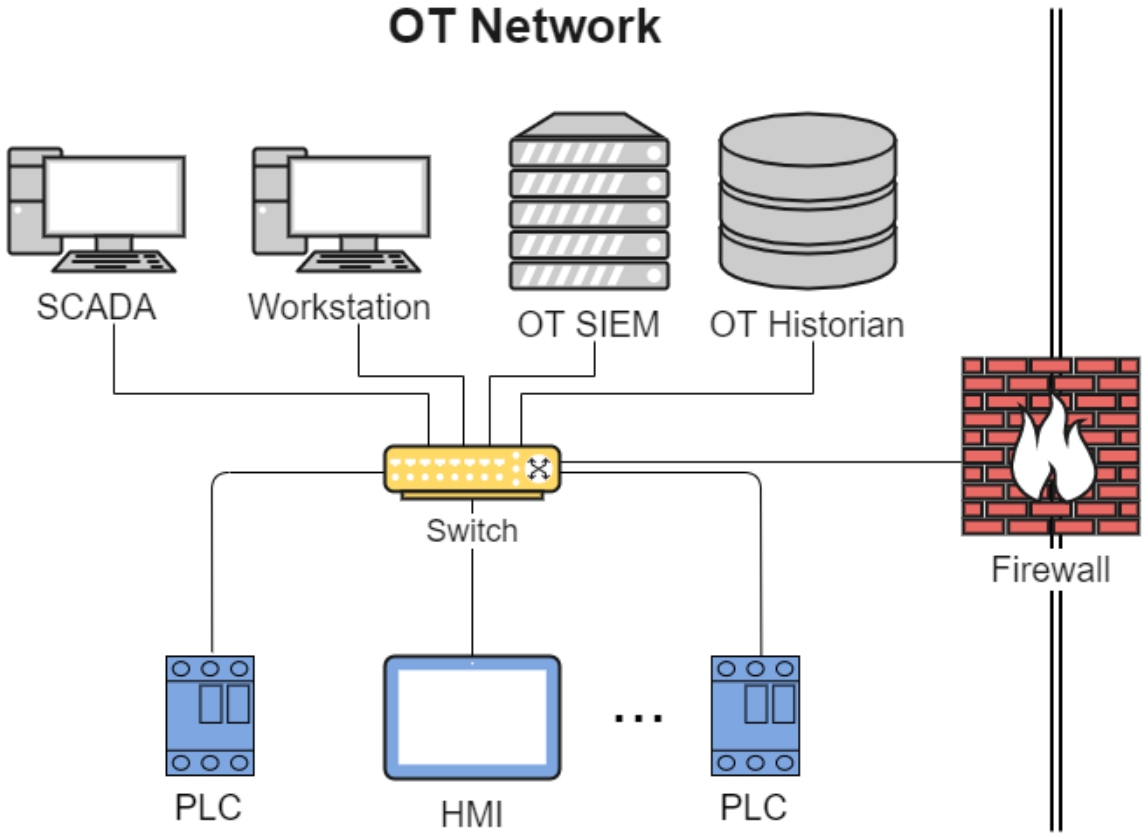
To aid in forensic analysis the OT SIEM should store all historical OT processes in an authentic, integer and confidential way for a long time. The retention length will vary by organizational policies and resources.

A dedicated database can be used to store historical OT data. The database could be backed up at regular intervals. Technological methods to ensure authenticity and integrity (like Hash Message Authentication Codes and Hashes) shall be used. As the information stored in such a database is critical, it should be encrypted in a way to ensure long-term confidentiality.

The OT SIEM database should be isolated from the IT SIEM database, however a seperate integrated IT/OT SIEM could be deployed.

Next

NPP OT SIEM – An Example seen during CRP J02008



Next

Summary and Outlook

An OT SIEM can help to detect and investigate cyber-attacks by aggregating and storing information from the process network within an NPP.

An OT SIEM has to be constructed in a manner to not interfere with plant operations. Here, planning and dedicated communication lines and systems are required.

The SIEM should store the gathered data in a secure (authentic, integer and confidential) way.

A first example of an OT SIEM was successfully tested during CRP J02008.