Segregating the ICS-OT "Insecure by Design" Architecture

Author: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Introduction

Industrial Control Systems (ICS)/Operation Technology (OT) experts are already in-agreement with the statement that ICS-OT and IT systems must be separately designed, deployed and assessed to verify their operation performance. Upon completing such testing, they can be securely interconnected, but must never be built as "converged networks".

Among the typical incidents, you find attacks that impact only the IT operation or may directly or indirectly also affect the industrial process, which might cause operation outage, damage and risk lives. To effectively protect industrial and utility plants, you must deploy SRA (Safety, Reliability, Availability) related defense measures. In some cases, these measures must also satisfy the data confidentiality related requirements.

Following the growing number of vulnerabilities detected in Programmable Logic Controllers (PLC), to minimize the risks created by exploitable vulnerabilities, experts now consider deploying segregating appliances within the ICS-OT zone. The open, yet-to-be-answered question is whether ICS-OT cyber security architects are allowed to deploy segregating devices within that zone. This paper aims to help the readers to understand the applicable considerations for correctly deployed segregation within the ICS-OT system.

Why is the ICS-OT considered as "Insecure by Design"?

ICS-OT architectures were designed to assure operating SRA and cyber security and data confidentiality were among critical requirements. In case an adversary gains access to a PLC or a remotely located smart device, the manipulated code might proceed to the control server and cause a failure. ICS-OT were traditionally air-gap-isolated, so cyber-attacks affecting the process were not among considered risks. This situation dramatically changed, after the Stuxnet attack in 2010, because that incident was an unexpected, internally generated attack, caused by inserting a malvertized appliance directly into the control zone. Experts instantly learned that the control architecture allowed lateral movement of the malware within the affected ICS-OT system.

Consequently, the obvious question came up, "can we install segregating appliances to prevent lateral movement within the ICS-OT network"? The answer to that suggestion is not straightforward, because deploying cyber security to the ICS-OT zone must not generate SRA related risks. Here are two examples where such segregation may contribute to secured operation:

a) In ICS-OT architectures, where the Human-Machine Interface (HMI) computer operates only as a thin client that HMI can be segregated from the control server using a Firewall (FW).

b) Segregation among ICS-OT zones operating at different levels of criticality may prevent lateral movement of a malware inserted at a less protected/less critical ICS-OT zone.

The use of remote access for maintenance by 3rd party service providers generates a significant risk to SRA. In the past, obtaining an approval for maintenance-related remote access was not easy, and organizations preferred to spend more money for maintenance on-site. The COVID-19 virus worldwide, changed this approach because experts could not travel to customers' sites. Consequently, the assurance of business continuity required to allow remote access via the internet, and this situation led to the introduction of secured remote access methods.

Deployment of Segregation among ICS-OT zones

Whereas the SRA concerns are critical, deploying a segregating measure within the ICS-OT zone is not allowed. Therefore, segregation between the IT and the ICS-OT networks became the main solution to prevent a cyber-attack that might undermine the SRA. The two diagrams, shown in Appendix A and B illustrate examples for secured design principles.

a) If you consider segregation among two ICS-OT zones, confirm that they have no mutual/ logical /dependent relationship. If the answer is positive, you can deploy segregating measures to prevent a lateral movement of a malware that might be present in one of the zones.

b) If you consider an ICS-OT sub-zone that is required to transfer operational data only in one direction (for example, transferring data to an area that runs an "Expert Process"), a Data Diode can effectively segregate among these zones.

c) If you consider two ICS-OT sub-zones that are required to transmit critical operational data in both directions, a more accurate diagnosis is necessary to analyze what might happen in case a faulty segregating appliance stops the data transfer among these sub-zones.

- If the operation of two ICS-OT sub-zones requires bi-directional critical communication, a failure of the segregating appliance might lead to an unstable/unsafe operation, in such cases, do not deploy a segregating appliance among these sub-zones.
- If the operation of two ICS-OT sub-zones requires bi-directional communication and a malfunction of the segregating appliance might cause only loss of data but not unstable/ unsafe operation, you may deploy a segregating appliance among these sub-zones.

Fail Safe vs. Fail Secure

To minimize the risk caused by a cyber-attack, important to differentiate between these terms. In cases where a failure or an incorrect action by an authorized person or a cyber-attack might cause danger to lives, the system must turn to Fail-Safe mode. In other cases where the loss of critical data is the only concern, the system must turn to Fail-Secure mode. It is essential to emphasize again that operation safety is ranked as the highest priority for industrial plants. Finally, it must be strengthened here, that Cyber Security is a critical precondition to Operation Safety, and Physical-Perimeter protection is vital precondition to Cyber Security.

Conclusions

Understanding the principles listed above is critical whether we consider buying a new system, upgrading an existing one, or signing a contract with a 3rd party service provider. So, to be at least one step ahead of hostile attackers, how can we create a secured architecture? The IT and ICS-OT experts must contribute their knowledge toward deploying correctly designed cyber defense, and the role of the management is to allocate the needed resources.

@@@@@@

Daniel Ehrenreich, BSc. is a consultant and lecturer acting at Secure Communications and Control Experts (SCCE) and periodically teaches and presents at industry conferences on the integration of cyber defense with industrial control systems; Daniel has over 32 years of engineering experience with ICS and OT systems for electricity, water, gas, and power plants as part of his activities at Tadiran, Motorola, Siemens, and Waterfall Security. Re-selected as Chairperson for the **8th ICS CyberSec 2023** in Israel on 20-11-2023. *LinkedIn*

Appendix A

Figure 1 below outlines a theoretical ICS-OT architecture, divided into three zones, which includes components located at Purdue Levels (P.L.) 0,1 & 2. It includes the main trusted network (in the center), two types of remote sites, remote view by a service provider, mobile view devices, and more. The table below describes the main characteristics included in each zone.

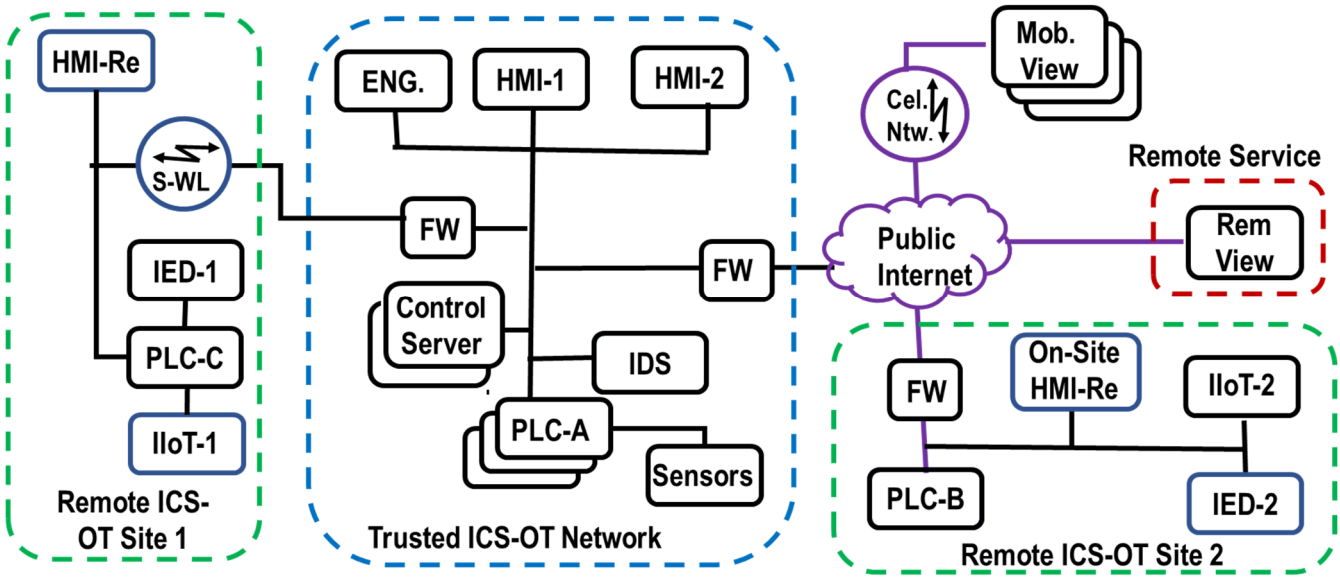

Figure 1. Illustration of the ICS-OT architecture

Components	PL	Description of the Characteristics
• Trusted ICS-OT zone	0,1,2	All components included in the ICS-OT zone, serving the main and the mostly critical processes.
• Eng., HMI-1, HMI-2	2	Responsible for programming and supervising the processes.
• Firewalls (FW) – (left)		Controlling the traffic to & from the trusted ICS-OT zone
• PLC-A & Sensors	1, 0	Responsible for on-site controlling the ICS-OT processes.
• Control Server	2	Responsible for central controlling the ICS-OT processes.
• IDS operation	2	Network-Based IDS (NIDS) for anomaly behavior detection
• Remote ICS-OT site-1	0,1,2	Remote, physically protected site, segregated by Firewall and a secure Wireless link (typically serving less critical functions).
• PLC-C	1	Responsible for controlling the processes at remote sites.
• IIoT-1 & IED-1(left)	0	Responsible for monitoring specific functions at the remote site
• Sec. Wireless Link		Responsible for encrypted communication to the remote site
• HMI-Re (left & right)	2	Allows monitoring of the ICS-OT process from remote sites
• Remote ICS-OT site-2.	0,1,2	Remote, physically protected site, segregated by Firewall and a public internet network (typically serving less critical functions).
• IIoT-2 & IED-2 (right)	0	Responsible for monitoring specific functions at the remote site
• On-site HMI Terminal	1	Allows monitoring of the ICS-OT process at the remote site
• Firewall (FW) (right)		Controlling the traffic from the internet to the remote site
• Remote Service Connection	2	Allows only remote monitoring/view of the ICS-OT processes. Segregated from the main ICS-OT zone by a Firewall
• Mobile device view via a cellular network.	1	Allows only remote monitoring/view of the ICS-OT functions. Segregated from the main ICS-OT by a Firewall

Appendix B

Figure 2 below outlines a theoretical ICS-OT architecture for an entire organization, which includes components located at Purdue Levels (P.L.) 0,1, 2, 3, & 4. It consists of the ICS-OT network and connected zones inside and outside the organization. The table below describes the unique, security-related characteristics of components included in each zone.

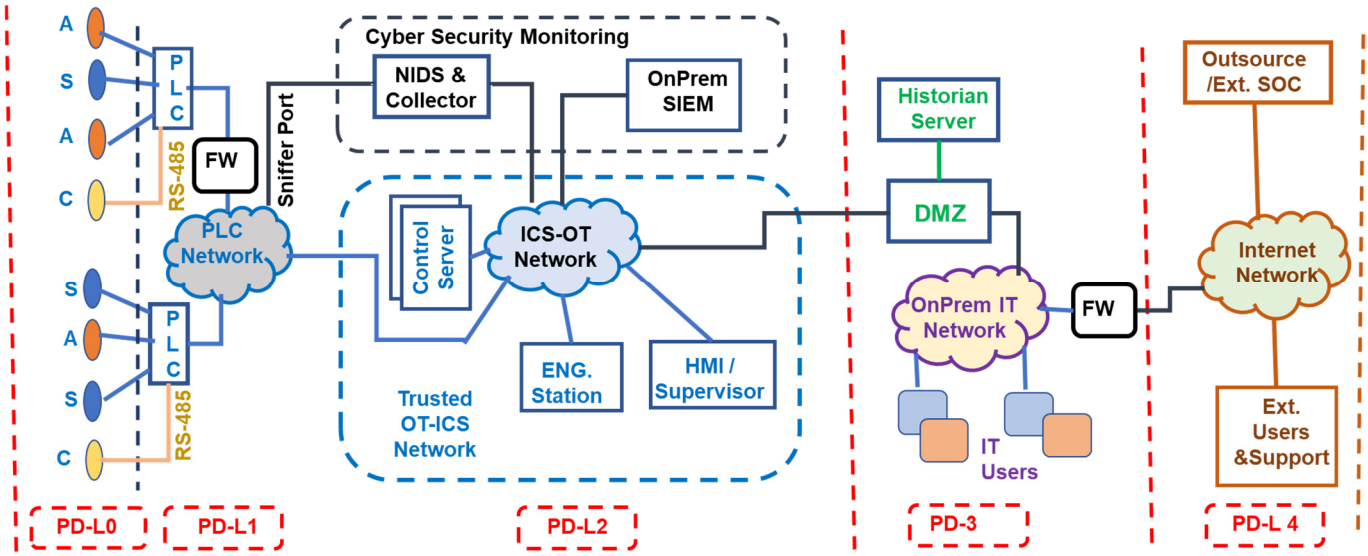

Figure 2. Illustration of a complete organization architecture

Components	P.L.	Description of the Characteristics
• PLCs and Sensors (left side)	0,1	The drawing shows two PLCs and sensors. One is directly connected to the ICS-OT. The other, less critical PLC and its sensors are segregated with a FW. That PLC must not run highly critical processes which depend on the FW's normal operation.
Trusted ICS-OT network	2	Here you will find all the components in the critical zone, which are directly connected to each other (without FW segregation). This zone is running the main process in the plant.
• ICS-OT appliances in the main zone		The Control Server directly manages the PLCs connected to the network. In addition, there are data collection devices for the Network Intrusion Detection System (NIDS) operation.
• External users' connection	4	External users/service providers are connected to ICS-OT zone of the architecture via Demilitarized Zone (DMZ). It serves as a secured segregation mechanism, much stronger than a FW.
• Historian Server for the ICS-OT & the IT	3	The Historian Server is protected by the DMZ, which performs segregation between the ICS-OT zone and the IT zone. It can be accessed from both the IT and the ICS-OT networks.
• Use of Firewall		The Firewall on the right side of the chart is segregating between the IT network and the ICS-OT network.
• Access for IT users to ICS-OT	3	In this architecture, IT users may access the ICS-OT zone via the DMZ, which allows secured 2-way data transfer.
• External Cyber security Services	4	The log-data is collected via the Security Information Event Management (SIEM) computer, and the organization may export it to a 3rd party Security Operation Center (SOC).