Searching Beyond Traditional Solutions for Protecting ICS

Author: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Introduction

Deployment of a strong and effective cyber defense for Industrial Control Systems (ICS) remains a challenge for experts worldwide. We all know the famous statement "there is no silver bullet", and therefore experts must search for innovative technologies beyond the passive Intrusion Detection System (IDS), however without violating important principles and limitations. Considering a solution which requires changing the ICS architecture or an Intrusion Prevention System (IPS) which might interrupt the process or a pen-testing of the ICS (similar to IT inspection), are all not appropriate choices. While being exposed to a broad range of ICS Cyber defense technologies for protecting manufacturing operations and critical utility infrastructure, even experts might face difficulties when trying to determine which one is right for a specific ICS used in their organization.

In this paper I'll describe four independent approaches, which may effectively help you reducing the ICS cyber-attack risks against your organization. Selecting the right method must take into consideration your architecture, the level of probability and the impact of an attack.

Secure Authentication for ICS Networks

Nowadays, ICS networks are required to be securely connected both to corporate networks and occasionally also to external entities. Enforcing secure authentication to systems like Engineering Workstations, Human Machine Interface (HMI) station and various servers is a critical security measure to prevent unauthorized access. Advanced Multi-Factor Authentication (MFA) solutions can hardly be deployed in these environments because they require software agents on each computer, deployment of inline proxies in OT networks, or code changes. Furthermore, in many cases and a wide range of applications there is no support for legacy ICS that is commonly found in these environments.

The preferred solution shall be based on use of an authentication server, capable of enforcing MFA on any sensitive system without requiring software agents, proxies or code changes. That authentication service shall require users to validate their identity with an authentication solution like a one-time password (OTP). That solution may also be installed within the supervisory control LAN or a layer above that. Again, the most important requirement shall be that no change to the system architecture is required and the enhanced authentication shall be completely agnostic to type of commuters, control devices, software vendors etc.

Deployment of a Deception technique

Typical ICS cyber defense involves several protecting layers, including a range of technologies such; as firewalls, DMZ, unidirectional gateways, authentication, encryption, anomaly conditions' detection, visibility analysis, but even a combined set of these is not expected to deliver absolute defense.

Deception technologies, also known as "honeypot", may distract the attacker from his search for the critical PLC and guide him to the zone where the attack action can be detected and quarantined. There are few high concern topics which the cyber engineer shall evaluate: a) select the layer within the Purdue model, where the deception mechanism shall be optimally installed, b) how the alert created by the deception mechanism shall be communicated, c) at which priority level shall this defense method be selected, etc.

Using this method: a) it shall not create a "strong noise" attracting attackers to your organization, b) you cannot not place it in the DMZ where critical functions are processed, and c) you will also not put it within the ICS, where the attacker might by "mistake" detect the real system while being "guided" to the deception zone. Naturally, there is no firm nor a best answer to these difficult questions and each system architect will have to make the own decision matching the specific system architecture and the level of risk.

Sensor's signal analysis.

ICS related sensors (at Purdue level o) measuring: temperature, pressure, flow, line voltage or current, vibration, etc. are typically measured according to resolution of the analog conversion. If the normal value of a specific parameter is in range of 30% to 60% of the maximum, it means that within that range it will be indicated by the Programmable Logic Controller (PLC) as normal. However, if the measured value is frequently fluctuating within the normal range, a legacy-type PLC might mistakenly consider it as a normal condition. During this period, the turbine, compressor pump or steam boiler might go through a severe stress, which might lead to a severe malfunction, operation outage, damage or even a safety incident.

Adding a 2nd or redundant PLC, using an out of band media, (monitoring the same sensor) but capable of high-speed sampling allows detecting the faulty condition, which the legacy-type PLC missed. Such detection is practically not hackable by software tools and provides a "parallel reference" for validating sensor's health and also allow more granular ICS process optimization. Enhanced signal sampling and analysis can be deployed using a separate / compatible sensor operating in parallel to the original device.

Important mentioning here, that deployment of such solution can be done without lengthy interruption of the ICS operation (just few minutes), and it does not require performing changes in the standard PLC process. Furthermore, such enhancement contributes to reducing maintenance cost reach higher operation safety.

PLC programs' verification

Passive ICS assessment provides a series of important indications including detection of unauthorized components, details on hardware and software versions, characteristics of the communication sessions among computers and PLCs, etc. But, is this enough for detecting an internally generated attack caused by unauthorized connection directly to the ICS network? For sure not, and cyber security experts need additional measures for detecting a manipulated configuration within a PLC.

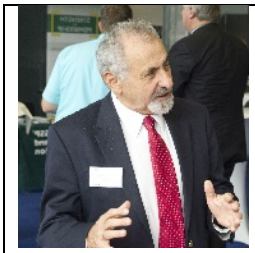
This process requires uploading the configuration and the application program files from the PLC (compiled or the run-time code) to a service computer and comparing these files to the genuine files, which are stored exactly for these purposes. Important noting that doing it "on the fly" during the normal production may be considered as an active intervention (!), which is not allowed. Therefore, you must evaluate the risk to the operation safety if that process is considered. Prior starting that inspection, it is recommended that you consult with the PLC hardware and software vendor and also with the ICS integrator.

Summary

In this article I evaluated four cyber defense methods which can be considered beyond the traditional visibility analysis. No matter which method you consider, the decision must take into consideration the structure of the ICS architecture, the probability of occurrence and the potential harm caused by an attack. While the cyber defense for IT-type system is selected according to CIA considerations (Confidentiality-Integrity-Availability) triad, for the ICS, in addition you shall consider the SRP (Safety-Reliability-Productivity) triad.

The CISO and the C-level in every organization shall conduct proactive analysis of applicable technologies for mitigating the risk of cyber-attacks as much as possible and assure business continuity.

@@@@@



Daniel Ehrenreich, BSc. is a consultant and lecturer acting at Secure Communications and Control Experts, and periodically teaches in colleges and present at industry conferences on integration of cyber defense with industrial control systems; Daniel has over 27 years of engineering experience with ICS for: electricity, water, gas and power plants as part of his activities at Tadiran, Motorola, Siemens and Waterfall Security. Selected as the Chairman for the ICS Cybersec 2019 conference taking place on 24-9-2019 in Israel and for the Asia ICS Cyber Security conference taking place in Singapore on 27-11-2019. *LinkedIn*