CONTROL
PROMOTING EXCELLENCE IN PROCESS AUTOMATION



# Unfettered Blog

Control Systems Cybersecurity Expert, Joseph M. Weiss, is an international authority on cybersecurity, control systems and system security. Weiss weighs in on cybersecurity, science and technology, security emerging threats and more.

## Changing the paradigm of control system cyber security

Submitted by Joe Weiss on Sun, 06/10/2018 - 18:57

Control system cyber security is to prevent impacts on reliability, safety, productivity, and/or regulatory compliance. Preventing compromise of data for any other reason is an IT function. Monitoring of control system OT networks is necessary, but NOT sufficient, to protect control systems and processes.

Process sensors (they are NOT OT) are the input to all control system OT networks yet have minimal, if any, cyber security or authentication. However, the process sensor packet is ASSUMED to be "gold" and deep packet inspection and other OT network monitoring techniques are used to assure the packet isn't compromised. The OT network monitoring also erroneously ASSUMES the anomaly detection correlates to actual system impacts because the OT network does not have the capability to DIRECTLY monitor the process. The paradigm shift would be to monitor the electrical characteristics of the process sensors (e.g., pressure, level, flow, temperature, voltage, current, etc.) which provide a direct view of the process. Monitoring of the electrical characteristics of the process sensors identifies the actual state of the process sensors and the process which provides a level of trust as electrical characteristics can't be hacked. Correlating the process sensor electrical characteristics to network anomaly detection can help determine if the actual system impacts are cyber-related.

Cyber security of process sensors has effectively been ignored. The ICS CERT vulnerability disclosures have been on IP-network connected devices not on process sensors. Additionally, there is no discussion about the actual process impact of the ICS CERT disclosed vulnerabilities. Situational awareness is dependent on the validity of the process sensors. If the process sensors are either inaccurate or compromised, situational awareness is suspect. Therefore, the cyber security driver for monitoring the electrical characteristics of process sensors is to plug the hole that currently exists with the lack of cyber security and authentication of process sensors (and process sensor networks) and the resulting impacts on situational awareness.

The process sensor cyber security issue is partly due to the unintended consequence of the filtering done by the serial-to-Ethernet convertors (gateways) that transform the analog sensor values into Ethernet packets. The transformation effectively filters out the electric characteristics (process noise) BEFORE the process sensor values become Ethernet packets which is why the OT networks cannot directly monitor the process. Additionally, there have many cases where the gateways themselves have been compromised leaving a path directly into the sensors (numerous ICS cyber vulnerability disclosures including the "bricking" of gateways in the 2015 Ukrainian grid cyber attacks). Process and process sensor failure modes from instrument drift, flow-induced vibration, plugged sensing lines, cyber attacks, or supply chain issues are found by monitoring the process noise which won't be seen by the Ethernet packet. As existing process sensors and sensor networks have essentially no cyber security or authentication, it is possible to hack process sensors before they become Ethernet packets and the OT network anomaly detection systems would not be aware nor would the PLCs or HMIs (a demonstration of hacking an ANALOG sensor is currently being prepared).

Process sensor cyber-related issues (doesn't have to be malicious) can, and have, caused catastrophic damage and

injuries/deaths yet were not identified as being cyber-related. Examples of catastrophic failures from process-sensor related cyber issues include the Buncefield tank farm explosion, the Texas City refinery explosion, and the Taum Sauk dam collapse. It should be obvious that detecting process sensor issues that can cause these types of problems before the catastrophic failures are important whether the cause is malicious or unintentional. Without monitoring the electrical characteristics of the process sensors, it may not be possible to effectively monitor the system before the catastrophic failure or to have post-event forensics to determine if the event was malicious or unintentional.

Cross-correlating the electrical characteristics of “like” sensors (e.g., pressure, level, flow, temperature, and motor speed) in real time provides a new capability to change the paradigm of control system cyber security as well as reliability, availability, productivity, and safety monitoring. The monitoring of the electrical characteristics of process sensors is not a new idea. I was doing this analysis more than 25 years ago to monitor sensor health, flow-induced vibration, pump vibration analysis, loose parts monitoring, core barrel motion, and post equipment failure forensics in nuclear power plants. At that time, the monitoring was a snapshot in time. Modern machine learning technology and the ability to monitor sensors in real time have provided a new capability to improve cyber security, system reliability, process safety, productivity, and regulatory compliance.

The benefits for monitoring the electrical characteristics of the process sensors include:

- Electrical characteristics of process sensors are independent of the type of process being monitored and cannot be hacked. This improves cyber security, reliability, productivity, and process safety.

- Monitoring electrical characteristics of the process sensors are independent of the HMI providing additional redundancy and resiliency. With Stuxnet, when the man-in-the middle attack compromised the HMI, sensor monitoring of the electrical characteristics would have identified that motor speed and flow sensor characteristics were changing which was inconsistent with the compromised HMI indicating nothing was changing. The Taum Sauk dam failure is an example of an unintentional incident where process level sensors changed condition as the wall attachments broke. The erroneously low level signals were not identified by the HMI as such and directly led to overfilling a reservoir and the resultant dam collapse. Monitoring the electrical characteristics of the level sensors would have identified a distinct change when the sensors' elevation changed as they pulled out from the wall.

- Monitoring electrical characteristics provides confidence in the data input to network anomaly detection, process historians, predictive maintenance programs, and first principles models.

- As sensor monitoring is independent of the network, zero days and other advanced cyber threats including supply chain compromises become a secondary concern for operations. If the process sensors aren’t changing in an unexpected manner, cyber threats are not an immediate concern and operational decisions can be made as process conditions dictate.

- As process sensors have no cyber security, cyber vulnerability assessment methodology is not appropriate. However, monitoring the electrical characteristics of the process sensors provide a real time “vulnerability/state” assessment of the sensors and the process. By knowing the state of the process better, it is expected that the real time monitoring may be used to justify extending very expensive testing intervals.

- Cross correlating the electrical characteristics of process sensors in real time can effectively provide sensor health monitoring.

Control systems are engineering systems and need to be monitored accordingly. Monitoring of the electrical characteristics of the process sensors can provide early indications of malicious or unintentional problems as the impacts can be similar.

Joe Weiss
833 reads

Permalink

Show Comments

## Free Subscriptions

E-Newsletters | Digital Editions

### controlglobal.com E-Newsletters

Biweekly updates delivering feature articles, headlines with direct links to the top news stories that are critical to staying up to date on the industry — company news, product announcements, technical issues and more. Subscribe Today.

## Most Popular

Past 7 Days | Past 30 Days | Past 6 Months | All Time

01 Is your SIS getting the job done?
Grandfathered systems now require a formal determination of adequacy

02 American Association of Water Distribution & Management (AAWDM) critical infrastructure video
The water industry doesn't have an organization that specifically…

03 Slip rings use CC-Link IE for gigabit data transfer
Conductix-Wampfler has chosen CC-Link IE open gigabit Ethernet to provide…

04 Data cable solutions for the flourishing smart factory

05 Winsted's Impulse Dual Sit/Stand Consoles


PutmanMedia®