MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

74th Annual Instrumentation and Automation Symposium
For the Process Industries
January 22-24, 2019 | College Station, Texas

Changing the Paradigm of Control System Cyber Security - Monitoring Process Sensor Health

Joe Weiss PE, CIS, CRISC
Applied Control Solutions, LLC
Cupertino, CA
joe.weiss@realtimeacs.com

Amir Samoiloff, CEO
SIGA OT Solutions
Beersheba, Israel
amir@sigasec.com

Abstract

Process sensors are the input to all controllers and HMIs to safely and reliably monitor and control a process. Network cyber security anomaly detection systems assume that process sensors provide secure, authenticated input, however, there is no cyber security or authentication in these devices or device networks. One approach to address the intersecting issues of reliability, safety, and cyber security is to understand the validity of the sensor input by monitoring in real time the electrical characteristics of the process sensors before they become Ethernet packets. This monitoring provides multiple benefits including identifying sensor drift or sensors out-of-calibration, providing a basis for extending calibration/testing intervals, and providing a basis for continued operation when network monitoring identifies cyber vulnerabilities. Process sensor cyber concerns are not idle considerations as there have been multiple catastrophic failures from process sensor-related events. This presentation will provide case histories to demonstrate how monitoring the electrical characteristics of the sensors can improve cyber security resilience, identify previously unknown sensor problems, and improve safety. It can also make an intractable network cyber security problem a tractable engineering solution, changing the paradigm of control system cyber security by making it a reliability and safety issue with cyber security "coming along for the ride."

Keywords: Process sensors, cyber security, safety

Process Sensor Background

Process sensors detect events or changes in their environment and convert the magnitude of a physical process parameter into an electrical signal (Figure 1).

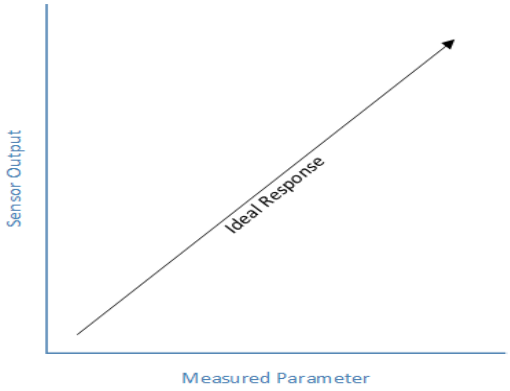

Figure 1 Ideal Sensor Response

Electronics then change the electrical signal (e.g., 10 milliamps) into a process variable (e.g., 50 psi). The electrical signal needs to be sent timely and accurately as it represents the true measurement of that parameter applied to the sensor. Generally, the sensor response is assumed to be from the sensor (not altered or modified) and accurate. However, these assumptions may not be appropriate, as legacy process sensors have no authentication (Is the signal really coming from that sensor?) and may be inaccurate (sensor drift, miscalibration, cyber attack, etc.)

As process sensors are physical devices, their accuracy may vary over time due to manufacturing processes, environmental conditions, material degradation, electronic component drift, or other reasons. Sensor drift can have significant impacts. Because of sensor drift, a major pipeline organization had a PLC shut down, causing $1.9 million in lost revenue because the deviation over time was so small, it wasn't noticeable from the HMI. This degradation in accuracy requires periodic calibration to a known source to assure adequate sensor capabilities (accuracy of data, timeliness of data delivered, etc.). Calibration adjustments for sensors usually involve two parameters: Zero and Span. The Zero adjustment sets the output signal to 0 Vdc when the process condition applied to the sensor is 0. The Span adjustment is used to set the output signal to full scale. (Figure 2)

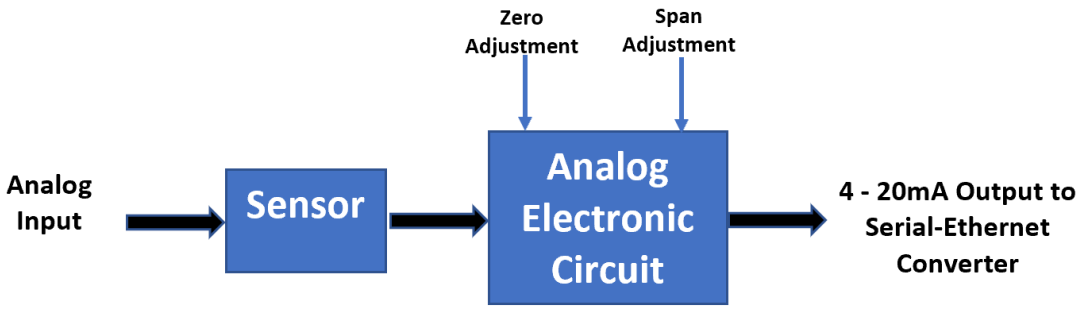

Figure 2 Process Sensor Configuration

Process sensor noise is generally a result of technology used to sense or measure the process variable. The raw sensor electrical signal consists of a spectrum of frequencies. Higher-frequency components are indicative of physical conditions such as vibration, Brownian motion, etc., and are indicative of the health of the sensors and their process. Consequently, it is important for sensor noise to be monitored. The previously mentioned case with the drifting sensor could have been detected by monitoring the process noise of the sensor. The signal conditioning, such as amplification and filtering (with multi-second refreshment rates) through the serial-Ethernet converters, filters out useful information, preventing the ability to understand sensor and process health. Consequently, the information about any discrepancy of the sensors relating to the process is not available for network anomaly detection comparison.

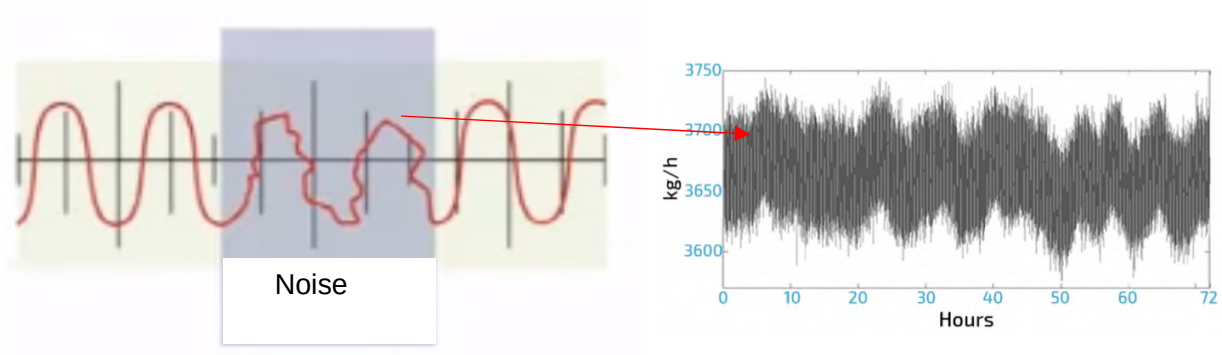

Figure 3 Sensor Electrical Signal Filtered and Raw Sensor Signal

Previously, this analysis has only been used for historic comparisons for incidents; however, as technology advances, it is now possible to have comparisons performed more accurately in real time.

Current Status

Sensors, valves, and motors have smart electronics and send serial data (4-20 mA) to the serial-Ethernet converters where data packets are produced and sent onwards through the IP network. The raw signal and its higher-frequency components (Figure 4) are filtered out by the gateways. Network monitoring starts from the serial-Ethernet converters (also known as “serial gateways”) where Ethernet IP data packets are created from analog data from the field devices with the higher-frequency noise filtered out. The network monitoring systems therefore only monitor the data packets, and network anomaly detection has no other option but to assume that the sensor provides the correct information, is authenticated (actually comes from the sensor), and is uncompromised.

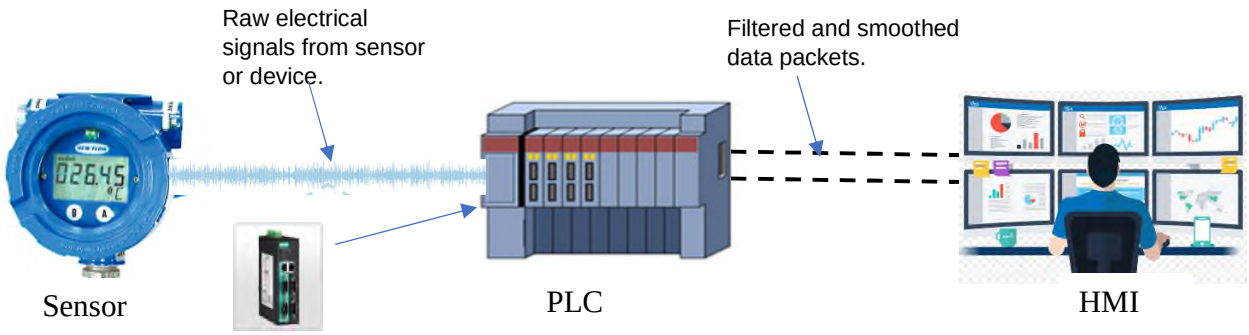

Figure 4 Process systems with network anomaly detection

If the Zero or Span adjustments are manipulated, then this could potentially prevent a sensor from ever reaching a set point or to reach a set point long before it should. The network anomaly detection would not be able to detect such changes to Zero and Span whether authorised or not. As stated above, the sensors, valves, and motors have no security and no authentication. The serial-Ethernet convertors can -- and have been -- compromised, as they were in the 2015 Ukrainian cyber attack[1] where access was allowed to these unprotected field devices.

The assumption is the sensor value is correct and authenticated. Consequently, there is a need to check the raw sensor data before it becomes network packets. A major shortcoming in most industries is that although there is no way of correlating malware to physical impacts (i.e., detecting differences between process readings and the conditions the network is reporting or believes to true). There is a need to be able to look at the process, cross correlate it to the network anomaly, and be able to determine if there is malware and that the process is changing. Assuming the process is working as expected in real time, there is no need to make changes despite what is coming from the HMI, as opposed to today when there is no real-time, unmodified view of the process.

There is, therefore, a flaw in the network monitoring confidence levels, which will not allow a true risk-based assessment to be made ifmalware is discovered on the network when there might not actually be any issue with the process. Higher confidence levels will be achieved when the process can be correlated to the network anomaly.

A petrochemical facility was investigating opportunities to increase processing uptime and optimize unit production. As part of the investigation, the company focused on operator workload and the effectiveness of the existing alarm system. Several areas stood out as opportunities for improvement. Addressing field-related issues, which were typically instrument failure or improper ranging of scale, could reduce nuisance alarms by 50%.[2]

[1] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

[2] Optimize Alarm Management - Chemical Processing November 2018 Hiroaki Tanaka Yokogawa Electric

https://www.securityweek.com/ics-security-experts-share-interesting-stories

A risk assessment of this vulnerability is required for each process plant. It is envisaged that HAZOP, CHAZOP, LOPA, FMEA and reliability studies, as well as cyber-specific studies, will be drawn upon to identify a number of critical field devices for which sensor health technology should be installed.

Process Sensor Cyber Security

The unofficial Information Technology (IT) definition of a cyber incident is, the system is connected to the Internet and is using Windows, and the attacker is maliciously compromising the data. Effectively, this is referred to as "Information Assurance." This also implies that all cyber vulnerabilities are important and need to be expeditiously addressed regardless of any process system impact. Yet, the most important factors for plant operations are reliability and safety – not data. The NIST definition of a cyber incident in FIPS PUB 200 is: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." This definition is more relevant to the ICS community with one critical modification: the definition needs to add the letter S (Safety). It is also important to note that the term "malicious" is not mentioned in the NIST definition. Effectively, this is Mission Assurance, which means cyber vulnerabilities are important if they can impact the mission. The additional reasons for not using the term malicious is the lack of adequate ICS cyber forensics as well as lack of sufficient ICS cyber security technologies. In many cases, the only difference between an incident being malicious versus unintentional is the motivation of the individual involved.

These are not idle considerations. Process sensors have been hacked and the PLC and HMIs have been unaware. In one case, a process sensor was maliciously hacked and a turbine was unable to synch to the grid. In another case, a combustion turbine was unable to restart because a temperature sensor was bad (not malicious, but that's irrelevant). The serial-to-Ethernet convertors that convert the process sensor analog signals for use in an IP network are a "two-way street" into the sensors as well as the networks, and have been demonstrated to be vulnerable. Changing sensor configurations can affect reliability (prevent restart) or safety (remove equipment protection) with minimal forensics.

Correlation of Safety and Security

Industrial deployments are designed with process sensors (e.g., temperature, pressure, level, flow, voltage, current, etc.) to monitor and feed interlocks to assure that system safety is maintained. However, legacy process sensors have no cyber security or authentication, and adequate real-time process sensor forensics are generally unavailable. An example is the temperature sensors that monitor turbine/generator safety systems to prevent generators from operating in unstable or unsafe conditions. These process sensors are integral to the operation of the system and cannot be bypassed. If the temperature sensor is inoperable for any reason, it can prevent the equipment from restarting, whether in automatic or manual.

Legacy field level devices include process sensors, drives, actuators, analyzers, and power supplies. These devices and their low-level networks (e.g., Wired and Wireless HART,

Foundation Fieldbus, Profibus, ProfiSafe, serial Modbus, etc.) are considered to be engineering systems and reside in what is typically classed as Purdue Reference Model Level 0 and 1 (Figure 3).

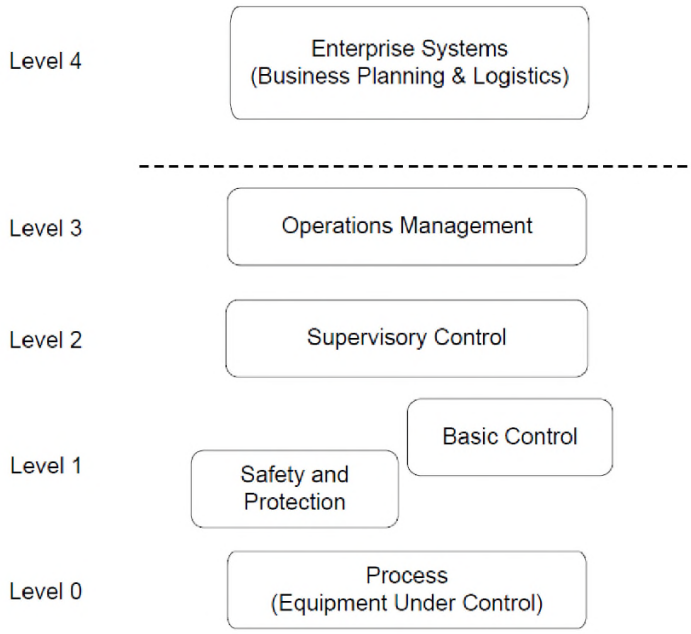

Figure 3 ISA Purdue Reference Model[3]

As safety and security are related but not the same, it raises questions about the term "risk." For example, in one plant, an installation utilized hardwired, certified trip amplifiers to connect the analog sensors to the safeguard analog final elements. In the second plant, the installation utilized a certified programmable electronic logic solver utilizing a broadly applied computing operating system to connect intelligent sensors to the safeguard final elements with built-in webservers. From a safety perspective, the risk to both are the same, but from a security perspective, the risk would be different (Figure 4).

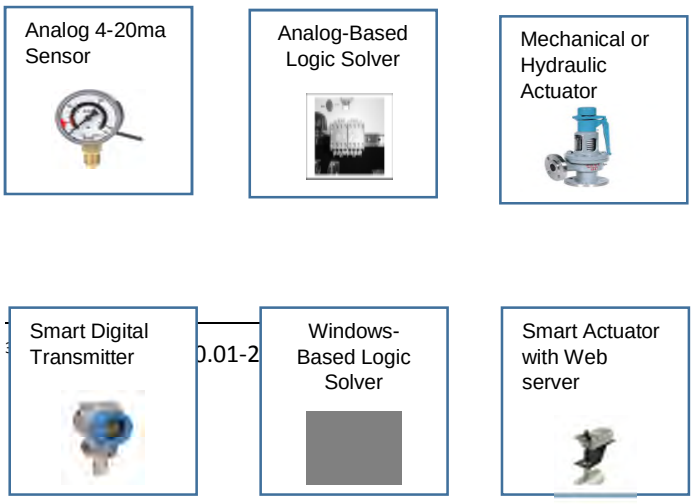

Figure 4 Differences in cyber security in safety systems

Operational Technology (OT) is generally viewed as the control system networks. not the field-level devices, which are engineering systems. In many systems that focus on safety and reliability, there is no means of sensor validity nor forensics at the physics layer before the creation of network packets.

There have been numerous catastrophic (upwards of several billion dollars) control system cyber incidents, many of which have resulted in injuries and deaths. In general, in many cases, these accidents have not come from network problems, but from compromises or problems with control system devices. The real safety and reliability impacts come from manipulating physics, not data.

In a physical-cyber world, threats are not just about protecting the network and consideration must also be given towards protecting the operational systems/process. Many assume process sensors are secure, authenticated, and correct. No matter how well secured communications are, if the sensors and actuators that constitute the ground truth of any industrial process are compromised or defective, it will not be possible to have a safe, reliable, or optimized process. Consequently, not only do cyber security standards such as the IEC62443 series of standards need to be assessed for applicability to legacy field devices (this was done via ISA99WG4TG7), so do safety standards such as ISA84.

The purpose of control system cyber security is to protect the control systems and the processes they monitor and control. Networks are a support function in the overall objective of safety, reliability and productivity. Existing cyber security and safety standards do not adequately address the security and authentication vulnerabilities of legacy field level devices and their networks.

Industrial control systems consist of process sensors connected to controllers, actuators, and HMIs (effectively, the control system network). The sensors and actuators operate almost exclusively in near-real-time (microseconds to milliseconds), whereas the HMI provides operator information on the order of seconds to minutes. The sensors and actuators can operate, and in most cases were designed to function, without the IP network. Figure 5 provides a representation of the equipment and information flows in a typical process system from the Process (Level 0) to the ERP (Level 4). Equipment Under Control (EUC) is controlled by sensing parameters and having field devices such as valves and drivers act upon those measurements to both control the parameters in the EUC and detect conditions in which to shutdown on abnormal conditions. These sensors, valves, and drivers are generally classed as Level 1 devices or Level 0 edge devices in the reference model (Figure 1). Safety is dependent on the Level 0 - 1 devices and instrumentation networks as well as the higher-level Internet Protocol (IP) Ethernet networks. Communications, the Control Centre and the ERP are generally controlled by the IT discipline and use Commercial-off-the-Shelf technology (e.g., Windows).

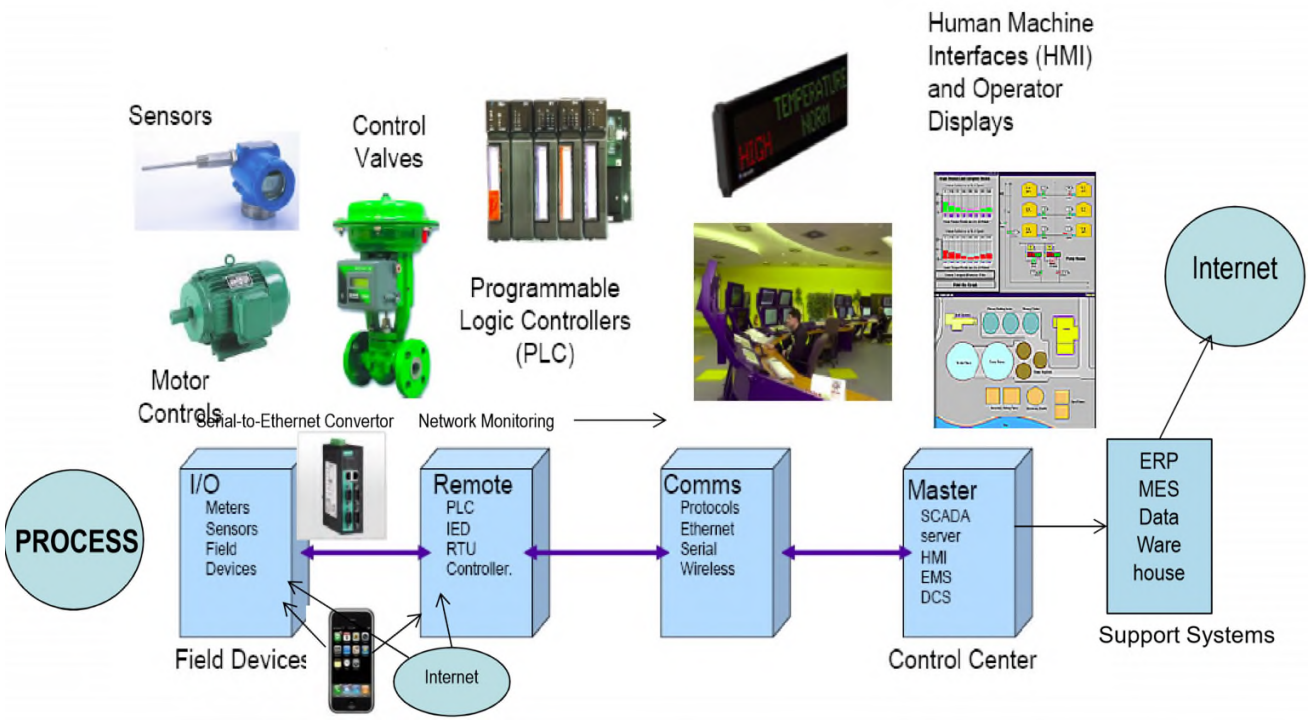

Figure 5 System Diagram from Level 0-4

The Level 0 - 1 sensor protocols, such as wired or wireless HART, Profibus, and Foundation Fieldbus, are cyber-vulnerable. There is not only no security in them but they were designed to be insecure from a cyber perspective with minimal cyber forensics. It is important that engineers understand this problem as a threat to safety and vulnerability to allow for action to be taken as early as possible when the process is starting to fail for any reason.

Another issue is that I/O cards allow instruments to communicate bidirectionally. Data diodes are not effective when smart sensors are in use as they are unidirectional. Smart sensors are digital and carry out all conversions at the sensor layer, and are bidirectional.

Changing the Paradigm of Control System Cyber Security

The current approach for control system security is to monitor the network for malware or other network anomalies. There are several concerns with this approach:

- There are many control system devices that have no cyber security, authentication, or cyber forensics.
- There are no means to correlate network anomalies with physical processes or individual pieces of equipment. That is, if there is malware, what does it mean to a specific pump, valve, motor, relay, etc.? Also, what does it mean to the process?

In other words, what actions should be taken if malware is detected? A network-based approach cannot provide this critical information. Consequently, there is a gap in the network monitoring

confidence levels, which will not allow a true risk-based assessment to be made when there is the discovery of malware on the network and there might not actually be any issue with the process. The approach to assure the process is performing as required is to monitor the process sensors in real time (within milliseconds). Cross-correlating "like" (similar) sensors, such as pressure, level, flow, temperature, and motor speed, can minimize false negatives and false positives. Higher network monitoring confidence levels can be achieved when the process can be correlated to the network anomaly.

A risk assessment of this vulnerability is required for each process plant. It is envisaged that HAZOP, CHAZOP, LOPA, FMEA and reliability studies, as well as cyber-specific studies, will be drawn upon to identify a number of critical field devices for which sensor health technology should be installed.

Process Sensor Monitoring Case Histories

Real-time process senor health monitoring needs to start with the raw sensor signal (Figure 6).

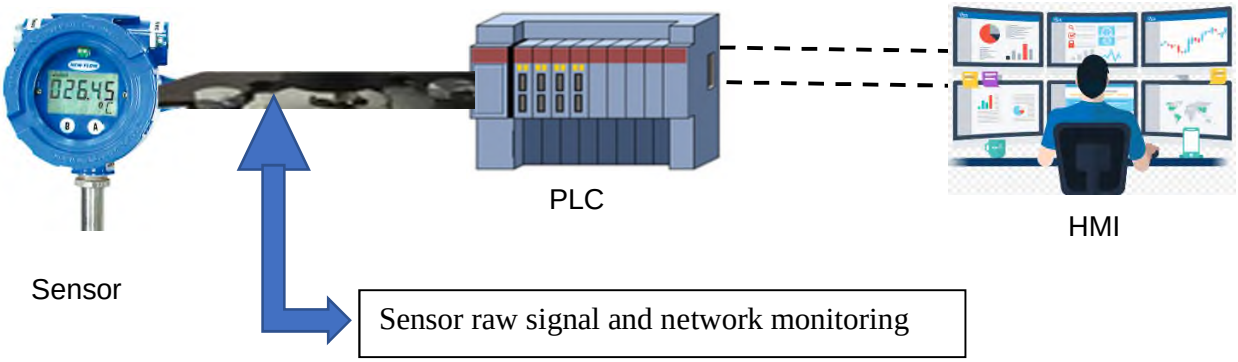

Figure 6 Process Systems with Network and Sensor Health Anomaly Detection

SIGA OT Solutions has developed sensor health monitoring of the raw sensor data, and has implemented the technology in actual field applications. The following case histories highlight the value of this type of monitoring:

1) A power utility gas turbine failed to stabilize and deactivated upon fuel feed from both automatic and manual restart. Even after replacing a control card on the main controller, the situation could not be remedied. A costly turbine outage was scheduled. Monitoring the raw sensor data showed an activation cross-fire (bad temperature sensor) that was not visible from HMI. The resulting adjustment allowed for safe turbine activation without costly outage. The recent DARPA Plum Island grid test assumed the diesel generator could be manually restarted as "Black Start" for the grid[4]. The gas turbine case illustrates that equipment may not be able to be restarted because "bad" sensors can act as security interlocks.
2) Bromine reactor anomalies in pH values have a direct impact on production quality and volumes. The sensor monitoring technology quickly identified a previously undetected

[4] https://www.wired.com/story/black-start-power-grid-darpa-plum-island/

anomaly at the source, showing that a critical process exceeded the norm, changing pH values and decreasing production. Early identification of the pH process failure enabled immediate correction, saving raw materials and vital process time, and allowed for clarification of work procedures and reporting.

3) Existing predictive maintenance was not adequate to address reservoir pump status and process health. The technology monitors more granular data than SCADA. Also, the technology is independent of the SCADA HMI, providing an additional measure of control and resilience (Figure 7). Because of the additional granularity, the technology identified an impending pump fault and provided additional system resilience.

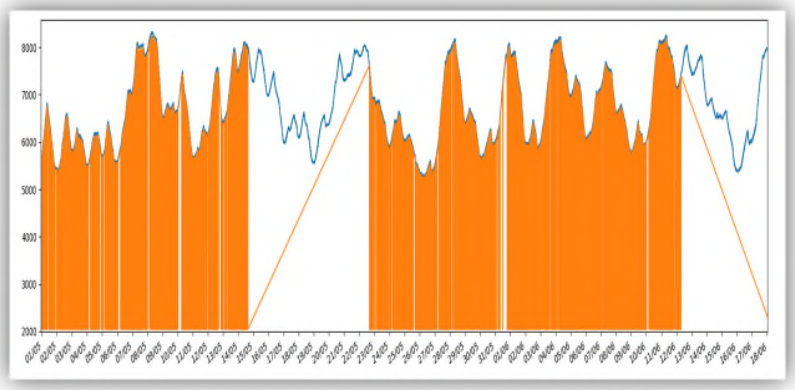

Figure 7 – Sensor monitoring continues even with SCADA HMI disruption

4) Metropolitan Water Reclamation District's (MWRD) main purpose is the reclamation and treatment of wastewater and flood water abatement in Chicago and Cook County to protect the health and safety of citizens and of area waterways. The technology has been installed at MWRD's Lockport Powerhouse on the Chicago Sanitary & Ship Canal, a facility that generates an average of 40 million kWh of electricity per year. Preliminary results illustrate the technology's ability to detect minute electrical signals that are not visible on MWRD's SCADA system.
5) The technology has been installed for monitoring building control system devices, such as Variable Frequency Drives, in real time.
6) In 2005, the Taum Salk earthen dam in Missouri[5] failed in part because of a failure in level sensing. The attachments to the level sensors broke, resulting in the level sensors becoming detached from the wall and providing erroneous low level information to the SCADA system. As a result of the low level indication, the SCADA system initiated pump operation until the upper reservoir overfilled and the dam collapsed. SIGA performed a small prototype demonstration with a small plastic tank filled with water and a sensor embedded in the lid of the tank connected to a PLC. When the lid of the tank was lifted, the actual level was obviously unchanged. However, the electrical characteristics of the sensor that was embedded in the lid changed. This change in electric

[5] http://damfailures.org/case-study/taum-sauk-dam-missouri-2005/

characteristics of the sensor could have provided a warning of a change in sensor behavior that should have been investigated.

Conclusions from Real-Time Process Sensor Monitoring

This approach can validate process operations through an autonomic system that learns the process through data obtained directly from sensors, independent from and without knowing the process. The machine learning algorithm supports *understanding of all processes,* correct readings of values, and compatibility with the operating pattern. The technology *identifies deviations* related to changes in the dynamics of the process or sensor deviation that can include cyber, supply chain, sensor drift, etc. Because of the granularity of the data, the technology can detect process/sensor anomalies not identified by the HMI.

From a cyber security perspective, one of the most important considerations is that this technology is independent of Windows or any other commercial-off-the-shelf HMI. Consequently, it continues to monitor operations independent of HMI, which provides not only a measure of security but also resiliency. As the technology is independent of Windows, it cannot be affected by a man-in-the-middle attack like Stuxnet.

Summary

Safety and reliability should be the most important input for cyber security. Level 0-1 sensors, drives, and final elements do not include cyber security or authentication. This vulnerability poses a major threat to safety and reliability for process plants and other infrastructures, and must be addressed. As the field devices are assumed to be engineering systems, vendors performing cyber security have focused on the network, and IT has focused on data packets, leaving the field devices vulnerable. Vendors providing predictive maintenance capabilities also have assumed the sensors to be correct. New technology is available to allow coordination of process anomaly and network anomaly detection, provide implicit authentication, and assure sensor health for reliability and safety considerations.