Precision Digital Presents

Fail-Safe Solutions Against Cyber Attacks

PRECISION DIGITAL

Presenter

Joe Ryan
VP of Sales & Marketing

Joe brings more than 15 years of process industry experience in the design, support, manufacturing, marketing, and sales of process measurement and control devices. Joe has extensive field and support experience with process displays and controls, and a strong technical background including a bachelor's degree in Electromechanical Engineering and a master’s degree in Computer & Electrical Engineering.

Agenda and Takeaways

01 Understand the threats cyber attacks pose on industrial and municipal plants.

02 Learn how industrial control systems can benefit from redundant local control and alarming.

03 Discover how Precision Digital can provide fail-safe solutions against cyber attacks using local displays.

Cyber Attacks Threaten Industrial & Municipal Plants

The Dangers of a Cyber Attack

A hacker altered chemical levels at the water treatment plant in Oldsmar, FL, on 2/5/21.

- Hacker tried to increase the amount of lye used to treat the water to dangerous levels.
- Plant safeguards would have detected the chemical alteration before water reached consumers.

"'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town"

The New York Times, 2/8/21

"Hack Exposes Vulnerability of Cash-Strapped Water Plants"

The Associated Press, 2/9/21

"U.S. Water Supply Has Few Protections Against Hacking"

The Wall Street Journal, 2/12/21

Cyber Attacks Stats

77%

of organizations do not have a cyber security incident response plan [1]

$5.2M

is the average cost of a single breach in the industrial sector [1]

67%

of municipalities surveyed reported experiencing a cyberattack where their network security was compromised at least once a year [2]

52%

of municipalities surveyed cited lack of funding as a barrier to achieving high levels of cyber security [2]

9.6

Days

is the average downtime that results from a ransomware attack in municipalities [3]

1. Chandrayan, Rahul. (2020, June 17). *Industrial Impact Due To Cybersecurity*. Industrial Automation Review. https://industrialautomationreview.com/industrial-impact-due-to-cybersecurity/
2. Thompson, Lisa N. (n.d.). *Cybersecurity Best Practices for Municipalities*. New Hampshire Municipal Association. https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities
3. *The Economic Impact of Cyber Attacks on Municipalities [White Paper]*. KnowBe4. https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf

Leveraging Redundant Local Control and Alarming Systems

What is Redundancy in Control Systems?

Redundancy in a control system eliminates dependence on a single system while at the same time provides multiple options in case of failure.

- Some processes demand the availability of systems at the highest level at all costs.
- It is also important in the system where the processes are irreversible.
- Some industries simply cannot afford to restart the system because restart time is not a small task.

Why is Redundancy Important for Control Systems?

Redundancy in control systems is important because it makes resources available in case any problems arise.

It also ensures a plant is not completely vulnerable to cyber attacks.

- For instance, if a control system is compromised, then a local 4-20 mA display can serve as a backup local monitoring, control, and alarm system.

NIST Security Recommendations

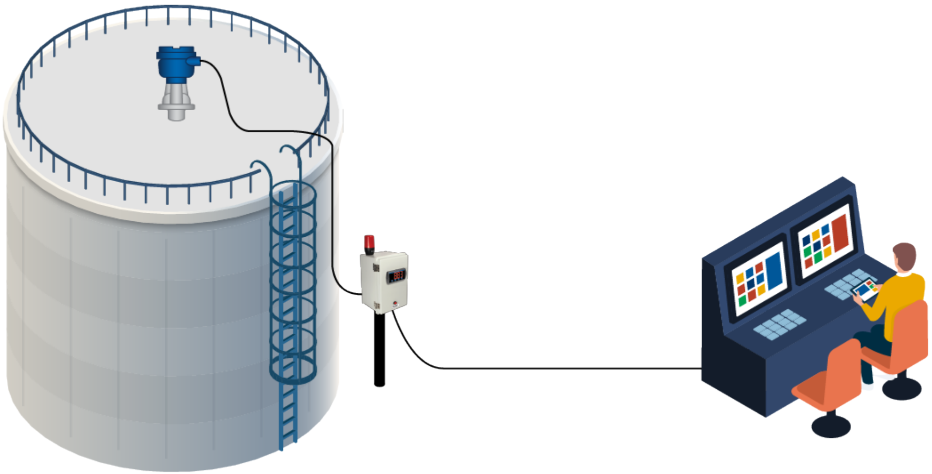
FILTER NO.3 AND NO.4 CONTROL CONSOLE
BACKWASH RATE OF FLOW (G.P.M.)
FILTER NO.4
FILTER EFFLUENT TURBIDITY (N.T.U.)
0.413
FILTER LOSS OF HEAD (FEET)
0.22
LUENT RATE OF FLOW (G.P.M.)
0

Analog devices (e.g., meters, alarms) may help reduce any negative impact of a cyber attack on the control system and must be part of the risk assessment process [4].

- Meters that measure and display the state of the physical system can provide the operator with accurate information in situations when the control system is compromised.
- Visual and audible alarms can alert operators of alarm conditions.
- Manual control mechanisms (e.g., manual valve controls, physical breaker switches) provide operators with the ability to manually control an actuator if the control system is unavailable or compromised.

4. Stouffer, Keith, et al. (May, 2015). *NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-82r2

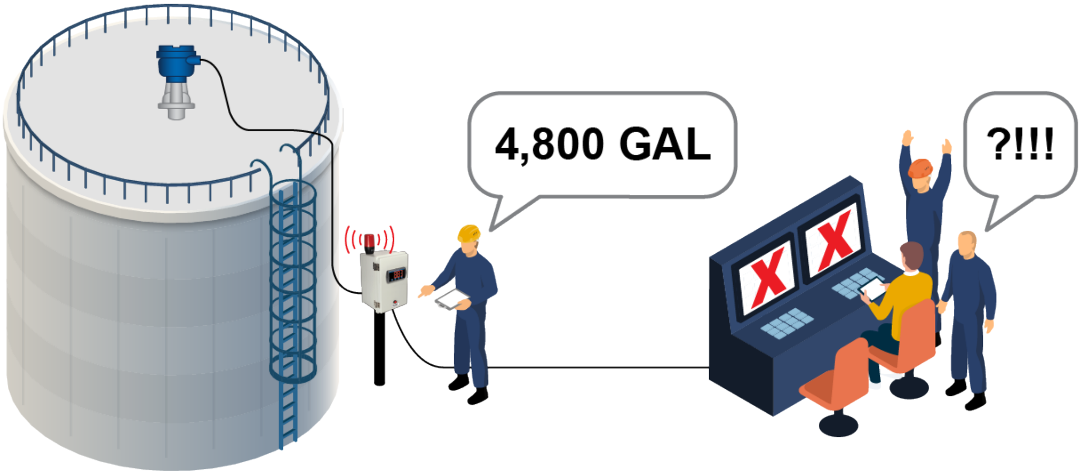
Leveraging Redundant Local Control and Alarming Systems



Normal Operation

- Under normal operation control systems monitor important processes of the plant.
- A remote display provides redundant local monitoring, control, and alarming.

Leveraging Redundant Local Control and Alarming Systems



Compromised Operation

- If the control system is compromised, then the display's redundant local monitoring, control, and alarming can keep things in check.
- The local display is not affected by external threats and keeps critical information available.

Fail-Safe Solutions Against Cyber Attacks

Fail-Safe Solutions Against Cyber Attacks

Gain Back Control of a Loop

- A 4-20 mA set point generator can manually control a final control element if the main control system is compromised.

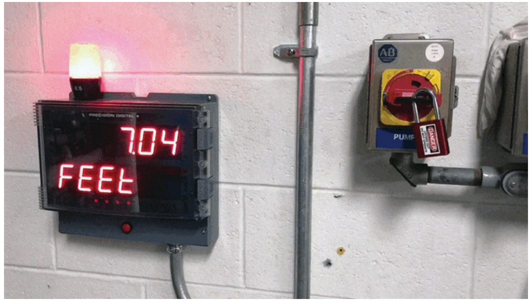
Keep An Eye On Critical Loops

- Add visibility to critical processes with an easy-to-install 4-20 mA loop-powered digital display. Give operators the ability to confirm control room information from the field.

Fail-Safe Solutions Against Cyber Attacks

Trigger An Alarm Before Danger Strikes

- A 4-20 mA digital display with up to four relays can provide alarms, drive external alarm devices, or allow for local backup control.



Monitor & Control Multiple Processes Without PLC Programming

- The ConsoliDator+ provides redundant or manual control and local alarming of multiple measurements, all without the need to program a PLC or HMI.

Questions?

If you have any questions or would like to discuss an application, then feel free to reach out to us.

Joe Ryan
VP of Sales & Marketing

jryan@predig.com