Cody P. Bann and David Nolan, *SmartSights, Austin, Texas*

Combat cyberattacks with advanced software technologies

Advanced software technology ensures critical infrastructures remain resilient against cyberattacks and enables real-time collaboration between operators, engineers and technicians who resolve process issues.

Learning **Objectives**

- **Understand how** capturing data from machine assets helps continuous operational improvement.
- **Learn the importance** of real-time data.
- **Discover how organizations** can manage critical infrastructure with a thoughtful approach to remote access that exposes alerts and insights in context rather than open access.

The need for strong cybersecurity software to identify and prevent attacks is paramount. Several sectors are particularly vulnerable to these threats and have been identified by the United States government as critical infrastructures (CIs). Those include:

- Transportation
- Oil and gas production and storage
- Water supply
- Emergency services
- Government services
- Banking and finance
- Electrical power
- Telecommunications
- Chemical
- Commercial facilities
- Manufacturing
- Defense

These threats present unique challenges.

Critical infrastructure faced a 30% increase in cyberattacks in just one year, showing how outdated frameworks that support vital sectors can affect the essential sectors we rely on, such as energy, water, transportation, healthcare and finance, according to a KnowBe4 report. Moreover, according to a recent Kyndryl Readiness report, 44% of critical IT infrastructure is approaching end-of-life. This means almost half of the world's most critical infrastructure is more vulnerable to cyberattacks and at higher risk for prolonged outages.

None of these CI sectors are immune to cyberattacks and downtime. Recently, a cyber incident at the Port of Seattle and Seattle-Tacoma International Airport highlighted the ongoing vulnerabilities and how critical infrastructure disruptions or outages can impact crucial avenues for travel, logistics and even power. However, embracing cyber resiliency allows organizations to ensure that critical systems can continue to function during and after a cyber event.

Responding quickly to these incidents can minimize damage and restore operations. Different sectors of CI face unique challenges when it comes to cyber resilience, but all share a common need for stronger, more adaptive defenses.

One component of resiliency is embracing and integrating advanced software technologies.

Capturing data from machine assets

The modern industrial environment requires addition¬al advanced technology to improve operational efficiencies, including process optimization, real-time analytics and automation. Integrating these is paramount for maintaining a competitive edge in an increasingly globalized market.

However, with this escalating need comes a rise in the risks of plant downtime and cyberattacks, which can significantly hamper competitiveness and productivity and negate the cost savings of automation.

Continuous operational improvement starts with capturing data from machine assets. This data provides immediate insights for both people and sy stems, enabling them to make better, faster decisions and drive automation.

Once real-time process information is gathered, the next step is to define conditions of concern on those process variables. Supervisory control and data acquisition (SCADA) systems provide for such conditions to be defined and tracked, monitoring pro-

FIGURE 1: Not only can OPC UA be used to relay the real-time values like sensor readings to SCADA HMI screens across vendors; it can also relay alarm conditions that SCADA builds on top of those variables, so that dangerous or costly deviations can be quickly identified and addressed. Courtesy: SmartSights

cess variables and surfacing active conditions to human-machine interfaces. These condition-based events and alarms add another level to optimizing the process. They facilitate greater situational awareness for plant operators by calling attention to irregularities and suboptimalities. Real-time process variables and alarm conditions can then be captured over time and calculations can be performed to improve planning and offer solutions to detect patterns in the data.

Real-time data is also critical to providing IT teams with insights about the security of a network or related topics, promptly acting on them and mitigate threats sooner.

Advantages of remote alarm notification software for cyberattacks

A key theme of Open Platform Communications Unified Architecture (OPC UA), industry 4.0 and smart operations is greater connectivity — increasing connectivity between devices, industrial networks and physical assets and the cloud.

Growing connectivity allows for greater process transparency and the added potential for predictive analytics and sentinel alarm conditions. Smart plants allow potential issues to be addressed before they become problems, but only by extending that connectivity to the final hop — to the people who operate and optimize assets. Connecting devices to people and getting the right information with increased sophistication of modeling to the right people at the right time is the strength of remote alarm notification software. Remote monitoring and alarm management enables operators to take on more proactive, hands-on tasks in the field or at the plant, without hiring additional staff.

Smart technology and OPC UA are reshaping the deployment of remote alarm notification software solutions and their connectivity. As assets and processes become more populated with smarter sensors and are increasingly modeled at lower operational levels, the ability of remote alarm notification software solutions to connect to both SCADA and non-SCADA information sources is increasingly important.

Advanced notification workflows will call for the synthesis of information from multiple OPC UA servers in response to unfolding alarm events in SCADA. It's nice to know that a pressure sensor is registering a low alarm; it's better to know that information in the context of the status of the valves and pumps associated with that pressure, the maintenance information for that asset and the downstream impact of the low pressure.

Increased connectivity and information modeling will empower decision-makers, enable faster response times and drive increased productivity. Smart technology ready alarm notification software solutions connect to both the leading SCADA packages and to OPC UA servers and provide for such advanced notification workflows.

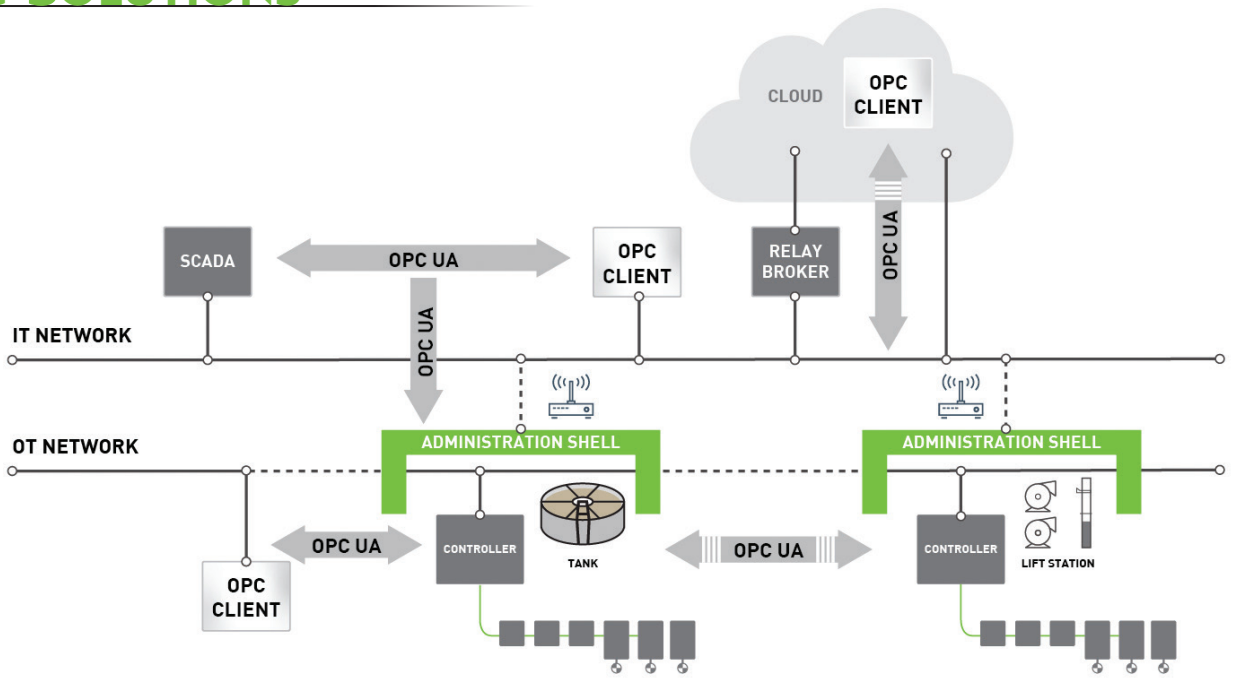


FIGURE 2: OPC UA helps water utilities meet the challenge of secured exchange of structured data between devices, equipment and services. OPC UA is also designed to share that data upwards from the OT network to IT networks and to the cloud beyond. Courtesy: SmartSights

Data is critical to efficiency

The Environmental Protection Agency (EPA) rescinded its previous mandate that required states to expand inspections of water systems to include cybersecurity threats. It encourages states to still review cybersecurity practices for public water systems on a voluntary basis under the sanitary survey or use another equivalent process.

The EPA regulation states that water utilities can conduct a self-assessment, or have it done by an approved third-party resource such as a Cybersecurity and Infrastructure Security Agency cybersecurity adviser through the EPA's water sector cybersecurity evaluation program or a state-approved private sector technical assistance provider. Currently, the only approved third-party assessment resources are limited to the Department of Homeland Security, EPA and states, which makes this activity hard to scale across the breadth of water utilities across the country.

The goal of sanitary surveys is to ensure that states effectively identify significant deficiencies and that public water systems (PWS) then correct those deficiencies — including cybersecurity-related weaknesses — that could impact safe drinking water. To help with this, the EPA is offering considerable technical assistance and support to states as well as to PWS to help close cybersecurity gaps.

While accurate, real-time data is pivotal to operations, harnessing this data effectively requires advanced technology and analytical capabilities. Vast amounts of data are collected for industry reporting, predictive maintenance and safety enhancements, for example, but organizations may be challenged to effectively manage and analyze the data. While monitoring and alarms can improve system efficiency, they don't automate the labor-intensive reporting process or provide much-need analytics that extract raw or summary values over a discrete period.

Automated third-party reporting software, however, tracks all areas in a production facility. The finished reports are then distributed directly to preferred destinations, which streamlines the decision-making process and enhances operational efficiency. The ability to harness this data effectively can lead to smarter decision-making, improved processes and a competitive edge. Analyzing historical data allows operations management to identify patterns, trends and anomalies that may otherwise go unnoticed. Historical data analytics can help companies transition from reactive to proactive planning and keep planning aligned with operations. As the data is collected it is summarized as key metrics and the final output is published into a formatted document accepted by regulatory agencies, such as for an EPA surface water treatment compliance report.

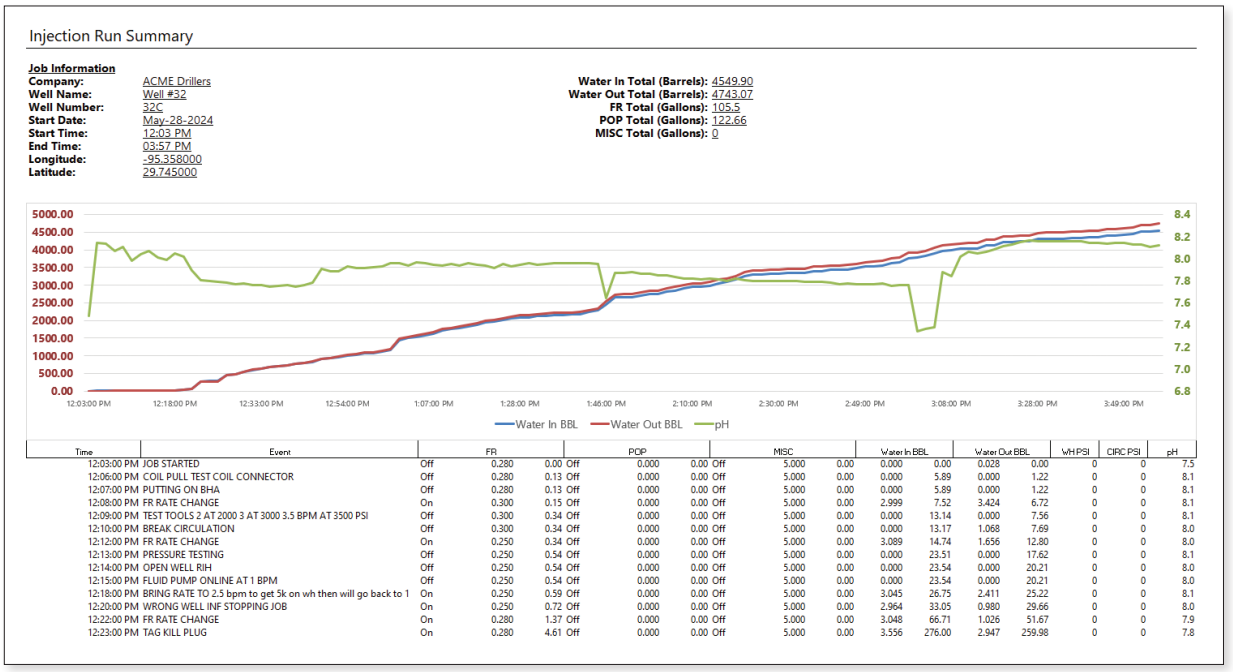
The critical role alarm management plays in reducing cyberattacks

A robust alarm management system enhances operational efficiency and enables timely detection of failures. A comprehensive alarm system provides actionable information to the operator and assists in taking corrective action. Research has shown that a well-managed alarm system results in production

Insights

Cyberattack insights

- **Quick response** times are critical to recovering from cyberattacks.
- **Smart technology** and certain standards are helping reshape the response protocol to cyber threats.
- **Critical infrastructures** (Cis) are becoming more vulnerable each year to cybersecurity attacks.



Injection Run Summary

Job Information

Company:	ACME Drillers
Well Name:	Well #32
Well Number:	32C
Start Date:	May-28-2024
Start Time:	12:03 PM
End Time:	03:57 PM
Longitude:	-95.358000
Latitude:	29.745000

Water In Total (Barrels):	4549.90
Water Out Total (Barrels):	4743.07
FR Total (Gallons):	105.5
POP Total (Gallons):	122.66
MISC Total (Gallons):	0

Time	Event	FR			POP			MISC			Water In BBL		Water Out BBL		WH PSI	CIRC PSI	pH
12:03:00 PM	JOB STARTED	Off	0.280	0.00	Off	0.000	0.00	Off	5.000	0.00	0.000	0.00	0.028	0.00	0	0	7.5
12:06:00 PM	COIL PULL TEST COIL CONNECTOR	Off	0.280	0.13	Off	0.000	0.00	Off	5.000	0.00	0.000	5.89	0.000	1.22	0	0	8.1
12:07:00 PM	PUTTING ON BHA	Off	0.280	0.13	Off	0.000	0.00	Off	5.000	0.00	0.000	5.89	0.000	1.22	0	0	8.1
12:08:00 PM	FR RATE CHANGE	On	0.300	0.15	Off	0.000	0.00	Off	5.000	0.00	2.999	7.52	3.424	6.72	0	0	8.1
12:09:00 PM	TEST TOOLS 2 AT 2000 3 AT 3000 3.5 BPM AT 3500 PSI	Off	0.300	0.34	Off	0.000	0.00	Off	5.000	0.00	0.000	13.14	0.000	7.56	0	0	8.1
12:10:00 PM	BREAK CIRCULATION	Off	0.300	0.34	Off	0.000	0.00	Off	5.000	0.00	0.000	13.17	1.068	7.69	0	0	8.0
12:12:00 PM	FR RATE CHANGE	On	0.250	0.34	Off	0.000	0.00	Off	5.000	0.00	3.089	14.74	1.656	12.80	0	0	8.0
12:13:00 PM	PRESSURE TESTING	Off	0.250	0.54	Off	0.000	0.00	Off	5.000	0.00	0.000	23.51	0.000	17.62	0	0	8.1
12:14:00 PM	OPEN WELL RIH	Off	0.250	0.54	Off	0.000	0.00	Off	5.000	0.00	0.000	23.54	0.000	20.21	0	0	8.0
12:15:00 PM	FLUID PUMP ONLINE AT 1 BPM	Off	0.250	0.54	Off	0.000	0.00	Off	5.000	0.00	0.000	23.54	0.000	20.21	0	0	8.0
12:18:00 PM	BRING RATE TO 2.5 bpm to get 5k on wh then will go back to 1	On	0.250	0.59	Off	0.000	0.00	Off	5.000	0.00	3.045	26.75	2.411	25.22	0	0	8.1
12:20:00 PM	WRONG WELL INF STOPPING JOB	On	0.250	0.72	Off	0.000	0.00	Off	5.000	0.00	2.964	33.05	0.980	29.66	0	0	8.0
12:22:00 PM	FR RATE CHANGE	On	0.280	1.37	Off	0.000	0.00	Off	5.000	0.00	3.048	66.71	1.026	51.67	0	0	7.9
12:23:00 PM	TAG KILL PLUG	On	0.280	4.61	Off	0.000	0.00	Off	5.000	0.00	3.556	276.00	2.947	259.98	0	0	7.8

FIGURE 3: Third-party reporting software streamlines operational and compliance reporting from data sources like SCADA, HMI, and historians. Courtesy: SmartSights

efficiency, improved product quality and better operator effectiveness.

Since 1991, alarm management standards have been published and currently the International Society of Automation 18.2 and International Electrotechnical Commission 62682 are the most widely accepted. The standards define a seven-step alarm management cycle program from identification to monitoring and assessment.

A cloud-connected alarm management system provides access to real-time alarms even when working remotely to decrease response times and help reduce unplanned downtime. Alarm audits and reporting provide an efficient means to document and track the history of individual alarms, consequences, response time and the action taken to mitigate the alarms. As this rationalization is performed, continued system-level monitoring and assessment reports validate that these efforts are driving real improvement.

Alarm management is a critical aspect of industrial operations, particularly in high-risk industries such as oil and gas, chemical processing and power generation. The ability to effectively manage alarms can prevent accidents, minimize downtime and improve overall operational efficiency.

The seamless interoperability of OPC UA

A challenge with organizations' varied networks is the secure, standardized exchange of data and information between devices, equipment and services, which is where OPC UA comes in. OPC UA is an extensible, platform-independent standard that enables the secure exchange of information in industrial systems. It is compatible with Windows, macOS, Android and Linux and works on PCs, cloud-based infrastructures, programmable logical controllers, micro-controllers and cyber physical systems.

It doesn't stop there though; OPC UA is also designed to structure and share that data upward to IT networks and to the cloud beyond. It's the comprehensive information modeling framework provided by OPC UA that allows it to relay context for information and go beyond simple data transmission, context that is critical for the data to be interpreted and used correctly by external systems. A process variable coming from a sensor value can be modeled with engineering units to allow proper interpretation, operational limits to validate modifications and adjust display and servicing information to provide an approximation of accuracy.

The security of cloud-based platforms has been a growing concern over the past decade. As OPC UA is a communication layer for machine-to-machine and machine-to-cloud communication, it operates with two security layers. The first layer sets up an encrypted channel connection between the client and server. This layer provides confidentiality, integrity through message signing and certificate-based authentication. The application layer then manages user authentication and user authorization.

OPC UA allows OPC to be used as a client or a server; it will provide data to various devices and applications to control equipment functions. OPC

> **Analyzing historical data** allows operations management to identify patterns, trends and anomalies that may otherwise go unnoticed.

Organizations require systems to protect operational data from unwanted access and to keep track of significant system events.

UA server applications allow data exchange for machine-to-machine and PC-to-machine communication. OPC UA server uses include Remote Terminal Units (RTUs) field service applications. Another benefit of OPC UA is that assets can be upgraded to this as they are repaired by deployed edge gateway devices as budgets allow.

A key theme of OPC UA is increasing connectivity — increasing connectivity between devices, networks and physical assets and the cloud. Increasing connectivity allows for greater process transparency and the added potential for predictive analytics and sentinel alarm conditions. Additionally, beyond delivering alerts or metrics to people, this advanced technology can deliver information to other software systems to reduce unplanned downtime. Integrating issues management software with ticketing systems, for example, further enables real-time collaboration between operators and engineers.

Protecting data to combat cyberattacks

"Failing to address cybersecurity risk in a proactive way can have devastating results. Failing to take reasonable measures and employ best practices to prevent, detect and swiftly respond to cyberattacks means that organizations and the people who run them will face greater damage — including technical, operational, financial and reputational harm — when the cyberattacks do occur," said a report, "Cybersecurity Risk & Responsibility in the Water Sector," from the American Water Works Association.

Organizations require systems to protect operational data from unwanted access and to keep track of significant system events. Although replacing legacy systems and networks can be extremely costly, it is essential to work with vendors and cybersecurity experts to implement updates and, if necessary, overhauls of outdated systems. Invoke the help of internal or external advisors to prioritize risk and develop a realistic approach and plan for enhancing cybersecurity. At a minimum, comply with basic standards including restricted physical and technical access, firewalls, logging and encryption.

Additionally, many SCADA systems are simply over-exposed to the internet by remote desktop applications (RDP) (e.g., TeamViewer). To provide process and asset information to operators, organizations have provided much more, ignoring the principle of least privilege and opening their control systems and their hosts to remote desktop access by unnecessary parties.

Advanced remote alarm notification software allows remote operators access to only the information they need from SCADA and not access to the SCADA itself or its operating system host. Such notification software is compatible with more secure, layered networks in which a series of firewalls provide added protection from attacks. This is done by deploying notification solutions alongside the SCADA system at the network's control level and using notification modalities that are not internet facing or distributing internet-facing notification processes to higher levels.

There are several steps that organizations should take to improve their cybersecurity:

- Update any software to the latest version.
- Deploy multifactor authentication.
- Use strong passwords to protect remote desktop protocol credentials.
- Ensure antivirus systems, spam filters and firewalls are up to date, properly configured and secure.

CIs should also take steps to secure any remote access software. They shouldn't use unattended access features and IT leaders should configure the software such that the application and associated background services are stopped when not in use. Integrating these advanced software systems through the SCADA system is critical to further reducing cyberattacks.

Cyber resilience ensures this critical data is accessible and secure at the time of an attack. Whether it be customer data, financial information or licensed proprietary technologies, this resilient approach limits sensitive data exposure and loss during any incident.

According to McKinsey & Co.'s report, "Critical Resilience: Adapting Infrastructure to Repel Cyberthreats," cyberattacks should be thought of as a certainty akin to the forces of nature. Just as engineers must consider the heaviest rains that a dam may need to contain in the next century, those digitizing infrastructure must plan for the worst in considering how an attacker might abuse or exploit systems that enable infrastructure monitoring and control.

Cody P. Bann *is vice president of engineering at SmartSights.* ***David Nolan*** *is the industry solutions manager at SmartSights.*