GE VERNOVA

MODERN HMI/SCADA GUIDEBOOK FOR EFFICIENT OPERATIONS

- High Performance HMI
- Rapid Application Development
- Improved Security Practices
- Mobility
- Centralized and Remote Operations
- Industrial Data Management for IoT

Explore Tips & Best Practices

INTRODUCTION

GE VERNOVA

Enter the world of today's industrial plant:

- Aging infrastructure
- Increasing revenue challenges
- Retiring experienced workers
- Increasing service level expectations
- Regulations

What's more, resources for capital programs are usually limited, making it difficult to carry out infrastructure modernization, expansion, and technology upgrades.

How can you address these critical challenges while delivering the best return on investment to investors, private or public? Chances are, your budgets will remain tight with expectations continuing to increase.

So you're left to become as efficient as possible with the assets and people that you have. This means you've got to look at your operations holistically to understand and predict what's happening to make the best decisions for modernizing and optimizing.

Greater Efficiency with the Modern HMI/SCADA

The good news is the technology and solutions are here. They revolutionize what's possible for industrial organizations.

By modernizing your existing HMI/SCADA system, you can have High Performance visualization, real-time information when and where you need it, and the ability to connect the dots between your data, leveraging the Internet of Things (IoT).

The modern HMI/SCADA lets you guide newer operators through the right steps to take. And, you can enable mobility and remote monitoring for greater efficiency.

Welcome to the modern HMI/SCADA system—where machines, data, insights, and people are connected.

TODAY'S CHALLENGES

In general, challenges at an industrial plant are related to three main areas:

- **Availability and reliability:** Examples include aging infrastructure, stability of the system, and reliability of the data coming in.
- **Risk:** Examples include compliance concerns, cybersecurity and physical security, reporting, and errors due to high workforce turnover and experienced operators retiring.
- **Cost:** Examples include raw materials, training newer operators, energy costs, maintenance.

Operations professionals are constantly facing the challenge of finding the right balance between availability and reliability, risk, and cost.

How to reduce cost without compromising availability? How to mitigate risks while keeping costs under control?

Value of Modern HMI/SCADA

The modern HMI/SCADA helps to reduce operating cost, maintain a high level of service, ease compliance with evolving regulatory standards, and increase the efficiency of operators.

Additionally, industrial organizations can use this control layer as a foundation for digital transformation to be better prepared for the future.

By modernizing HMI/SCADA, you can directly address challenges in the three key areas in several ways:

High availability and reliability

- Secure-by-design SCADA
- Disaster recovery architecture
- Information anytime, anywhere

Risk Management

- Reliable data management
- Effective alarm management
- Consistent operating processes
- Improved communication and collaboration across teams

Cost Management

- More efficient operators
- Enhanced operations visibility
- Effective data analysis

View Demo

Technology suppliers in the automation ecosystem have the challenge and opportunity to help industrial companies cope with these changes while achieving their desired outcomes.

HMI/SCADA SUPPORTS DIGITAL TRANSFORMATION

In today's rapidly changing industrial landscape, manufacturers and utilities must embrace modern HMI/SCADA and digital transformation to keep up with the pace of change, meet growing operations challenges, and remain competitive. The foundation starts with capturing industrial data, combining it with other meaningful data sources for context and managing a historic record. It is data, turned into information, that provides the basis for meaningful outcomes.

Modern HMI/SCADA, including data historian and centralized visualization technologies, empower users to unlock the value of their data. The outcome is a high-productivity development and visualization environment that enables optimized plant operations, supported by faster development, a democratization of tools and capabilities throughout a plant, improved operational performance, lower costs, a changed mindset among employees, and a culture of continuous improvement. Examples of market leaders from multiple sectors illustrate the outcomes companies are achieving.

THE INDUSTRIAL LANDSCAPE IS RAPIDLY CHANGING

Technological innovations are reshaping the industrial landscape. These innovations include cheap sensors, a high-speed telecom infrastructure that can move huge amounts of data, unprecedented computation power, mobile and touch interfaces, and a standards-based open ecosystem for interoperability. This ecosystem includes web-based technologies, APIs for connectivity, machine learning, and AI.

As these technologies evolve and take hold, organizations desire outcomes that include increased revenue and productivity, lower costs, and more consistent quality. Industrial organizations are also dealing with high rates of retirement of aging workers who have deep knowledge and expertise. These individuals are being replaced by younger workers who lack the same knowledge but are digital natives with skills and experience with mobile devices and web-based technologies.

HIGH PERFORMANCE HMI: PRACTICAL LESSONS FOR GETTING STARTED AND LEVERAGING DATA

Our research shows that 90% of companies are collecting industrial data but only 30% are analyzing that data. Even less, just 2%, are acting on the information. With so much money being spent on collecting data, why aren't organizations better utilizing it?

The answer is often simpler than you might expect. Too often, data isn't accessible in an easy-to-interpret way. The good news is this is a barrier we can start removing quickly by following these four steps to enabling High Performance HMI and making important, data-based information jump out.

Step #1

Bring the team together.

High Performance HMI projects with high adoption rates share a common trait. Involving your key stakeholders early on in a project can help solidify the common challenges, explore the best opportunities, prepare requirements and even test user interfaces. Ensure operators are included in this team, they will make or break the success of your program.

Step #2

Build a workshop mentality into your review processes.

It's not enough to bring a group of stakeholders together, brainstorm and then send them on their way. Your stakeholders should have planned review checkpoints to optimize results. These checkpoints are critical for stakeholders to feel part of the journey, raise concerns earlier in the program cycles and ensure there is a high likelihood of agreement.

Step #3

Document and share more.

Write it down, write it all down. This can't be said enough. The advice is so simple, yet it is a step that many overlook. Documenting decisions, learning and work plans is a critical requirement to aligning the team and holding each other accountable.

Step #4

Go after low-hanging fruit

Projects often begin with a boost of excitement but quickly dissipate because the core team gets pulled back into their day-to-day tasks. The most effective path to keeping everyone focused on the long game is to build low-hanging fruit milestones into your project plan. These keep the team motivated and help paint a path to your future vision.

When it comes to designing High Performance HMI, there are a number of design options which should be considered low-hanging fruit improvements. Below are seven options that make a world of difference.

- Replace data links with gauges. A picture really is worth a thousand words. Rather than ask operators to link to data in another location, make it easy for them to quickly visualize what needs attention.
- Display trending objects. Numbers don't always tell the full story. By tracking trends, you can quickly see what might be improving or degrading over time. This will impact the actions taken by operators in both the immediate and long-term time horizon.
- Update piping/other PID elements. Illustrations that mimic piping and other system elements in realistic fashion can make it difficult for operators to quickly isolate issues. Simplify representations and make sure they are accurately depicting the current state of your equipment.
- Remove distracting visual elements. This includes gradient coloring, animations and flashing objects. These design elements distract the operator rather than draw them in to what most needs attention.
- Add or modify background color to improve contrast. It's remarkable how changing the background of a display improves the human eye's ability to process visual information. Our eyes are trained to look for contrast.
- Encapsulate process areas in a card. Make it easy for your team to see related processes next to each other, even if the physical footprint of your solution is separated.
- Consistent fonts, units and naming conventions. Consistency is key to processing visual information. This is a simple fix that can quickly make it easier for operators to focus on what's critical.

INTELLIGENT ALARMING

From proactive analysis to guiding operator response, modern alarming technologies use the IIoT's connected systems, layered with new apps, to help eliminate alarm noise and confusion while driving the right corrective actions.

What's the biggest challenge on the plant floor?

According to a recent GE Vernova survey, managing alarms is still the biggest challenge.

But, in today's digital age, every organization can manage alarms. With intelligent alarming and the Industrial Internet, companies can send the alarms that matter, when they matter, to the right person. Engineers and operators can receive prioritized alerts with instructions, helping them react to and resolve alarms quickly.

AN ALARMING SITUATION

According to HMI/SCADA experts at GE Vernova, about 75% of all alarms are noise. Many companies want to examine their systems and reduce the number of alarms to improve operator effectiveness. However, this is often an endless cycle. Integrators and in-house engineers typically find new alarms that must be added, while looking to reduce the number of alarms and flags in the system.

Too often, companies are forced to accept that there is a level of noise from alarms, and operators must know what to pay attention to and what does not require action. A problem arises with temporary staff operating machines or new operators coming on board. The temporary or new personnel usually don’t have the experience to filter through the alarm noise and make sense of it.

Additionally, one problem can cause a flood of alarms hitting an operator. Recently working with a major metropolitan area’s transportation team, a proof-of-concept showed how one problem on a train line triggered an initial alarm, followed by another alarm, followed by ten more alarms, then twenty, and the situation continued. The operators on the trains were inundated with alarms and, in this confusion, unable to identify the real problem.

Reduce alarm noise with machine learning

In the Industrial Internet world, today's HMI/SCADA can filter alarms better to increase efficiency. Now, we can use machine learning to look at all the raw alarms in underlying systems, determine a root cause, and guide operators through the right corrective actions. This can take place in a control room or in the field—with instructions going to a mobile device of choice—and deriving intelligence from the raw data.

Machine learning puts traditional alarm rationalization on steroids. HMI/SCADA today, based on the IIoT connected enterprise, can provide full-scope alarm management and optimization, facilitating alarm rationalization by providing visibility to all alarms, the respective alarm priority or tier, frequency of occurrence (for a specified period of time), and more, delivering on an alarm philosophy that improves efficiency, reduces unscheduled downtime, and decreases risk.

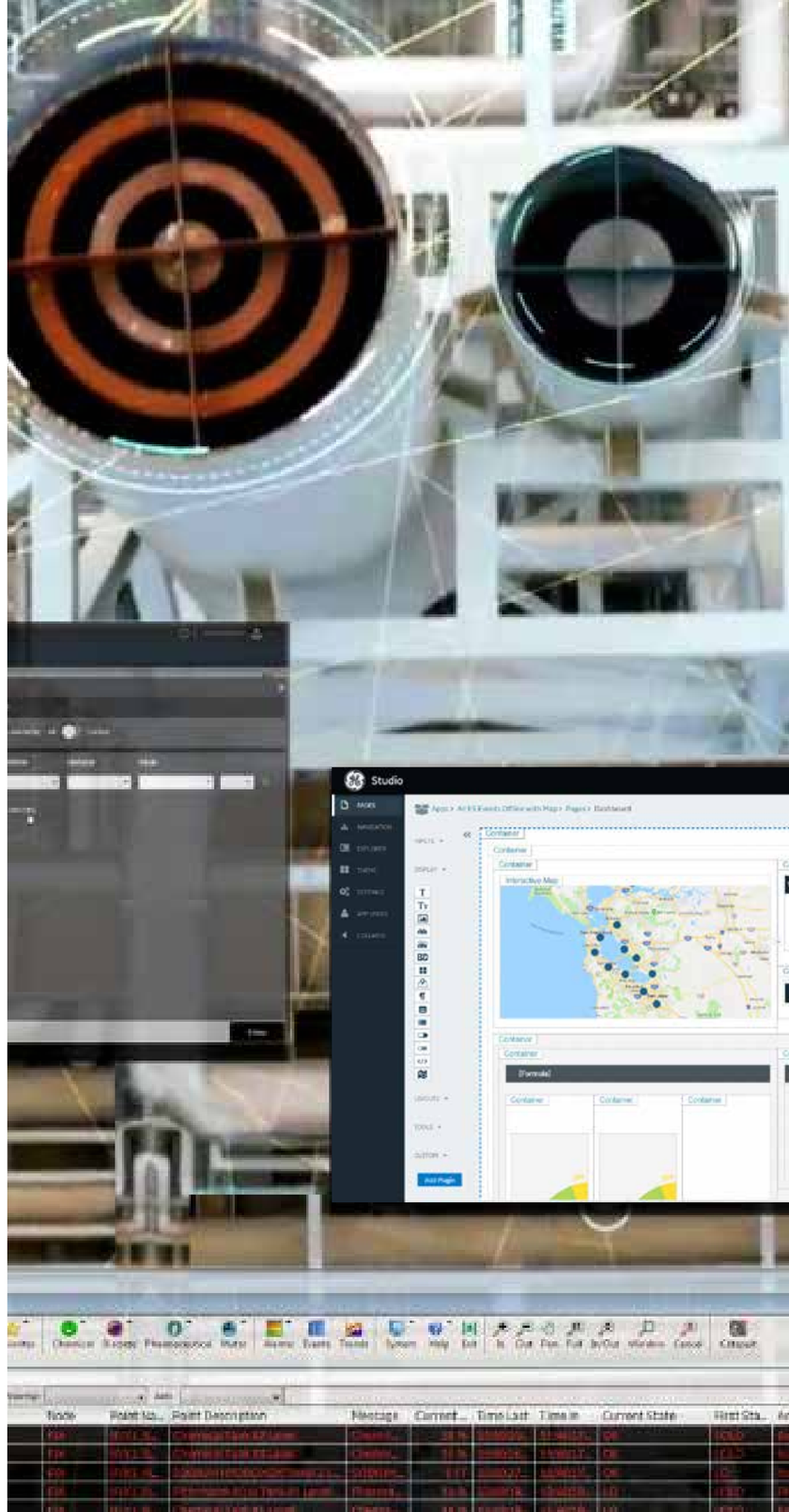
Be proactive with analytics

Furthermore, modern HMI/SCADA can add a layer of proactive analysis to deliver predictive intelligent alarming. Today's technology isn't just about delivering the right information after an event has happened, it is also about delivering information before a catastrophic issue occurs and preventing it from taking place.

Consider if a plant monitors a temperature, which exceeds the upper control limit and an alarm goes off. Traditionally, an operator would now react to the alarm. Analytics have made it possible to evolve from being reactionary to now predicting when the event will occur and taking proactive steps.

As an example, a food manufacturer can monitor the temperature data point, put an analytic on it, and predict the temperature based on a statistical model. The company can push an alarm to an operator to ensure that action is taken faster, before a batch is ruined.

This applies to other industries as well, such as pharmaceutical with multi-million dollar batches of product, as well as maintenance events on discrete equipment. The application of predictive knowledge, delivered as an intelligent alarm, is far reaching across all industries and offers new possibilities for consistently optimized operations.



ALARMS TO THE RIGHT PERSON, AT THE RIGHT PLACE—IN CONTEXT

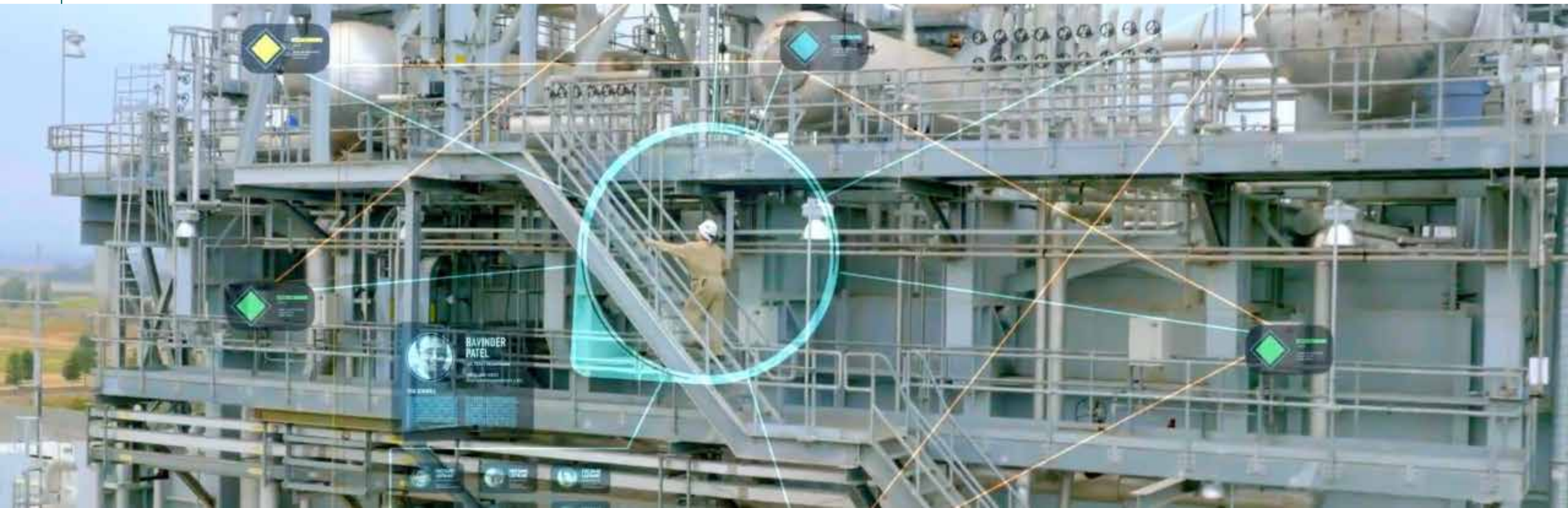
Furthermore, our IoT world helps us send alarms in context. This means, once an alarm fires, an operator should be able to understand contextually, not just where in the plant the issue is occurring (from a location standpoint), but more directly, where and when in the process there is an issue occurring.

Operators need to be able to understand the corrective action required to resolve an alarm. As such, seeing that alarm in context is important. In the past, operations teams relied on years of experience for that context—the so called “machine whisperer” who understood that if “x alarm” occurred under “y circumstances,” then it meant a conveyor, for example, was moving too fast and they knew exactly how to tweak a dial. With our changing workforce, those days are gone—and digitization must be the foundation for providing the context to newer, inexperienced workers.

Lastly, HMI/SCADA gets the alarm, in context, to the right person in the right place. Organizations can deploy alarms to an operator, engineer, or manager based on role and physical location. As an example, an engineer is standing on Floor 4 in front of a mixer and an alarm triggers related to a machine on Floor 1, which is 25 minutes away. Does it make sense to deploy the alarm to that engineer?

Today’s HMI/SCADA system can determine that a colleague is standing 100 feet away from the machine in alarm—and instead send the signal to the closest engineer for faster, more efficient response.

The right information, in context, finds the right person in the right location, which is drastically different from the traditional SCADA world and drives faster action.



SMARTER OPERATORS WITH INTELLIGENT ALARMING

Today's HMI/SCADA is not just monitoring and visualization, with alarms rolling in. For operators, HMI/SCADA is their decision support system, and intelligent alarm management is critical. Here are two golden rules to think about:

Don't allow technology to complicate the operator experience.

Use technology to improve the operator experience and manage alarms for greater efficiency.

With just a glance, operators should be able to recognize which information requires their attention and what it indicates. You can enable smarter operators with intelligent alarming for faster alarm detection, greater understanding, and improved business outcomes.

Take operations to the next level with GE Vernova's proven HMI/SCADA solutions.

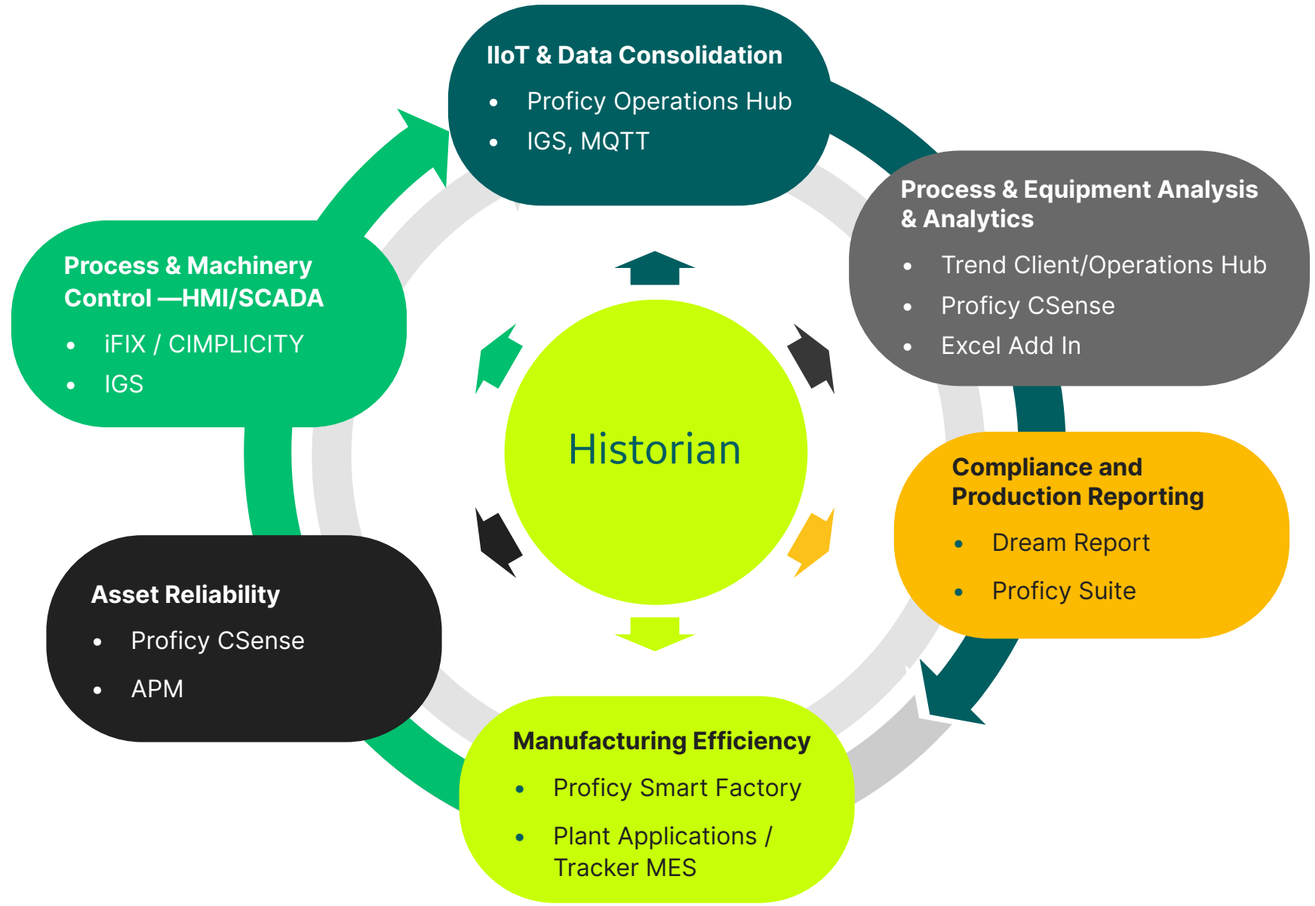
JOIN US TODAY

HMI/SCADA AND INDUSTRIAL DATA MANAGEMENT

Data is the foundation for delivering outcomes, data historians provide the common thread. This supports organizations to drive IoT initiatives, process and equipment analysis, compliance reporting, and more.

In addition to a data historian, another key component to turning data into information is via an asset model, to provide context that personnel of all levels can understand — from the plant floor to the operations center.

"For us, the first step in creating information is putting the data that has been collected in a context everyone in the organization can understand."



HMI/SCADA + DATA HISTORIAN DELIVER THE FOUNDATION FOR DIGITAL TRANSFORMATION

Collect Data

- Time-series process data and alarms & events data from industrial equipment and processes
- Native collectors
- Store & Foward capability

Store & Normalize

Scalable from small to large:

- Millions of tags
- High availability
- Data compression
- Secure-by-design

Distribute

- HMI/SCADA
- HTML5 clients
- Native API & Methods to move data
- Big data on-ramp

Organizations need the ability to aggregate near real-time data from sensors along with historical data from ERP systems, quality systems, HMI/SCADA, and other data sources. In addition, users need to know the data is clean, valid, and high quality.

At the core of data management is a plant—or enterprise-wide data historian, that facilitates data collection, storage and normalization, and distribution.

It stores time-series process data and alarm and event (A&E) data from industrial equipment and processes. Data can be collected from hundreds of different types of control systems and should be scalable from a small set of data tags to millions. Data should be distributed from a data historian by an integration with HMI/SCADA clients, through HTML5 clients, or via APIs.

"The nice thing about Proficy Historian is it lets organizations start very small and have a roadmap to long-term and very robust and intense data analytics."

CENTRALIZED VISUALIZATION: HMI/SCADA AND BEYOND

Visualize and Share Data to Derive Value

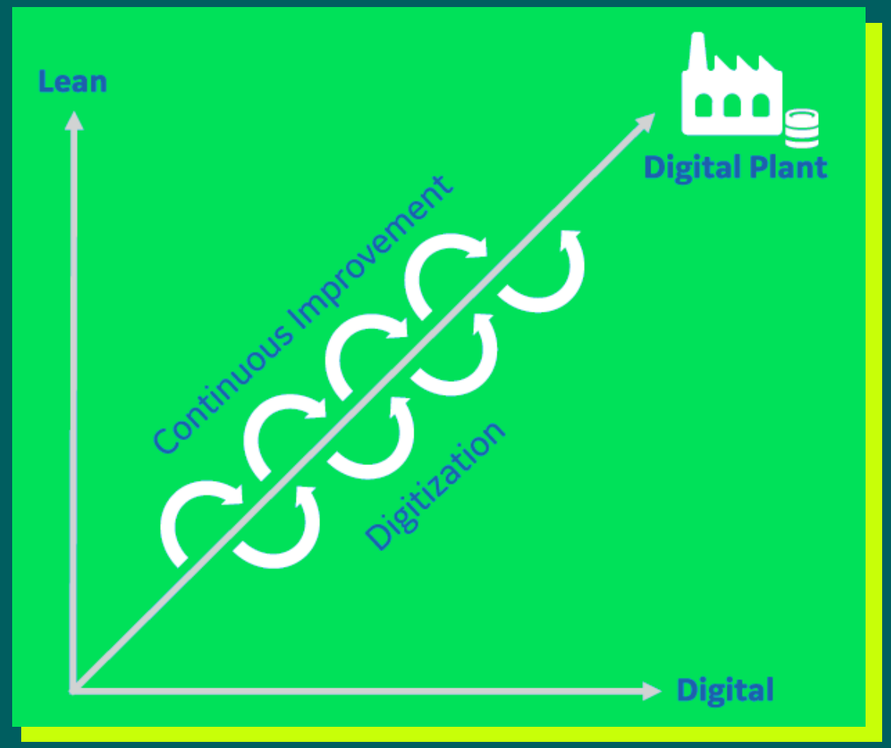
To provide customers with a data management solution that has both asset model context and visualization, GE Vernova developed Proficy Operations Hub, which integrates with historian technology such as Proficy Historian, HMI/SCADA such as iFIX and CIMPLICITY, as well as other systems. This combination enables manufacturers and utilities to unlock the value in their data through shared information and collaboration as well as rapid application development (RAD) tools.

What's the value of data if it can't be shared and visualized across a plant and enterprise?

Proficy Operations Hub is an industrial application platform for aggregating data from multiple sources. Proficy Operations Hub's code-free environment allows industrial applications to be rapidly built and deployed. It enables improved plant operations through comprehensive information that is easier to analyze and act upon. Key aspects include:

- Connecting to all systems in a multipurpose, multi-use plant and enterprise
- Democratizing tools so they are accessible throughout the organization and easy to use by all
- Visualizing data across all levels of a network
- Scalability in being useful for both small initiatives and massive undertakings

Connectivity is critical, and some methods include OPC UA, MQTT (Message Queue Telemetry Transport), and REST APIs.



*"A key part of our belief is that tools have to be democratized . . .
we want the tools to be accessible and usable by everyone."*

CONTEXTUALIZED DATA IS THE BASIS OF DIGITAL TRANSFORMATION

If I'm an engineer, I need to know about my equipment. How many pumps are in the field? What kind of equipment is on Line 1? What's the status of all of my packaging machines? How is the bearing temperature of Motor 1 compared to Motor 2?

This is data in context versus tag names with values in my system. I need the data to tell me what I need to know, when I need to know it and in a centralized environment that enables me to act upon that data anywhere, any time.

IoT needs ten times the data in today's changing industrial landscape. Sensors are cheaper, so they are easily deployed in multiple scenarios. High speed networks provide the ability to manage huge amounts of data that come from those sensors at a reasonable cost. Unprecedented computational power through the cloud and the proliferation of mobile and touch interfaces increase the amount of data available.

Digital transformation is a journey. Companies worldwide are looking to connect, collect and store, visualize and analyze, and optimize their data. They are looking for solutions that can connect, aggregate and visualize their data across multiple assets to drive down operational costs and achieve consistent quality in their plants – regardless of industry.

The visualize and analyze piece is where companies are looking to Democratization of Data to unlock the value of existing data. How do we pull in non-traditional data, historical and data from other systems? Contextual data analysis gives you a view that you didn't have before. An operational view. How do we enable this?

Proficy Operations Hub is a solution from GE Vernova that offers centralized visualization/configuration, digitized processes and democratized digital tools to enable collaboration and continuous improvements. It provides visualization enabled across all levels and roles within the plant and enterprise for business intelligence.

A democratized tool in the hands of all plant users enables them to increase operational efficiency and make better decisions based on comprehensive information – real time, historical, automation and MES, and third party – that's easier to analyze and act upon independent of location.

As one example, a customer has employed Proficy Operations Hub to democratize their digital tools within the plant. Managers and supervisors promote KPIs to plant dashboards to be seen and be accessible by all employees on the plant floor. Users create KPI trends, dashboards and favorites to monitor utilities. All users in the plant use the tool to analyze, troubleshoot and monitor operational information through a timeline of events and then share dashboards that result in improvements, which ultimately benefit the business.

Increased visibility into production process status and progress in real time enables continuous improvement through digital tools. Unlock your operations intelligence to realize optimized plant operations.

ASSET MODELS FOR CONTEXT

Enable more employees to make better use of the data being collected

What does the tag ALB_BLDG1_L1_M47_DISPUMP1_RPM mean?

We often hear statements like “we only get value from 5% of the data collected.” New approaches help industrial organizations overcome the challenges of getting real value from the data being collected.

The first step in turning data into information is creating context for the data.

What does this mean?

Whether data is from an HMI/SCADA system (collected from PLC memory locations), time series and Alarm and Event data from a Historian, or IoT sensor data, industrial data is typically identified by a “tag name.” People that work with the data every day may understand how these “tags” correlate to signals coming from the plant equipment or other sensors. The problem is that set of people represents a small percentage of the people that could potentially get value from the data.

The answer is to create a mapping between the tag data and a representation of the machine/line/plant…/enterprise – called an asset model. Any user who wants to know the value of any specific sensor (such as RPMs of a pump) can find the specific pump in the model and see the data values associated with the pump, RPMs in this example.

Asset modeling today includes the ability to create standard object types (think templates) that include the standard set of information associated with a type of equipment. Having standard object types (templates) that can be referenced for each similar piece of equipment further enhances users’ ability to understand the plant equipment. Comparison of the parameters associated with multiple examples of a given equipment type becomes simple.

So what does the tag ALB_BLDG1_L1_M47_DISPUMP1_RPM mean?

Probably only a few people know the answer. However, almost everyone can understand what the RPM parameter for the discharge pump number one on Mixing Machine 2 in Building 1, Line 1 in Albuquerque means. And if they want to compare the behavior of Discharge Pump 1 and Discharge Pump 2, no problem. Context makes all the difference.

Putting information (Data in context) in the hands of every user

One of the fascinating impacts of the age of IoT is the merging of two trends – a workforce of digital natives that are comfortable with technology and technology toolsets that simplify the task of creating applications that show operators the right mashups of information from various business systems, on their device of choice.

The newest generation of web technology based application development tools are designed with the following capabilities:

- Drag and Drop, code free application building
- Mobile operator support, including responsiveness to device type (desktop, tablet, phone, smartwatch)
- Asset model context for data and analysis tools
- Security features allowing control of data visibility and application functionality (read only vs read write, for example)
- Unlimited developer and runtime licenses

The combination of easy to use tools and data in context of an asset model has created an opportunity for individuals to create web-based applications that show plant data in the way they want to see it. Individuals can build mini apps (web pages), link them together, and share them amongst their peers. Since the mini apps are asset model aware, other users that manage similar assets elsewhere in the organization can use the mini apps unchanged by navigating to the asset they manage within the context of the app and asset model. All of this is possible within the network and IT security infrastructure that exists within plants today.

This ability for the individual to explore, create, test, modify, and share tools that enable better outcomes represents a sea change from the current paradigm where system design is managed by a few “experts.” DCS’s, HMI/SCADA’s, historians, and even operator interfaces – all require a level of expertise, access to development tools, and change management processes. For these operational systems, the engineering practices are applied to systems that interact with plant equipment. The new generation of tools is designed to interface with these source systems and other data sources (smart sensors, other business systems) to provide information which enables better decision making in a novel way.

For companies looking to accelerate their digitization journey and take advantage of the skills of the new digital native generation of employees these new web technology-based tools can play a key role in achieving these goals.

UNDERSTANDING AND MINIMIZING HMI/SCADA SYSTEM SECURITY GAPS

Introduction

Being at the heart of an operation's data visualization, control and reporting for operational improvements, HMI/SCADA systems have received a great deal of attention, especially due to various cyber threats and other media-fueled vulnerabilities.

The focus on HMI/SCADA security has grown exponentially, and as a result, users of HMI/SCADA systems across the globe are increasingly taking steps to protect this key element of their operations.

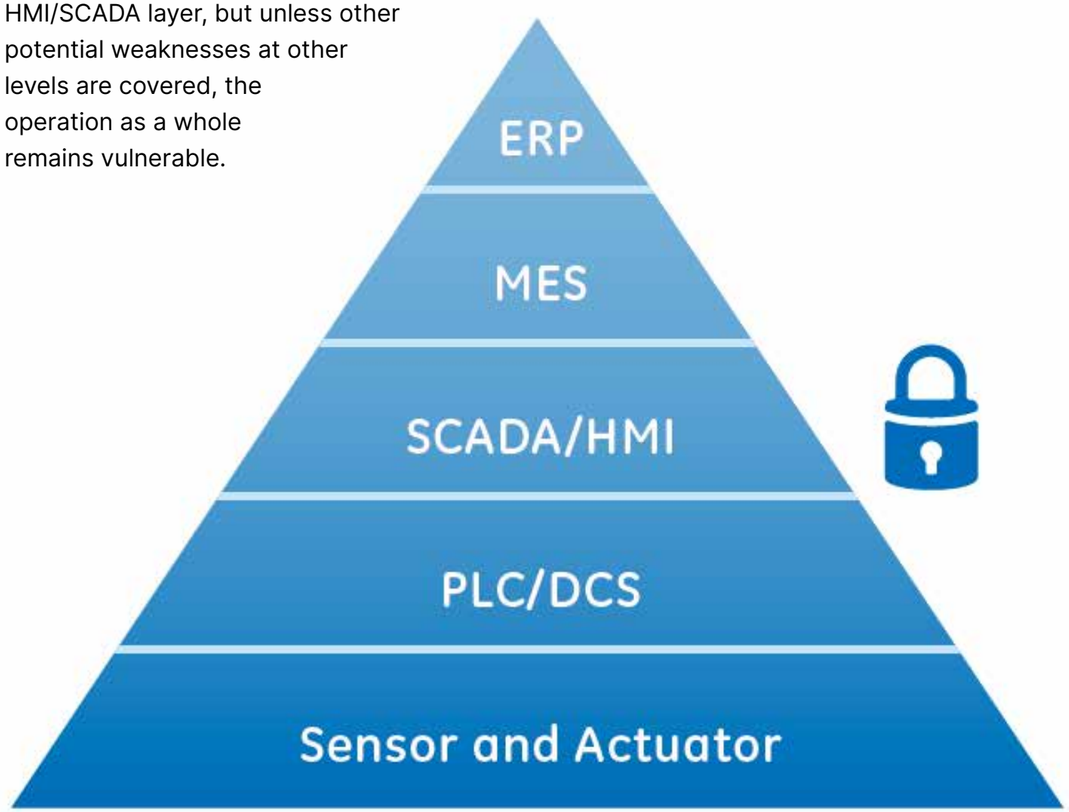
The HMI/SCADA market has been evolving with functionality, scalability and interoperability at the forefront. For example, HMI/SCADA software has evolved from being a programming package that enables quick development of an application to visualize data within a programmable logic controller (PLC) to being a development suite of products that delivers powerful 3-D visualizations, intelligent control capabilities, data recording functions, and networkability.

With HMI/SCADA systems advancing technologically and implementations becoming increasingly complex, some industry standards have emerged with the goal of improving security. However, part of the challenge is knowing where to start in securing the entire system.

The purpose of this chapter is to explain where vulnerabilities within a HMI/SCADA system may lie, describe how the inherent security of system designs minimize some risks, outline some proactive steps businesses can take, and highlight several software capabilities that companies can leverage to further enhance their security.

SCADA security in context

The International Society of Automation (ISA) production model demonstrates the layered structure of a typical operation, and shows that HMI/SCADA security is only one part of an effective cyber-security strategy. These layers of automated solution suites share data, and wherever data is shared between devices, there is a possibility for unauthorized access and manipulation of that data.
This chapter concentrates on the HMI/SCADA layer, but unless other potential weaknesses at other levels are covered, the operation as a whole remains vulnerable.



COMPONENT VULNERABILITIES WITHIN AN HMI/SCADA SYSTEM

To minimize existing security gaps, companies need to first understand where potential vulnerabilities typically lie within the system. Powerful software features, along with the advancements in automation hardware and industrial communications, have made control systems multi-layered, complex and susceptible to threats. An HMI/SCADA system's level of security is best understood if broken down into two major elements: Communication and Software Technology.

Communication

Communication advancements have made large-scale HMI/SCADA system implementations successful for many industry applications. There are two levels of communication that exist within the system—information technology (IT) and the field, which have notable security level differences.

IT – Components of an HMI/SCADA system are modular, not only to allow for easy troubleshooting but also to distribute the computing load and eliminate a single point of failure. It is not uncommon to have multiple thick, thin, web and mobile runtime clients connected to the main HMI/SCADA server hub over an internal Ethernet-based network; however in some cases, systems may use external leased lines, modems, wireless, cellular, or satellite technologies as well.

The main HMI/SCADA server hub also consists of multiple networked servers to distribute the load, ensure uptime, and store the mass amount of data. With these components all networked in some way, they use standardized common protocols to transfer data—all of which are largely unencrypted, requiring weak or no authentication.

Field – HMI/SCADA implementations frequently consist of a number of widely dispersed remote sites with a control or data gathering function, all connected to a central control and monitoring point. Data has to be passed between the control room and the remote terminal units (RTUs) over a network (which may be fiber optic, telephone or wireless), and the protocols for passing this data have frequently been developed with an emphasis on reliability and ease of implementation rather than security.

Modern computing facilities have made secure practical encryption almost impossible to defend against a determined hacker, so communications between devices need to employ several layers of defense with the primary aim to make access to the data difficult, and detect if the data has been compromised.

Software technology

Software over the years has largely become feature-bloated as companies keep adding new capabilities while maintaining all of the existing ones, increasing the complexity of software security. There are two separate but dependent software technologies in the system, the HMI/SCADA software and the Platform Operating System, which have distinct differences when it comes to security.

HMI/SCADA Software – Most HMI/SCADA software installations have either external network connections or direct Internet-based connectivity to perform remote maintenance functions and/or connect up to enterprise systems. While these types of connections help companies reduce labor costs and increase the efficiency of their field technicians, it is a key entry point for anyone attempting to access with a malicious intent.

Platform Operating System – Operating systems that employ elements of consumer or "open" source operating systems such as Windows Server, Linux and Unix variants are increasingly popular since they help reduce costs. This trend toward open technologies has made proprietary custom, closed, highly secure systems a direction of the past, but it increases the risks.

Also, due to the fact that HMI/SCADA systems are complex and contain multiple layers of technology, even a simple system patch is a major undertaking that requires planning, funding and time. The risk elements are also substantial because many systems now rely solely on their HMI/SCADA system for visualization, data recording and some control elements. And to this point, some companies hold back on patches, service packs and upgrades, while others choose not to apply any new patches, employing a "it works, don't touch it" policy. Furthermore, software patches have generally been developed to cover for a security breach that has already occurred.

Some would say that even if companies could keep their platforms current, with the fast pace of consumer-based operating systems and large number of system exploits, platform operating systems are the single largest security risk in the system.

THE INHERENT SECURITY OF SYSTEM DESIGNS MINIMIZES SOME RISKS

The good news is that some vulnerability is minimized by the nature of system design and HMI/SCADA software design, whereby the fundamental principles and canons of engineering mandate safe and reliable systems. This ensures a basic level of security to protect against an intruder.

Engineers design systems with intentionally broken automated chains—meaning in some cases functions require physical confirmation prior to the software performing commands and in other cases, the SCADA software only does a portion of the command, requiring one or many additional manual steps to execute the function. Inherent system security is best surmised at the software and hardware levels.

Software: With many viewing HMI/SCADA software as a visualization tool that provides a means for dynamic operator input and visualization as a flexible information terminal, the reality is that HMI/SCADA software capabilities are much more exhaustive. When elements are added such as control and logic capabilities, system engineers must examine the risk from a potential failure standpoint and the extent of control that is allowed without being in line of sight of the area being controlled.

Software is also developed from the operator's perspective and uses company guidelines throughout the application to ensure the operator is controlling with intent. While this doesn't necessarily bring additional security from external intruders, it does provide enhanced protection against mistakes. For example, the "select before operate" design philosophy is typically used in HMI/SCADA applications, which requires the operator to select an item on the screen, pull up the controlling elements, operate the item, and finally confirm to send the command. While this may seem like a simple ideology or a drawn out process, this intentional design ensures that an operator's actions are deliberate as opposed to a hasty reaction to an urgent situation.

Hardware: At this level, design engineers employ many techniques to ensure safe control, either physically or by the HMI/SCADA software. Thousands of individual devices and RTUs can exist in a system and are typically implemented with an area-based manual or automatic control selection; field technicians use manual control to perform maintenance or to address a software failure—locking out the software control and establishing local control.

Additionally, when engineers design this level of the system, many hardware-based fail-safes are built in the design such as fusing or hardwire interlock logic to examine the local situation, so when components are commanded by the HMI/SCADA software, there is a hardware level of checks to ensure it can be executed. This protects the system from unsafe or even incorrect software control. Furthermore, many critical applications use triple and quad redundant logic controllers to ensure continuous operations.

Taking into account the general design rule that system engineers apply for all levels of a system can be surmised by "if a single point of failure exists, protect it or provide secondary means." Therefore, design philosophies typically drive a holistically safe and secure-by-design environment, which can severely impede an intruder's ability at the HMI/SCADA level to impact the entire system.

INHERENT SECURITY EXAMPLES

1. Manufacturing and Part Movement

a. An HMI/SCADA system is programmed to command an automated gantry to move manually.

b. To move the automated gantry, the HMI/SCADA “soft” button must be engaged as well as separate manual pushbuttons.

c. The automated gantry system is also interlocked with photoelectric sensors, and will not move if it detects any object within its operating area.

d. Additionally, there are two physical mats on the plant floor outside the operating area within line of sight of the gantry on the plant floor—one in front of the HMI/SCADA terminal and one in front of the manual pushbutton station. These mats have built-in sensors to ensure that someone is physically present prior to operating.

e. All conditions must be true for the automated gantry systems’ manual functions to be powered up and engaged. This type of system design is largely for the safety of the workforce, but also ensures that hackers cannot independently operate this function if they have control of the HMI/ SCADA system.

2. Water Treatment and Chemical Control

a. An HMI/SCADA system in a water treatment plant is the main control point for chemicals being added to the water.

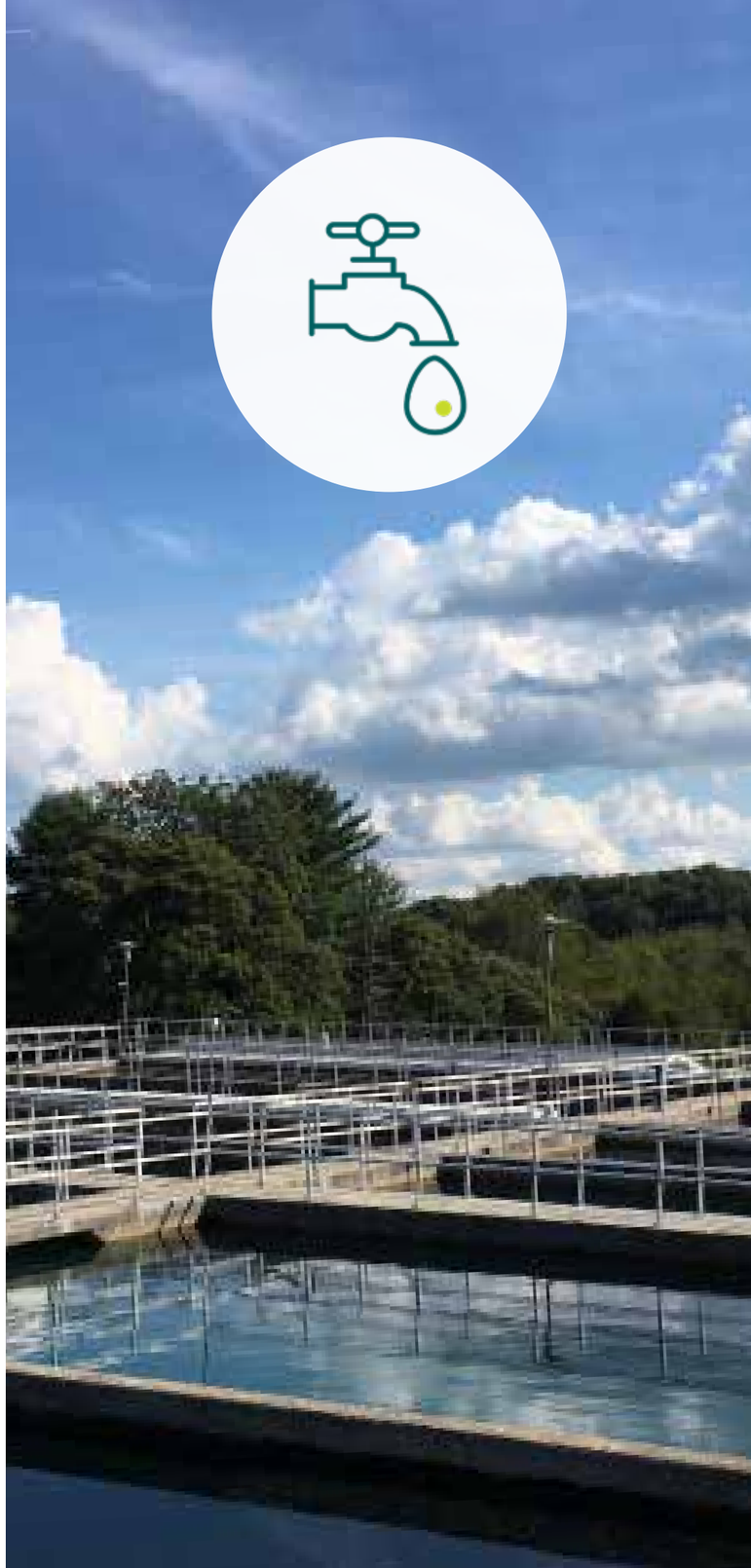
b. One of the key chemicals controlled by the HMI/ SCADA system is chlorine. Excessive amounts of chlorine could be hazardous to public health, and conversely too little can also put people in danger, so engineers have designed a level of safety into the automation system.

c. While the HMI/SCADA system controls the main chlorine values, downstream chlorine meters continuously measure the concentration level and have the ability to cut off the chlorine addition in the event of abnormal levels.

d. The metering control elements are isolated from the HMI/ SCADA control with the only interaction between the systems being a one-way alarming connection to annunciate in the event of abnormal levels of chlorine.

e. Additionally, water treatment facilities are mandated to frequently test the chemical makeup of the outgoing water. The system’s operators analyze the test results daily and have the ability to cut off and bypass the chemical systems based on the test results.

f. With this multi-tiered automation and manual ability designed into the system, the system as a whole has an inherent level of security against rogue remote control and malicious attacks.



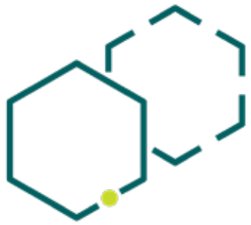
CONSIDERATIONS TO CRITICALLY EXAMINE YOUR SYSTEM

1. Examine your field assets, particularly older, remote components

- How does the SCADA communicate with them? Can this be secured?
- Is the control network adequately separated from other networks?
- Where are the points of entry/failure? Are there redundant options?

2. Examine your IT assets

- Are the services/software running on an asset the minimum needed to maintain functionality?
- How secure is that software and does the software employ passwords, biometrics or retina protection?
- Do you have easy access to the operating system and SCADA system patches? Is this performed regularly?



3. Examine your change management software policy

- What is the policy for implementing an operating system and SCADA patches – does it cover all assets?
- Are all assets protected (covered by firewalls and anti-virus software)?
- How easy is it to manage user accounts across all layers of software – is there an integrated system that includes the operating system and software products or does each product have separate user accounts and passwords?

4. Examine your access control

- Does your SCADA software allow anonymous client connections?
- Is there a robust login policy with regular renewal of passwords?
- Does each user have an appropriate limit to their actions?

BE PROACTIVE: ENHANCE YOUR SECURITY WITH SOFTWARE CAPABILITIES

However, even the safest system design and industry standards cannot secure a system 100%, and therefore, companies should not rely on them wholly to protect their systems. Instead, they should take a proactive approach to enhancing security, and a good starting point is knowing what technologies are available to help them best meet their needs.

Selecting a trusted solution provider with deep expertise, experience and advanced technologies is also critical. Off the- shelf solutions such as GE Vernova's iFIX and CIMPLICITY HMI/SCADA software have successfully helped companies minimize their security gaps with a broad range of security-based software technologies, including:

- **Biometrics** – When bio-security elements are integrated to the system, customers can program their system to require finger scans to perform specific functions such as switching on and off the grid's main switch gears, which ensures that the appropriate person be physically present to execute the order. This type of integration eliminates the possibility of a hacker performing the same operation virtually—reducing the overall potential impact and enhancing the overall system security.
- **Electronic Signature** – Many view this option as a simple reporting tool, however the features are much more comprehensive. For example, it can introduce authentication potential at the command level to verify the user performing the operation with a username and password as well as a separate authentication, typically a manager, for verification. The information is then stored in a system audit trail that can be recalled in the future; some customers also choose to integrate this feature with biometrics to eliminate the use of a single, widely known username and password.
- **Authorized Connections & Client/Server Data Encryption** – Many off-the-shelf HMI/SCADA software products now have built-in features that limit the allowable client connections to known computers and use integrated data encryption for client communications. This protective capability eliminates the possibility of a hacker simply loading the HMI/SCADA client and connecting over the network.
- **Domain Authentication** – To leverage complex alphanumeric passwords at the HMI/SCADA level, some software packages offer an add-on capability that introduces Windows® Domain Authentication security integration. For example, GE Vernova features an application add on that maps group memberships to its HMI/SCADA software roles and when integrated, the users and subsequent passwords are managed at the IT level. This allows for the HMI/SCADA application to leverage existing group IT-level policies, which are typically very stringent and can exceed industry requirements.

INVESTING IN SYSTEM SECURITY IN TODAY'S BUSINESS CLIMATE

Improving an overall system's security can be a costly endeavor, and companies must find the right balance between spend, design and process to make their systems safe. This is especially true as companies face increasing cost reductions mandated in today's challenging economic environment. In response, off-the-shelf HMI/SCADA vendors have developed industry solution packs that include specifically tailored tools to help reduce development and overall system costs.

For example, GE Vernova offers several solutions with complete, pre-developed, HMI/SCADA drag-and-drop elements, graphics, toolsets and configuration tools that significantly reduce both the initial and ongoing costs associated with HMI/ SCADA software. Companies can then re-route the resulting cost savings into additional security software and hardware to augment the inherent safety of their systems—reducing overall vulnerability.

The cost of implementing an HMI/SCADA security policy should also be evaluated against the risk of a security breach—in terms of reputation, liability and intellectual property. Companies may discover a proactive approach actually reduces overall costs by ensuring business continuity when compared to the potential operational and financial loss that can occur due to the exposure of an unprotected system.

Always refer to your software provider's Secure Deployment Guide.

CONCLUSION

The vulnerabilities of HMI/SCADA systems can pose a serious threat, and the complexity of multi-layered technologies can make it difficult to completely secure one's operation. As discussed in this chapter, the inherent safe design of most HMI/SCADA systems offers some protection, but they are by no means enough to fully protect systems.

That's why it's important for companies to better understand where vulnerabilities exist within their systems and to take a proactive approach to address those susceptible areas. Off-the shelf HMI/SCADA vendors offer software solutions with security based capabilities, which can help companies enhance the protection of their critical infrastructure assets and reduce costs for a sustainable competitive advantage.