Understanding and Minimizing Your 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.

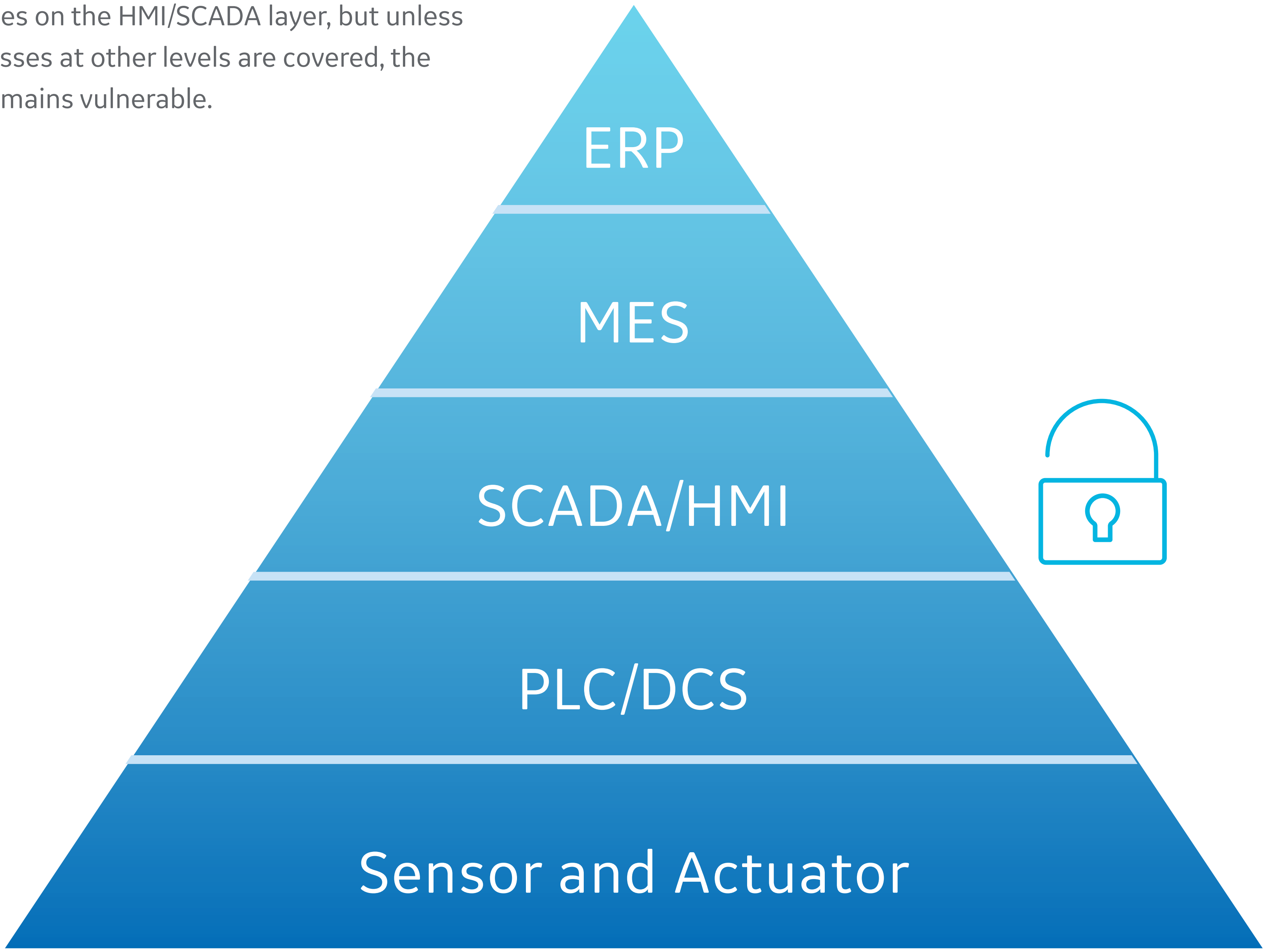
The HMI/SCADA market has been evolving with functionality, scalability and interoperability at the forefront. For example, HMI/SCADA software has evolved from being a programming package that enables quick development of an application to visualize data within a programmable logic controller (PLC) to 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 paper 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 white paper 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 Internetbased 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 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 builtin 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 a hacker cannot independently operate this function if he has 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 automatic?
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-theshelf solutions such as GE Digital's HMI/SCADA iFIX 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 switchgears, 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 Digital 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.

Funding 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 Digital 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 the exposure of an unprotected system.

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 paper, 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-theshelf HMI/SCADA vendors offer software solutions with securitybased capabilities, which can help companies enhance the protection of their critical infrastructure assets and reduce costs for a sustainable competitive advantage.

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.ge.com/digital