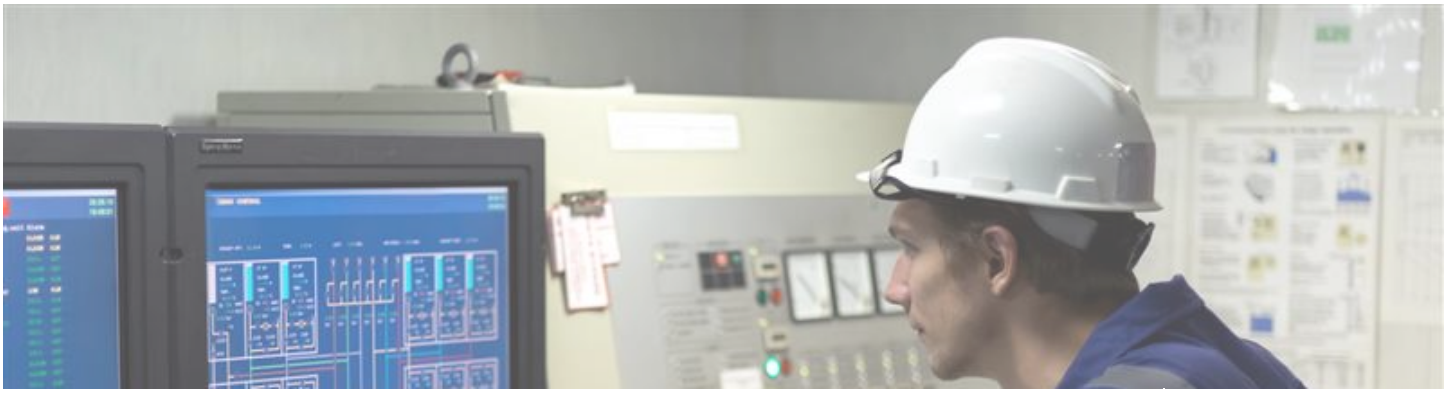
One Flaw too Many: Vulnerabilities in SCADA Systems

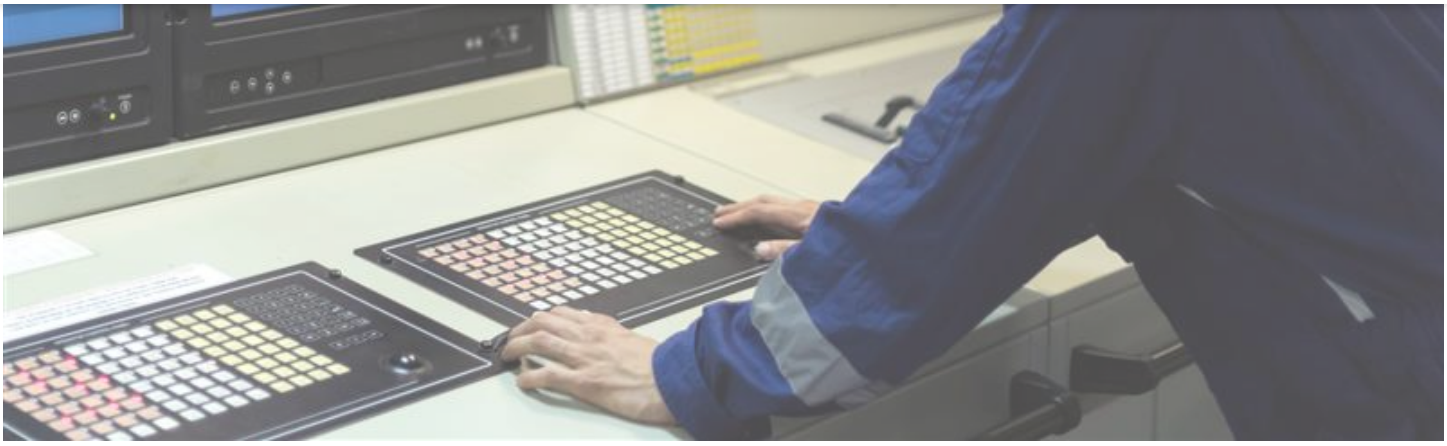
December 16, 2019

What is the current state of SCADA vulnerabilities? Staying informed is essential in the fight against exploits and cyberattacks with real-world consequences.

Supervisory control and data acquisition (SCADA) systems have been at the heart of processes used by many different industries, from the control of machinery in power plants to the management of traffic lights in cities. Because SCADA systems play important roles in very critical processes, an unchecked weakness could cause grave real-world consequences.

As they have taken on more capabilities over the years—both as a product of an increasingly connected world and to meet new demands—it is important to revisit what kind of vulnerabilities have been discovered in SCADA systems and learn how to secure them.

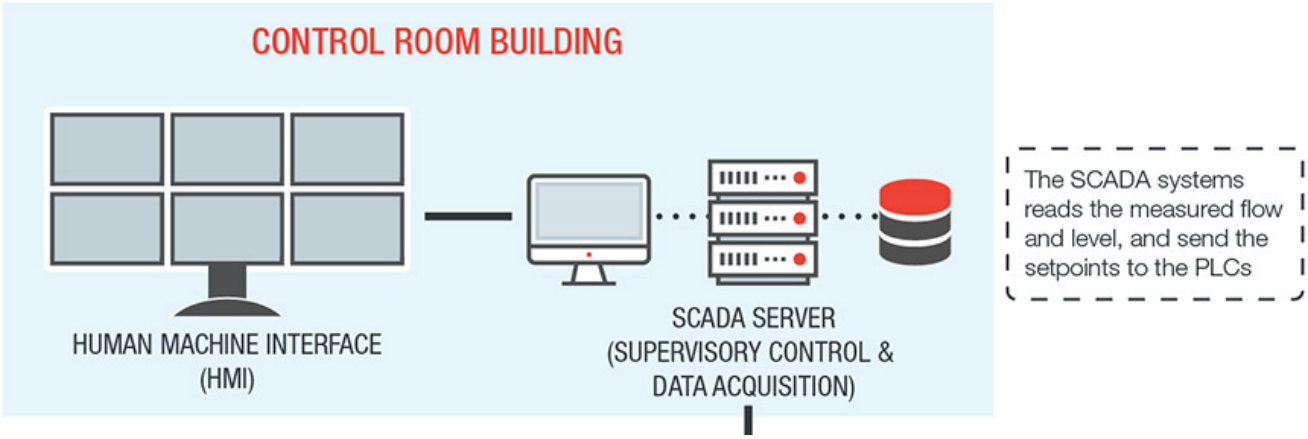


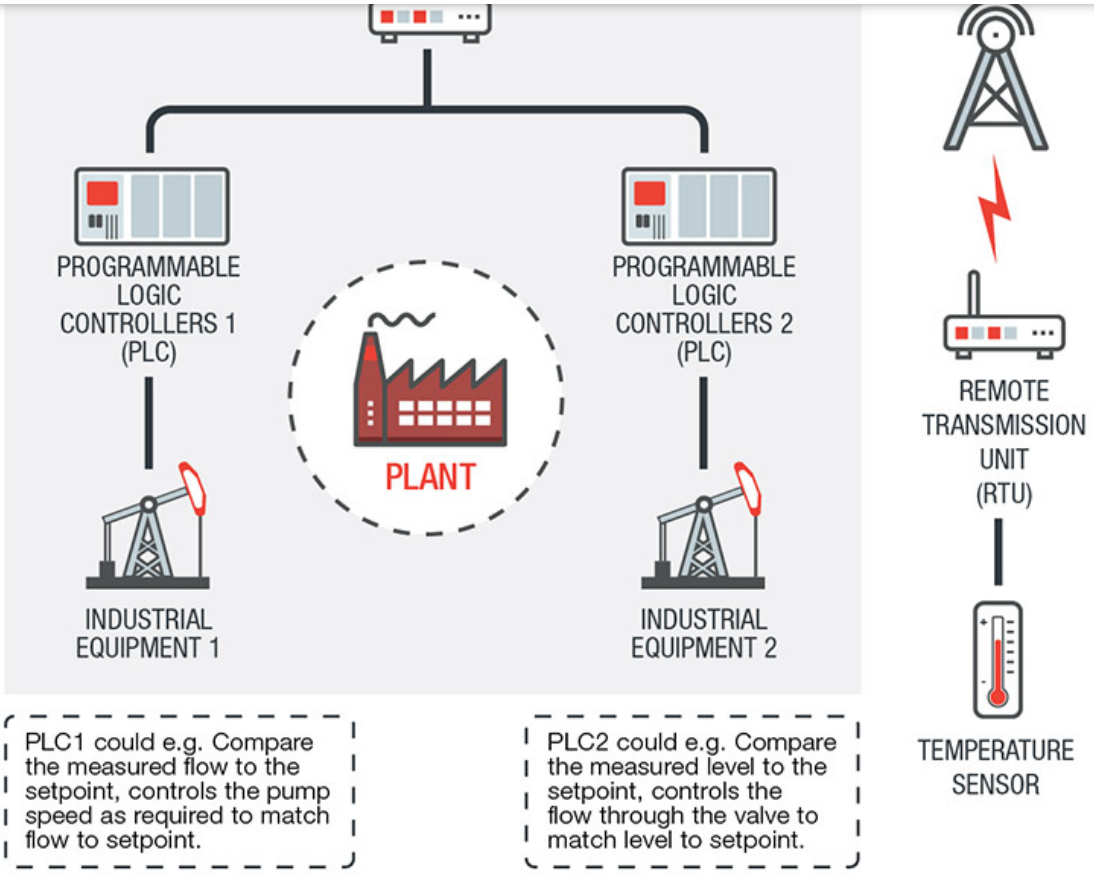


What are SCADA systems and where are they found?

Understanding the components of SCADA systems and their functions allow us to see where vulnerabilities are likely to exist in them. SCADA systems have been around for decades. They're a product of the automation era of manufacturing, and continue to exist in the dawning era of cyber physical systems (CPS), or Industry 4.0.

In a nutshell, SCADA systems are industrial control systems (ICS) that specifically provide supervisory-level control over machinery and/or industrial processes that span a wide geographical area (such as energy distribution plants). SCADA systems contain Supervisory Computers as well as many other devices, chief of which are Programmable Logic Controllers (PLCs) and Remote Transmission Units (RTUs). Both PLCs and RTUs participate in the local management of more specific sub-processes. PLCs have sensors and actuators that receive commands from and send information to other components of the SCADA system.





PLCs, RTUs, and other sensors connected to SCADA systems collect data that help plant supervisors make critical decisions based on real-time information. Supervisors need only to look at the Human Machine Interfaces (HMIs), where the different functions and data elements of SCADA systems are presented for human review and control.

As can be surmised from its functions, SCADA systems are versatile and can be found in all kinds of industrial settings and infrastructures. Here are some of the sectors and infrastructures that apply SCADA to their processes:

Smart buildings

Smart cities and transportation networks

Oil and gas

Energy generation and distribution

Waste water treatment and distribution

Manufacturing

Food production

The current SCADA market indicates that industries continue to see the benefits modern SCADA systems provide their processes. In fact, the market is forecast to reach US$47.04 billion by 2025. However, SCADA systems' vulnerabilities and the evolving threats that target them present a challenge for its integrators. Not only can these vulnerabilities lead to potential financial losses; they can also easily translate to cascading effects down the supply chain, especially in the case of critical infrastructure.

Critical Infrastructures Exposed and at Risk: Energy and Water Industries

Securing energy and water should remain top priority in the continuing integration of the industrial internet of things in these critical sectors.

What is the state of SCADA vulnerabilities?

Unfortunately, based on the continued reports received by Trend Micro Zero Day Initiative (ZDI), vulnerabilities have been and will likely continue to plague SCADA systems for some time. In the last five years, 2018 saw the greatest number of

general idea of where weaknesses can be found when it comes to SCADA systems.

Total number of discovered vulnerabilities per year from 2015 to October of 2019

In 2015, vulnerabilities were found in Schneider Electric's ProClima software which is designed to help in the thermal management of an environment. By tricking a target user to open a malicious file or visit a malicious URL, threat actors can execute arbitrary code on the system.

2016 saw a spike in discovered vulnerabilities, most of which from the vendor Advantech. Its WebAccess SCADA software had 109 discovered vulnerabilities during this year. An example of these include the inadequate validation found in one of its components that could lead to threat actors executing arbitrary code.

The slight decrease in 2017 was followed by a jump in 2018. A large portion of this count were from WebAccess and Wecon's LeviStudioU, an HMI software. Delta Industrial Automation and Omron were also among the vendors that had newly discovered vulnerabilities in 2018. For the former, most of the vulnerabilities were from DOPSoft, while for the latter it was CX-Supervisor. Both are HMI software packages.

In 2019, many of the same vendors had vulnerabilities reported in their SCADA software. Same as the previous year, WebAccess and LeviStudioU recorded the

Vendors with the greatest number of discovered vulnerabilities in the past 5 years

Even within the limits of the data set, the varied source and nature of these discoveries seem to imply that a wide range of vulnerabilities still exist across the vendors in the market. It should be noted that SCADA system vulnerabilities still frequently include unsophisticated bugs like stack and buffer overflows, as well as information disclosure and others. These vulnerabilities allow attackers to execute arbitrary code (RCE), perform denial of service (DoS), or steal information.

Where can vulnerabilities be found in SCADA systems?

Rooting out where vulnerabilities can exist in SCADA systems can help integrators understand how and where to apply mitigations to prevent exploitation and neutralize attacks. Unfortunately, SCADA systems oversee a large number of devices, sensors, and software, which equates to a wider attack surface.

HMI

The State of SCADA HMI Vulnerabilities

A complete discussion of the different vulnerability categories, including case studies of vulnerable SCADA HMIs.

HMIs display data from various sensors and machines connected to a SCADA system to help users make decisions that they can also implement using the same interface. Because of its capabilities and role in SCADA systems, HMIs can be an ideal target for potential threat actors aiming to gain control over processes or steal critical information.

Mobile applications and web interfaces

Mobile applications are used both locally through tablets that help engineers control PLCs and RTUs, and remotely allowing engineers to connect to the ICS through the internet. However, a vulnerability in such applications can mean openings for attacks in exchange for convenience. Some research in 2018 by Alexander Bolshev and Ivan Yushkevich revealed a total of 147 vulnerabilities from 20 applications with some that could allow potential threat actors a chance to directly influence industrial processes or give them an opening to trick operators into making wrong decisions regarding these processes.

MQTT and CoAP: Security and Privacy Issues in IoT and IIoT Communication Protocols

We looked into MQTT brokers and CoAP servers around the world to assess IoT protocol security. Learn how to prevent risks and secure machine-to-machine (M2M) communications over MQTT and CoAP in our research.

Protocols

Communication protocols such as Modbus and Profinet help control different mechanisms supervised by SCADA systems. But they lack the security capabilities

malfunction of a SCADA system should they modify the data sent from PLCs and RTUs or tamper with firmware.

Other Components

There are countless technologies in place to make individual parts of SCADA systems stay connected, dynamic, and work in real-time. Some of these components may be ill-equipped for the threats currently faced by different industries. These components may not necessarily be used for SCADA systems exclusively, but are staples for other technologies and systems. One such example is the set of vulnerabilities known collectively as URGENT/11 which greatly affected the medical industry and SCADA systems.

What is the impact of these vulnerabilities?

Previous attacks against industrial facilities have highlighted the impact of attacks on SCADA systems. Possibly the most well-known was the Stuxnet worm in 2010 that targeted industrial facilities through SCADA vulnerabilities. In 2016, the malware known as Industroyer caused power outages in Ukraine. While in 2017, the Trojan Triton targeted industrial safety systems that caused an operational shutdown. Such cyberattacks continue to exist today—an Indian nuclear power plant was discovered to have suffered from a cyberattack that may have been meant for espionage and data exfiltration.

where we found an interest and curiosity in SCADA software and industrial equipment like smart meters. Though these forums seem to show that many don't have a sophisticated monetization scheme in place for SCADA-related attacks, researchers predict that attacks will become more common as more PLCs and HMIs are found online. They also surmise that should a monetization scheme materialize, it would likely involve extortion, with cybercriminals threatening organizations with downtime.

What further raises the urgency of fixing vulnerabilities in SCADA systems is how they enable the success of future cyberattacks with similar, if not more severe consequences as those that have happened in the past. The impact of an attack on SCADA systems could range from downtime, production delays, cascading effects down the supply chain, damage to equipment, to critical human safety hazards. These are consequences that organizations and governments would like to avoid, and are consequently easy to leverage by cybercriminal groups of whatever motivation.

Defending against SCADA attacks

Thankfully most of the vulnerabilities that were reported and mentioned above have already been addressed by their respective vendors. Ultimately, the fight against exploits means being vigilant for new vulnerability discoveries as well as applying new patches to fix them. Aside from managing vulnerabilities, organizations must also maintain security measures that can defend against cyberattacks, especially given the consequences these attacks imply.

Here are some steps organizations can follow, some of which are based on National Institute of Standards and Technology's NIST's guide to ICS security:

- **Use virtual patching to help manage updates and patches**. Patching for vulnerabilities though critical for SCADA systems means heavy planning and scheduling to prepare for possible downtime these patches may require. Virtual patching can help manage vulnerabilities and prevent exploits when patches cannot be immediately deployed or at all implemented.
- **Apply network segmentation**. Partitioning networks can prevent the spread of malware and efficiently contain attacks. Network segmentation also minimizes the chances of exposure of sensitive information.

firewalls between such networks can prevent the lateral movement of attacks from one to another.

- **Properly manage authorization and user accounts**. Regularly monitoring and assessing who has authorization and access to certain facets of SCADA systems can help reduce unexpected openings for both cyber and physical threats.
- **Use endpoint protection on engineering workstations connected to SCADA for device programming and control adjustments**. Adequate endpoint protection creates a stronger defense against perimeter threats.
- **Maintain strict policies for devices that are allowed to connect to SCADA networks**. Implementing strict policies for connecting devices to SCADA networks reduces unforeseen entry points for potential attacks.
- **Restrict the roles of transitory SCADA nodes to a single purpose**. Having a single purpose for transitory nodes lowers the chances of unknowingly exposing these nodes or having them accessed by unauthorized users.
- **Prevent the use of unknown and untrusted USB devices**. Removable devices are potential attack vectors that can be overlooked by users. Using only trusted USB devices can minimize the chances of malware infection.

RECENT POSTS

Mispadu Banking Trojan Resurfaces

Securing Enterprise Security: How to Manage the New Generation of Access Control Devices

Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals

New Bait Used in Instagram Profile Hacking Scheme

The Basics of Keeping Kubernetes Clusters Secure

RELATED POSTS

Securing Enterprise Security: How to Manage the New Generation of Access Control Devices

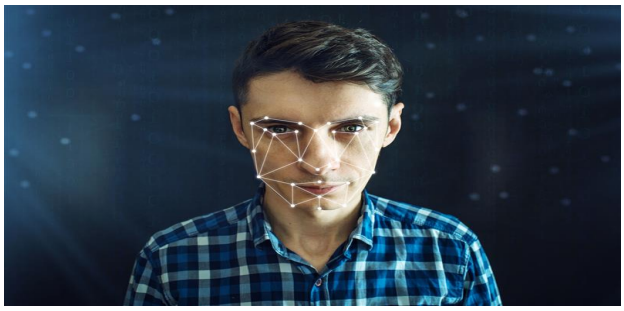
Securing the Pandemic-Disrupted Workplace: Trend Micro 2020 Midyear Cybersecurity Report

Lost in Translation: When Industrial Protocol Translation goes Wrong

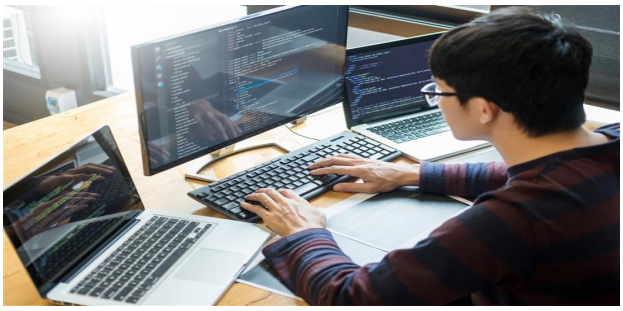
Unveiling the Hidden Risks of Industrial Automation Programming

Posted in Vulnerabilities & Exploits, Internet of Things, Vulnerability Research, Exploits

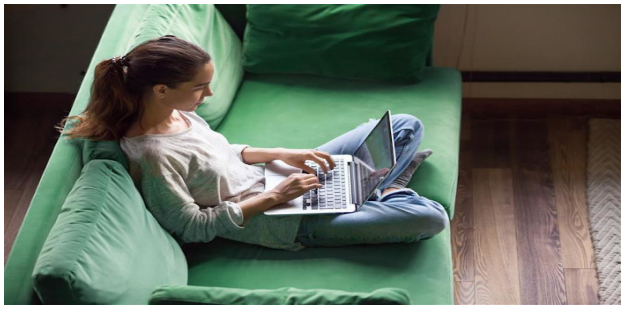
We Recommend



Securing Enterprise Security: How to Manage the New Generation of Access Control Devices



The Basics of Keeping Kubernetes Clusters Secure



Know the Symptoms: Protect Your Devices While Working From Home

Alexa and Google Home Devices can be Abused to Phish and Eavesdrop on Users, Research Finds

Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats.
View the 2020 Security Predictions

Our 2020 Midyear Security Roundup delves into the pertinent challenges faced amid a pandemic, including Covid-19-related threats and targeted ransomware attacks. Read more as we share how to secure systems in this increasingly precarious landscape.
View the 2020 Midyear Security Roundup