# INDUSTRIAL CONTROL SYSTEMS

## WHAT ARE INDUSTRIAL CONTROL SYSTEMS AND WHY IS IT IMPORTANT TO SECURE THEM?

*Ir. Tejinder Singh, CISSP*

*Typical control room*

What is an Industrial Control System (ICS)? You may have heard a lot of different acronyms that purport to describe ICS, SCADA or Supervisory Control and Data Acquisition, DCS Distributed Control System, PLC or Programmable Logic Controllers.

Basically ICS is any system – whether it is a PC or other purpose-built hardware or software – that is actually controlling a process in the real world. You can find these types of systems in industries like manufacturing, oil & gas, petro-chemical and other types of industrial sectors. One of the key things in defining industrial control systems is to really get the differentiation between other terms like critical infrastructure and Internet of Things.

In industrial control systems, the keyword is INDUSTRIAL. A system that automates milking cows would definitely fall into the category of an industrial control system; however, I would not consider this as critical infrastructure.

Likewise, something such as a Wall Street financial system is certainly critical infrastructure but is probably not an industrial control system as it contains only information-based type assets and does not control anything in the physical world. Certainly there is a lot of overlap between ICS and critical infrastructure. Think about electricity and water for example.

The last thing to talk about is the Internet of Things (IoT) Here the keyword is "things". This is where networks merge with previously-unconnected everyday items such as door locks, cars, toasters, trains and drones; it is a big trend in both the consumer and the industrial sectors.

You can have something that is a part of IoT and which is also in an industrial control system and certainly something that's part of the IoT in an industrial control system which is also part of critical infrastructure.

### WHAT TO THINK ABOUT WHEN BUILDING AN ICS SECURITY PROGRAM

In traditional enterprise IT, we think about information security as achieving confidentiality, integrity and availability of information with confidentiality being our primary concern. We want to protect data like personal identifiable information, credit card numbers or intellectual property. We want to keep secret data secret.

In ICS, our primary consideration is safety, followed by availability, where we ensure the control system stays up and running. Integrity here ensures that what is on the control room screen actually matches what is going on in reality. There can be some intellectual property on the plant floor or maybe on an engineering laptop, so confidentiality does come into play. However, information like the fill level of a particular tank doesn't require the same level of security controls that you will have on sensitive data that you will find on the IT network.

## THINGS TO KEEP IN MIND WHEN BUILDING AN ICS SECURITY PROGRAM

1. Industrial control systems are really hard to change, as some of them have 20/30-year lifecycles. The attitude in the ICS world is if it's working, don't touch it. This makes traditional enterprise IT security activities such as security testing and patching very difficult in the ICS space.
2. There is a lot of different technology and significant differences between the IT and the ICS environment. If you have a great IT security program, it may not necessarily cover your ICS assets and there are a couple of reasons for that.

Firstly, your IT team may not actually be managing your ICS assets. ICS systems are commonly acquired along with the equipment they control, so they are mostly installed, configured and run by plant engineers on site, not IT. This means IT does not know what control systems are being used, and there is rarely a reliable inventory.

Secondly, ICS is generally vulnerable. Some of the security features that you would expect in the enterprise IT security space, like authentication and encryption, aren't necessarily available on ICS communication protocols.

We also find that ICS is a lot more connected to enterprise IT networks and to the Internet than some asset owners think, hence creating a lot more exposure there. This provides a vector for bad guys to pivot from one network to another.

When building a cyber-security program for your organisation, we recommend taking into account both the IT and ICS assets and build an overarching Enterprise program that addresses the needs of both.

## WHY IT IS IMPORTANT TO SECURE INDUSTRIAL NETWORKS

I shall discuss four different iconic industrial controls systems attacks that had occurred in the past decade.

### *ATTACK ON A NUCLEAR PROCESSING FACILITY*

STUXnet (a.k.a. Operation Olympic Games) was the name given to a computer worm that was widely believed to have been created by a nation-actor, allegedly the USA and Israel, though neither country admitted it. Its initial purpose was to disrupt manufacturing at a uranium-enrichment facility at the Natanz plant in Iran for the explicit purpose of slowing down Iran's nuclear power program. First launched in 2008 as a series of cyber-attacks, it wasn't clearly identified until two years later.

STUXnet spreads by moving from machine to machine looking for PLC software. This software controls programmable logic controllers (PLC). PLCs are devices which control industrial processes. In this case, the process affected was the gas centrifuges that enriched uranium. The worm, having infected these machines, began to continually replicate itself. It became dormant when it encountered a machine that had no PLC software. Once the worm detected a machine with the software on it, STUXnet fed the PLC with false information, intercepted the data the PLC generated using the false information and reported normal operation back to PLC so that it appeared that everything was working within operating parameters. The affected software was and continue to be prevalent in industrial controls networks.

When the centrifuges began malfunctioning, the plant operators did not know about it until it was too late. How did the worm infiltrate the production network? It is plausible that the agent used was the IT networks of the subcontractors. There the subcontractors became the attack vectors when they transferred files from their laptops to USB drives and, unknowingly, infected the plant control networks.

Other repeated attacks continued to take place before the Iranian authorities, in June of 2010, with the aid of security consultants, realised that their plant was the victim of a cyber-attack and responded by identifying the Command & Control servers, blocking them and eventually taking them offline. The infections were purged over the next several months.

This attack is seen to be iconic and unprecedented due to both the geopolitical context surrounding the attacks and the magnitude of the operation. It is the first known attack to have succeeded in undermining operations of a critical infrastructure and damaging the facilities.

### *UKRAINIAN ELECTRICAL POWER ATTACKED, NOT ONCE BUT TWICE BLACKENERGY3/ CRASHOVERRIDE/INDUSTROYER*

December 23, 2015, was a watershed day in the history of cyber-security. That was the day that Ukraine's electrical grid came under a cyber-attack. Approximately 225,000 people were affected, 30 electrical substations were switched off and consumers were without electricity for between 1 and 6 hours.

The malware responsible for this cyber-attack was BlackEnergy. It was also the second ever to be designed and deployed for disrupting physical industrial processes (STUXnet was the first).

There are still many grey areas surrounding this cyber-attack which targeted the Ivano¬Frankivsk power station in West Ukraine. No nation-actor was attributed in this attack, though sentiment ran high that it was the Russian group, The Sandworm, that was behind the attack. What was

Source: www.bankinfosecurity.com

interesting was that the attack was synchronised and coordinated and that it affected three regional electric power companies.

The cyber-attack was complex and could be broken down to the following steps:

1. Prior compromise of corporate networks using spear-phishing emails with BlackEnergy malware
2. Seizing SCADA under control, remotely switching substations off
3. Disabling/destroying IT infrastructure components (uninterruptible power supplies, modems, RTUs, commutators)
4. Destruction of files stored on servers and workstations with the KillDisk malware
5. Denial-of-service attack on call-center to deny consumers up-to-date information on the blackout.

Further study of the attack showed that six months before the attack, the BE malware was sent, via phishing emails, to plant engineers and operators. Here the malware managed to gather legitimate login credentials, with which the attack was mounted. After the attack was concluded, another malware, KillDisk, was deployed to delete certain files from certain targeted systems, to overwrite firmware and to disrupt communications to server Uninterruptable Power Supplies (UPS) so as to interfere with restoration efforts.

One year later, a week before Christmas, Kiev suffered a power blackout which left 80,000 homes without electricity. The malware, called CrashOverride/ Industroyer, that attacked the Kiev grid, turned out to be more sophisticated, adaptable and dangerous than the cyber-security community had imagined. Together, these two attacks (2015 and 2016) comprise the only confirmed cases of hacker-caused blackouts in history.

### *JEEP HIJACKED BY HACKERS*

Imagine you're driving on the highway when suddenly, someone has remotely taken control of your vehicle. The air-conditioning vents start blasting hot air. The radio blares metal rock music at high volume. Your car dashboard lights up like fireworks. The windshield wipers turn on. Your steering is locked. You can't move. You're stuck. You panic.

Sounds far-fetched? It shouldn't. It's been done.

In 2015, two American researchers, Charles Miller and Chris Valasek, and a journalist from Wired magazine, Andy Greenburg, proved that it was possible to remotely take control of a connected vehicle. From the comfort of their living rooms, the researchers hacked the control system of a Jeep that was being driven by Greenburg. They were able to remotely take control of the vehicle using the Uconnect software that connected the Jeep to the Internet. They then went

Source: Andy Greenberg/Wired.com

on to activate the radio, the ventilation system, and other systems, while the driver watched helplessly from behind the wheel.

The researchers also stopped the engine while the Jeep was speeding along the highway at 63 mph. A further example saw the braking system being switched off while in a parking lot and they also took over the steering system.

The researchers and journalist wanted to use this exercise to show how vulnerable connected cars could be when dealing with attackers.

Furthermore, this exercise is a clear example of what industry players face with when designing new systems.

In this case, IT infrastructure was not the only target: Products and services were the main focus of the attackers' attention. Manufacturers often think their products are protected because their product development approach is hidden. However, "security by obscurity" and "security by air gap", which involves stopping attackers penetrating directly into the information systems, just aren't enough.

Cars are exposed to the same types of risks as other industries; in the past, these products were not linked to the Internet. Now, everything, including factories, vehicles and personal devices are connected and, as a result, they are left vulnerable and in need of more efficient and effective protection from cyber-attacks.

* Note: Jeep recalled 1.7 million vehicles after the vulnerability was made public.

## ICONIC ATTACKS: LESSONS LEARNT

Three attacks, three motives, three operating models. Attacks are becoming more diverse, methods are continually evolving, actors are increasingly bold. While motives are often different, their kinetic impact is dramatic. This is why raising awareness among industry players is paramount in the effort towards predicting, preventing, detecting and responding to similar attacks.

In each of the above mentioned scenarios, the approach to these attacks had a common theme. In most cases, industrial attacks took advantage of the human element of cyber-security, followed by insecure systems, i.e. vulnerable computer networks and a lack of knowledge on the part of the individual operator.

A deeper look into those attacks on physical facilities revealed a common denominator. In the physical facilities attack, it was apparent that the plant operator did not know what was in the control network. There was no insight at all.

It is highly recommended that production/control networks be scanned as part of a security assessment exercise. How do you protect something that you do not know that you have? Once an initial scan of the control network is done, a plan can be made to remediated the findings and trigger the relevant processes.

The initial scan of the network will enable the facility to map out the control network. In most cases an accurate network diagram is not available. Once the network topology is known, several risk mitigation strategies can be put in place.

Strategies include setting up a layered defence which addresses security throughout the entire ICS extended network. There should be proper physical and logical separation between different types of networks. For example, access to PLC and SCADA devices should not be available on the corporate network. Security policies, people awareness and sufficient training are among other steps to be undertaken in setting up a defence. In many critical infrastructure attacks, the malware entered into the control networks after infecting the enterprise network via a USB drive. Policies prohibiting the usage of similar devices can be drafted and enforced.

Another recommendation would be to properly segment the network and install an industrial firewall in that network. The usage of a data diode is gaining traction as that allows control signals to flow one way and allows information to flow the other way, like a normal diode.

Practices from the enterprise security world could also be applicable in industrial control security. Practices such as very strict user privileges, independent from corporate network credentials, using strong passwords and authentication techniques are all applicable in industrial control systems security.

Securing industrial control systems is an ongoing affair and should not be at the expense of safety and uptime of the industrial facilities as lives are at stake. ■

Further reading: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

### Author's Biodata

***Ir. Tejinder Singh** is as an electrical engineer with a major focusing on engineering advisory and consulting services, operating in a space that intersects energy efficiency, energy management, automation, artificial intelligence and cybersecurity.*