abhisam

THE 2020 INDUSTRIAL CYBERSECURITY REPORT

The Road Ahead in 2021 and beyond

ABOUT THIS DOCUMENT

This document is a compilation of papers from individual authors regarding Industrial Cybersecurity. All rights regarding the individual papers rest with the respective individuals, except where they have referred to other works by other authors and organizations. You may freely use the contents of this document for any non commercial purposes, however, please appropriately credit the individual author as the source, or link to this document at the link below

https://www.abhisam.com/Reports/IndustrialCybersecurityReport2020.pdf

This attribution shall, under no circumstance, indicate that Abhisam or the authors endorses you or your views.

The information in this document has been provided on an "as-is" basis. While due care has been taken while preparing this document, it should be noted that Abhisam or any of the individual authors will not be held responsible, either individually or jointly in any way, for any errors or omissions in the information provided. Neither Abhisam nor the authors accept any liability arising out of your use of the information provided.

Nothing in this document can be construed as legal, safety or regulatory information. You are advised to use your own judgement while using the information provided. This document is not a substitute for any standard or legal regulatory framework.

All views expressed by individuals are their own and may be different from their employers or clients.

ABOUT THE EDITOR

MANDAR PHADKE

CEO-Abhisam Software Group

Mandar Phadke graduated in Engineering from the University of Bombay, India and did his post graduation in Management from LaTrobe University, Australia. He is currently heading Abhisam Software (www.abhisam.com), a company involved in developing e- learning programs, certifications and provides consulting in areas like Industrial Cybersecurity, Process Safety, Functional Safety, Hazardous Areas & Industrial IoT. Prior to Abhisam, he has worked for more than two decades in the chemical process industry, for marquee multinational companies in different parts of the world, in leadership roles related to project design, engineering, commissioning, operations, maintenance, safety and decommissioning. He can be reached at mandar.phadke@abhisam.com

FOREWORD BY THE EDITOR

I am pleased to present the Abhisam 2020 Industrial Cybersecurity report to you. This report gives you a snapshot of the State of Industrial Cybersecurity in the year 2020, as viewed by professionals from diverse industries and backgrounds. They also give you a glimpse of where we are headed going forward in 2021 and beyond.

The idea for this report came about from a realization that there is not much publicly available information regarding Industrial Cybersecurity, which is not from cybersecurity solution vendors or regulatory authorities. So we wanted to gather and disseminate information from individual professional users about their own experiences and views.

Therefore, we invited many professionals in leadership roles from various domains, to express their views. These individuals are from different industries & backgrounds, having decades of experience as well as a high level of knowledge and expertise in Industrial Cybersecurity.

Not everybody who initially agreed to contribute, could actually go ahead and do it, owing to time constraints and work exigencies. To all those professionals who did contribute, a VERY BIG THANK YOU to all of you from me!

In this report, we present viewpoints of Industry leaders from different domains, including Water, Oil & Gas, Industrial IoT and DCS/SCADA/ Control & Safety System domains. This is vendor neutral as well as regulator agnostic information, so I feel it will be useful all over the world, not only in specific geographies.

If you have any comments or feedback regarding this report, or if you would like your views to be included in the next edition, please get in touch with me via email.

I am sure you will find every article in this report, engaging, insightful and useful.

CONTENT

1a ARE YOU READY FOR CHAOS?

Author:

LEO FERRER

ABOUT ME

I am a senior specialist at ICS/Scada with over 30 years' experience in the chemical, petrochemical, oil & gas and energy industries. During these years I have designed, installed and maintained ICS for the major manufacturers worldwide. I am currently working in a chemical industry. I like to define myself simply as a technician.

https://www.linkedin.com/in/leopoldoferrer/

1a ARE YOU READY FOR CHAOS?

THE 5 PHASES OF AN INDUSTRIAL CYBERSECURITY INCIDENT

When talking about the life cycle of an industrial cybersecurity system, the following five words are often used to name the phases: Identify, Protect, Detect, Respond and Recover. All these phases are important, but from my point of view, there is one that is especially critical: Recover (the last phase), which must be done when all the previous phases have failed. This is critical when we talk about Industrial Control Systems (ICS)

WHY IS THE RECOVERY PHASE IMPORTANT?

I am going to explain why I consider the fifth phase so important. In January 2020, in the chemical company where I work, we suffered a serious incident. An explosion in a reactor destroyed one of our plants and an attached control room. In consequence, we have lost the 90% of the ICS equipment of one of our plants. The only positive part is that we had collected all the necessary information to be able to rebuild the ICS.

Have you ever wondered what would happen in your industrial facility if you had an incident that caused a partial or total loss of the ICS?

Have you thought about the consequences for the viability of your company?

INCIDENTS & EVENTS

When we talk about an incident, we mean any event that affects the integrity and functionality of the system. The events can be a cyber-attack, a fire or explosion, a hardware failure, etc. Any event, however small it may seem, can seriously affect the operation of the industrial installation, and this is going to have repercussions on the production.

You may think that this will never happen to you, but believe me when I tell you that the likelihood of suffering an incident like the ones mentioned above, is more likely than you would think; it may be a minor incident or a light one, but these incidents happen. Hardware failures, for example, occur more often when the ICS is older. When the ICS is new there are three or four years without incident, but it would be strange if in the following years a hard disk of a computer or a motherboard of a PC, for example, didn´t fail.

1a ARE YOU READY FOR CHAOS?

DOES AN ICS RECOVERY PLAN EXIST?

Most of the companies I know, have implemented an IT recovery plan, but not for the ICS. In the best of cases they have "partial" backups of control systems. These backups are partial because the staff who maintain them don´t know exactly what information they should keep from an ICS; this is more critical if the ICS is a PLC/SCADA solution, versus a DCS solution.

The ICS, seen by profane eyes, aren´t more than a few computers located in a control room, but the reality (at hardware and software level), is that these are complex systems.

The ICS based on SCADA solutions are rarely composed of a single application (Scada, databases, recipe or manufacturing programs, reports, historian, advanced control systems, communications, networks, ...). Saving the configurations of all the applications is a good maintenance practice and allows us to have all the necessary information collected to undertake future tasks, like for example, a migration of the SCADA.

SYSTEM INVENTORY

In order to undertake a good backup, there is a previous step that must be done. This step is to know exactly what we have: How many computers and equipment do we have? What do we have installed in each computer? This information is known as a list of hardware and software assets. This list must be very precise, including even the version of the software installed. If, for example, the list includes Microsoft Office, we must know which version is installed (version 2010, 2013, 365), because if we do not install the correct version, it may not work correctly.

Another important point is to have controlled where is physically all that installation software and the licenses of all the components of the ICS. Usually there is a cabinet in every factory where all the software is stored, but the problem is that we probably have the previous versions stored as well. We must clearly identify what we have stored.

Is all the above important? Yes. Because it directly affects the recovery time, which is the time from when the incident occurs until the normalization of the system. This amount of time is often unknown to company management. How long do you think it takes to fully recover a single computer from your ICS system? The standard response time is usually between six and eight hours, although from my experience I can tell that this time is usually longer, between twelve and sixteen hours. But remember that we are

talking about one single computer. If the computer you were losing was critical to the operation of the facility, it would be the minimum amount of time that your installation could be down. These are the times if you have all the software to be installed and a backup of all the applications, if not, the time will be much longer, with an average minimum time between five and seven days. All these times described are based on my personal experiences.

Ideally, you should have an automatic backup and recovery system as in the IT area. Software solutions exist (Acronis, Veeam, Veritas...), but these solutions must be validated by the manufacturer of your ICS, although when they are asked that question, they will rarely give a clear answer. These backup systems must be deployed with caution and performing a test backup and a recovery to verify the effectiveness of the backup. These systems make a complete backup of each computer and all its contents. If a backup system is available, the recovery time is between 15 and 40 minutes.

If you don´t have an automatic backup system, you can make a complete backup of each PC manually; it is slower and more laborious, but there is no excuse to not do it.

THE 9 IMPORTANT QUESTIONS THAT YOU MUST ASK!

If you are a CEO, a head of maintenance or a head of engineering, I invite you to call a meeting with your technical staff and ask them the following questions:

1. Do we know what we have? We have a list of Assets that make up the ICS, computers and PLCs, including network addresses and software installed per equipment.
2. Do we know how it´s connected? We have an updated and complete network architecture of the ICS.
3. Do we make a backup? The backup is updated every time something is modified.
4. Where do we keep the backup? External USB disk in a fireproof safe or at a place other than the factory.
5. Do we have a complete backup? We have a complete backup of all the PCs in the ICS, which allows us to recover the PC in a short time.
6. Do we have the source programs saved? We have a backup of all the PLC and Scada source programs.
7. Where do we have the installation software and licenses? We have controlled where the software and licenses are installed. It must contain the installable of all the ICS applications including the necessary OS patches.

1a ARE YOU READY FOR CHAOS?

8. Do we have the critical physical equipment virtualized for support and testing? This allows us to have an exact and executable image of a PC (it is like taking a photo), with all the software installed and to be able to verify the configurations in case we have lost the physical machine. If our staff has not participated in the ICS installation project, it is possible that some critical data is forgotten when they are making the backup.
9. Do we know how to reinstall a machine? We have a complete server reinstallation manual with a step-by-step description, to make a clean installation.

If you receive more than two negative responses at that meeting, it is highly likely that you may have a problem in the future.

The implementation of the nine points, I will not fool you, it's hard work, but believe me that it's better to do something, even if it ends up being not worthwhile, than to regret it later.

When you reach this point in the article, you may think that all this is common sense, but remember that common sense is not the most common of senses.

Author:

LEO FERRER

ACERCA DE MI

Soy especialista senior en ICS/Scada con más de 30 años de experiencia en industrias químicas, petroquímicas, Oil & gas, energía. Durante estos años he diseñado, instalado y mantenido ICS de los principales fabricantes a nivel mundial. Actualmente desempeño mi cargo en una industria química. Me gusta definirme simplemente como técnico.

1b ¿ESTAS PREPARADO PARA EL CAOS?

LAS 5 FASES DE UN INCIDENTE DE CIBERSEGURIDAD INDUSTRIAL

Cuando se habla del ciclo de vida de un sistema de ciberseguridad industrial, a menudo se usan estas cinco palabras para nombrar las fases: Identificar, Proteger, Detectar, Responder y Recuperar. Todas las fases son importantes, pero bajo mi punto de vista hay una que es especialmente crítica: Recuperar (la última fase), que debemos hacer cuando todo lo anterior ha fallado. Esto es crítico cuando hablamos de Sistemas de Control Industrial (ICS)

PORQUE LA FASE DE RECUPERACIÓN ES IMPORTANTE

Les explico porque considero tan importante la quinta fase. En Enero de 2020, en la compañía química donde trabajo sufrimos un incidente grave. Una explosión en un reactor destruyo una de nuestras plantas y una sala de control anexa. Las consecuencias son que hemos perdido el 90% de los equipos del ICS de una de nuestras plantas. La única parte positiva es que teníamos recopilada toda la información necesaria para poder reconstruir el ICS.

¿Se ha preguntado alguna vez que pasaría en su instalación industrial si tuviese algún incidente que provocase una perdida parcial o total del ICS?

¿Ha pensado en las consecuencias que tendría para la viabilidad de su compañía?

INCIDENTES Y EVENTOS

Cuando hablamos de un incidente nos referimos a cualquier evento que afecte a la integridad y funcionalidad del sistema. Los eventos pueden ser desde un ciberataque, un incendio o explosión, un fallo de hardware, etc. Cualquier evento por pequeño que parezca puede afectar gravemente a la operatividad de la instalación industrial, y esto repercutirá en la producción.

Puede ser que piense que esto no le va a suceder nunca, pero créame cuando le digo, que la probabilidad de sufrir un incidente de los descritos es más probable de lo que piensa; puede que sea un incidente menor o leve, pero estos incidentes ocurren. Los fallos de hardware, por ejemplo, ocurren con mayor frecuencia cuando el ICS es más antiguo. Cuando el ICS es nuevo hay tres o cuatro años sin incidentes, pero sería extraño que en los años sucesivos no fallase un disco duro de un ordenador, o falle una placa base de algún PC, por ejemplo.

1b ¿ESTAS PREPARADO PARA EL CAOS?

¿TIENES UN PLAN DE RECUPERACION?

La mayoría de las compañías que conozco tienen implementado un plan de recuperación en IT, pero no para el ICS, en los mejores casos tienen backups "parciales" de los sistemas de control. Estos backups son parciales porque el personal que los mantiene no conoce exactamente qué información debe guardar de un ICS; esto es más crítico si el ICS es una solución PLC/Scada frente a una solución DCS.

Los ICS visto a los ojos de un profano, no dejan de ser más que unos cuantos ordenadores ubicados en una sala de control, pero la realidad (a nivel de hardware y software) es que son sistemas complejos.

Los ICS basados en soluciones Scada raramente están compuestos por una única aplicación (Scada, bases de datos, gestor de recetas o fabricación, informes, historian, sistemas de control avanzado, comunicaciones, redes, …) Guardar las configuraciones de todas las aplicaciones es una buena práctica de mantenimiento, y nos permite tener recopilada toda la información necesaria para acometer tareas futuras, por ejemplo, una migración del Scada.

INVENTARIO DEL ICS

Para acometer la realización de un buen backup hay un paso previo que debe efectuarse, es conocer exactamente lo que tenemos: ¿Cuántos ordenadores y equipos tenemos? ¿Qué tenemos instalado en cada ordenador? Esta información se conoce como listado de activos hardware y software. Este listado debe ser muy preciso, incluyendo hasta la versión del software instalado, ¿por qué? Si el listado incluye, por ejemplo, Microsoft Office, debemos conocer que versión está instalada (versión 2010, 2013, 365) ¿Por qué? si no instalamos la versión correcta, puede ser que no funcione correctamente.

Otro punto importante, es tener controlado donde esta físicamente todo ese software de instalación y las licencias de todos los componentes del ICS. Suele haber en todas las fábricas un armario donde se guarda todo el software, pero el problema es que es probable que tengamos también guardadas las versiones anteriores. Debemos identificar claramente que es lo que tenemos guardado.

¿Es importante todo lo anterior? Si. Porque afecta directamente al tiempo de recuperación, que es el tiempo desde que el incidente se produce hasta la normalización

del sistema. El valor de ese tiempo suele ser desconocido para las gerencias de las empresas. ¿Cuánto tiempo piensa que se tarda en recuperar por completo un solo ordenador de su sistema ICS? El tiempo estándar de la respuesta suele entre seis a ocho horas, pero mi experiencia me dice que ese tiempo suele ser más largo, entre doce y dieciséis horas, pero recuerde, que estamos hablando de un solo ordenador. Si el ordenador que pierde es crítico para el funcionamiento de la instalación, será el tiempo mínimo que puede tener su instalación parada. Estos tiempos son siempre teniendo todo el software a instalar y un backup de todas las aplicaciones, si no es así, el tiempo será mucho mayor, con un tiempo medio mínimo entre cinco y siete días. Los tiempos descritos son en base a mi experiencia personal.

Lo ideal debería ser tener un sistema automático de backup y recovery como en la zona IT. Las soluciones software existen (Acronis, Veeam, Veritas…) pero estas soluciones deben ser validadas por el fabricante de su ICS, pero cuando se les hace esa pregunta, no es normal recibir una respuesta clara. Estos sistemas de backup deben ser desplegados con cautela y efectuando un backup y una recuperación de prueba para verificar la efectividad del backup. Estos sistemas efectúan un backup completo de cada ordenador y todo su contenido. Si se dispone de un sistema de backup, el tiempo de recuperación esta entre 15 y 40 minutos.

Si no se dispone de un sistema automático de backup, se puede efectuar manualmente un backup completo de cada PC; es más lento y laborioso, pero no hay excusas para no hacerlo.

LAS 9 PREGUNTAS IMPORTANTES QUE DEBERIAS RESPONDER

Si usted es un CEO, jefe de mantenimiento o jefe de ingeniería, le invito a que convoque una reunión con su personal técnico y les haga las siguientes preguntas:

1. ¿Sabemos que tenemos? Tenemos un listado de Activos que forman el ICS, ordenadores y PLCs, incluyendo direcciones de red y software instalado por equipo.
2. ¿Sabemos cómo está conectado? Tenemos una arquitectura actualizada y completa de red del ICS.
3. ¿Hacemos un backup? Se actualiza el backup cada vez que se modifique algo.
4. ¿Dónde guardamos el backup? Disco USB externo en una caja ignifuga o que no esté en la fábrica.

1b ¿ESTAS PREPARADO PARA EL CAOS?

5. ¿Tenemos un backup completo? Tenemos un backup completo de todos los PCs del ICS, que nos permita recuperar el PC en poco tiempo.
6. ¿Tenemos los programas fuentes guardados? Tenemos un Backup de todos los programas fuente de PLC y Scada.
7. ¿Dónde tenemos el software de instalación y licencias? Tenemos controlado donde está el software y licencias instaladas. Debe contener los instalables de todas las aplicaciones del ICS incluido parches SO necesarios.
8. ¿Tenemos virtualizadas los equipos críticos físicas para soporte y pruebas? Esto nos permite tener una imagen exacta y ejecutable de un PC (es como hacer una foto), con todo el software instalado y poder verificar las configuraciones en caso de que hayamos perdido la máquina física. Si nuestro personal no ha participado en el proyecto de instalación del ICS, puede que se olvide algún dato crítico a la hora de realizar el backup.
9. ¿Sabemos cómo reinstalar un equipo? Tenemos un manual de reinstalación completa de servidores con una descripción paso a paso, para hacer una instalación limpia.

Si en esa reunión recibe más de dos respuestas negativas, es altamente probable que pueda tener un problema en un futuro.

La implementación de los nueve puntos, no le engaño, es un trabajo arduo, pero créame que es mejor hacer algo, aunque no valga para nada, que luego arrepentirte.

Cuando lleguen a este punto del artículo, pueden pensar que todo esto es de sentido común, pero recuerden que el sentido común no es el más común de los sentidos.

2 COORDINATING THE FUNCTIONAL SAFETY AND CYBER SECURITY FOR INDUSTRIAL PLANTS

Author:

DANIEL EHRENREICH

Consultant and Lecturer, SCCE

Daniel Ehrenreich, BSc. is a consultant and lecturer acting at Secure Communications and Control Experts, periodically teaches in colleges and present at industry conferences topics on integration of cyber defense with ICS; Daniel has over 29 years of engineering experience with ICS/OT for: Electricity, water, oil and gas and power plants as part of his activities at Tadiran Electronics, Motorola Solutions, Siemens and Waterfall Security. Selected as the Chairman for the **5th ICS Cybersec 2021** conference taking place in Israel on 11-2-2021.
https://www.linkedin.com/in/daniel-Ehrenreich-2b0752/

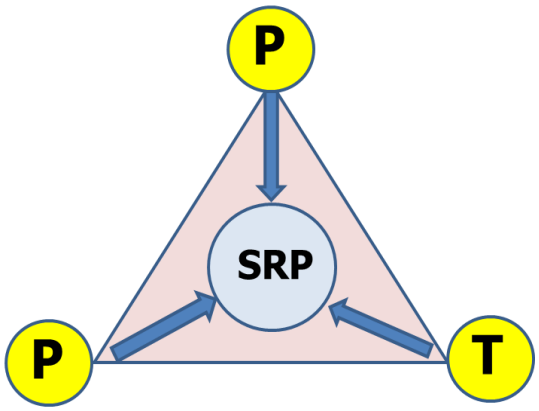
2 COORDINATING THE FUNCTIONAL SAFETY AND CYBER SECURITY FOR INDUSTRIAL PLANTS

INTRODUCTION

During the past decade, cyber security experts worldwide started seeing growing number of severe attacks aimed to harm industrial facilities, utility operations and manufacturing processes. While for protecting IT organizations we use the term "Confidentiality-Integrity-Availability (CIA)", for protecting physical operations supervised by Industrial Control Systems (ICS), we shall firmly say "Safety-Reliability-Productivity (SRP)". Achieving the SRP goals, must combine multiple expertise's; in the field of ICS processes, physical security and secured IT technologies.

Physical security is a critical precondition to cyber security and cyber security is a mandatory factor for achieving safety. Therefore, experts must follow the guidelines referring to ICS cyber security outlined in the ISA-IEC 62443 or the NIST 800-82 and the International Safety Standards IEC 61508, specifically referring to the Safety Instrumented Systems (SIS).

According to what is understood from the PPT (People-Policies-Technologies) Triad, there is no single factor which may achieve the defined goals, and adherence to all three defense processes is mandatory. This paper is aimed outlining the practical guidelines for deployment of cyber defense solutions which support operation safety for critical infrastructure.



SAFETY AND CYBER SECURITY INCIDENTS

Among the published cyber security incidents which have been directed to harming industrial operations and lives of people we may recall the attack occurred in April 2020 on one of Israeli water plants by trying to manipulate Chlorination systems that supply drinking water to cities. The malicious actor probably gained initial access remotely to some elements within an ICS environment and had established its access to one of the network elements by using weak or default passwords.

2 COORDINATING THE FUNCTIONAL SAFETY AND CYBER SECURITY FOR INDUSTRIAL PLANTS

Earlier in 2020 a hostile country initiated a severe attack on a regional water utility. The attacker managed to penetrate the SCADA system due to insufficient protection. Upon the penetration the uploaded multiple SCADA screens and translated the meaning of displayed location and functions. Initially the attacker stated turning on off the pumps in order to create water wave shock and rupture the water pipe. The ultimate goal of the attackers was manipulating the process PLC and modify the chemical formula of the distributed water in order to hurt people. The attack was discovered and actually no harm happened.

Another critical event occurred in March 2019 which affected all 35,000 Norsk Hydro employees across 40 countries, locking the files on thousands of servers and PCs. That attack started several months earlier when one employee unknowingly opened an infected email from a customer. That allowed hackers to invade the IT infrastructure and disabling the computerized control of most of their production facilities.

Another event occurred in 2017 called the Triton attack on Sadara Chemical in Saudi Arabia, and it was directed to disabling the operation of the on-site SIS. Luckily that attack was discovered early enough so no damage happened. However. if a severe malfunction occurred and the SIS was not active that could turn to a severe damage to the world's largest oil producer and a huge panic at the oil and gas markets.

TECHNOLOGY ASPECTS OF VULNERABILITIES

The extended use of IP-protocol based communication in the industrial zone and the need for periodic maintenance processes increase the potential risk, and without cyber defense to ICS, the safe operation of critical equipment cannot be assured. Thanks to the increased awareness, all know that without ICS cyber security measures you cannot trust the SIS, even if deployed according to IEC 61508. Therefore, the assessment of functional safety and industrial cyber security shall be periodically conducted.

As the global COVID-19 pandemic is affecting more people and more organizations around the globe, there is a growing need to allow remotely performed routine maintenance task for the ICS plant. Moreover, the intensive deployment of Industrial Internet of things connected to ICS platform is also expanding the cyber-attack surface and increasing the risk of cyber-attacks.

2 COORDINATING THE FUNCTIONAL SAFETY AND CYBER SECURITY FOR INDUSTRIAL PLANTS

A stronger cyber defense and operating safety can be achieved by deploying an on-site cyber range, which is as similar as possible to the real ICS and SIS architectures. It can be used for testing software patches, analyzing vulnerabilities and training of operators. The exercises shall be specifically tuned to each group and shall be professionally guided by experts who are have combined expertise in the field of industrial control, IT technologies and cyber security.

Knowing the fact that the negligent behavior of employees might contribute to high percentage of "successful cyber-attacks", enhanced operating safety and cyber security can be achieved by upgrading the awareness of people (P), enforcing the corporate policy (P) and upgrading the deployed technologies (T), called the PPT triad mentioned above.

THE "PEOPLE" FACTOR

The P-People factor offers the highest Return on Investment (RoI), because it involves training and drills at all organization levels including operators, engineers and outsourced service providers:

- ICS operators at industrial facilities shall be trained to detect unusual and anomaly conditions in the ICS process and respond instantly to prevent risk to lives and assure business continuity.
- Engineers and service providers must perform their task with operation safety in mind. It means that the maintenance of ICS component shall be performed securely and subject to supervision.
- Integrators must be trained to carefully design the control architecture by utilizing principles of secure development. This process must be guided by ICS as well as ICS Cyber security experts.
- Organizations must supervise the entire supply chain (including all operation segments) and limit the amount of information employees are providing to external service providers.
- Operators must be trained how respond during an incident caused by a severe fault, cyber-attack or sabotage in order to mitigate the risk to people, minimize the outage time, reducing damages.

2 COORDINATING THE FUNCTIONAL SAFETY AND CYBER SECURITY FOR INDUSTRIAL PLANTS

THE "POLICY / PROCEDURES" FACTOR

- Operating safety and cyber security must be supported by strongly enforced policies, based on Identity and Access management (IAM) and role-based access (RBAC) principles.
- The access control to all computers, process controllers and cyber security related components at the plant shall be configured as "access blocked" as the default condition.
- The computerized operation at the entire plant shall be configured for collecting logs and relevant information which can be analyzed during forensics investigation after an event.
- The organization policy shall define the internal communication and reporting processes applicable during normal operation of the plant and specifically during emergency conditions.
- Organizations must have predefined plans for Business Continuity Preparedness (BCP) and Disaster Recovery Processes (DRP) in order to support the business goals of the plant.

THE "TECHNOLOGY" FACTOR

- ICS architectures can be built with commercial off the shelf (COTS) hardware, software and utilize compensating and complementing measures to minimize cyber security risks.
- The plant must have strong cyber security-oriented technologies in place in order to allow secured remote access (SRA) for maintenance operations without increasing the risk.
- Specifically, the access control shall utilize technology-solutions performing strong authentication of connecting devices and people and include strong encryption.
- Critical industrial plants shall include on-site intrusion detection systems (IDS), security information and event management (SIEM) system for managing emergency conditions.
- In order to enhance the cyber secure operation and operating safety, the facility shall connect to a Security Operation Center (SOC) or outsource such service to an expert service provider.

2 COORDINATING THE FUNCTIONAL SAFETY AND CYBER SECURITY FOR INDUSTRIAL PLANTS

DEALING WITH LEGACY SYSTEMS

Industry experts are well aware that in systems built a decade ago, both the ICS and the SIS architectures were always based on different and independently selected technologies. However, with introduction of modernized systems, industry 4.0 related technologies and the need to communicate more data between the ICS and IT zone the situation change, and all legacy systems shall be gradually upgraded and retrofitted with modernized communication and control technologies. In order to achieve cyber-security and operating safety goals we must periodically invest in a range of proactive actions directed to both the ICS and the SIS.

SUMMARY AND CONCLUSIONS

Selecting a cyber-security technology is a complex process, because cyber-attack scenarios constantly evolve and the risk factors are changing. Operators of ICS for in critical facilities must be aware of the risks related to major malfunctions, cyber-attacks and sabotage which might cause severe damage to business operations and hurt lives of people. Coordinated assessment and periodic upgrades of SIS measures and ICS cyber security solutions will lead to enhanced operating safety and productivity and business continuity. Therefore, plant managers must be provided with adequate resources and available expertise to be at least one step ahead of attackers.

3 WHY CYBERSECURITY AND PROCESS SAFETY

Author:

SINCLAIR KOELEMIJ

CISSP, CISSP-ISSAP, CISM, CRISC

ABOUT ME

I am an OT cyber security professional with over 40 years of experience in process automation working for Honeywell Inc. I started my career with Honeywell in field service and continued it as a system and application programmer of process automation computers. During that time I participated in over 25 major factory automation projects in Europe and the Middle East. Learned to configure BPCS and SIS and developed advanced process control applications in the process computers of those days. After that period I continued my career in the recent 18 years as a cybersecurity and network specialist for process automation systems. I participated in at least 40+ projects conduction security assessments and mitigation projects. In recent years I have focused on OT security risk analysis conducting detailed risk analysis for refineries, chemical plants and the offshore industry. I am a US patent holder in the area of cyber security risk (US 9,800,604 B2).

Apart from my professional career I write occasionally blogs that can be followed at: www.otcybersecurity.blog These blogs and this article I write an individual, the opinions expressed in this article and in my blogs represent my own opinions and are not those of my employer.

You can contact me at LinkedIn: https://www.linkedin.com/in/sihoko/

3 WHY CYBERSECURITY AND PROCESS SAFETY

ABSTRACT:

The threat landscape for cyber physical systems has undergone a significant change in recent years. This article discusses the change in the threat landscape and some basic mitigation measures that would reduce the overall cyber security risk.

CONTENT:

Cyber security attacks can cause several types of loss, such as: production loss, damage to equipment, damage to the corporate image, violation of regulations and safety related consequences such as personal injuries and even fatalities depending on the physical process.

Ignoring several specialized functions an automation system for a production process typically has two components:

- Basic Process Control System (BPCS);
- Safety Instrumented System (SIS);

BPCS's job is to perform the automation functions required to make a product, such as a chemical, gasoline or the electrical power for the grid. The SIS is a "watchdog" that enforces the production process to remain within the physical limits required for safe production. Its task is to enforce process safety. Both the BPCS and SIS are programmable electronic functions and as such vulnerable to cyber attacks. If we consider the various protection and control layers surrounding a production process we get the following picture:

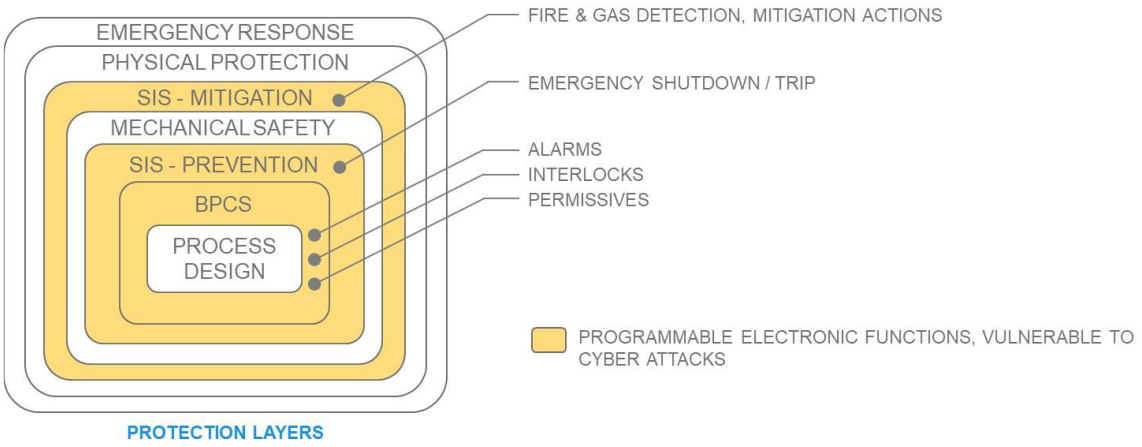


Figure 1 - Protection layers in an automated production process

3 WHY CYBERSECURITY AND PROCESS SAFETY

In addition to the automation functions, the BPCS usually includes the process alarm, interlock and permissive functions. The SIS has two independent tasks: a prevention task that disables parts or the entire production process and a mitigation function that activates protection functions when fire or gases are detected.

In the past 10 years, we have seen a range of cyber attacks that impacted both the BPCS and SIS functions. These attacks had various consequences.

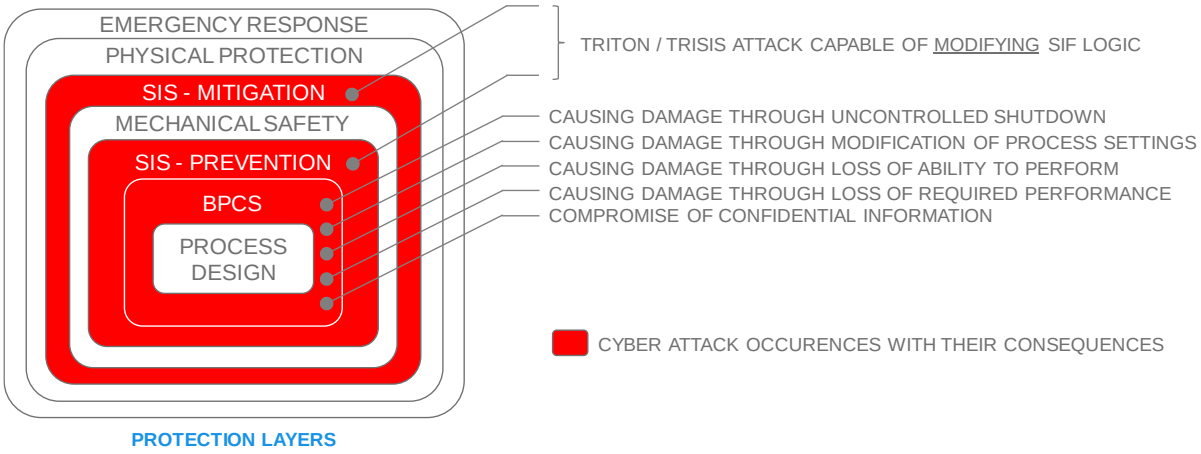


Figure 2 - Some actual consequences of cyber attacks in recent 5 years

The most dangerous attack, from a process security point of view, was the TRITON attack or also known as the TRISIS attack. This cyber attack targeted a Schneider Electric Triconex safety system and was able to modify the Safety Instrumented Function (SIF), the SIS's program logic.

Under normal circumstances, a cyber attack on the BPCS should never endanger process security, the SIS must be able to bring the production process to a safe state under all circumstances. When cyber attackers are able to attack the SIS, by disabling the SIS function or even modifying the function, we enter a new era. Although the TRITON / TRISIS attack failed due to a programming flaw, the attack showed that SIS is vulnerable to cyber attacks and that attackers devote considerable effort and resources to carry out such an attack.

Although there are currently no direct victims as a result of a cyber attack, attacks against SIS greatly increase the likelihood that this will happen in the near future.

3 WHY CYBERSECURITY AND PROCESS SAFETY

This new threat with a whole new set of potential consequences has significantly changed the importance of cybersecurity for physical systems. This is compounded by the lack of any specific reason to attack the chemical plant in Saudi Arabia. While the notorious Stuxnet attack on a uranium enrichment production facility in Iran had strong political motivation, the attack on the chemical plant in Saudi Arabia seems to lack such motivation. Yet the threat actors were willing to invest years of effort and planning in this attack. The failure of the attack ultimately destroyed most of this investment and triggered the community to reconsider the cyber security of their SIS, strengthening the resilience against this type of attack.

If we picture the consequences of cyber attack in a diagram showing the consequences that have occurred with industrial control and safety systems (ICSS) we can depict this using following diagram.

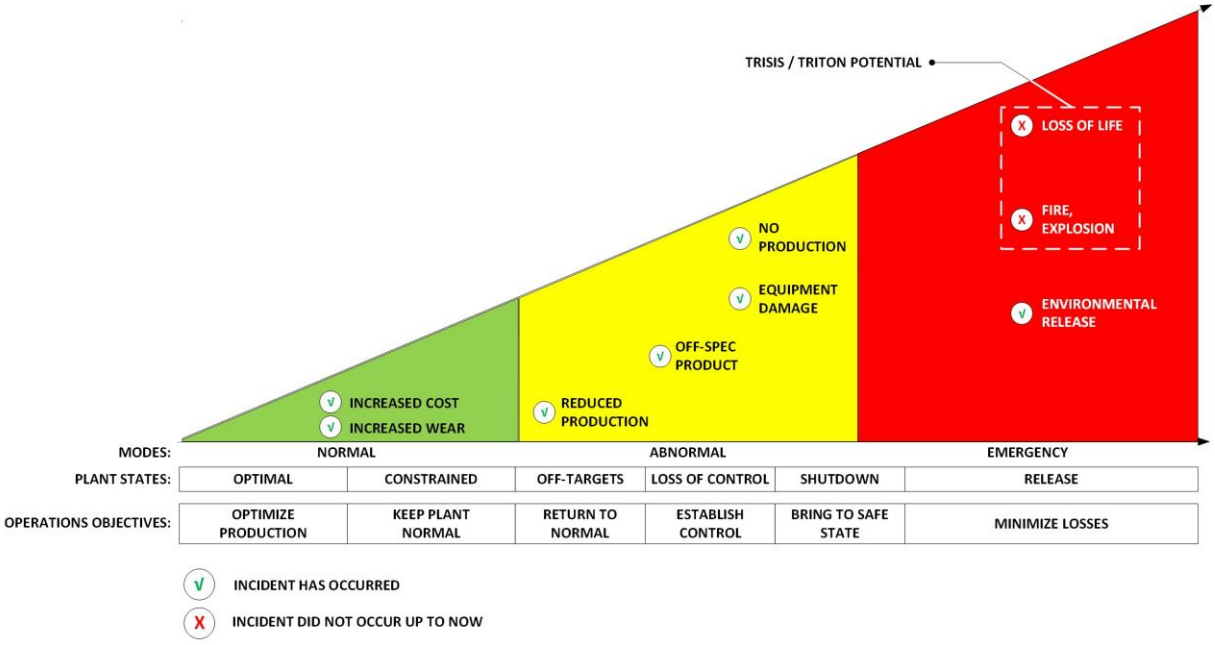


Figure 3 - Overview of consequences from attacks on ICSS

So far we have no documented examples of fires and explosions or loss of life caused by a cyber attack on a production system. Of course, we know that this is quite possible, if we consider the accidents caused by failure of automation systems in the past. Therefore, it is reasonable to assume that cyber attacks also have the capacity to trigger them.

3 WHY CYBERSECURITY AND PROCESS SAFETY

If we consider protection of the ICSS against this type of advanced attacks we need to consider several security controls to reduce the risk of such an attack to be successful. When we analyze these controls, we need to consider how much risk these controls reduce. Risk reduction of a control is a function of both the control's effectiveness and the control's reliability. If we look at the different controls we have at our disposal to address threats like the TRITON / TRISIS attack we can consider the following set of technical controls:

1. Antivirus engines;
2. Application white listing solutions;
3. USB access control solutions
   3a: with enforcing AV check,
   3b: without enforcing AV check;
4. Isolation;
5. Network segmentation
   5a: logical,
   5b: physical;
6. Application segmentation;
7. Perimeter protection using stateful packet filter firewall;
8. Perimeter protection using next generation firewall;
9. Perimeter protection using data diode;
10. Anomaly detection solutions;

The effectiveness of a security control also depends on the capabilities of the threat actor, for example, a highly capable threat actor would test the malicious code to pass an antivirus' signature inspection, before launching the attack. As such, an AV engine would not much reduce the risk of a targeted malware attack on the production system. However, an AV engine can be very effective against a non-targeted ransomware attack from cyber criminals. But not only the effectiveness of the control plays a role, the reliability of the control is also important. A control that uses some inherent physical constraints is more reliable than a control that runs active checks to enforce constraints. For example, a firewall uses active controls to throttle traffic, while a data diode uses the physical unidirectional constraints of a fiber-optic connection. The active controls can be bypassed by a smart attacker, the physical restrictions cannot be bypassed.

3 WHY CYBERSECURITY AND PROCESS SAFETY

In the following diagram I show the contribution to risk reduction for the mentioned set of security controls incase of a targeted attack against the ICSS.

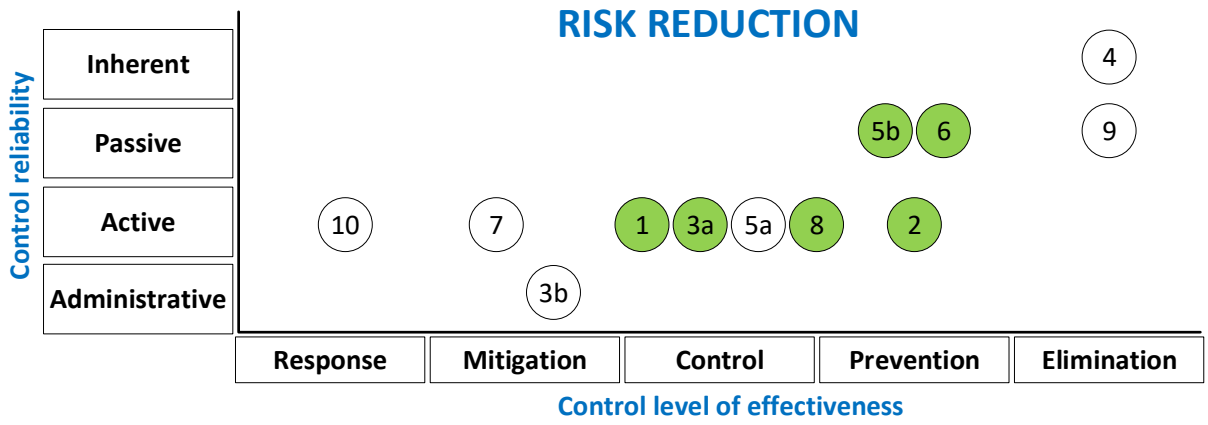


Figure 4 - Risk reduction of controls against a targeted attack on ICSS

The controls marked in green are a minimum of security controls necessary to reduce the risk to an acceptable level. If these controls would have been in place the mentioned TRITON / TRISIS attack scenario would not have been possible. In particular, the combination of application white listing, physical network, and application segmentation would have been a difficult hurdle to get around. Let's look at some typical architectures to explain.

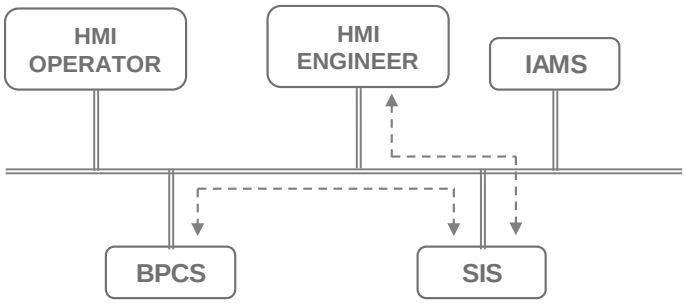


Figure 5 - Typical ICSS architecture

WE SEE HERE 3 PRIMARY FUNCTIONS:

- Basic Process Control System (BPCS);
- Safety Instrumented System (SIS);
- Instrument Asset Management System (IAMS).

3 WHY CYBERSECURITY AND PROCESS SAFETY

Together with the HMI functions and the network, these functions can be used by a threat actor to compromise the process safety of the production process. The above architecture, is called an integrated architecture. The BPCS and SIS normally exchange information. The BPCS is used to control the production process, for this the process operators (HMI operator) also need information about the status of the SIS functions. SIS field transmitters and actuators can also fail or require maintenance, for this process, operators need the ability to temporarily override a Safety Instrumented Function (SIF). A process operator therefore has the option to send an override command, to force a process point in the SIS to a certain value if necessary. Additionally, a shutdown can be partial, in those cases, the control loops in the BPCS need to be aware of the shutdown to prevent windup of the control loop.

So where BPCS and SIS have traditionally been completely isolated, this is often not easy to achieve in modern process designs. For process safety, these two functions must remain independent, as they are separate layers of protection. This requires that we make it difficult for the attacker to attack BPCS and SIS at the same time. If a simultaneous attack is possible, the "watchdog" function of SIS is compromised.

HAVE YOU CONSIDERED YOUR INSTRUMENT ASSET MANAGEMENT SYSTEM?

The IAMS is a relatively new feature, perhaps a little over 20 years old. This function primarily manages the field instrumentation. It is possible to configure field instruments via an IAMS and receive status information from the field instrumentation. The security of the IAMS is important for both SIS and BPCS because this system has the potential to access all field equipment, both transmitters and actuators. For example, changing a range of a pressure transmitter changes the process value reported to the process regulator or safety controller. In the case of a safety controller, this process value can be part of a trip point that initiates a safety action. By changing the value, the safety function cannot occur or can occur prematurely. To better protect the architecture in Figure 5 we can apply network segmentation and application segmentation.

3 WHY CYBERSECURITY AND PROCESS SAFETY

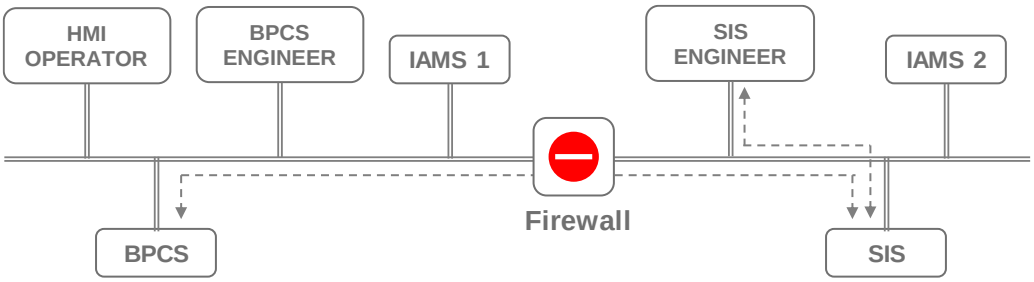


Figure 6 - ICSS integrated architecture after applying physical network segmentation and application segmentation

A very important application of segmentation is to never install the engineering function that manages the SIS, in the same station as the engineering function that manages the BPCS. These functions must be located in separate stations and on separate network segments. It is considered good practice not to allow changes to the SIS using remote access. So it is best to place the SIS engineering function and the SIS logic solvers on a separate network segment, shielded by a firewall that controls access.

If a system has an IAMS, we can consider splitting the IAMS as well, one for each segment. Another option would be to use tamper-resistant field instruments on the SIS side. These are instruments that have a physical switch or clip to protect them from overwriting configuration settings. In this case, the settings cannot be changed from the IAMS before entering the field and changing the write protect switch on the field instrument. This is a very effective control, unfortunately not a very reliable control because people often "forget" to switch back to the write-protect mode.

USING AN INTERFACED ARCHITECTURE INSTEAD OF AN INTEGRATED ONE

An entirely different approach is to select an interfaced architecture, in this architecture we don't have a common network connection between BPCS and SIS.

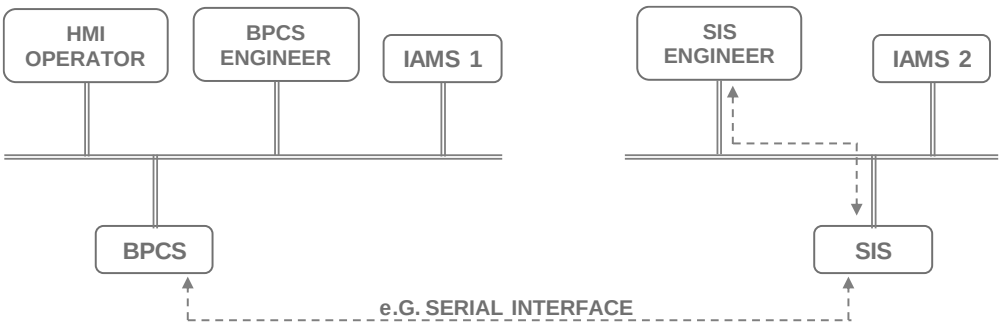


Figure 7- ICSS using an interfaced architecture

3 WHY CYBERSECURITY AND PROCESS SAFETY

An interfaced architecture will make use of dedicated point-to-point connection between a process controller and a logic solver. Often using a serial interface or a dedicated Ethernet connection. In this case, the SIS network segment becomes fully isolated from the BPCS network segment. The main drawback is the higher cost and maintaining the security on the isolated segment. For example, updating the antivirus signatures, or exchanging information with the engineering function.

The architectures of Figure 6 and Figure 7 need additional security controls to protect the functions against malware attacks. Antivirus, based on a blacklist, is the most commonly used check. But as stated, not very effective against capable attackers. The combination of antivirus and application white listing offers much more protection. Application white listing protects the system against the execution of unauthorized code. Each program or program module must be "whitelisted" before it can be used. Code that is not whitelisted is blocked from execution.

USB media are often used by engineers to exchange data. These media can contain malicious code, so it is important to limit access for these devices as much as possible. It is good practice to select a control that restricts access and at the same time, if access is allowed, enforces the data to be scanned for malicious code. As we can see in Figure 4 a control that combines this (3a) is better than one that would rely on an administrative policy that requires an engineer to scan the USB for malware before using it (3b). The reliability of the latter is lower.

OVERALL REDUCTION OF THE ATTACK SURFACE

While the above controls provide good protection for the SIS, more is needed for overall protection. For example, we need to reduce the attack surface of each function by disabling or removing all communication functions not used by the system. We must enforce a policy of least privilege, where users are limited to the functions they need to perform their job and functions that are not needed should be not accessible. By applying the same principle to network communication, we must enforce access restrictions to communicate with nodes, based on what is allowed. Functions that should not be accessed remotely, should not be accessible from other computers.

3 WHY CYBERSECURITY AND PROCESS SAFETY

This article does not suggest that by implementing the proposed segmentation and adding antivirus engines, application whitelisting and USB control, the SIS is 100% protected. Cyber security risk is never zero, but adding the proposed controls would have stopped the attacks on ICSS so far. So it's a good start to implement them before investing in controls that offer less risk reduction.

I have not discussed detection mechanisms such as anomaly detection systems in this article, mainly because these systems are very dependent on adequate responsiveness. This is a big gap at the moment, as these systems generate a plethora of false positive alerts and require detailed knowledge of the inner workings of protocols often developed by vendors. They are expensive and I consider them less important from the point of view of risk reduction than the preventive measures mentioned. So from a safety investment planning, in my opinion, it is better to focus on the preventive controls and hope that the detective controls like the anomaly detection systems mature in the meantime to complete the protection strategy in the future.

In summary, the threat landscape has changed significantly as threat actors can change the logic of the SIS. This capability poses a serious threat to the process safety of the manufacturing process and thus increases the protection requirements for manufacturing facilities that can fall victim to targeted attacks. Implementing some simple controls significantly reduces the risk.

4 INDUSTRIAL CYBERSECURITY IN OIL & GAS-STATUS IN 2020 AND WHAT WE SHOULD EXPECT IN 2021

Author:

H SREEDHAR

B.E. (Instrumentation)

H Sreedhar completed his B.E. (Instrumentation) from the University of Bombay in 1990 and has over 30 years experience in various industries including Oil & Gas, manmade Fibers and EPC companies. He has worked for several organizations including Chemtex, Black & Veatch, Fluor, Technip, AMEC & ADNOC in various countries including the US, India, Kuwait and UAE. He has been a part of several greenfield and brownfield automation projects in various roles.

The views expressed in this article are his own and not of his past or present employers.

4 INDUSTRIAL CYBERSECURITY IN OIL & GAS-STATUS IN 2020 AND WHAT WE SHOULD EXPECT IN 2021

RECENT HISTORY OF AUTOMATION IN OIL & GAS

The Oil and Gas industry (O & G for short) has been a pioneer in embracing digital technology. It was one of the first industrial sectors to transition to Distributed Control Systems(DCS), from analog electronic control equipment and pneumatic instruments. This transition started in a big way, about 35 years ago, when DCS were a "hi-tech" thing.

O & G is still a tech pioneer, in the era of Industry 4.0 and the Industrial IoT. It quickly embraced concepts like the Digital Oilfield. However, this has led to newer problems related to security.

The development of digital control systems and the networking, particularly with the internet, has led to increased risk of cyber-attacks which are engineered by isolated hackers, criminal organizations or state services. The ensuing disruptions, can result in untenable stoppages in production and danger to people, property and the environment, leading to potential disaster scenarios in sensitive installations of energy production and other similar major infrastructure.

INDUSTRIAL CYBERSECURITY CHALLENGES IN O & G

In the context of the fourth industrial revolution, which involves an increased degree of connected systems and integration of digital technologies into the manufacturing process, cyber-security is a major issue today.

The industrial systems are heterogenous and built on commercial off the shelf (COTS for short) generic components. The selection of the components are made for their functionality, not security. Authentication management at the equipment level is difficult and updating software, firmware or hardware is difficult and not done regularly. Although we consider these existing DCS, PLC and SCADA systems as "modern", the reality is that at the time when these control system technologies and protocols were developed, cyber-attacks did not exist (or were not considered as a credible threat).

Hence these systems are insecure and very vulnerable. There are many installations which still use them. In cases where the most recent installations are implemented around the Industrial internet of things (IIoT), the complexity and (ironically) the flexibility of these networks, makes them very vulnerable.

4 INDUSTRIAL CYBERSECURITY IN OIL & GAS-STATUS IN 2020 AND WHAT WE SHOULD EXPECT IN 2021

Cyber attacks are evolving in sophistication and complexity from the simple viruses in 1980's to the malicious software today capable of communicating with outside entities, capable of growing to become widespread and attacking remote installations.

Instances of attacks on industry installations like the WannaCry (Symantec 2017), Stuxnet attack (Falliere,2011) aimed at Uranium production which led to Plant shutdown and operating losses or the Triton attack which rendered even Safety Instrumented Systems inoperative, are warning examples of the need to treat this issue with the prioritized urgency that it deserves.

The rapid evolution of technology had led to the Industrial control systems (ICS) being connected to other networks for transfer of production data to the Company IT systems for remote download or auto download of updates. There is an increasing convergence of protocols towards common protocols increasing the vulnerability of control systems. It is unrealistic to expect the control systems to be stand-alone and not connected to any other systems.

A cyber-attack can be in myriad ways eg. the USB key as In the Stuxnet case; or if the industrial network is connected to the IT corporate network the IT system can be attacked with malicious programs that infect the industrial network, where the industrial network is connected to the internet(albeit temporarily), for maintenance or configuration, thereby exposing the network to potential attacks. Many organizations are migrating to the Cloud, to upload the data to enable system updates from the manufacturer's site with remote access, thereby increasing the system's attack surface and increasing its vulnerability.

Functional safety as per IEC 61508 does not focus on computer security, as it was not identified as a credible or important hazard, at the time the standard was originally written.
(Note: There are SIS related security clauses in the latest edition, but they are sparse and direct the reader towards other standards such as IEC 62443)

Information security and operational safety are managed by different approaches: ISS risk management process is covered in ISO 27000 Security of information standards and PHA, HAZOP, FMEA or LOPA are the risk analysis methods for industrial processes.

4 INDUSTRIAL CYBERSECURITY IN OIL & GAS-STATUS IN 2020 AND WHAT WE SHOULD EXPECT IN 2021

IEC 62443 aims to transcribe number of functional safety concepts (like SIL levels) for cybersecurity, to align approaches. Unified approaches for risk analysis are being proposed with the concept of SLs (Security Levels)

Depending on the issues and context, the cyber security solutions will be different. The crisis management plan, recovery and business continuity plan, need to be in place, based on the detection system and the alert chain. This will be based on the cost-benefit ratio.

PROBLEMS IN PREVENTING ICS CYBER ATTACKS IN THE O & G WORLD

Probable economic consequences, with detailed cost-benefit analysis, is required to determine the level of cyber-security measures required to be taken. With oil prices in a steady decline, all costs are being controlled with an eagle eye and spending on cybersecurity is not an exception.

Anti-virus software is not effective on many devices that run on proprietary software, or real time operating systems. Common Firewall problems include limits related to filtering rules not being configured properly and even if data flows are limited, it does not prevent all attacks passing through, as evident in the Ukraine electrical energy management attack of 2015.

Virtual private networks(VPN's) have their own limitations, as many VPN's use outdated technology or even if one of the Workstations connected to VPN is infected, it risks the entire network getting infected. The Information Security system (ISS) limits efficiency and is expensive.

STATUS IN THE YEAR 2020

The culture of "production first" and not changing something that works, is deeply entrenched in Oil & Gas. It is imperative to enforce a culture, where the authentication management is rigorous, and updates are not always made on a regular basis. There is need to have an ICS security management policy including management of sub-contractors, subject to specific measures, a user rights management policy defining possibilities of action and prohibiting access to outsiders.

4 INDUSTRIAL CYBERSECURITY IN OIL & GAS-STATUS IN 2020 AND WHAT WE SHOULD EXPECT IN 2021

In the Oil and Gas Industry, increasingly the challenge of potential targeted cyber-attacks is now on the operating technology (OT) side of the network. The increased focus in 2020 of the Oil and Gas Industry was to secure the OT segment of their digital infrastructure. This need has arisen due to the increased cases in the cyber-attacks on OT peripheral devices. In the Oil and Gas industry the levels of connectivity between the IT and OT networks are increasing.

WHAT LIES AHEAD IN 2021 AND BEYOND?

The next focus in Oil and Gas increasingly in 2021 is the threat to supply chains including Contractors, Sub-contractors and Vendors that tie-in to the Company's databases/IT environment during project execution and potentially bring threats/vulnerabilities.

Now I would like to highlight another aspect of Industrial cybersecurity. Today the focus on Industrial Cybersecurity is mainly ICS Security (which can be considered a subset of the broader domain of Industrial Cybersecurity) and you will see a lot many developments related to it. However we should also consider other allied engineering activities, which are now done "in the cloud" and can affect industrial operations.

Due to the COVID 19 crisis, a lot of design and detail engineering work is being done increasingly in the cloud, with many stakeholders connecting to it including EPC contractors & sub contractors. Although strictly speaking, this is not considered as part of "Industrial" cybersecurity, yet any attacks on these systems can affect industrial operations too, especially for brownfield development projects, where time is critical and budgets are low. Imagine nightmares like data corruption of as built drawings, or damage to old P & IDs (with no hard copies available). Recovering from these incidents will not be a pleasant experience and can set back urgent modernization projects by years.

The need is to set up Cyber-security processes in place so that all the third party entities are fully aware and adhere to the Cyber-security policies of the Company.

For an effective cyber-security solution, it is imperative to think in terms of protection, prevention and early intrusion detection, by means such as abnormal traffic suggesting a preparatory attack.

4 INDUSTRIAL CYBERSECURITY IN OIL & GAS-STATUS IN 2020 AND WHAT WE SHOULD EXPECT IN 2021

The Cyber-security solution must be implemented in consultation with the user, taking into account ground-realties supporting new operating modes, without limiting the user's operating possibilities excessively.

That is the challenge that is being addressed in 2020 and in 2021 will further require concentrated attention from various stakeholders, increased budget allocations for cybersecurity and increased collaboration from both cyber-security solution providers and the users.

5 INDUSTRIAL CYBERSECURITY IN THE UK WATER INDUSTRY

Author:

MANDAR PRADHAN

ABOUT ME

I am an Instrumentation Control and Automation engineer with 20 years of experience in instrumentation and process automation. The early part of my career was spent as a systems and application programmer of PLCs and SCADA. My exposure to the UK Water and Waste Water industry started in Asset Management Programme 3 (AMP3). Here, I worked as a Systems Integration Engineer on more than 50 United Utilities water and waste water sites. I then joined Black & Veatch, where for the last 14 years I have worked on many different types of water and waste water projects for utility clients in the UK, the US, Singapore and Australia.

I am ardent fan of safety in design and look to implement it, where appropriate, on projects; this article being an extension of that in the area of cyber security.

The opinions expressed in this article are entirely my own and are not those of a past or my current employer.

You can contact me at LinkedIn:
https://www.linkedin.com/in/mandar-pradhan-b84254a

5 INDUSTRIAL CYBERSECURITY IN THE UK WATER INDUSTRY

UK WATER INDUSTRY

The water industry in England and Wales is regulated by Ofwat. The regulator has a duty to protect customers' interests and ensure that companies carry out their functions correctly and sets water prices. Eighteen water companies serve England and Wales, whilst Northern Ireland is served by Northern Ireland Water and Scotland has a single publicly-owned water and sewage company – Scottish Water.

UK WATER INDUSTRY – CYBERSECURITY CHALLENGES

The UK Water Industry provides a unique challenge when it comes to implementing cyber security. The combination of critical national infrastructure, complex investment cycles and legacy hardware at sites, alongside an evolving regulatory framework means that most companies are now juggling priorities to address the risks identified alongside other significant investments. Threats from cyber-attack are increasing at the same time as legacy technology reaches its end-of-life, creating a pressure on companies to prioritise investment strategically. In addition, the technology landscape is changing and presents new challenges to traditional information technology and operational technology investment. Such changes must be managed and balanced against competing commercial and industrial challenges. Additionally, water companies are organisations of varying sizes, structures, asset histories, and capabilities. Across the industry, this presents a challenge in developing a common approach to cyber security.

EU DIRECTIVES

The NIS Directive (Directive on security of network and information systems) is the first piece of EU-wide legislation on cyber security, it relates to loss of service rather than loss of data, which falls under the General Data Protection Regulations (GDPR), so whilst covering different areas of cyber security there is significant overlap between them and both may sometimes apply to the same incident.

To consider the NIS Directive further, it defines an **Operators of Essential Services (OES)** as:

- Entities that provide "a service which is essential for the maintenance of critical societal and/or economic activities; the provision of that service depends on network and information systems; and an incident would have significant disruptive effects on the provision of that service".

5 INDUSTRIAL CYBERSECURITY IN THE UK WATER INDUSTRY

Water (Drinking water suppliers and distributors) are deemed essential, as follows:

Sector	Subsector	Essential Service	Identification Thresholds
Drinking water supply and distribution	N/A	The supply of potable water to households.	Operators with serving 350,000 or more people.

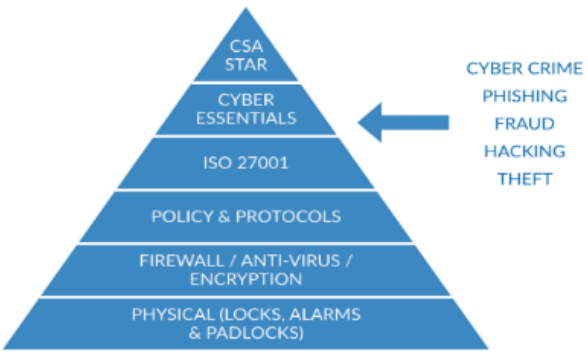
An OES must demonstrate that it is applying appropriate measures to manage the risks to their network and information systems. In other words, it must meet the UK Government's "high-level security principles".

HIGH LEVEL SECURITY PRINCIPLES:

- Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.
- Proportionate security measures in place to protect essential services and systems from cyber-attack.
- Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.
- Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

There are two relevant international standards that set out a best-practice approach:

- **ISO/IEC 27001:2013** – the standard for an information security management system (ISMS).
- **ISO 22301:2012** – the standard for a business continuity management system (BCMS).



5 INDUSTRIAL CYBERSECURITY IN THE UK WATER INDUSTRY

Using their guidance provides a documented cyber resilience framework that will protect networks and IT systems from most threats and help recover quickly and efficiently when an incident occurs.

CYBER SECURITY STANDARDS

- **IEC 62443, 61511** – Security for IT and Control Systems.
- **NIST 800-53, 82** – Federal Information Systems.
- **ISO 27001, 27002** – Information Security.
- **NERC CIP** – Critical Electrical Infrastructure Cyber Security Standards.
- **ISA 99, 84** – Industrial Automation and Instrumentation.
- **API Institute 1164** – SCADA Security.

VULNERABILITIES

Recent cyber risk reviews by government cyber experts identified significant opportunities for the water sector to operate at a higher level of cyber security maturity. This is necessary to manage the risks effectively.

The ongoing implementation of automated Industrial Control Systems (ICS) with the increasing interconnection of information systems, remote connections with reliance on third-party suppliers and integrators has broadened the attack surface of water companies' information systems.

Vulnerability allows attackers to penetrate the system, being able to alter conditions in the Control Software and potentially causing damage to the process. Typical vulnerabilities include:

- Centralized IT and decentralized OT in the same system.
- Legacy OT with protocols not designed for security.
- Demand for more integrated business data.
- Default configuration often lack security features, or they have been disabled or removed.
- Lack of training in security.
- Unsecure remote connections (via Internet).
- Infected laptops.
- Unsecure modems.

5 INDUSTRIAL CYBERSECURITY IN THE UK WATER INDUSTRY

- Unsecure 3rd party software.
- Infected USB Keys.
- Unsecure serial connections.
- Infected PLC Logic.

THREATS

There are credible cyber threats to all of the UK's critical national infrastructure (CNI), including the water sector. These could lead to serious consequences, particularly as increased automation and connectivity reduces the scope for standalone or manual operation of the water supply system.

A number of threat actors including terrorists, hacktivists, criminals and foreign state actors can use cyberspace as a means to exploit vulnerabilities and cause damage. This could manifest itself in a number of ways, including through the disruption of water supply or affecting the quality of the water supply. Technological developments have increased the attackers' reach and made their identification more difficult.

Cyber threats should not be viewed in isolation. Capable adversaries could also seek to employ cyber methods as part of a 'blended attack' to enable or reinforce a physical attack, or to seek to control industrial plant and control systems at a water plant.

The cyber threat is evolving rapidly as technological advancements increase opportunities for hostile actors. Within the next decade, cyber tools and techniques that are presently the preserve of nation states will be much more widely available and the offensive cyber capabilities of state actors will improve. The possibility of terrorist cyber attacks capable of exploiting vulnerabilities in the UK's CNI and causing disruption is therefore likely to increase if defences are deficient.

As the threat increases, so too must the industry's ability to defend itself. Over time, exploitation of cyber vulnerabilities in the UK's water sector, either to access and remove sensitive information or support more complex attacks, will become more likely as will the potential for greater resultant impact. The threat extends beyond critical national infrastructure could result in significant reputational damage and reduce both investor and customer confidence.

5 INDUSTRIAL CYBERSECURITY IN THE UK WATER INDUSTRY

A strategy to minimize the risk should address each of the factors above:

1. **Set Security Goals.** Define outcomes, conditions and/or performance and what norms, standards, rules and laws your organization needs to comply with.
2. **Inventory Cyber Assets,** identifying systems and networks in your Organization, including IT Systems, Control Systems, HMI, Smart Devices, RTUs, SCADA and everything else that is interconnected in your Organization. It is important to have a complete picture of all assets that are interconnected via any kind of network.
3. **Assess Risks** by combining potential direct and indirect consequences of a breach, hazard or attack. Identify vulnerabilities and threats, by:
   - Interviews with system owners.
   - Document reviews to assess the organization's policies and procedures.
   - Vulnerability assessment to identify weaknesses in hardware, software and policies.
   - Penetration testing to identify vulnerable systems and potential gaps in policies and procedures.
   - Staffing assessments provide organizations with recommendations regarding staffing levels, required skills and training.
   - Product testing involve testing a device within its cybersecurity lab against known attacks and other intrusion techniques.
4. **Prioritize Investments** and actions based on risk and cost and determine protection that provides the greatest mitigation of risk. Develop a strategy that prioritizes the most critical improvements, based on cost and duration, where the vulnerabilities were found, what assets are most important to protect from attacks and compliance with norms and standards.
5. **Implement Protective Programs** or actions to reduce or manage risks identified and secure the resources needed to address priority initiatives. This could include installation of new hardware, software upgrades or implementing procedures.
   - Develop policies and procedures.
   - Engineering.
   - Select vendor.
   - Select hardware and software.
   - Write RFP documents.
   - Systems Integration.

6. **Measure Effectiveness,** using metrics and other evaluation methods to measure progress and the effectiveness of the protective programs.

   Perform the assessment in Step 3 again and compare the cybersecurity before and after implementing the protective programs.

   - Have the security goals been reached?
   - Does the system now comply with norms, standards and regulations?
   - Have the gaps between baseline and target risks been eliminated?
   - Have the critical vulnerabilities been eliminated?
   - Have the necessary changes to the Organization's policies and procedures been implemented?

CURRENT SCENARIO

Previously, less importance was given to ICS security. At times, it meant physical access control, in that the kiosk/building that housed the ICS would be risk accessed and appropriate level of protection was provided by Physical security loss of prevention certification board (LPCB) rated locks for kiosk doors. Additionally, the SCADA would have a password security for multiple roles and yes there would be firewalls between the IT and the OT.

Thanks to the new normal of remote working, the maintenance/commissioning teams are less likely to visit site; instead, they access PLCs and SCADA remotely, which potentially introduces an additional vulnerability, especially if it involves supply chain system integrators.

Recent attacks on water treatment plants in Israel by non-state actors (the attackers could manipulate valves via SCADA to increase chlorine levels in water, shut off valves, etc.) have exposed vulnerabilities in water treatment plants and also highlighted the capabilities of hackers who wish to exploit them. These vulnerabilities are not only at OT side but also there are possibilities of crossovers from and to the business side of the companies that manage it (can malware travel from say billing systems to OT? and vice versa?).

Compliance to Cyber security can be seen as type of insurance, although it may not be easy to directly justify the direct cost - except for the realisation that if its not there

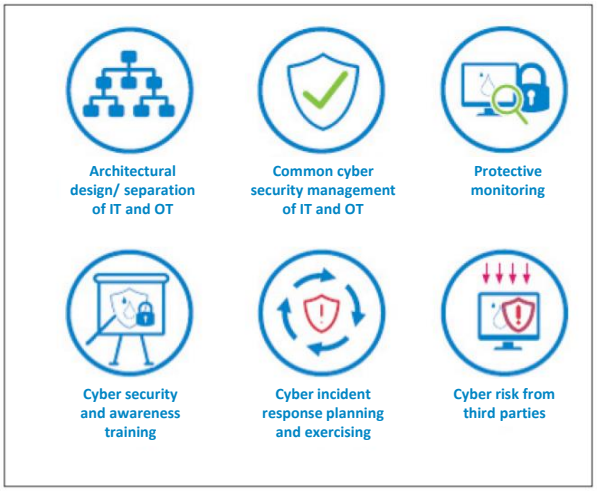
then, the company may end up paying out much more; both financially and reputationally.

In UK operators of essential services (Drinking water supply and distribution companies) serving more than 350,000 or more people must demonstrate that they are applying appropriate measures to manage the risks to their network and information system. The EPC contractors that help build or refurbish these water treatment plants also should ensure that they have taken appropriate risk identification and mitigation measures associated with cyber security. Such requirements need to be passed on to the supply chain too, as that can be seen as the weakest link in an otherwise strong corporate offering.

The UK water industry work together to produce common sets of mechanical and electrical engineering standards – Water Industry Mechanical and Electrical Specifications (WIMES). It remains to be seen whether they produce a 'WIMES' standard for cyber security. It would appear to be in their interest to do so.

FOCUS AREAS IN 2021

A cyber risk review identified the following as focus areas for cyber security activities:



Architectural design/separation of Information Technology (IT) and Operational Technology (OT): Ideally, IT and OT systems or networks should be separated to prevent infections in IT systems spreading and impacting processes that could cause physical damage.

5 INDUSTRIAL CYBERSECURITY IN THE UK WATER INDUSTRY

Common Cyber Security management of IT and OT: While IT and OT networks should be separated, the two should come under a single set of security policies.

Protective monitoring: Protective monitoring refers to the use of sensors and software to provide information about what is happening within a network or device. Examples of monitors include intrusion detectors, activity logs and firewalls. Monitoring should be proactive to be effective in detecting malicious activity.

Cyber security and awareness training: Cyber security should not be seen as the preserve of the IT department. Cyber-attacks can target any member of an organisation, so awareness campaigns for all employees could be an effective tool in defending against cyber-attacks.

Cyber incident response planning and exercising: Any organisation needs a set of plans and procedures to implement in the event of a cyber-attack. These plans should set out clear roles, responsibilities and procedures that are easy to follow under pressure. Incident response plans should be exercised regularly to ensure that everyone is familiar with what the plans contain and what their role is within them.

Cyber risk from third parties: Company networks are increasingly accessed by third parties, such as equipment suppliers, software suppliers and contractors. Often, these entities require the ability to upload software onto systems, make alterations and plug their equipment into the host network. Policies need to be in place to manage this risk; for instance, by restricting the number of people with external accesses to a network and ensuring that devices plugged into the host network are not carrying malware.

5 INDUSTRIAL CYBERSECURITY IN THE UK WATER INDUSTRY

A well known methodology for Cyber Security and the attendant systems, procedures and policies to help manage those risks is the UK's National Cyber Security Centre '10 Steps to Cyber Security':

Photo courtesy – NCSC - UK

CREDITS

- Cyber Security principles for the Water Industry – Water UK
- Water Cybersecurity Strategy – DEFRA
- Andrew O'Sullivan – EICA Chief Engineer Water- Europe B&V
- Erik Wreschner – Project Manager B&V

6 SECURITY IN IOT AND IIOT SYSTEMS

Author:

JAYDEEP DEOLEKAR

Jaydeep is a Michigan based software professional with over 27 years of experience in software development and leading multiple projects in automotive, financial, and manufacturing industry. He has a strong software solution development, business analyst and architecture background and is expert at software solutioning, presenting alternate solutions for business and technical requirements and providing end to end solutions from proof of concept to go-live. Jaydeep is a Microsoft certified Azure IoT Solution Architect. In the past he has worked on several IoT projects including SAP Leonardo and OPC UA.

Jaydeep currently works for General Motors. The views expressed in this article as his own and do not reflect those of his past or present employers and clients.

LinkedIn Profile: www.linkedin.com/in/jaydeep-deolekar

6 SECURITY IN IOT AND IIOT SYSTEMS

IoT is one of the latest frontiers of technology. It offers new opportunities to reduce costs, increase revenue and has a lot of potential to transform businesses. IIoT refers to the Industrial Internet of Things, which is increasingly becoming popular as an Industrial automation technology. IIoT can be considered to be the Industrial flavor of IoT.

Many businesses, however, are hesitant to embrace IoT yet because of their concerns about IoT security and privacy. The infamous Mirai botnet attack on October 12, 2016 was an eye opener for the world, regarding how vulnerabilities of IoT devices could be exploited to cause a massive interruption in the technology services that we heavily rely upon. In this article we will take a look at IoT system security and what approaches are available today to mitigate the security risks in the IoT systems.

SYSTEM SECURITY IS A CROSS-CUTTING CONCERN

Cross-cutting concern represents a key area of an architecture design that is not related to a specific layer, or component in the solution. It expands across the design. Security is one such cross-cutting concern that affects IoT architecture.

IOT SECURITY NEEDS TO BE BUILT GROUND UP

- It is critical that security is considered in every one of the sub-systems.
- It is particularly important that devices should be securely provisioned.
- Devices themselves must be inherently secured. Not only securing logging into devices but devices should be physically secured as well.
- Device connectivity to cloud should be secured and it should be ensured that device communication with cloud cannot be intercepted.
- Need for secure integration between IoT cloud and backend solutions.
- Finally, the data storage should be secured once the data is at rest by using strategies such as data encryption.

DESIGN WITH SECURITY IN MIND

It is especially important to understand potential security threats before designing the system, so that the defenses can be added in the design while building the system.

6 SECURITY IN IOT AND IIOT SYSTEMS

IOT THREAT MODELING

IoT Threat modelling is a structured approach to identifying threats, the outcome of which is a **Threat Model** document. The Threat Model contains key information which invites cross-team discussion about identifying all the threats that may apply to the system. It helps identify attack vectors upfront. Having list of attack vectors helps ensuring that mitigations are designed for these attack vectors. These mitigations are captured in the Threat Model so that they are tracked in the documentation. Having these mitigations documented helps continuity of knowledge in the evolution of the product. It also helps capturing the lessons learnt from previous iterations. It helps onboarding new team members as well as articulation of product security coverage to the customers.

The areas that a Threat Model focuses on are

- Security and privacy features
- Features where failure relates to security such as single sign on or user specific data which could cause a vulnerability.
- Features that touch a trust boundary. A Trust boundary is the boundary between two areas of program execution needing different levels of trust to access. There may be elevation of privileges happening when a user accesses different system components and it should be ensured that bad actors do not take advantage of the elevated privileges.

HOW TO THREAT MODEL

- Model the application
- Enumerate security threats
- Mitigate threats
- Validate by reaching out to a broader team to ensure that everything is covered. This is an iterative process and newer threats could be identified that need to be mitigated.

MODELLING PROCESS

- Create an architecture diagram with areas of vulnerability.
- Start with breadth-first approach. Look at the overview of the system and understand it as a whole. Don't drill down too early before identifying all the areas needing focus.

- Drive the process, don't let the process drive you. Understand the problem domain, environment, and the team skillset. Use the steps as guidelines.

CORE ELEMENTS TO BE CONSIDERED IN THE THREAT MODEL

- **Processes** such as web services or web applications
- **Data Stores** such as databases, configuration files and logs
- **Data Flow** where data moves from one component to another
- **External Entities** such as users or external data sources

THREAT CATEGORIES - THE STRIDE MODEL

There are six threat categories covered by the STRIDE Model developed by Microsoft.

- **S** – Spoofing
- **T** – Tampering
- **R** – Repudiation
- **I** – Information Disclosure
- **D** – Denial of Service
- **E** – Elevation of Privilege

Stride Chart

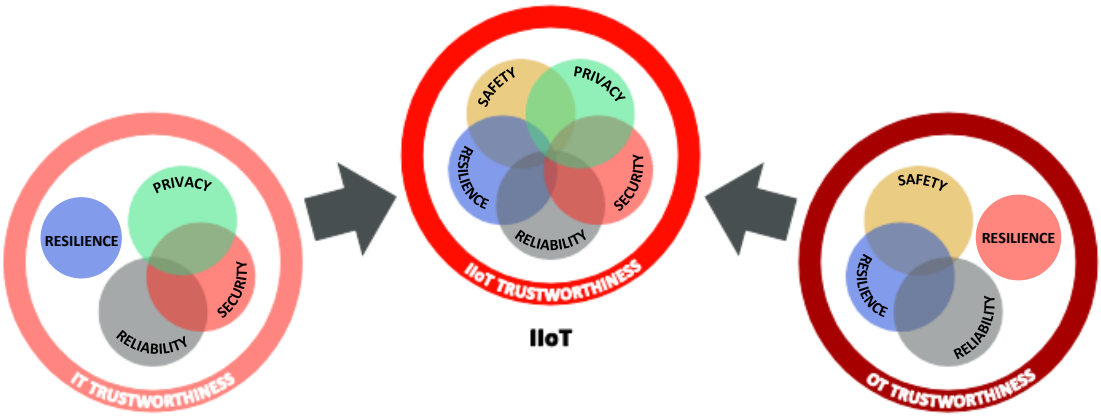
Property	Threat	Definition	Example
Authentication	Spoofing	Impersonating something or someone else	Pretending to be a valid IoT device
Integrity	Tampering	Modifying data or code	Modifying telemetry data as it is transferred via the network
Non-repudiation	Repudiation	Claiming to have not performed an action	Not enforcing digital signing of messages
Confidentiality	Information Disclosure	Exposing information to unauthorized viewing	Leaking confidential system performance data
Availability	Denial of Service	Deny or degrade system access	Blocking receipt of telemetry data
Authorization	Elevation of Privilege	Gain capabilities without proper authorization	A read-only user deleting devices

HOW DOES THE STRIDE MODEL APPLY TO THE CORE ELEMENTS?

SECURITY IN INDUSTRIAL INTERNET OF THINGS (IIOT)

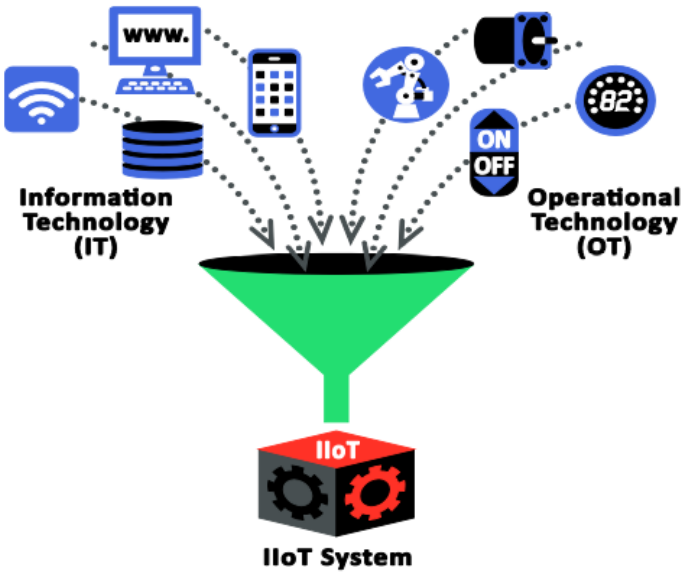
An Industrial Internet of Things (IIoT) connects and integrates industrial control systems with enterprise systems, business processes and analytics. These systems differ from traditional industrial control systems, by being connected extensively to other systems and people, increasing their diversity and scale. They also differ from traditional information technology (IT) systems in that they use sensors and actuators in an industrial environment. These systems typically interact with the physical world where an uncontrolled change can lead to hazardous conditions. They are also referred to as "cyber-physical" systems due to the close coupling of the physical and cyber components.

This potential risk increases the importance of security, safety, reliability, privacy, and resiliency beyond the levels expected in many traditional IT environments. The cultures of operational and information technology differ, leading to a need to integrate these cultures and have implications on how these systems can be secured.



6 SECURITY IN IOT AND IIOT SYSTEMS

Traditionally, the security of Information Technology (IT) and Operational Technology (OT) systems has been evaluated independently, but an Industrial Internet of Things (IIoT) system is more than a simple merge of the two. Trustworthy IIoT systems require their security functions to be evaluated end-to-end across both IT and OT.



BROWNFIELD VS GREENFIELD DEPLOYMENTS IN OT

The term brownfield describes an environment where new solutions and components must coexist and interoperate with existing legacy solutions. The term is used in contrast to greenfield, where legacy systems are absent, removing such constraints. Often OT systems are deployed as brownfield, due` to the size and capital expense involved in building and retrofitting the industrial processes they encompass.

IOT SECURITY MATURITY MODEL (SMM)

The IoT Security Maturity Model (SMM) proposed by the Industrial Internet Consortium (IIC) enables Internet of Things (IoT) providers to set security targets and invest appropriately in sensible security mechanisms that meet their requirements. Security Maturity is a measure of the understanding of the current security level, its necessity, benefits, and cost of its support.

The SMM provides a conceptual framework to help organizations select and implement the appropriate security controls from the myriad options. It helps an organization determine what their security maturity target state should be and assess their current state. Repeatedly comparing the target and current states identifies where further improvement can be made.

6 SECURITY IN IOT AND IIOT SYSTEMS

There is no silver bullet that can address security needs for every system. Organizations have differing needs, and different systems need different strengths of protection mechanisms. The same technology can be applied in different ways and to different degrees, depending on needs. The SMM helps organizations determine the priorities that drive their security enhancements and the maturity required to achieve them.

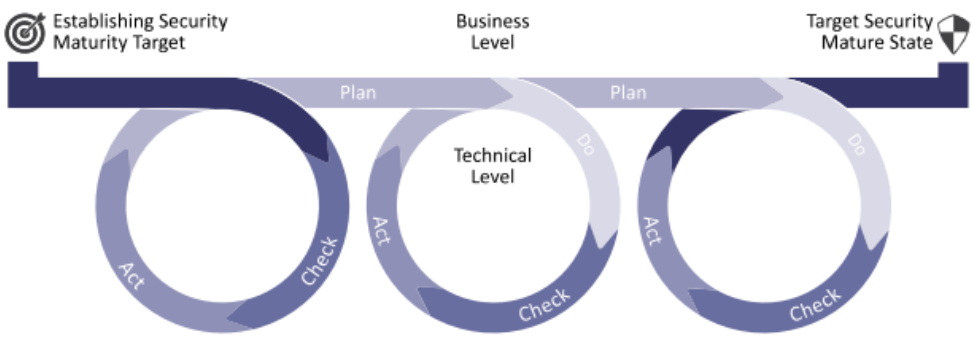
The model fosters effective and productive collaboration among business and technical stakeholders. Business decision makers, business risk managers and owners of IoT systems, concerned about proper strategy for implementing mature security practices, can collaborate with the analysts, architects, developers, system integrators and other stakeholders who are responsible for the technical implementation.

To drive proper investment, the IoT Security Maturity Model includes both organizational and technological components. Organizations use the model to set their target maturity, understand their current maturity and determine what they need to do to move to a higher maturity state.

Maturity is about effectiveness, not the arbitrary use of mechanisms. The SMM aligns the comprehensiveness (degree of depth, consistency and assurance of security measures) and scope (degree of fit to the industry or system needs) of security needs with the investment in appropriate practices.

Not all systems require the same strength of protection mechanisms or procedures to meet their security requirements. The organizational leadership determines the priorities that drive the security enhancement process, making it possible for the mechanisms and procedures to fit the organization's goals without going beyond what is necessary. The implementations of security mechanisms and processes are considered mature if they are expected to be effective in addressing those goals.

SMM IS AN ITERATIVE PROCESS.



6 SECURITY IN IOT AND IIOT SYSTEMS

There are already more IoT devices (or things) than the humans on Earth. There are approximately 7.62 billion humans on our planet, yet there may be more than 20 billion IoT smart devices before the beginning of 2021. That brings us to the inevitable need for securing these devices before they get deployed in the field. They will need to be secured right when they are manufactured and mistakes such as having same default password for each device should be avoided.

As of now in 2020 the status of an IoT device is that the same device is deployed in different environments with differing security requirements.

For example, take an IoT device like a monitoring camera - the same model may be deployed in a consumer, commercial or industrial environments. This was a business decision because it would be much more expensive to design and manufacture three different designs and models for essentially the same product. But now going forward, this will be no longer acceptable.

The application environment will dictate the security and privacy components to be installed on the camera. Although the underlying basic hardware may be the same, product companies will have to be more aware of the environments where the product is deployed from a security and privacy perspective – since what could be considered not so much of an issue in one environment, could be a major breach in another. There must be a philosophy where product manufacturer will ship them with the security hardware and software appropriate for the application environment. So, although the main basic design functions of the camera may be the same (light sensor, image processing, etc), the security part may need to be tweaked appropriately, depending on the application environment.

Companies will have to become more and more aware of their security and privacy needs and the Security Maturity Model (SMM) is a step towards that. Security Threat Model helps product companies to build the security ground up in the system and the Security Maturity Model helps the product companies to assess and understand the security needs of their customers. The two models help IoT devices to be built with the right amount of security for the environment in which they will be deployed.

In coming years, we should see organizations becoming more and more matured in understanding their security and privacy needs and appropriately choosing the IoT

products to meet their requirements. Also, as the IoT industry matures, we should also see the corresponding regulations and standards fine-tuned for the environments in which the IoT devices are to be deployed as one size will not fit all. Companies will need to be aware of where their products are used, since an IoT device made with security considerations for one environment, if used in another environment may be breaching the regulations.

REFERENCES:

Microsoft IoT Security Architecture
https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture

Industrial Internet Consortium – IoT Security Maturity Model
https://www.iiconsortium.org/smm.htm

7 INDUSTRIAL CYBERSECURITY IN 2020 AND A WISHLIST FOR 2021

Author:

MANDAR PHADKE

CEO-Abhisam Software Group

Mandar Phadke graduated in Engineering from the University of Bombay, India and did his post graduation in Management from LaTrobe University, Australia. He is currently heading Abhisam Software (www.abhisam.com), a company involved in developing e- learning programs, certifications and provides consulting in areas like Industrial Cybersecurity, Process Safety, Functional Safety, Hazardous Areas & Industrial IoT. Prior to Abhisam, he has worked for more than two decades in the chemical process industry, for marquee multinational companies in different parts of the world, in leadership roles related to project design, engineering, commissioning, operations, maintenance, safety and decommissioning. He can be reached at mandar.phadke@abhisam.com

7 INDUSTRIAL CYBERSECURITY IN 2020 AND A WISHLIST FOR 2021

The year 2020 was unusual, mainly due to the COVID 19 pandemic that disrupted normal life. As regards Industrial Cybersecurity, there were a few Industrial Cybersecurity incidents, as well as quite a few positive developments too, which I list below in one big list. Further on, I will also show you my wishlist for the Year 2021 and beyond.

SOME DEVELOPMENTS IN THE YEAR 2020

1. **Cyberattacks on Israeli water infrastructure.**
   These were not one single attack, but multiple ones on different types of water related infrastructure, such as agricultural pumps, as well as trying to manipulate Chlorination systems that supply drinking water to cities. The attackers tried to increase the Chlorine level beyond safe limits and if successful, could have caused mild poisoning to the consumers.
   https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

2. **US President Donald Trump issuing an Executive Order**
   US President Donald Trump issued an Executive Order regarding cyber security of the bulk electric supply and power grid in May 2020. https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/
   This also included among other things securing the electric power utilities from supply chain attacks (using compromised components with backdoors that can be exploited at some time in future by adversaries). This was after he extended the National Cyber emergency state in March 2020.

3. **MITRE ATT&CK for ICS being made publicly available.**
   The MITRE ATT&CK was earlier available only for Enterprise Cybersecurity but they have also now developed an ICS specific matrix. Link here https://medium.com/mitre-attack/launching-attack-for-ics-2be4d2fb9b8

4. **The US Cybersecurity and Infrastructure Security Agency (CISA) released its five year Industrial Control Systems security strategy**
   According to the agency "A Unified Initiative, is a multi-year, focused approach to improve CISA's ability to anticipate, prioritize, and manage national-level ICS risk.

Through this "One CISA" initiative, CISA will work with critical infrastructure (CI) owners and operators to build ICS security capabilities that directly empower ICS stakeholders to secure their operations against ICS threats". https://www.cisa.gov/publication/securing-industrial-control-systems

5. **ISA 99 committee released the ISA/IEC 62443-3-2**
   This is one part of the multi-part ISA/ IEC 62443 standard, that deals with risk assessment of Industrial Control Systems.
   https://webstore.iec.ch/publication/30727

6. **UL (Underwriters Laboratories) formally announced that they have launched a system to assess cybersecurity in the supply chain.**
   Although it is not exclusively for ICS cyber security, yet it could be used as an alternative to the ISA Secure system to ensure that Industrial Automation system components are secure and do not become backdoors that can compromise ICS security of the host system. https://www.ul.com/news/ul-announces-industry-first-comprehensive-supply-chain-cybersecurity-solution

7. **Sanctions against Russian agency for suspected TRITON involvement**
   In Oct 2020, the US Government's Department of the Treasury's Office of Foreign Assets Control (OFAC) designated, pursuant to Section 224 of the Countering America's Adversaries Through Sanctions Act (CAATSA), a Russian government research institution that is connected to the destructive Triton malware. As you probably know by now, the TRITON malware targets TRICONEX Safety Logic Solvers and was first discovered sometime in the year 2017 in a Saudi Arabian petrochemicals plant. It did not cause any kind of asset damage or accident, but the implications made plant owners and operators, pretty nervous. https://home.treasury.gov/news/press-releases/sm1162

8. **Secure Coding practices for PLCs**
   A need was felt for defining and listing secure coding practices for PLCs. Until now there was apparently nothing like it anywhere, even in the standards. Hence an online forum named "Top 20 list of PLC secure coding practices and supporting

documentation for engineers, security professionals and management" was set up through the efforts of Jake Brodsky, Dale Peterson of S4 Events/Digitalbond and Sarah Fluchs from admeritia. Details about the project are here https://gca.isa.org/blog/the-top-20-secure-plc-coding-practices-project

The forum is hosted by ISA. The aim is to use these secure coding practices while programming PLCs to avoid having security issues later. The forum is located here https://top20.isa.org/ and can be accessed by anybody after registration, not just ISA members.

The above list is a compilation of Industrial Cybersecurity related events upto now in the year 2020. Now we will take a look at my wish list for the year 2021 and ahead. Feel free to contact me to add your wishlist points and I will include it in the next report.

WISHLIST FOR THE YEAR 2021 AND BEYOND

There are some ambitious (and some might argue not very doable things in the span of one year) in the list. However, one must start somewhere. Hopefully, somebody or some organization can take these up.

1. **Control System Vulnerability Reporting Platform & Knowledge Repository**
   We should have an alternate way to report, collate and share information among stakeholders, including asset owners and system integrators, at a global level. Perhaps, professional non-governmental bodies, like ISA, IEEE or IET should take the initiative, so that the platform/repository is vendor neutral, as well as government neutral. There should be a way to anonymously share information not only about known vulnerabilities, but also about actual incidents, suspected incidents, detection of counterfeit devices (and/or malware loaded booby trapped components). This should be updated as frequently as possible and monitored by plant and asset owners, so that they can take quick, corrective actions. To the best of my knowledge, there is no such system now. I guess the main roadblock in getting this done is funding and no possible ROI for the investors, unless subscriptions can pay for it.

At present the US Government agency CISA is playing a similar role, but it is limited to listing vulnerabilities and alerts, which are not only ICS specific. It depends on various vendors and others to spot vulnerabilities and report them. Presumably, these are addressed by vendors via updates (patches).

2. **Securing Industrial Systems against Supply Chain attacks**

There should be a better way to secure Industrial Systems against supply chain attacks. As of now, there does not seem to any specific standard for this. ISA Secure is a good initiative, but it can be better. The owner of the IACS should also be sure that no counterfeit products are being used in their system. You can buy a model of a network switch that has passed the ISA Secure tests, but how will you know if the actual box in your hands is genuine and not counterfeit?

One of the switches below is fake, can you spot which one it is?

Difficult, eh? Take a look at the report here, regarding fake CISCO switches (the image above is from the report link below), discovered by F-Secure labs and also see which one of the two is the fake one.

https://labs.f-secure.com/publications/the-fake-cisco/

https://labs.f-secure.com/assets/BlogFiles/2020-07-the-fake-cisco.pdf

It is exceedingly difficult for even an experienced professional to distinguish the fake switch from the original one.

3. **Automation Services and Software Supply chain resilience**

The term "Supply chain", should include not just physical devices that are used in Industrial Automation and Safety systems, but also software programs and services, including the individual persons who provide these.

As of today, software patches and programs have been covered in IEC TR 62443-2-3:2015 and system integrator/automation vendor services have been covered in IEC 62443-2-4:2015 (and amended in 2017). These are steps in the right direction but there should be commonly agreed due diligence practices, as regarding background checks of personnel who work on these systems as well as vetting of their equipment.

How do you know that the system integrator's engineer who normally maintains your system, does not have a compromised laptop that he plugs into your automation system? Are these people aware of Industrial Cybersecurity? Do they diligently follow good practices?

Beginning 2021 we should aim towards making all participants of the Industrial automation supply aware about Industrial Cybersecurity and also be competent in the subject. Once this is done, we can be sure that the Industrial Automation supply chain has become more resilient towards thwarting attacks.

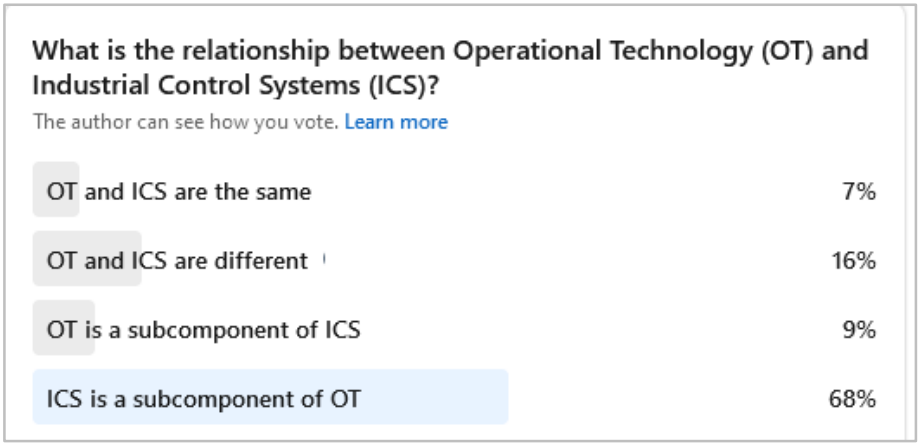
4. **Secure Automation network protocols (e.g. Secure Fieldbus)**

In my opinion (and you can of course disagree with it), the Zone and Conduit philosophy of protection as given in ISA/IEC 62443 for IACS is at best a stop-gap arrangement. Once a malware breaks through a DMZ/firewall into a Zone, it can pretty much own everything inside the Zone. This is because almost none of the Instrumentation & Control Systems protocols used in the process industry, have authentication and encryption at the field level, or many times even at the controller network level. Hence, we do need a new automation protocol at the field level that has authentication, as well as encryption. The Industrial IoT phenomenon presents us with such an opportunity and again, professional engineering associations like ISA or IEEE should take the initiative. There have been proposals by some IEEE members in the past (P. Swaminathan, K. Padmanabhan, S. Ananthi and R. Pradeep,

"The Secure Field Bus (SecFB) Protocol - Network Communication Security for secure Industrial Process control," TENCON 2006 - 2006 IEEE Region 10 Conference, Hong Kong, 2006 Ref: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4142362&isnumber=4142121) However, apparently this has not been developed further or become popular. If you know of any similar initiatives, do let me know.

5. A generally accepted taxonomy about Industrial Cybersecurity terms

Taxonomy and definitions, regarding Industrial Cybersecurity seem to be still in development. For example, recently a poll was carried on LinkedIn by ORIGNIX Inc asking people what they thought about the terms, OT and ICS and the results were as given in the image below.



Since the poll responses have been from mostly people in the Industrial cybersecurity field, it is evident that there are varied ideas of what constitutes OT and ICS sometimes even diametrically opposite of each other (e.g. OT is a subcomponent of ICS versus ICS is a subcomponent of OT).

This is troubling because if we do not agree about what these terms mean, then it will be difficult to have conversations, as well as contracts, between owner/operators, automation and safety system vendors/system integrators, engineering design companies and others.

A well agreed system of definitions and a commonly accepted Taxonomy is therefore urgently needed.

7 INDUSTRIAL CYBERSECURITY IN 2020 AND A WISHLIST FOR 2021

FINAL WORDS

Thank You for having the patience to read upto this point. I hope that you have found this article and the entire report useful and an enjoyable read.

You can contact me at mandar.phadke@abhisam.com for any comments, ideas for the next edition or anything else regarding Industrial Cybersecurity.

If you are interested in knowing more about Industrial Cybersecurity, then you can take a look at the Abhisam online training program here
https://www.abhisam.com/industrial-control-system-cybersecurity/

REFERENCES & CREDITS:

As given above via URLs. The photo of the CISCO switches is from the F-Secure report.
All logos and trademarks mentioned belong to their respective owners.

abhisam

www.abhisam.com

Email: mail@abhisam.com