NATO
ENERGY SECURITY
CENTRE OF EXCELLENCE

GUIDE FOR PROTECTING INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS AGAINST CYBER INCIDENTS

January 25, 2022 ver. 1.7

In Critical Energy Infrastructure

This guide provides an analysis of technology based threats, both intentional and unintentional, to the safety, reliability, resilience and performance of critical energy infrastructure and how cyber risks to the technologies used to monitor and control physical processes in CEI can be addressed.

Prepared by Vytautas Butrimas
NATO Energy Security Center of Excellence
Vilnius, Lithuania
2022

Outline

Preface

I. Introduction to industrial cyber security
   - Approach to cybersecurity
   - The 3 questions

II. IACS operator considerations
   - Initial self-awareness questions
   - Discussion

III. How we can protect identified assets from identified threats?
   - enterprise cybersecurity program

IV. Tools in the enterprise Cybersecurity Program toolbox.
   - Asset management system
   - Standards
   - Documentation
   - Evaluating and improving the level of maturity in industrial cybersecurity
     - Testing
     - Exercises
   - Secure Coding Practices for PLC's
   - Patching and updating software and firmware
   - Network security
   - Project management with integration firm
   - Backups
   - Source code control system
   - Self-integrity monitoring
   - User and role access ids
   - Industrial Cybersecurity Operations Center ICOC

V. Thoughts for the future
VI. Conclusion
VII. Acknowledgements
VIII. Appendixes

Preface

The NATO ENSEC COE prepared this Guide in response to unsettling trends in cyberspace where a wide spectrum of threat actors have chosen to target critical energy and other infrastructures that support modern economic activity, national security and well-being of society. The military sphere is not isolated from these threats as any interruption in the steady supply of energy can adversely affect military operations. In contrast to the enterprise or office environment, cybersecurity measures to mitigate cyber threats to industrial operations have come late. Industrial systems were designed with an emphasis on safety and reliability with little regard for cybersecurity. However, this design approach introduced serious vulnerabilities that if exploited by a cyber-attack could result in serious physical harm in terms of injured personnel, damage to property and to the environment. While the work of hardening Office/Enterprise IT cybersecurity has developed into a level of maturity over two decades, developing measures for reducing the cyber risks to critical industrial operations have only just begun. Furthermore, this task is made difficult in that IT data centric cybersecurity measures tend to dominate solutions which do not fully apply to industrial environments where protection of a physical process is the priority. The Guide is based upon studies and site visits to operators of critical energy infrastructure from 2011 to 2021. It must also be remembered that industrial systems that monitor and control the physical processes found in critical energy infrastructure are not uniform as there are operations that are more digitalized while others are older, more analogue or manually controlled. Since cybersecurity is related to digitalization, the Guide naturally will focus on those aspects. However, this guide will also offer advice on how to implement a digitalized solution when analogue based operators decide to modernize their control systems. This Guide notes the criminally motivated cyber-attack (ransomware) on a major fuel pipeline in the Eastern United States in May of 2021, which forced operators to shut down an 8000 km long pipeline. This incident has initiated a review in the United States[1] and in other countries of the cybersecurity of control system architectures used in industrial operations.[2] The recommendations in this Guide are applicable to any asset owner that relies on industrial automation and control systems (IACS)[3] for the control and monitoring of a physical process. Any inaccuracies found in this Guide are solely the responsibility of the author.

---

[1] US DHS, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, July 20, 2021https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

[2] Hoffman, M., Winston, T., Recommendations Following the Colonial Pipeline Cyber Attack, Dragos May 11, 2021 https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/?utm_campaign=Q221%20-%20Colonial%20Pipeline&utm_medium=email&_hsmi=126958352&_hsenc=p2ANqtz--lqHZjRdFZRwD6A7ql-tlxPsiiMMZXSwJ4AsYnBHa-Uu8_EcOBUYwVu2rWWKJ7FsiMxeW8WCCxpMqKGzEoQAlSZI3XpPP4c4EWB2TIphxPu6X1uLw&utm_content=126958352&utm_source=hs_email

[3] Industrial Automation and Control System (IACS) :collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation
Note to entry: These systems include, but are not limited to: a) industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety-instrumented system [SIS] functions, whether they are physically separate or integrated.) b) associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems. c) associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes. ISA-62443-1-1 Security for industrial automation and control systems Models and Concepts Draft 7, Edit 2 June 2019 https://www.isa.org/products/isa-62443-1-1-2007-security-for-industrial-automat

I. Introduction to industrial cyber security

Development and implementation of a cybersecurity policy that will improve safety, availability, reliability, integrity, performance and resilience of pipeline operations during an accidental or malicious cyber incident is dependent on the degree of care taken in answering 3 security policy questions:

- What are the functions and assets that have to be protected?
- What are the likely threats to those chosen assets and functions?
- How will identified assets and functions be protected from identified threats in the most cost efficient way?[4]

A major challenge in correctly answering these questions is avoiding policymaking dominated by an Office IT bias that focuses on the protection of data or information on networks as opposed to the protection of a physical process governed by the laws of physics and chemistry. Established policies and procedures governing the IT security in office environments have been in place for many years. To put it simplistically, this is the environment where the administrators and accounting departments work. Most people are familiar with the IT environments found in their offices, on their desks and in their homes. The work here is information or data centric with the protection of confidentiality, integrity and availability being important. There are very good standards and best practices that have a proven record of accomplishment for application in this environment such as the SANS 20 CIS Controls (formerly known as Critical Security Controls) [5] and ISO/IEC 27000[6] series of standards for information security management. While these standards and practices work well for office IT, they fall short in insuring the safety, reliability, integrity, performance and resilience of the physical processes found in industrial operations. Serious operational and safety issues can arise from operator screen locking, compatibility issues coming from applying antivirus solutions, patching practices that can disrupt operations and additional network traffic caused by backup activities that can block safety control messages[7]. More applicable standards and best practices are available such as the Top 20 PLC Secure Coding Practices[8] and ISA 62443[9] Industrial Automation and Control System (IACS) security standard[10], which will be briefly introduced in this Guide.

The targets (what needs protection)

In employing this 3-question approach, the first question is the most important for it will inform the value of answering the following questions. In a pipeline system, besides protecting the fuel pipes and other

[4] Butrimas, V., Towards a Cyber Safe Critical Infrastructure: Answering the 3 questions, SCADASEC, 21 February 2018. https://scadamag.infracritical.com/index.php/2018/02/21/towards-cyber-safe-critical-infrastructure-answering-3-questions/
[5] https://www.sans.org/blog/cis-controls-v8/
[6] https://www.iso.org/isoiec-27001-information-security.html
[7] https://gca.isa.org/blog/white-paper-excerpt-applying-iso/iec-27001/2-and-the-isa/iec-62443-series-for-operational-technology-environments?utm_campaign=ISAGCA%20Communications&utm_content=172805693&utm_medium=social&utm_source=linkedin&hss_channel=lcp-164473
[8] https://www.plc-security.com/index.html
[9] https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c
[10] https://cdn2.hubspot.net/hubfs/5382318/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

physical structures, the protection of the industrial automation and control systems (IACS)[11] is a priority. IACS is a "collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation as defined by the International Society of Automation (ISA)[12]".

This includes the hardware and software used to monitor and control the physical processes unique to industrial operations. However, this technology is broadly used in industrial operations. In pipeline operations for example these technologies are found in the dispatch (control center), pumping stations, depots, fueling stations, seaports (where product enters the pipeline), access pits and associated infrastructure elements such as:

Monitoring and Control systems

- DCS, SCADA, PLC
- Networked sensing and control, diagnostic systems
- Leak Detection System
- Process sensors
- Basic Process Control System
- Safety Instrumented Systems

Associated information systems

- Advanced/multivariable control
- Online optimizers
- Dedicated equipment monitors
- Graphical interfaces (Human Machine Interface –HMI)
- Process historians[13]

Threats to IACS (who threatens and how)

Now let us look at the threats to the assets selected above.

In 2010, we learned that the most sophisticated attacks from cyberspace shifted to targeting engineering systems when STUXNET malware took away the view and control of an industrial process from the hands of the operators[14]. The disabling of safety systems, sending false data to operators and the denial of an

[11] Authors note: While many use the term Information Technology (IT) as a catch all to describe the processing of data and information on computers, servers, and mobile phones that take place in our offices, ministries and at home, there are several terms used that more accurately describe industrial operations such as Operational Technology (OT), Industrial Control Systems (ICS) and Supervisory and Data Acquisition (SCADA). This guide will settle on using the term IACS as it comes from an international standards organization (ISA) and applies to the physical process found in pipeline and other industrial/manufacturing operations as opposed to the data centric work found in IT.

[12] [Source: ISA-62443-1-1 (D7E1), May 2019] https://www.isa.org/products/isa-62443-1-1-2007-security-for-industrial-automat

[13] Ibid.

[14] As discussed by industrial security practitioner Ralph Langer in 2012 at the S4 conference on his research of STUXNET, Langner's Stuxnet Deep Dive, S4x12, https://www.youtube.com/watch?v=zBjmm48zwQU

operators' view and control of critical physical processes, all done without the need for an Internet connection, were to become familiar features found in attacks throughout the decade.

In 2012 Saudi Aramco, one of the largest energy companies in the world, suffered a "denial of computer" attack which erased data on the computers and servers supporting the administrative activity of the company. The threat actor however did not or could not, perhaps due to lack of required engineering skills, affect IACS operations found in the oil fields and refinery operations. Some commentators speculated that this was a revenge response of the victim nation to the STUXNET operation two years earlier[15].

In 2013 it was discovered that a remote access Trojan[16] (Havex) was being used by a malicious state actor to target the energy sector. In a sign of things to come, the attackers succeeded in planting this malware on the websites of the manufacturers where vendor software updates were offered[17]. This threat actor, which sought intelligence information about industrial operations, the poisoning of manufacturers web sites with bad software updates had the potential to compromise industrial devices.

In 2014, according to a German Government report, a cyber-attack caused the operators of a steel mill to lose the view and control of a mill's operations, which resulted in the "uncontrolled shutdown of a blast furnace, leaving it in an undefined state and resulting in massive damage"[18].

In December 2015 the operators of a regional power grid in Ukraine grid watched their control screens in amazement as the "mouse" started moving and proceeded to "click" open breakers at 30 substations putting a quarter of a million people in blackout just before Christmas. The attackers also sought to inhibit the operators' ability to respond and recover from this attack by proceeding within seconds and minutes to install compromised code on the Serial to Ethernet servers (essentially "bricking" them) used by the SCADA to monitor and control the affected substations. Simultaneously a denial of service attack (DOS) targeted the utility's telephone system, which made it hard not only for customers to inform their service provider that they were without power, but also inhibited the operator's understanding of the extent of the blackout. The attack ended with the execution of wiper malware, which erased all the data on the workstations[19].

---

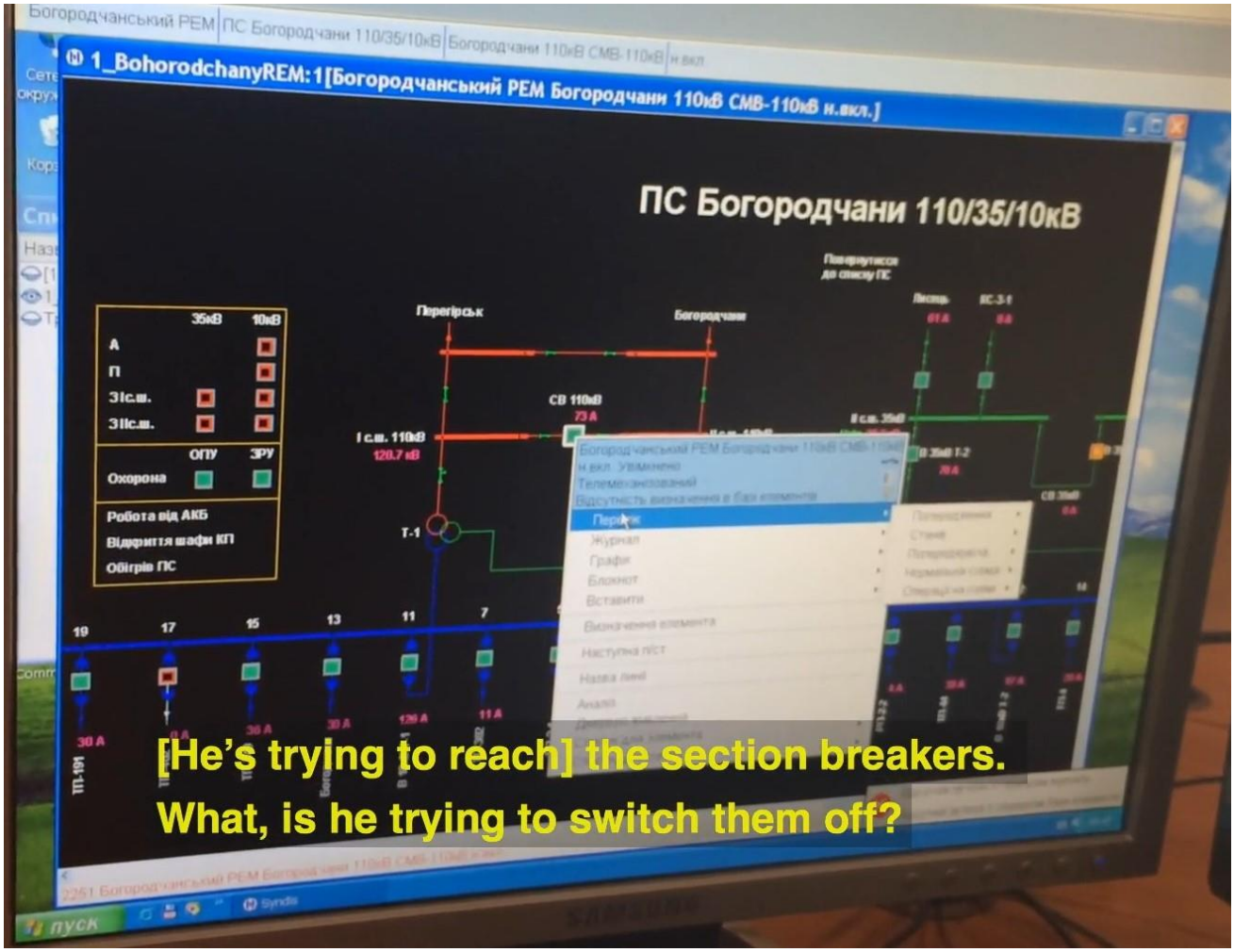
[15] Perlroth, N., In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, New York Times, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html October 23, 2012,

[16] A malicious program that remotely accesses infected resources. Trojans of this type are among the most dangerous because they open up all kinds of opportunities for remote control of the compromised system. RAT capabilities usually include program installation and removal, file manipulation, reading data from the keyboard, webcam hijacking, and clipboard monitoring.https://encyclopedia.kaspersky.com/glossary/remote-access-trojan-rat/

[17] Kovacs, E., Attackers Using Havex RAT Against Industrial Control Systems, Security Week, June 24, 2014, https://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems .

[18] The State of IT Security in Germany 2014, Federal Office of Information Security, p. 31. 2014 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3

[19] ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure, February 25, 2016 | Last revised: August 23, 2018 https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01



Actual moment photographed by an operator at a workstation when he realized he lost the view and control of a power grid during a cyber-attack on a regional power utility in Ukraine on December 23, 2015. For a while he thought the IT department was playing a funny trick on him as he watched how the mouse moved by itself and clicked open the breakers at 30 substations under his control and in front of his eyes. The investigation after the attack revealed that the system was penetrated and compromised months before the actual attack. If no one is looking out for this kind of activity then such scenes will happen again.

A short-lived but potentially more dangerous cyber-attack on the power grid occurred a year later when part of Kyiv, the Ukrainian capital lost electrical power. This time the investigation in addition to revealing the same long-term stealth techniques of undetected intrusion and reconnaissance also found that attempts were made to compromise the preventative relays. These relays act as safety systems for power grids which perform the function of disconnecting (tripping) bulk power equipment in cases of detected anomalies such as overcurrent, overload, undercurrent, or reverse current.[20] What is the possible motive for disabling a protective relay one may ask? One is to damage or destroy bulk power equipment.

[20] https://www.electgo.com/what-is-a-relay/

A compromised relay could complicate and make restoring power more costly by eliminating the protection devices that would isolate expensive and hard to replace bulk power equipment such as transformers from an anomalous electrical event during power restoration operations[21].

In the summer of 2017 the safety instrumented systems (SIS) made by Schneider Electric caused two unplanned shutdowns of one of the world's largest petrochemical facilities in the world[22]. The first cyber-attack did not register on the plant's IACS nor did the manufacturer discover anything wrong with the affected controllers, which passed the manufacturer's inspection. Only after the second shutdown was it determined[23] that a cyber-attack originating from outside had been underway inside the plant for months.[24] It was also obvious from the fact that outside cybersecurity experts were called in to investigate, **that the plant had little internal cyber-attack detection or investigation capability**.[25] The intentional attempt to compromise a safety system represents a serious escalation of the cyber threat to critical infrastructure. Control and safety systems are used in an industrial process to protect property and most importantly, people from serious harm resulting from an industrial process that has gone outside of set parameters. These parameters are used to program an automatic response in the SIS to bring a system back to a safe state when changes in temperature, flow rates, pressure, frequency, or other system state indicators exceed set levels. These are the systems that automatically respond for example, by opening or closing valves on a pipeline when pressures or flow rates go beyond pre-set parameters.[26]

Also, in the same summer of 2017, a new variant of these disruptive malware attacks, which some described as a "weapon of mass disruption"[27], occurred with the appearance of a ransomware program on accounting software used by the private sector to pay taxes to the Ukrainian Government. NotPetya spread outwards from Ukraine hitting industrial/manufacturing targets in Africa and Europe. Most notably the worldwide shipping operations of Maersk came to a standstill. Interesting enough, the ransomware module for payment (for which, after payment, the victim could unlock the encrypted files) in NotPetya did not work. This to some commentators indicated that the perpetrators were not interested in financial gain but in spreading this destructive malware as fast and as widely as possible.[28]

In March of 2019 international manufacturing and power company Norsk Hydro was a victim of a ransomware attack causing it to shut down its automated systems and go to manual paper based control.[29]

---

[21] Slowik, J., CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack, Dragos Inc. August 2019, https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[22] Perlroth, N., Krauss, C., A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. March 15, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[23] Gutmanis, J., Triton - A Report From The Trenches S4 Conference March 2019, https://www.youtube.com/watch?v=XwSJ8hloGvY

[24] Sobczak, B., The inside story of the world's most dangerous malware, E&E News, March 7, 2019 https://www.eenews.net/stories/1060123327

[25] Gutmanis, J., Triton-A Report from the Trenches, S4 Conference Presentation, March 2019, https://www.youtube.com/watch?v=XwSJ8hloGvY

[26] Recacha, O., Butrimas, V., Securing the Industrial Internet of Things: Policy Considerations for reducing cyber risks to industrial control and safety systems, Operational Highlights No. 13. 2020. p. 46, NATO ENSEC COE. https://www.enseccoe.org/data/public/uploads/2020/03/nato-ensec-coe-operational-highlights-no13.pdf

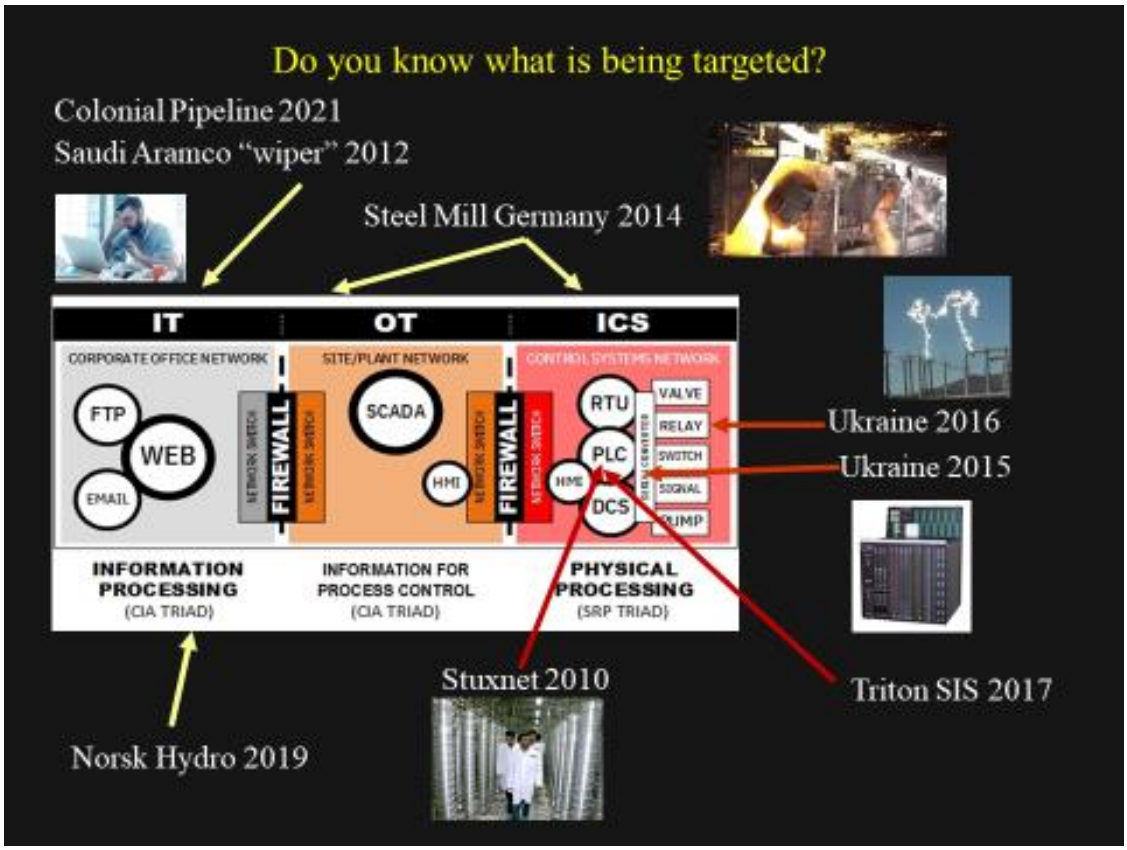
[27] https://secureservercdn.net/166.62.108.22/5kb.d9b.myftpupload.com/wp-content/uploads/2020/07/Weapons-of-Mass-Disruption-ICIT-July-2020.pdf

[28] Greenberg, A., The Untold Story of the most Devastating Cyber Attack in History, Wired, 2018-08-22 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[29] https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

The ransom was not paid but still the additional labor intensive cost of going to manual reached over 50 million euro after only 3 months.

This leads us to the most recent, at the time of this writing, ransomware attack on the Colonial Pipeline Company in the first week of May 2021.[30] According to early reports, ransomware was planted on the administrative IT side (billing) of the company which resulted in denial of the necessary data and other information required to process and keep track of fuel orders[31]. While the operational technology (IACS) operations side of the pipeline which monitors and controls the physical processes inside the pipeline were not directly affected by this ransomware, the loss of billing and accounting information kept on the paralyzed IT side forced the operator, out of caution, to shut down the pipeline.[32] The equipment and control technology supposedly were not affected by the ransomware, but there were no instructions on what to do with the fuel being pumped down an 8000 km. long pipeline. In terms of ensuring the safety, reliability and performance of operations this should not have been allowed to happen. There were several shortcomings in the design of the industrial operations that could have been easily remedied, but apparently this was not done.



[30] Panettieri, J., Colonial Pipeline Cyber Attack, MSSPAlert, Jun 7, 2021 https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/
[31] Bertrand, N., Colonial Pipeline did pay ransom to hackers, sources now say, CNN May 13, 2021, https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html
[32] Osborne, C., Colonial Pipeline attack: Everything you need to know, ZDNET May 13, 2021, https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

In seeking to protect industrial operations, we must remember that it is not just about protecting the IT in the office - the devices closest to the physical process are also targets. Adapted graphic used with permission of Robert Radvanovsky from http://icsmodel.infracritical.com .

Missing or poorly developed was a comprehensive **Corporate Cybersecurity Program** (see Section III) that included standards for IACS cybersecurity. In particular, the International Society of Automation (ISA) ISA 95 standard addresses enterprise integration including transfer of information between plant instrumentation and corporate information systems.[33] This if applied in the system design phase could have reduced the problems encountered by the company and public during the incident. The ISA/IEC 62443 Standard for IACS[34] could also have supported the development of the Corporate Cybersecurity Program.

We must of course, be cautious and not get carried away by the malicious intentional attacks of threat actors reported with some inflation by the media. The majority of failures occurring at industrial sites that work with the laws of physics and chemistry come from unintentional events or accidents.[35] These failures can occur unintentionally through human error[36], not following established procedure[37], equipment failure or a bug in the IACS software[38] or firmware. The management of these intentional and unintentional based risks needs to be done in the framework of a corporate cybersecurity program further discussed below.

Lessons learned:

What trends are evident from the cases above? Below is a short list of the evident trends in industrial cybersecurity over the past 11 years:

- Technologies that ensure safety, reliability and efficiency of industrial operations are being targeted by highly persistent and skilled threat actors (the physical process is being targeted, not just the data);
- Attempts to disable industrial safety systems (SIS);
- Little or no industrial cyber forensics available;
- IT centric cybersecurity approaches fall short for critical energy infrastructure protection;
- This activity (for a state) is effective, cheap and deniable;

[33] https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95
[34] https://cdn2.hubspot.net/hubfs/5382318/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf
[35] For an idea on the kinds of incidents that occur refer to the SCIDMARK database: http://search.infracritical.com/
[36] Krebs, B., Cyber Incident Blamed for Nuclear Power Plant Shutdown, Washington Post, June 5, 2008 https://waterfall-security.com/wp-content/uploads/2009/11/CyberIncidentBlamedForNuclearPowerPlantShutdownJune08.pdf
[37] FERC/NERC Staff Report on the September 8, 2011 Southwest Blackout Event, April 2012, https://www.nerc.com/pa/rrm/ea/September%202011%20Southwest%20Blackout%20Event%20Document%20L/AZOutage_Report_01MAY12.pdf
[38] Cavas, C., LCS Milwaukee Breakdown Likely Due To Software Issue, Defense News, Feb 7, 2016, https://www.defensenews.com/naval/2016/02/07/lcs-milwaukee-breakdown-likely-due-to-software-issue/

- In most cases, victims believed they were compliant[39] with industry standards and best practices (i.e. segmentation, updates, firewall);[40]
- The advanced, persistent and resourced attacker does not give up and finds a way to breach and compromise the system;
- System penetration and exploitation take place well before asset owners and even security solution providers are aware their critical systems have been compromised;
- System architecture that did not adequately separate Internet facing Office IT from the operational or IACS side monitoring and controlling a physical process.

These trends indicate the importance of correctly answering the first two cybersecurity policy creation questions. When we have determined what the critical assets for our operations are and the kinds of threats that can affect their safety, reliability and efficiency, then we can start considering the third question: how to protect identified assets from identified threats in the most cost-efficient way to improve the safety, reliability, performance and resilience of critical operations?

II. IACS operator Considerations

Some of the cybersecurity considerations in this Guide stem from information gathered during site visits to liquid fuel, natural gas pipeline and power grid operators and from responses to a questionnaire (See Appendix 1).

Responses to the Questionnaire

In terms of level of digitalization, the operators that responded form into two groups. One with less automated or less digitalized operations (characterized by manual or local control) and one with greater complexity and digitalization.

The first group has a much simpler system of control to deal with. For example, instead of a sophisticated system that uses Programmable Logic Controllers (PLC), a manifold may have pressure switches attached that are set to different pressures or an analogue instrument that feeds to a valve actuator. Such systems can operate autonomously without failure but may also require more personal to monitor and maintain. The detection of malfunctions may be performed physically by an engineer or technical staff who goes down and inspects the pipes or by reading and recording information about the process displayed on a few gauges. This kind of older simpler design is far less vulnerable to cyber-attacks, which require a digitalized environment to propagate.

[39] Cybersecurity failures: Top 6 reasons, CEOVIEWS, accessed August 23, 2021, https://theceoviews.com/top-6-reasons-for-cybersecurity-failures/

[40] Moldes, C., Compliant but not Secure: Why PCI-Certified Companies Are Being Breached, CSIAC May 9, 2018, https://csiac.org/articles/compliant-but-not-secure-why-pci-certified-companies-are-being-breached/#:~:text=In%202013%2C%20%EE%80%80Target%EE%80%81%20was%20certified%20PCI%20DSS%20%EE%80%80compliant%EE%80%81,deemed%20their%20company%20%EE%80%80compliant%EE%80%81%20for%20six%20consecutive%20years.

The second or more digitalized and automated group does operate in an environment where both malicious intentional and unintentional system failure due to cyber incidents can occur. Judging from the responses to the questionnaire some interesting cybersecurity concerns do emerge:

- Belief in security through obscurity. Operator confidence that their industrial automation and control systems are not connected to the Internet. One operator firmly believes that since there are no Internet connections there "are no security risks and potential threats from cyber-attacks".
- No patching policy. Operator confidence that the implementation of a firewall makes patching and updating hardware and software on the operational side unnecessary ("We do not patch").
- Little or no on-site capability to monitor and check on anomalous process flows, equipment performance, and data flows with a goal of detecting a cybersecurity breach within 24 hours[41] ("there is no specific application to discern if anomaly is due to machine failure, incident or cyber incident"). One operator did indicate the possibility of asking for outside help (Military Intelligence Service, Defence IT provider) in investigating a suspected cyber incident. However, it was not clear whether the investigators have the skills to investigate an industrial automation and control system cyber incident where instead of data/information it is the safety and availability of a physical process governed by the laws of physics and chemistry that may be under a cyber-attack.
- Not clear if all operators have enough documentation about the pipeline operation itself that would allow for prompt restoration of operations after a severe disruption caused by an intentional cyber-attack or incident. One operator indicated they did not have a Control System Narrative, which is a very detailed description of exactly what the controllers do, and how processes work, under all conditions – normal and adverse.[42]
- Remote access to internal control networks was reported as permitted by some respondents but no details on how this access is managed to minimize possibilities for an unauthorized intrusion, let alone a capability for detection.
- Unclear policies and protocols in response to a breach from cyberspace. One operator simply responded by saying their general policy is done according to the organization's minimal repair and restoration capability policy. However, this is a high-level document that only advises on implementing a "minimum repair capability".

Discussion

It is important to think of one's operations as targets and act appropriately to make it harder for the adversary to access your critical control systems and if there is a breach, to have means already in place to respond and recover quickly. All operators of CEI should be aware of what may motivate a highly skilled and resourced adversary to degrade or disrupt their operations:

[41] After 24 hours the chances of discovering an intruder who is actively seeking to establish a stealth presence and cover tracks will drop considerably

[42] Brodsky, J., How a Process Works, SCADASEC 201—07-27, https://scadamag.infracritical.com/index.php/2017/07/27/how-a-process-works/

- To disrupt the fuel supply just when the adversary's military does something they know will draw a nation's or response;
- To contribute to service disruptions of dependent civilian critical infrastructures (for example in transport);
- To show that they can do bad things in order to intimidate;
- To sow fear, uncertainty and doubt (FUD) that disrupts well-being and trust in society at time of crisis;
- Economize on offensive assets, cyber weapons are reusable and relatively cheap (for a state actor) while physical (bombs and humans) are not;
- Using disruptive cyber tools is a very attractive option as it is Effective, Cheap (for a state)[43], and most importantly, a deniable malicious activity intended to achieve a desired policy objective.

Industrial cybersecurity was not a major topic 20 years ago. Even now, very few fully understand what is at stake and why it matters. Many IT experts think they understand it when they first see it, and immediately bring habits they have learned from office applications.

Unfortunately, what works in securing the data and information processed in office or administrative environments can be counterproductive or even dangerous in an industrial environment. Therefore, the word of advice to IT specialists working in the IACS (physical process) environment is to work carefully and in consultation with the plant engineer.

Examples of the differences between office and industrial applications are as follows: First, consider a web page. If it takes an extra second to appear in a browser, people hardly notice. However, in an industrial application if one inhibits traffic for half a second between a controller and the I/O[44] it is polling, the controller will be forced to fault. This is by design. If it can't get the poll done in under 100 milliseconds, it is usually no longer deterministic. It must fault or fail. Commonplace scanning tools such as Nmap[45], while very useful, have toxic default rates of operation. Using them in IACS or SCADA systems is a good idea, but one must take care to ensure that the scanning rates are appropriate for the application. Do not assume that any defaults for commonly used security tools are safe to use.

Second, consider when an office[46] does out of service maintenance: It is usually after hours, when few are likely to be inconvenienced. However, in a control system, out of service maintenance should be done during working hours so that operators and technicians will be ready to run equipment manually as needed. There can be no compromise here.

This is one very good reason why control system networks are not just segmented away from office equipment networks; they use physically separate equipment. Sooner or later someone is going to have to

[43] Flanagan, B., Former CIA Chief speaks out on Iran Stuxnet attack, The National News, December 15, 2011 https://www.thenationalnews.com/business/former-cia-chief-speaks-out-on-iran-stuxnet-attack-1.392917
[44] Data input-output device
[45] https://nmap.org/
[46] A typical office IT environment such as a pc workstation at a ministry or administration part of a small/medium/large business.

take a switch, router, or firewall down for routine tasks such as patching firmware or configuration updates. One way or another there will be overtime. The scheduling headaches alone would justify separate LAN and possibly even WAN infrastructure.

Third, when an office application stops, everything comes to a halt. The IT systems are used to being the center of all activity. If they cannot function, nothing happens. However in IACS and SCADA, if the computers and controllers are offline, the physical process will continue to do something, even if the outcome is very undesirable. It helps to think of this in terms of turning off the autopilot of an airplane in flight. The airplane is still flying and it is still going somewhere. Turning off the autopilot (the IACS/SCADA) doesn't stop anything.

Most importantly, IACS and SCADA are about controlling a physical process. It is possible to recover from software problems in an office by restoring backups and recovering the lost information. However, in the process world, there will be a physical mess to clean up if things don't go well. That mess may be dangerous, toxic, or even tragic.

Consider the Olympic Pipeline disaster in Bellingham, Washington on June 10, 1999. The alarm subsystem in their SCADA system was not functional. It failed silently. While it was offline, over 277,000 gallons of gasoline poured into Whatcom Creek. Eventually the fumes reached an ignition source, killing an 18-year-old fisherman and two ten-year-old boys.[47] No backup can possibly fix that.

Conversely, most Control Systems Engineers know very little about software, networks, or security. Until very recently, if someone told one of these engineers that there was a vulnerability, the response was quite likely to be "well, don't do that!" or “we do not have cybersecurity incidents here”. Most engineers put very little thought into who might be getting access to a control system. For example, implementing automatic log on to a workstation that does not require manually entering a username and password leaves open the possibility of an unauthorized user to gain physical access to a system.

The focus of most of the process engineering has been on safety and reliability. Security was not considered. In fairness to engineers, they originally designed these systems as stand-alone or isolated from the business side. In the case of the enterprise it appears that the some individual systems are being operated and maintained by the designated national operator (NO) “as it was given to us” and tends to remain that way as few or no patches are apparently applied. The equipment providers also may no longer support patches and updates on ageing equipment.

The “our patching policy is that we do not patch” argument is understandable as patching may introduce an “industrial risk”. However, industrial risks do exist in trying to defend against a cyber-attack or incident when conducting operations with unpatched Linux, Win XP, Win 7 and other operating system software and device firmware. There are attack tools on the Internet that can execute attacker actions that can be applied to most of the unpatched vulnerabilities. **In an unpatched system, an attacker who gains access will likely find that all these unpatched vulnerabilities are available for easy exploit**. To be safe the operator needs to also have a “cybersecurity microscope” to see what else may be “living” in the IACS network. Unfortunately, the capability to monitor and detect malicious cyber activity in the control networks is minimal at best (there is usually no “cyber microscope” on the IACS side where the physical process is going on). To recall the discussion of the cyber-attack on a petrochemical plant described

47 https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf

earlier, neither the operator's control system nor the manufacturer's testing equipment noted any indication of compromise on the safety system after the first attack in June 2017.

Many people who see glorious opportunities for data analysis and mining are now coming with proposals to management and the engineers[48]. These people tend to see nothing wrong with attaching the process networks to their office networks and then, by default, even to the Internet (cloud). Therefore, it is should not be a total surprise to see sensitive systems with network connections that lead to places that nobody in the field or plant floor ever considered or discussed. Those that do not adhere to a strict policy of segmenting office IT from IACS networks are significantly adding to the list of potential causes of failure.

The longtime industry standard practice of placing a firewall before the IACS network is no longer an adequate defense in the current cyber threat environment where attackers have acquired skills to bypass firewall protections and enter the so called "isolated" or air gapped IACS control zone or network. Firewalls can block out malicious traffic from the outside **but will do nothing to help with detecting or removing malware that has already found itself "inside" the protected network**. Note well that in several cases of major cyber intrusions at large operations, most followed standard security practices including firewalls. Target Corporations hackers for example were able to get around the standard cybersecurity barriers using the unprotected access provided by the headquarters building's Heating Ventilation and Air Conditioning systems (HVAC)[49]. Adversaries successfully found passageways to the control systems used by power utilities in Ukraine in 2015 and 2016. A ransomware or disruptionware[50] attack on the administrative or IT part of the US Colonial Pipeline in May 2020 was able to make the operator shutdown all the physical operations of a 8000 mile long pipeline despite the fact that the pipeline's IACS was not affected by the ransomware.

The current faith in the traditional IT cybersecurity emphasis (as advised by IT security trained consultants who may not have much understanding of IACS in their backgrounds) on "protecting the network" or perimeter with firewalls can lead to a false sense of security[51]. The case histories of past advanced cyber-attacks on industrial control systems presented earlier in this guide all feature the fact that firewalls did not keep the attacker from accessing the devices on the IACS side of the operation. For an advanced persistent threat (APT)[52] actor the defenses put up by the defender are technical problems that will eventually be solved. Security is a 24/7 job (operated, supported and reassessed by staff with the relevant skills and required resources) and there is no reason to say after the implementation of a security measure that "we are done and can go on with our usual business now". There is no reason to believe that the APT attacker will also act the same ("oh this last measure by the defender is too hard for us, we quit") when confronted with a new security measure. Again, it is just another problem to solve for the attacker to achieve his given objective. We should do all we can with the resources available and in collaboration with our colleagues in industry to increase the likelihood of early detection, limitation of damage and short recovery time back to full operations. There is an old sailors' saying about a ship at sea. "If there is a weakness in the ship, the sea will eventually find it".

[48] This is a major selling point behind the proponents of Industry 4.0 or Industrial Internet of Things (IIoT) movement.
[49] Krebs, B., Target Hackers Broke in Via HVAC Company, Krebs on Security, Feb 14. 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[50] Spaniel, D., Hunter, J., Weapons of Mass Disruption: An Assessment of the Threat Disruptionware Poses to Energy Sector Continuity, ICIT July 2020, https://icitech.org/weapons-of-mass-disruption-an-assessment-of-the-threat-disruptionware-poses-to-energy-sector-continuity/
[51] See "Lesson Learned Risks Posed by Firewall Firmware Vulnerabilities", NERC 2019-09-06 https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf
[52] https://csrc.nist.gov/glossary/term/advanced-persistent-threat

Despite the best efforts by the operator, pipelines do experience fuel leaks and employ special measures to detect and react to them. Similarly, in terms of cybersecurity the possibility of a breach of an industrial control network assumed to be isolated from the Internet is real. This inadvertent exposure to the Internet (or of a breach by an unauthorized attacker from inside) often catches people by surprise. Several years ago, Robert Radvanovsky and Jacob Brodsky conducted an experiment by looking for signatures from search engines for industrial control systems and SCADA[53]. They were gathering and counting search engine "hits" of discovered industrial control system assets. They were looking for a peak in the data acquisition rates, indicating a baseline. Then they were going to study those baselines to see whether they were going up or down. However, a peak was never observed. The numbers of indications of control systems kept increasing at a great pace. They finally stopped after collecting more than 1.5 million potential hits. The lesson from this project is that the rate of new supposedly isolated systems showing up on the internet was increasing dramatically.[54]

The engineers and managers of these systems, which are probably observable on the Internet, may not be aware of this visibility. It is a mistake to assume without regular checks that our systems are not visible from the outside. As systems become more digitalized and complex the challenge of keeping track of what you have and what it is connected to increases. It is easy to forget to close off remote access temporarily granted to a vendor after they finish their work. Sometimes we forget to disable unneeded factory default communications settings (for example Bluetooth or Wi-Fi) which may be noticed by an intruder at the first scan.

Documentation is most important. Even though there was a high price tag paid by NorskHydro in its refusal to pay ransomware after its systems were compromised in 2019, the company was able to reconfigure its equipment and restore operations largely because it kept very good and updated documentation[55].

Having policies and protocols in place and tested before actually having to apply them during an incident is also important. However if applied separately without an enterprise cybersecurity program they will just be tools in a toolbox that will still require someone who knows when and how to use them. There needs to be a framework program or foundation for addressing threats emanating from cyberspace today.

III. How we can protect identified assets from identified threats

Corporate Cybersecurity Program

The policies we develop and employ to protect the technologies used in the Office IT and Process Control/IACS environments can be accomplished inside a cohesive framework called a **Corporate Cybersecurity Program (CCP)**.[56]

---

[53] Byres, E., Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting, Tofino Security, 2013-09-19 https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting accessed November 6, 2018

[54]https://scadahacker.com/library/Documents/ICS_Vulnerabilities/Infracritical%20-%20Project%20SHINE%20Findings%20Report%20-%20Oct%202014.pdf

[55] Norsk Hydro: The ultimate example in handling a data breach, ITCS, accessed 2021-07-14 https://www.itcs.co.uk/norsk-hydro-cyber-attack-example-for-us-all-in-business/

[56] The Cybersecurity Program discussed here while intended as a enterprise-wide policy it can also be applied at a smaller individual operator level.

The CCP is intended to address the fact that information, communications and control system technologies applied in these environments have similar but not identical security priorities.

Protecting data or information is a prime concern for Office IT systems. These systems typically are used to process business data and interact with the "outside world" and use various applications (email, web browsing, Cloud services, and IoT in non-industrial settings) that support the internal administrative functions such as dispatch, billing, accounting and interaction with enterprise personnel.

In the other environment of Process Control/IACS, the main concern is protecting the ability to monitor and control a physical process. For this purpose, IACS or Industrial Control Systems (ICS)[57] are used, in concert with associated Intelligent Electronic Devices (IED) and applications such as Supervisory Control and Data Acquisition (SCADA)[58] systems, Distributed Control Systems (DCS)[59], Programmable Logic Controllers (PLC) and Industrial Internet of Things (IIoT)[60] devices.

The CCP is developed in reference to cybersecurity standards that provide a context for reducing the likelihood of a successful cyberattack, the use of a common set of requirements among stakeholders, security throughout the lifecycle, and a reduction in overall lifecycle cost.

The CCP is the framework where both the IT requirements as represented by ISO 27000, and IACS requirements as represented by ISA/IEC 62443 are considered; where risks are evaluated and measures based upon consistent requirements, and deliverables are implemented to assure the safety, reliability and performance of both the business and operational functions. Inside this framework are measures to protect the IT business-related functions and those specific to protecting the IACS or physical functions of the pipeline.

The advantage of the CCP is that **it takes the cybersecurity environments of the entire enterprise into consideration and treats the Office IT and IACS environments not as separate entities but as contained in a comprehensive cybersecurity framework**. Funding for cybersecurity will not just focus on the needs of the IT department first but will also include operations as an equal. Two cybersecurity standards can be applied in developing an CCP. ISO 27000 addresses cybersecurity of IT information, while ISA/IEC 62443 addresses cybersecurity of IACS.

[57] Industrial control systems: Mostly computer based, used by infrastructures and industries to monitor and control sensitive processes and physical functions; Collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment; These include the hardware and software closest to the actual physical process such as RTU's, PLC's, actuators, sensors, and other field devices

[58] Supervisory Control and Data Acquisition (SCADA) used in larger scale environments, geographically dispersed in an enterprise-wide distribution operation. Slower, less reliable communications, RTU's available for local control. Source: Radvanovsky, R. (Editor), Brodsky, J/ (Editor) , Handbook of SCADA/Control Systems Security, Second Edition 2nd Edition, CRC Press, 2016. https://www.amazon.com/Handbook-Control-Systems-Security-Second/dp/1498717071/ref=mt_hardcover?_encoding=UTF8&me= page. 4.

[59] Distributed Control Systems (DCS) used within a single process or generating plant, or used over a smaller geographic area or at a single site, Highly reliable communications, higher bandwidth available, Ibid.,

[60] IIoT: Internet protocol devices and networks in industrial environments.

ISA/IEC-62443 addresses parts of the enterprise where ISO 27000 cannot generally be applied, including production areas with interlocks and regulatory control, industrial equipment monitoring, safety systems in hazardous areas, sophisticated analyzers, and special-purpose industrial networks.

The CCP cybersecurity program should include both ISA/IEC 62443 and ISO 27000 standards as shown in the diagram above. ISA-62443 addresses projects and operating facilities, while ISO 27000 is focused on the enterprise's administrative facilities. Note that typically, project cybersecurity standards are implemented by other Principal Roles, such as Integrators/EPCs[61], Vendors, etc.

IACS project design standards and deliverables, however, are a key part of the project Requirements that the enterprise owner provides to other Principal Roles.

Other International Society of Automation standards may also influence the enterprise IACS cybersecurity program such as:

ISA 84 – Safety instrumented systems to reduce risks such as fire and explosions;[62]

ISA108 – Intelligent device management for plant equipment such as software configured instrumentation;[63]

ISA 95 – Enterprise Integration including transfer of information between plant instrumentation and corporate information systems;[64]

ISA 100 – Industrial local area network design, configuration and operation.[65]

These standards are coordinated within ISA to improve the cybersecurity of these devices and systems.

Although ISA/IEC 62443 and ISO 27000 are the most important, additional standards may influence the IACS cybersecurity program, such as NIST[66], NAMUR[67] and other ISO[68] and IEC[69] standards.

The process of developing a CCP is briefly outlined below:

Typically, this program is initiated by an executive sponsor, such as the chief technical officer (CTO) as designated by enterprise or the operator.

The first step is an audit of "As-Is" IACS facilities, including an update of equipment and software inventory, and industrial network diagrams. A list of cybersecurity threats experienced is also recommended.

Second, an assessment of the probability of threats and consequences is made using the owner/operators' risk management procedures and criteria.

---

[61] Engineering, procurement, construction
[62] https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa84
[63] https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa108
[64] https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95
[65] https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa100
[66] https://www.nist.gov/industry-impacts/industrial-control-systems-cybersecurity
[67] https://www.namur.net/en/index.html
[68]https://www.iso.org/standard/43759.html#:~:text=The%20scope%20of%20ISO%2FIEC,the%20control%20of%20supporting%20processes.
[69] https://webstore.iec.ch/publication/33615

Third, once the costs and benefits of mitigating measures are estimated, a risk/benefit analysis is done, and the chosen mitigation measures are included in the IACS cybersecurity program.

Fourth, the IACS Cybersecurity Program is reviewed and accepted by stakeholders, the IACS Program is published including provisions for financing and training.

Fifth, a set of projects is established to manage implementation of risk reduction, training, and other objectives. These projects should be individually budgeted and assessed.

Finally, key performance indicators (KPIs) and/or other standard enterprise metrics, are used for ongoing assessment of these cybersecurity projects. A separate periodic audit of the overall program is also required.

Similar programs are needed for Vendors of IACS equipment and software, Integrators, and other Principal Roles discussed in ISA/IEC 62443.

A more comprehensive presentation of the cybersecurity program briefly described above is found in Appendix 4 : "Implementing an Industrial Cybersecurity Program for Your Enterprise"

IV. Tools in the enterprise Cybersecurity Program toolbox

This Guide will now cover the "tools" that can be employed after an CCP has been drafted and approved. However, if there is no common approved CCP the individual operator can still benefit from the following list of tools. However, these will still likely require an additional investment in staff, staff training and other resources.

- **Asset management system (AMS)**

The most important of the 3 security policy development questions asked in the introduction to this guide is "What to protect?" That question focuses on identifying those assets that are the most critical to the safety, availability and resilience of the enterprise. An AMS goes into further detail to determine what hardware and software is actually present and authorized to be working on-site. An AMS gathers asset information and other data for every device on your IACS, including software configuration, serial numbers, network connectivity, and, of course, patches and common vulnerabilities and exposure lists (CVE).[70] The AMS is the tool an asset owner uses to manage, keep track of and maintain IACS assets. There are several ASM tools available for use[71]; each portion of the enterprise needs to evaluate and select one for use.

- **Standards**

In addition to the (IACS) standard ISA\IEC 62443 which consists of a set of documents that describe a methodical engineered approach to addressing the cybersecurity of IACS throughout the system lifecycle,[72] the American Petroleum Institute (API) has relevant standards that apply to pipeline

[70] https://cve.mitre.org/
[71] One example: https://www.langner.com/ot-base/
[72] A Quick Start Guide and overview of the ISA/IEC 62443 standard is available from ISA. https://cdn2.hubspot.net/hubfs/5382318/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

operations. They are API 1164 SCADA Security[73] and API 1168 Recommended Practice, Pipeline Control Room Mgt.[74]

- **Documentation**

Documentation (Emergency Plan, Operator Handbook, Process Handbook, Functional Description and Technical Description) must be available on the site (Control room, Dispatch, Pumping Station) and readily accessible, for operator reference.

Two examples of documents that would be welcome are the **Process Description** and **Control System Narrative**. The Process Description document is an **overview of how the process is supposed to work** when things are working normally. The Control System Narrative is a detailed description of exactly **what the controllers and process do under all conditions – normal and adverse**. It describes in detail, for example, the failure of a valve closing in a timely fashion. If they are not available, an effort should be made to develop these two documents. The Process Description is most useful to provide to first responders in case of a major accident. Along with the normal modes of operations, the Control System Narrative describes failure modes and contingencies in case of failure due to accident or malicious actions.

- Operator awareness is important. If the operators do not know what to expect from the equipment's normal operation, then the attack will have more time and opportunity to damage equipment and hurt people.
- Good documentation is essential. This is very important because one of the side effects of automation is that people forget how things work. Using the airline analogy, if the autopilot is in use for 98 percent of the flight, will the pilots be able to handle an emergency when the autopilot disengages?

Related to documentation is the issue of training and development of operational staff. It is not clear what the average age of the enterprise staff is, but it may be a significant issue if several key people with decades of operational experience were to approach retirement age at close to the same time. This makes investment in staff training, continuity preservation and keeping a good record (documentation) key to orienting individuals to the importance of operational safety and availability. In a way, the future safety and availability of enterprise operations and products could be at risk from these personnel issues.

- **Evaluating and improving the level of maturity in industrial cybersecurity**

- Testing

Increase the frequency of testing the system and its components in order to move from a reactive to pro-active posture regarding incident handling. If something is not working correctly, a test can point out the fault before something unpleasant happens. Measures are required to insure that a resort to manual control exists and tested regularly[75]. It must be remembered, especially for those operations that have a high level of digitalization, that **going to manual control will likely require additional trained staff** that may not be initially available.

- Exercises

Conducting exercises on a regular basis and under realistic operating conditions can be most valuable for evaluating effectiveness of security measures, safety systems, system resilience, testing operating assumptions, identifying weaknesses and developing rationally based corrective actions before something

[73] https://global.ihs.com/doc_detail.cfm?document_name=API%20STD%201164&item_s_key=00451686
[74] https://www.api.org/~/media/files/publications/whats%20new/1168_e2%20pa.pdf
[75] Some made by SHAPE. See: SH/CyOC/PLANS OPL/64/21-009304,21 September 2021 NR

bad happens. The NATO Energy Security Center of Excellence in Vilnius holds regular Tabletop Exercises (TTX), which focus on specific aspects of energy operations. The TTX can in a non-stressful roundtable format, bring the main players (administration, management and plant engineers) involved in pipeline operations together to go over pre-agreed upon scenarios that maximize the generation of useful lessons learned for the participants.

- **Secure Coding Practices for the Programmable Logic Controller (PLC)**

PLC stands for Programmable Logic Controller. They belong to the family of Industrial Automation and Control System (IACS) devices used to monitor and control the physical processes found in critical infrastructure. Since the 1970's PLC's have played a major role in controlling physical operations of pumping and compressor stations found on liquid fuel and natural gas pipelines, as well as water supply systems, power generating stations and most industrial and manufacturing operations.

Unfortunately PLC's are now subject to cyber-attacks that can cause physical damage. The classic example is STUXNET from 2010 where the code of PLC's manufactured by SIEMENS was manipulated to cause damage to centrifuges at a nuclear enrichment facility. Controllers used in safety systems at a petrochemical plant in Saudi Arabia were also manipulated in 2017 which resulted in 2 emergency plant shutdowns (may not have been the intruders' objective). The Colonial pipeline incident is getting a lot of attention and perhaps for the wrong reasons. Many seem to overlook that the engineers with the aid of healthy PLC's were able to perform a successful controlled shutdown of a 8000 km long pipeline. Much worse would have happened if they could not shut down the physical process when they wanted to. An example is the failure of steel mill operators to shut down a smelter in Germany in 2014, which did result in physical damage[76].

It is strange to consider that the programming of these PLC's and other intelligent electronic devices are usually done by plant engineers (or done for them by vendors) with very little training in computer programming and secure coding practices used for years by software developers in the IT world. In June 2021, version 1.0 of the "Top 20 Secure PLC Coding Practices was published[77]". These coding practices are a valuable addition to our corporate industrial cybersecurity program toolbox. (see Appendix 2 for a list of the Top 20)

- Patching and updating software and firmware

Patching is an effective way to address a significant risk to the Safety, Integrity, and Availability of the enterprise. Among the risks are:

- The capability and desire to use cyber means in defeating robust security measures designed to block unauthorized access to critical control systems (IACS/ICS network segmentation/air gaps) and cause a cyber-physical effect has been publicly demonstrated
- A policy of not patching without adequate and regular review of advisories and security compensatory measures leaves a significant risk that remains exploitable. If an intruder breaches the defenses of the IACS network, the unpatched IED's and connected control systems are easy "low hanging fruit" for the attacker using a publicly available penetration testing cyber-attack tool (platform) such as Metasploit[78] which can execute code specifically designed to exploit an

[76] The State of IT Security in Germany 2014, BSI, page 31.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3
[77] https://www.plc-security.com/index.html
[78] Metasploit tool is available for download from the Internet: https://www.metasploit.com/

unpatched vulnerability. (for example, the Siemens SIMATIC WinCC OA has known vulnerabilities and countermeasures have been published.[79]

It is important to note that Windows and Linux OS both have exploitable vulnerabilities.[80] It would also be a mistake to think that the use of Linux automatically provides some extra security protection. Like any OS, it needs care and attention. For this reason, patching and update policies should also include reviews of Linux vulnerability bulletins and mitigations.

Procedures are necessary to insure that published advisories about control system equipment and software from the manufacturer are monitored, reviewed, and where it is judged appropriate, implemented. A 3-tier classification can be used:

- Patches that are not needed at all
- Patches that should be implemented at a scheduled time (during planned maintenance and shutdowns);
- Patches needed as soon as possible.

One important caveat: Any decision about a patch on an IACS system must include the "ok" from the senior plant engineer. This would be a better solution in terms of distributing the workload (the Senior plant engineer cannot be expected to "drop what he or she is doing" and make a snap decision about a patch) to have an Industrial Cybersecurity Operations Center (ICOC) supporting the senior plant engineer (See Appendix 3 for a description of an ICOC).

Lastly, this "no patching" risk is balanced against two possible evils: (1) an unwarranted (not needed) patch or upgrade performed on IACS equipment that results in an operational outage and (2) an operational outage that occurs because of a missing patch or upgrade.

If the "status quo" of a "no patching and updates" policy is in place, then some alternative or compensating controls must be implemented to mitigate the risk. In addition to a strict network segmentation policy, such a mitigation strategy needs to include a variety of both physical and operational controls implemented to prevent a would-be adversary from compromising a critical operation. The establishment of an ICOC may serve as this compensating mechanism.

Consideration should be given to developing and executing a regular technical 'refresh' plan to keep critical infrastructure and software current while having fault tolerant, alternative means to control and execute critical operational procedures where regular updates are not possible.

- **Network security**

Often when an operator of an industrial or IACS operation is asked about patching and updates, they express confidence in the secure arrangements of firewalls to protect IACS networks. It appears that in most cases the operator understands the importance of implementing robust network segmentation between IT and IACS networks. However, segmentation (or "air gap") does not guarantee protection from malicious activities already present inside the IACS network segment. For example, it is wrong to think that a firewall alone will provide enough protection to justify a "we do not patch" policy (see discussion of patching above):

"We do not patch. It is not considered necessary as the firewalls are on the restricted network".

[79] https://ics-cert.us-cert.gov/advisories/ICSA-18-109-01
[80] Cluley, G., "HiddenWasp malware seizes control of Linux systems"
https://www.tripwire.com/state-of-security/security-data-protection/hiddenwasp-malware-seizes-control-of-linux-systems/May 30, 2019

While it would be very difficult for the average to medium skilled attacker to breach this defense, this condition may not apply in the case of a targeted APT[81] attack against an enterprise. A common feature of publicly known APT attacks is the surprise on the part of the operator and manufacturer that a security breach has occurred. Most surprising is that later investigation determined that the initial breach occurred months or even years before discovery. The Trisis/Triton/Hatman incident is a good recent case to look at.[82] This risk is evaluated with a penetration test and some scanning (fully coordinated with the senior plant engineer). This of course requires resources in staff and time to perform.

As mentioned earlier, some operators also permit remote access to IACS:

"Yes, it is used remote access from outside to internal networks".

The practice of using "jump boxes" or other means to provide remote access to IACS is not uncommon. There are good operational reasons to justify it: operator wishing to monitor something over the weekend from home, allow a vendor who is unable to promptly appear on-site to remotely diagnose and correct a problem and so forth. Unfortunately, the commonly used communication protocols have well-known security vulnerabilities[83] and it is important that remote communications channels be periodically penetration tested by authorized personnel. Again, it should be noted that in the case of becoming a target the confidence in security through keeping operations inside an isolated (air-gapped) network can prove false. This should be a serious concern for the operations center, control room and/or or local pumping/compressor/substation location where there are fewer security measures (for example lack of patching, encryption) in place.

In the case where there is a continuous need for obtaining data from the IACS part (high side) by the administrative/office (low side) part of the enterprise, and vice versa, cybersecurity can be maintained by employing a hardware data diode[84] or a hardware and software based unidirectional gateway[85] that can be configured, according to the particular needs of the enterprise, to transmit or receive data in one direction only. The implementation of this one way data transfer solution has to be weighed against the advantages and disadvantages[86]. Among the advantages are:

- Substitution for an air-gap when data from the IACS is required is needed for business reasons
- Sending IACS historian data to business operations
- Safe monitoring of obsolete/legacy equipment and insecure operating systems;[87]

There are some disadvantages or caveats that should also be considered such as:

- Some Data Diode products on the market today have not been validated and approved for use by SCADA and DCS vendors that limit their application in the process control domain;

---

[81] APT advanced, persistant threat. Usually associated with sophisticated state recourced attacks where financial gain is not the motivating factor.

[82] Higgins, K.J, Triton/Trisis Attack Was More Widespread Than Publicly Known, https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661 1/16/2019.

[83] https://www.hackingarticles.in/vnc-penetration-testing/

[84] https://csrc.nist.gov/glossary/term/data_diode

[85] https://csrc.nist.gov/glossary/term/unidirectional_gateway

[86] Scott, A., Tactical Data Diodes in Industrial Automation and Control Systems, SANS GIAC Directory, May 18, 2015 https://www.giac.org/paper/gicsp/242/tactical-data-diodes-industrial-automation-control-systems/142041

[87] Ibid.

- Some communication protocols cannot pass through the data diode. The so-called "three-way" handshake built into TCP/IP will prevent any TCP/IP-based protocol from passing through a Data Diode. UDP based protocols lack a built in connection check, but even so, most UDP protocols need two-way communication. Unidirectional Gateways, however can overcome these limitations[88];
- Error control is a challenge. It is hard to know if a packet made it to its intended destination and, therefore, there is no way of resending the data if required.[89]

A network management system, Intrusion Detection, or Security Information and Event Management (SIEM[90]) system with a capability to monitor and react to cyber incidents or intrusions in the IACS side of operations can improve the cybersecurity posture significantly. It is recommended to establish a capability to conduct continuous monitoring on process networks for unusual behavior (See detailed description of the work of an ICOC in Annex 5).

- **Project management with integration firm**

It is important to seek a functional, close working relationship between enterprise operators and their supporting security and equipment vendors.

There is strong evidence that the cybersecurity environment has changed since 2010. For a security policy to remain relevant and effective it must undergo regular review and be modified as necessary when the security environment changes. If not already an established practice, enterprise operators should initiate a conversation about security with their vendors and cybersecurity support community. For example, if the manufacturer has placed a "backdoor" in their products, the operators should be informed and given the option to disable it. Another example is to discuss the patching process (evaluation, testing and selecting priority patches and those that can be safely ignored). In fairness to enterprise supporting vendors and manufacturers, if cybersecurity was not in the services procurement contract, they are not obligated to provide the service to the operator. If this is the case measures should be taken to make appropriate changes to the contract.

- **Backups**

a. One important tool for insuring system resilience and recovery from loss of data and operational information from ransomware or wiper malware attacks is to have an established back up policy. Testing the backup by restoring the IACS on a regular basis would improve confidence that the backup, if needed someday, will restore a lost system or component. A good backup policy is key for recovery from attacks. Having some level of hardware infrastructure backup is also a good "insurance policy". Backups are to be implemented, regularly tested and isolated from public internet connections.

[88] Ginter, A., Secure Operations Technology, Waterfall 2018 ISBN 978-0-9952984-2-2 https://waterfall-security.com/secure-operations-technology-the-missing-link-to-a-secure-industrial-site/

[89] Scott, A., Tactical Data Diodes in Industrial Automation and Control Systems, SANS GIAC Directory, May 18, 2015 https://www.giac.org/paper/gicsp/242/tactical-data-diodes-industrial-automation-control-systems/142041

[90] How to manage SIEM, Infosecurity magazine Q2, 2019 / Volume 18 / Issue1# pages 50-51 https://view.pagetiger.com/inmagq2/1#

- **Source code control system**

A source code control system (SCCS) provides a capability to detect unauthorized or even malicious code changes by employees or contractors.

Periodically, there should be a comparison between the SCCS software and the software in the backups to confirm that there are no undocumented changes. If there are discrepancies, they should be investigated immediately.

One other advantage of an SCCS: if an enterprise employee or supporting vendor representative with access to the control system programming tools were to depart under less than ideal circumstances, the SCCS could show what they had done (for example ,the SCCS could detect for potential "software time-bombs" that were left behind; in that case, without an SCCS, a complete and costly code review would be needed). While enterprise management may consider this to be an acceptable risk the consequences of mismanaged code changes, such as those Volkswagen experienced, can be significant.[91] All it takes is one such incident for the investment in SCCS technology to pay for itself. For more on the insider threat, see section "Threats to IACS" at the beginning of this Guide.

In the light of the incidents over the past 10 years we see that code manipulation for malicious purposes has been one of the goals of APT attackers. The operation of an SCCS can be one of the tasks assigned to an ICOC (see a complete list of ICOC tasks in the Appendix 3).

- **Self-integrity monitoring**

IACS need to manage their own integrity through monitoring activity on process networks for unusual behavior.

There are several ways that the monitoring can take place.

- Network Integrity monitoring
- Process Integrity Instrumentation
- Controller Integrity Monitoring
- OS Integrity Monitoring

Network integrity monitoring should include monitoring bandwidth and port states. If something goes off-line, knowing where and what ports are not alive is critical for fast response.[92] It is usually what everyone does first. However, this method has significant gaps.

The first is that intrusion detection systems usually cannot distinguish between a hostile industrial process activity and a routine one. Often the protocols themselves are not well monitored. For example, it is unusual to find a firewall that has deep packet inspection features for the IEC 60870-5-104 protocol.

---

[91] Petersen, A., Fung, B., The tech behind how Volkswagen tricked emissions tests https://www.washingtonpost.com/news/the-switch/wp/2015/09/22/the-tech-behind-how-volkswagen-tricked-emissions-tests/?noredirect=on&utm_term=.989e0fa5cc69 September 22, 2015

[92] Brodsky, J., "Communications and Engineering Systems, Radvanovsky, R., Brodsky, J., Editors, Handbook of SCADA/Control Systems Security, 2nd Ed., CRC Press 2016 p.241

Monitoring and investigating suspected intrusions might be difficult since available operational staff time may be fully devoted to operations. Some respondents said that "no specific application to discern if anomaly is due to machine failure, incident or cyber incident" and if it was determined that a case merited investigation the enterprise operator would contact a "military intelligence service" or some other department in the chain of command. This ad hoc and perhaps time intensive approach to investigation of an incident is not likely to catch a cyber-intruder in time. Nor is it likely that the above listed responders will have the necessary forensic skills to investigate an industrial cyber incident.

The second point, of **Process Integrity Instrumentation (Monitoring),** is quite simple: Disparate Systems with a common process function should be self-consistent.

For example, a tank of fuel should fill at a rate commensurate with the number and size of pumps running, as well as a rate that matches the integration of the flow readings. If it does not, it is time to start looking for problems. This is integrity monitoring. It is the consistency check of a process across multiple instruments that work in different ways.[93]

The third point to monitor, **Controller Integrity**, is very important. One should make a very careful evaluation of the controller logic cycle time. If the cycle time reads either too low or too high, then it indicates that some of the program is not being executed, or (more likely) additional code is being executed that is not supposed to be there.

Another part of controller integrity monitoring is to check that the code checksums (or preferably hashes) have not changed from what was supposed to be there. Operators should be aware of new code changes so that they know to look for any possible problems at their site.

The fourth way to monitor is to look at **Operating System Integrity**. All modern operating systems generate logs (or can be configured to generate logs). These logs should be reviewed by enterprise staff regularly - or better yet, fed to a Security Information and Event Management (SIEM)[94] system. They can also be configured to generate exception reports, or traps in the Simple Network Management Protocol (SNMP). A trap receiver added to the alarm subsystem can be used to alert operators right away to network connectivity problems, disk storage space problems, high CPU alarms, and to alert to new access from other accounts.

Self-Integrity Monitoring is much more than just network monitoring. This should be discussed with vendors and cybersecurity support community personnel to profile the tools, techniques and responses to various sorts of integrity problems. This will also help to discover security problems much sooner, and to make it harder for an attacker to conceal their efforts.

It is recommended that enterprise as part of implementing a enterprise Cybersecurity Program (further described in Section III) conduct a cybersecurity architecture design review enlightened by tools, techniques and responses to identify integrity problems discussed by industrial automation and control systems (IACS) vendors and cybersecurity support community members.

---

[93] I saw something like this recorded on paper during one of my industrial site visits. There was a clipboard where the IACS staff entered the volume of fuel before entering part of the pipe and the reading at the other end. There were discrepancies but I understand the differences were within norms. The question is what the procedure will be when the readings start to look unusual or not normal. There should be a procedure in place to address this event before it happens.

[94] https://www.gartner.com/it-glossary/security-information-and-event-management-siem

- **User and role access ID**

Good security practice dictates that there should be better granularity for defining User, and Role access to the SCADA and PLC network activities. There are significant questions that need to be answered before designing such a system. There should be traceability so that enterprise operators and consultants can determine when accounts get compromised and allow for recovery of control by using alternate accounts while shutting down access to compromised accounts.

It is not unusual to see at some industrial sites the use of the manufacturer's default password or a password pasted onto the viewing screen, which perhaps is shared by other operators using the same workstation. While this policy offers operational advantages (quick access to the workstation) it makes investigation of a cyber-incident difficult as it may not be clear who was in fact accessing the workstation and when.

It is worth noting that many companies leave "back-door" access IDs in their products. It would be appropriate to ask the vendor(s) if such back-door accounts or keys exist for their products. While there are valid reasons for having a "back-door" password, it would be a good idea to have the ability to disable this back door. Depending on the service level agreement and when it makes good operational sense, an alternate option is to leave the "backdoor" access, disable it and activate it only when needed. There should be a discussion with the vendor on what the consequences of disabling such access might be. Closing this gap may be useful in reducing the potential attack surface of these devices.

Furthermore, if this "back-door" access password is ever publicly revealed (for example in manufacturer's documentation or posted by a hacker on the Internet) the IACS could be attacked using this vector. The same steps taken to secure passwords (defaults have to be changed and passwords changed on a regular basis) should be applied in this case.

- **Cybersecurity Contingency and Recovery Plan**

Pipeline operations heavily depend on IACS, which are supported by information, communications and process control technologies that function in a cyberspace environment. It is recommended that the enterprises repair and restoration capability policy be reviewed to check for and if necessary include the requirement for operators to prepare, have in place and regularly test a Cybersecurity Contingency and Recovery Plan. This should include consideration for possible personnel and other resource limitations that can affect enterprise ability to "switch to manual control" in the case of lost or degraded IT and communications supporting infrastructure.

- **Industrial Cybersecurity/Security Operations Center (ICOC)**

It is crucial to the safety, reliability, performance and resilience of enterprise operations that some capability exists for monitoring and checking on anomalous process flows,[95] equipment performance, and data flows with a goal of detecting a cybersecurity breach within 24 hours.[96] If an intrusion is not detected by then, the intruder will likely have enough time to cover tracks and make detection far more difficult. The enterprise ICOC would help meet that requirement as well as being responsible for working with the

[95] For more about anomaly detection and its benefits look at NIST's draft document NISTIR 8219 "Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection" https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf

[96] After 24 hours the chances of discovering an intruder who is actively seeking to establish a stealth presence and cover tracks will drop considerably.

tools in the enterprise Cybersecurity Program toolbox as described in this section. (For a complete list and description of ICOC activities refer to Appendix 3).

V. Thoughts for the future

The new information and communications technologies (ICT) applied to the industrial sector provide exciting new functionalities and opportunities to streamline operations and save costs in terms of personnel and operations. However, they have also introduced increased automation and complexity. The automation has reduced the dependency on the human operator as machines manage other machines. The complexity has introduced new challenges for maintaining safety, reliability, performance and resilience of increasingly interdependent systems.

One of the new challenges comes from the Industry 4.0 or Industrial Internet of Things (IIoT) which has been otherwise called the "Fourth Industrial Revolution" (the first represented by James Watt's steam engine, the second by Henry Ford's assembly line for mass manufacture of automobiles, the third by Richard Morley's invention of the Programmable Logic Controller in 1968[97]).

Industry 4.0, to describe it briefly is the integration of manufacturing with business functions. Many sensors are added to collect data on all the machine-to-machine activity for data analysis. It is argued that the results of this analyzed data can be applied to improve efficiency, save on costs and to remain competitive. This is thought to be achieved through a focus on detecting serviced faults before they can negatively impact customers, provide critical data to support management's decision making and drive predictive analysis and machine learning capability approaching artificial intelligence to support operations. To connect all this activity together will be a network that will even include wireless communications[98].

Some have questioned the claims behind all the benefits proposed by supporters of Industry 4.0. For example, it is difficult to understand how much the implementation of Industry 4.0 technologies in an industrial enterprise will cost. It is not clear in the brochures and vendor selling pitches just how security issues dealing with the new device and attack surface that come with the technology will be managed.[99] How will the issues of trust in sensors be handled? Industry 4.0 depends on many sensors being introduced. What happens when the sensor sends incorrect data to the IACS? How will the machine action be checked to insure it makes good engineering sense and is overruled if necessary? An example of this issue comes from the two Boeing 737 Max plane crashes that killed all passengers and crew when

[97] Bacidore, M., The father of the PLC explains its birth, Control Design, May 18, 2015https://www.controldesign.com/articles/2015/the-father-of-the-plc-explains-its-birth/

[98] Crozier, R., Sydney Water to deploy Thousands more IoT sensors, itnews, June 1, 2020, https://www.itnews.com.au/news/sydney-water-to-deploy-thousands-more-iot-sensors-548806?eid=3&edate=20200601&utm_source=20200601_PM&utm_medium=newsletter&utm_campaign=daily_newsletter

[99] Langner, L., Brave New Industrie 4.0, S4 Conference presentation. Accessed July 16, 2021. https://www.youtube.com/watch?v=ZrZKiy2KPCM

a bad sensor, sent bad data to a flight control system which overruled the actions of the pilots who were trying to save the plane from crashing. [100]

Another important factor that will influence the success of those working to enhance energy security and resilience of critical energy and other sectors of infrastructure is climate change. Risks to national security interests may escalate as the physical impacts increase and geopolitical tensions rise on how to respond to the problem[101]. New research on the cost effectiveness of proposals to address climate change goals is required in order to develop effective plans and successful implementations of solutions. Solutions, which are likely to be heavily reliant on new and advanced technologies applied to increasingly complex and dynamic systems, which, together with powerful added functionality, will come with exploitable vulnerabilities.

Conclusion

It is still possible to hear threat summary reports from military institutions that focus only on threats emanating from the military domains of air, sea and land. It is sometimes forgotten by threat analysts that in 2016 NATO officially recognized cyberspace (as well as outer space[102]) as a new domain for military operations[103]. The adversaries, unfortunately, have noted this many years earlier and have adjusted their actions accordingly. Threats need to be evaluated comprehensively, informed by knowledge of the technologies used (it cannot be considered as "too technical" for applying to a program) and with reference to what is happening in the security threat environment. Evaluations of damage from kinetic operations and cyber-physical operations should not be seen as separate threats but as threats that are likely to appear in combination. The aggressive actions in the Russo-Georgian War of 2008 and the Annexation of Ukraine's Crimea province in 2014 and subsequent actions in that continuing war are examples of conflicts that employ, nearly simultaneously, both kinetic and cyber operations to degrade and destroy critical infrastructure. We need to employ comprehensive cybersecurity measures to protect our IACS in the hope that as asset owners we do not wake up one day with news that our critical systems and operations are compromised and cannot be trusted. Those were the circumstances faced by operators of that Saudi petrochemical plant after it realized that the two emergency plant shutdowns were not accidental. It is the hope of the author, that this Guide will help the enterprise operator to avoid that kind of situation.

[100] FINAL COMMITTEE REPORT THE DESIGN, DEVELOPMENT & CERTIFICATION OF THE BOEING 737 MAX, U.S. House Committee on Transportation and Infrastructure, September 20 https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf

[101] Office of the Director of National Intelligence NIC, National Intelligence Estimate, Climate change and international responses increasing challenges to US National Security through 2040, NIC-NIE-2021-10030-A, 2021. https://www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf

[102] NATO's approach to space, 17 June 2021, https://www.nato.int/cps/en/natohq/topics_175419.htm

[103] Brent, L., NATO's role in cyberspace, NATO Review, 12 February 2019 https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

VI. Acknowledgments

The preparation of such an ambitious work and for the first time could not be done without the help and professional advice of experienced industry professionals. I wish to thank Philippe Van Exem for his support in promoting the idea of an enterprise Cybersecurity Guide. Thanks for comments and suggestions made to the early drafts by Treavor Johnson, John Cummings, Jamila Boutemeur, Brandon Maroon and all the other enterprise operators who responded to questions and/or allowed a site visit for a brief glance into their operations. In particular, I would like to recognize the following industry opinion leaders for sharing their deep knowledge and insights on industrial cybersecurity:

Gary Rathwell

Jacob Brodsky

Robert Radvanovsky

Joe Weiss

Ray Parks

Andrew Ginter

Sarah Fluchs

Vytautas Butrimas
NATO ENSEC COE
Vilnius, January 25, 2022

Appendix 1

Initial questions for operators of IACS

1. How well are pipeline system processes documented?[104]

a. Process Description

b. Control System Narrative

c. PLC configurations

d. Are the above documents maintained and kept on site?

2. How autonomous is the process if communication is lost?

a. If your operations are not as autonomous, how do you detect malfunctions?

b. How does the system notify if something goes wrong?

3. Can you monitor and detect malicious/anomalous activity in your control networks and IED's?

4. How are security breaches in the control network detected and managed?

5. What are the policies and protocols for a breach?

6. What capability exists to gather forensics and investigate a cyber incident?

7. What is the capability to restore operations after an incident?

8. Patching policies. Do you patch or not? If yes then:

a. Who is involved in patching policy?

b. How are decisions made regarding a patch (to patch or not to patch)?

c. Who follows industry news about patches?

d. Who implements the patch or update and how?

e. If you do not patch then what security policies are in place to compensate?

9. Do you exercise and test? If yes, do you collaborate with an outside institution? (for example Pen testing security company or government institution)?

10. Do you use Jump boxes for remote access from outside to internal industrial networks?

Thank you for your help and look forward to collaborating with you in preparing a useful document to help improve the safety, reliability, resilience and performance of your pipeline operations.

[104] For more information about documenting system processes See Brodsky, J. How a Process Works, Infracritical, July 27, 2017 http://scadamag.infracritical.com/index.php/2017/07/27/how-a-process-works

Appendix 2

Secure PLC Coding Practices: Top 20 List
Version 1.0 (15 June 2021)[105]

1. Modularize PLC Code

Split PLC code into modules, using different function blocks (sub-routines). Test modules independently.

2. Track operating modes

Keep the PLC in RUN mode. If PLCs are not in RUN mode, there should be an alarm to the operators.

3. Leave operational logic in the PLC wherever feasible

Leave as much operational logic e.g., totalizing or integrating, as possible directly in the PLC. The HMI does not get enough updates to do this well.

4. Use PLC flags as integrity checks

Put counters on PLC error flags to capture any math problems.

5. Use cryptographic and / or checksum integrity checks for PLC code

Use cryptographic hashes, or checksums if cryptographic hashes are unavailable, to check PLC code integrity and raise an alarm when they change.

6. Validate timers and counters

If timers and counters values are written to the PLC program, they should be validated by the PLC for reasonableness and verify backward counts below zero.

7. Validate and alert for paired inputs / outputs

If you have paired signals, ensure that both signals are not asserted together. Alarm the operator when input / output states occur that are physically not feasible. Consider making paired signals independent or adding delay timers when toggling outputs could be damaging to actuators.

8. Validate HMI input variables at the PLC level, not only at HMI

HMI access to PLC variables can (and should) be restricted to a valid operational value range at the HMI, but further cross-checks in the PLC should be added to prevent, or alert on, values outside of the acceptable ranges which are programmed into the HMI.

9. Validate indirections

Validate indirections by poisoning array ends to catch fence-post errors.

10. Assign designated register blocks by function (read/write/validate)

Assign designated register blocks for specific functions in order to validate data, avoid buffer overflows and block unauthorized external writes to protect controller data.

11. Instrument for plausibility checks

Instrument the process in a way that allows for plausibility checks by cross-checking different measurements.

[105] For a downloadable copy with full descriptions go to: https://www.plc-security.com/index.html#download

12. Validate inputs based on physical plausibility

Ensure operators can only input what's practical or physically feasible in the process. Set a timer for an operation to the duration it should physically take. Consider alerting when there are deviations. Also alert when there is unexpected inactivity. 30

13. Disable unneeded / unused communication ports and protocols

PLC controllers and network interface modules generally support multiple communication protocols that are enabled by default. Disable ports and protocols that are not required for the application.

14. Restrict third-party data interfaces

Restrict the type of connections and available data for 3rd party interfaces. The connections and/or data interfaces should be well defined and restricted to only allow read/write capabilities for the required data transfer.

15. Define a safe process state in case of a PLC restart

Define safe states for the process in case of PLC restarts (e.g., energize contacts, de-energize, keep previous state).

16. Summarize PLC cycle times and trend them on the HMI

Summarize PLC cycle time every 2-3 seconds and report to HMI for visualization on a graph.

17. Log PLC uptime and trend it on the HMI

Log PLC uptime to know when it's been restarted. Trend and log uptime on the HMI for diagnostics.

18. Log PLC hard stops and trend them on the HMI

Store PLC hard stop events from faults or shutdowns for retrieval by HMI alarm systems to consult before PLC restarts. Time sync for more accurate data.

19. Monitor PLC memory usage and trend it on the HMI

Measure and provide a baseline for memory usage for every controller deployed in the production environment and trend it on the HMI.

20. Trap false negatives and false positives for critical alerts

Identify critical alerts and program a trap for those alerts. Set the trap to monitor the trigger conditions and the alert state for any deviation

---

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the “Top 20 Secure PLC Coding Practices”.

THE “Top 20 Secure PLC Coding Practices” IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE “Top 20 Secure PLC Coding Practices” OR THE USE OR OTHER DEALINGS IN THE “Top 20 Secure PLC Coding Practices”. License https://www.plc-security.com/index.html

Appendix 3 Tasks of an Industrial Cybersecurity Operations Center (ICOC)

- Monitor and check on anomalous Process Flows, Equipment Performance, and Data Flows with a goal of detecting a cybersecurity breach within 24 hours[106].
- Identification and recording of all the component pieces and versions in a cool system.
- Review available patches and updates of IACS devices found closer to the industrial process.
- According to configuration, change management and safety procedures test and apply selected patches and updates.
- Responsibility for monitoring control and safety system cybersecurity vulnerabilities.
- Monitoring the current patch levels, malware notifications, and newly discovered vulnerabilities as announced by cybersecurity institutions and by vendors.
- Take part in regular training and education on IACS cybersecurity including attendance at organized IACS security conferences and trainings such as S4, DEFCON, and Black Hat.
- Participation in NATO, EU and other organizations exercises[107] where cyber-attacks on IACS are included in the scenarios.
- Implementing the recommendations in this Guide that are beyond the means of current staff capabilities and resources.
- Operation of network management system, Intrusion Detection, or Security Information and Event Management (SIEM) system.
- Use of internal operating system health tools that can be used in both an investigative and in a forensic capacity to identify source of a problem.
- Organize and control use of antivirus and other malware scanning based according to established policies and procedures.
- Conducts and/or organizes (in keeping with established industrial safety requirements) with help of vendors with Certified Ethical Hackers full offline black box and white box penetration testing against the switches, routers, firewalls, controllers and instruments used by enterprise operators.
- Use of available tools, such as Metasploit, where one can use benign attack scripts to prove the existence of a device vulnerability in an automated fashion. This way one can demonstrate a conceptual attack on a test bench without damaging anything.
- Operation of a security test lab. This should be used to validate patches before deployment, to test security exploits on existing equipment and firmware, and to find and diagnose other bugs and test code before downloading it to the field.
- Ensure that user log-ons to the system and IACS configuration changes are documented, updated and made available on-site for operations personnel.
- Management of the cybersecurity contingency and recover plan.

[106] After 24 hours the chances of discovering an intruder who is actively seeking to establish a stealth presence and cover tracks will drop considerably

[107] https://enseccoe.org/data/public/uploads/2019/11/jrc118083_core_19_ttx_final_report_online.pdf

Appendix 4

White Paper on
Cybersecurity Program for Industrial Automation and Control Systems

(November 4, 2021 version[108] of this paper used with permission of the author, Gary Rathwell and International Society of Automation)

ISA/IEC 62443 provides a powerful tool to reduce the risk of financial, reputational, human, and environmental impact from cyber-attacks on Industrial Automation and Control Systems (IACS). However, since it is a "horizontal standard", 62443 is meant to address a wide range of industries, and any specific company is likely to find that while most of the standard applies to their IACS, parts of it may not. For example, some "normative requirements" that are appropriate for an interstate pipeline, may not be relevant to a chemical plant or a discrete manufacturing facility. There are also obvious differences between a large-scale corporation with many sites and thousands of employees, and a small company with a few dozen staff.

It is therefore recommended that each company establishes their own Industrial Automation and Control Systems (IACS) Cybersecurity Program to manage these cybersecurity risks. ISA/IEC 62443 2-1 provides guidance on how to establish a Security Program for IACS asset owners. This process might look like the following.

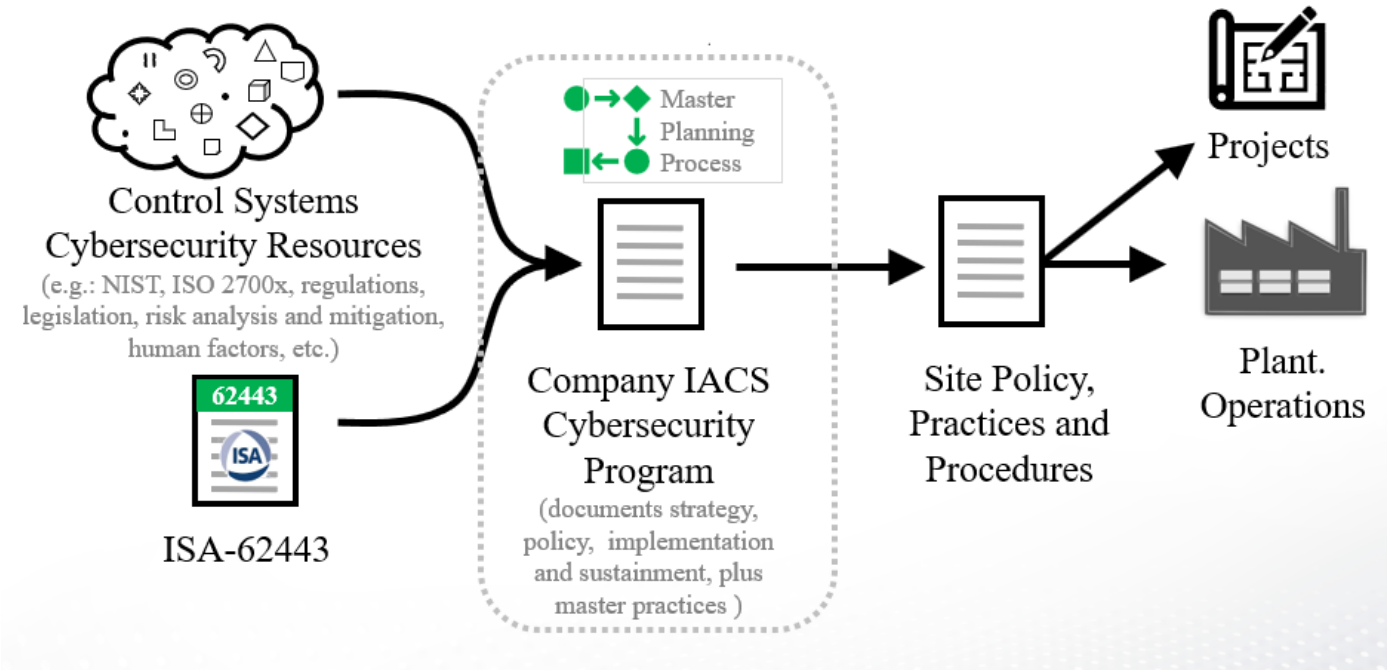


Figure 1 - IACS Cybersecurity Program Workflow

[108] This document has been updated and may be obtained here: https://www.isa.org/news-press-releases/2022/january/new-white-paper-implementing-an-industrial-cyberse

This white paper is intended to address the needs of Owner/Operators of industrial facilities. It will discuss the following:

1) What is an IACS Cybersecurity Program?
2) Preparing an IACS Cybersecurity Program
3) How does an IACS Cybersecurity program relate to IT Cybersecurity?
4) Costs and Benefits of an IACS Cybersecurity Program
5) What to do next

In the coming months, ISA Marketing plan to publish additional white papers intended for IACS vendors, suppliers of IACS products and services, Integration/engineering services, and possibly other major stakeholders such as insurers and regulators.

What is an IACS Cybersecurity Program?

An IACS Cybersecurity Program (yellow) defines the company's IACS security policies, practices, and procedures associated with the operation and design of the company's industrial facilities.

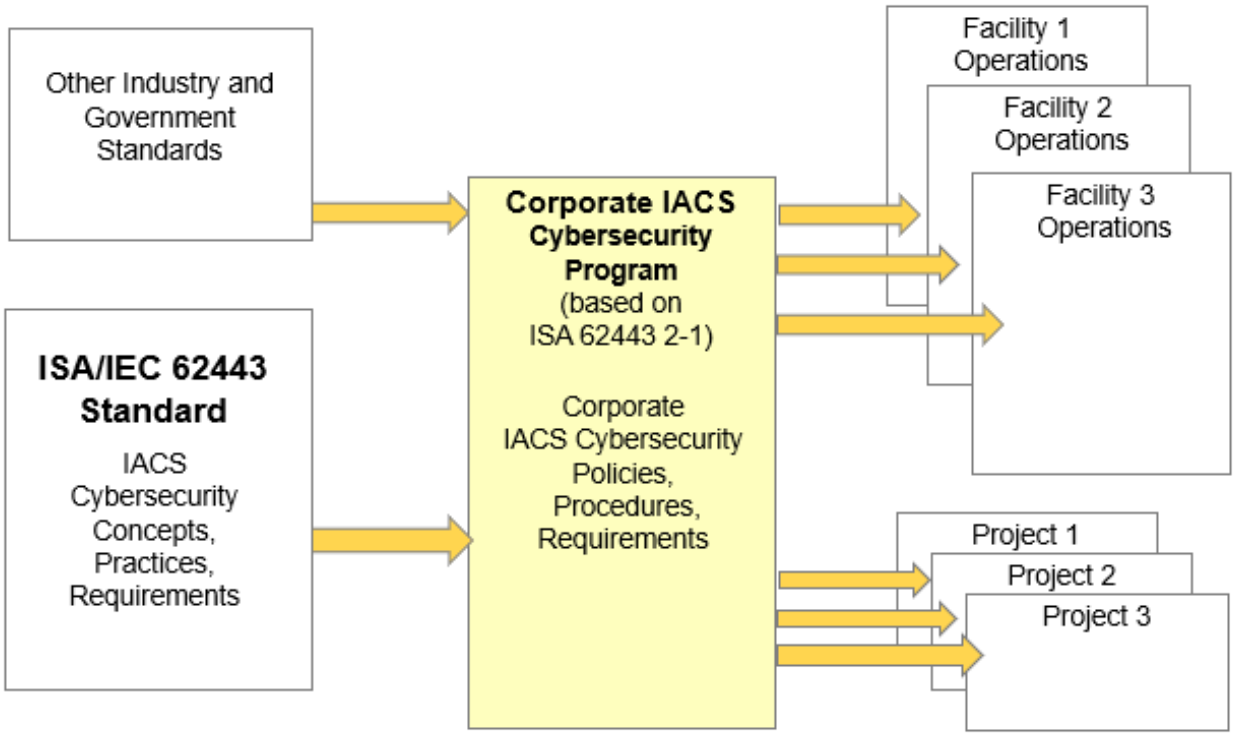


Figure 2 – IACS Cybersecurity Program Concept

As this diagram indicates, the ISA/IEC 62443 standard provides Concepts, Practices, and Requirements that may be included in a corporate IACS cybersecurity program.

Note that a Corporate IACS Cybersecurity program is a necessary first step, however, the Policies, Procedures and Requirements defined in this program, must then be implemented within existing Corporate and Facility procedures if they are to be effective. This implementation should be undertaken as one or more projects, with stated schedules, scopes, and budgets; and must include training and management of change to address human and organizational aspects.

At present, the 62443 standard identifies over 500 separate requirements that may be necessary for a given company's facilities. It is impractical to search through ISA/IEC 62443 to determine what is necessary for a given project or operating facility. A key objective of the IACS Cybersecurity Program is therefore to establish approved requirements that may then be incorporated in project or facility standards and procedures.

A corporate IACS cybersecurity program must select which ISA 62443 requirements to include for:

- A company's Existing Facilities
- New company projects that involve IACS

As shown in Figure 2, requirements and recommendations from other industry, national, and international standards, may also be considered for inclusion in the company's IACS Cybersecurity Program. Examples of these might include:

- ISA standards such as:
    - ISA84 (safety instrumented systems),
    - ISA95 (enterprise integration),
    - ISA100 (Industrial wireless networks), and
    - ISA108 (intelligent device configuration)

  Note: Since ISA standards are internally "harmonized", use of these together with ISA/IEC 62443 may save considerable time and effort for the Owner/Operator.
- Additional cybersecurity standards and guidelines from NIST, NAMUR, ISO, IEC, and others
- Standards and guidelines for human factors, risk analysis and risk mitigation.

Many of the above have been aligned with ISA/IEC 62443, including cross-reference documents and other whitepapers.

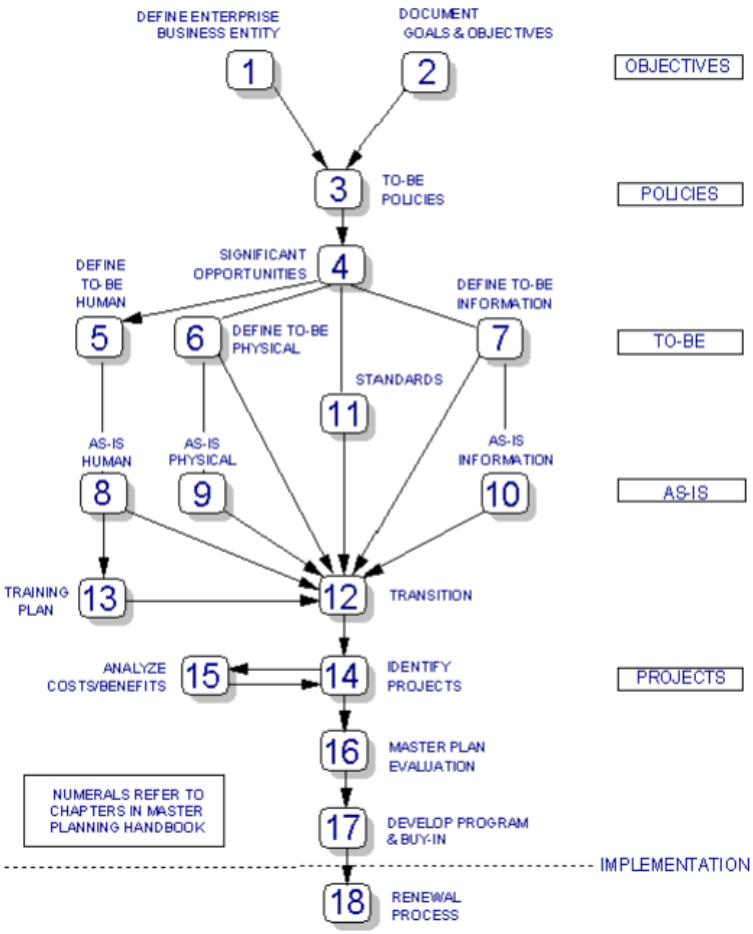
Examples of government standards include regulations and legislation at national, state, and local levels. These must also be considered when creating the Corporate IACS Cybersecurity Program.

ISA is currently active at US Federal, State, and local government levels, to gain acceptance and standardization of regulations based on ISA/IEC 62443. ISA is also participating in programs to promote use of ISA/IEC 62443 in multiple countries around the world.

Preparing an IACS Cybersecurity Program

A formal planning process is recommended to efficiently accomplish development of an IACS Cybersecurity Program. The corporation may have a standard program planning process in place, or may choose to use an alternative such as the PERA Master Planning process. Either way, the general objectives of the program remain the same.

There are a number of advantages to using the PERA Master Planning process for IACS Cybersecurity Planning along with ISA/IEC 62443.



PERA Master Planning is part of the Purdue Enterprise Reference Architecture (PERA) methodology, which is, in turn, the basis of ISA 95, ISA's Enterprise Integration Standard.

- PERA includes Human aspects at all stages of the Master Planning process (especially in steps 4 thru 12), including creation of a separate training plan (step 13).
- ISA99 has compiled a database of over 550 requirements from 62443 that can help automate the creation of a PERA Master Plan.
- PERA Master Planning results in a set of projects (step 14
- ISA99 and ISAGCA are working with INL, NIST, Purdue and educators to develop a "cybersecurity skills inventory" linked to 62443 requirements.

Figure 3 – PERA Master Planning Process

PERA Planning also addresses organizational design, including how to manage both responsibilities and reporting structures. This is particularly important, as the Corporate IT Information Security group normally reports through the IT and Finance (CFO) organizations, while IACS safety and security for Operations and Projects report through Engineering and the Chief Technical Officer (CTO). This IT organization is traditionally supported as corporate overhead, including career development, standards, and training. Engineering organizations have

traditionally been supported only by projects and operating budgets. If IACS cybersecurity is to be effectively implemented and maintained, a corporately-funded IACS cybersecurity function will be necessary.

Implementing the IACS Cybersecurity Plan

Once the Corporate IACS Cybersecurity Program has been approved (see Step 17 in the PERA Master Planning diagram), the facility may either use the Corporate Program, or, if necessary, create its own facility-specific Cybersecurity Program. In either case, the lifecycle for this IACS Cybersecurity Program will proceed approximately as follows:

a) The first step is an Audit of "As-Is" IACS facilities, including an update of equipment and software inventory, engineering network diagrams and P&IDs (i.e., what is there, and how it is connected). Creation of a list of cybersecurity threats experienced by the corporation and similar industries, is also recommended. ISA99 is assembling a database of threats that can be reported by Industry, Phase, Principal Role, etc.
b) Then, an assessment is made of the threats, vulnerabilities, consequences, and impacts (including the proposed risk mitigation measures), using the assessment methodology described in ISA 62443 3-2. These risks must also be aligned with the corporation's standard risk management procedures and criteria, to allow the company to make investment decisions on a consistent basis.

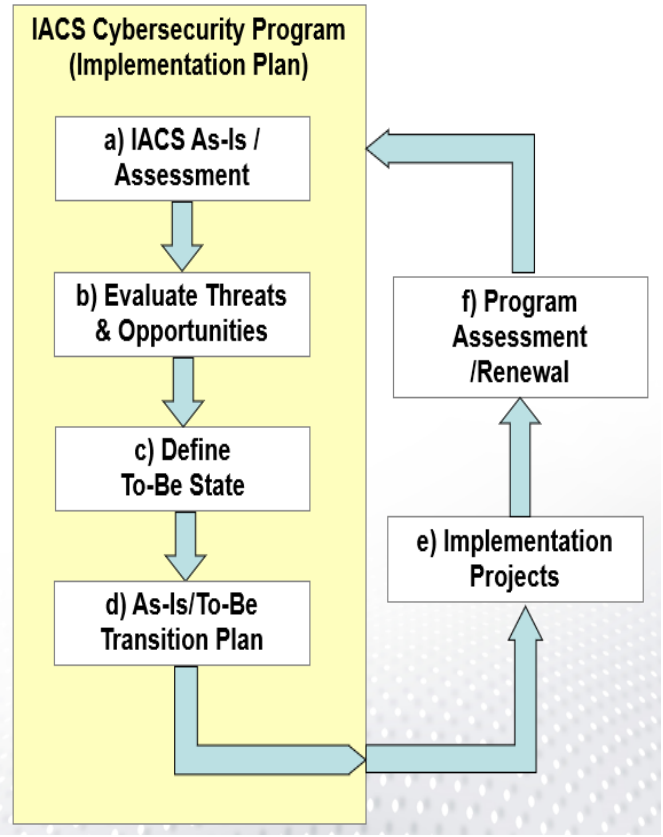


Figure 4 -IACS Cybersecurity Program Lifecycle

c) The risks, costs and benefits of the solutions defined in the IACS Cybersecurity Program are compared, including the selected risk mitigation measures (the To-Be State).

d) An As-Is / To-Be Transition Plan is then established, including provisions for financing, staffing, and scheduling of the individual projects, general cybersecurity training of all relevant personnel, and modifying appropriate company policies, practices, and procedures to address requirements defined in the IACS Cybersecurity Program.

It may even be appropriate to modify these procedures for different company facilities to address special requirements. Thus, a second level of review/approval could be required at each site.

Until a company has an IACS Cybersecurity Program in place, it may be expedient to implement certain 62443 requirements directly in company policy, practices, and procedures for a project or site. While this may be unavoidable for new projects or urgent plant situations, it is not recommended as a standard approach. It is likely that important issues will be overlooked, and in any case, the effort required to address a full suite of requirements "piecemeal" is more expensive than a systematic implementation.

Key Performance Indicators (KPIs) and/or other standard company measurements may be implemented to provide ongoing assessment of the IACS cybersecurity projects. Each IACS Cybersecurity project should be subject to regular review, and ineffective programs eliminated or upgraded.

A periodic audit of the overall IACS Cybersecurity program is also recommended (see Step 18 of the PERA Planning Process). This should include feedback to the corporate IACS Cybersecurity Committee. Changes to the program should be accomplished as part of the company's regular budgeting process.

How does IACS Cybersecurity relate to IT Cybersecurity?

Many corporations already have a corporate position responsible for cybersecurity of information. This position typically resides in the corporate IT (Information Technology) department. The most widely used standards for IT cybersecurity are the ISO 27000 series and selected guidelines from NIST.

Although not yet as common, many corporations are establishing a corporate role that is responsible for OT (Operations Technology) cybersecurity. While IT Cybersecurity is responsible for Information Cybersecurity, OT Cybersecurity is responsible for cybersecurity of IACS. ISA/IEC 62443 is widely accepted as the leading standard for IACS cybersecurity, much as ISO 27000 series is for Information Cybersecurity.

Thus, ISA/IEC 62443 and ISO 27000 are, in effect, "parallel" standards, as shown in the diagram below.

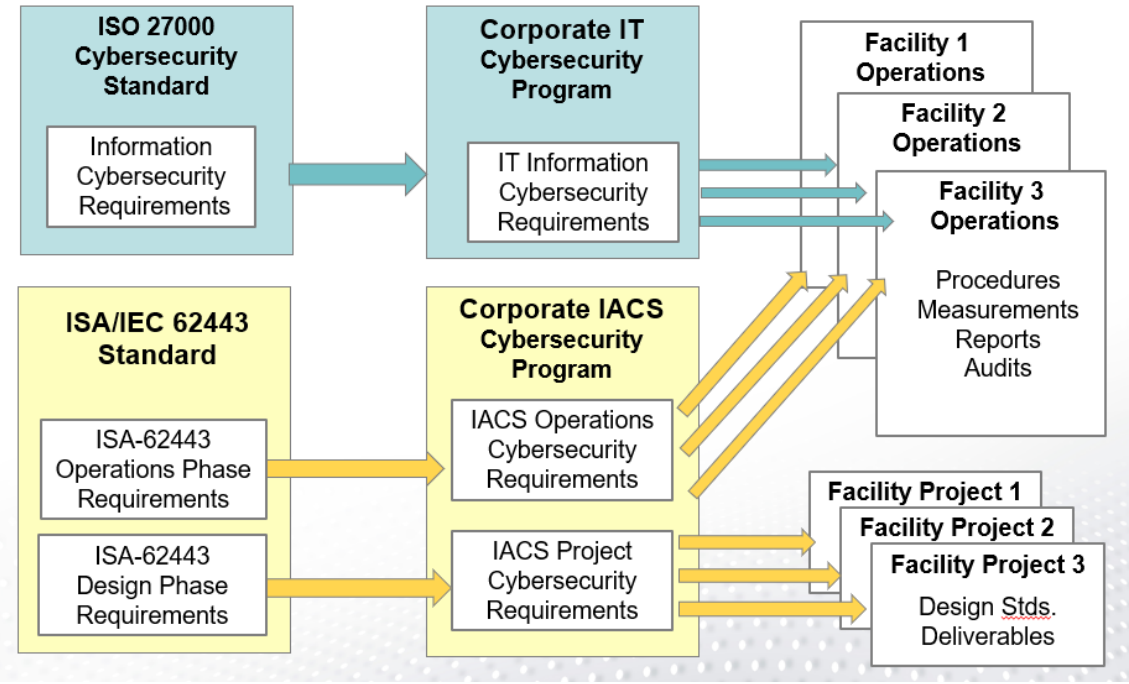


Figure 5 – Mapping of Cybersecurity Requirements

The distinction between where ISA/IEC 62443 and ISO 27000 are applied is also indicated in this diagram.

A Corporate IACS Cybersecurity Program (yellow) will contain Requirements for all enterprise phases of corporate facilities including project design phase and operations phase. These may include project deliverables such as design documentation and drawings (lower right in this diagram), or Operations deliverables such as Operations measurements (e.g., KPIs), incident reports, etc. (upper right in this diagram).

It should be noted that the security of IT information is focused on Operations phase at plants and corporate offices (blue arrows above). Although company information security objectives during project execution may be specified by the Owner, the actual security of information on projects is normally the responsibility of the Integrator, equipment supplier, or engineering contractor.

Typically, information security for IACS in plants (as an addition to equipment operating safety) should be managed by those responsible for the IACS Cybersecurity Program. However, company standards for security of this Information should be provided by the Corporate IT Information security program.

Once areas of responsibility for plant control and automation are agreed in the IACS Cybersecurity Program, the standards to be used for safety and security of IACS systems will be selected and documented (see Step 11 in the PERA Planning Diagram).

Finally, the corporate IACS cybersecurity program, and the corporate IT cybersecurity program, should be aligned, as they provide complementary parts of overall corporate cybersecurity.

Costs and Benefits

An IACS Cybersecurity Program should be assessed and budgeted like any other investment made by the corporation. Implementation of the proposed cybersecurity plan will be divided into a number of projects, each of which is individually justified, approved, and tracked (see Step 14 in the PERA Planning Diagram).

To facilitate this evaluation, cybersecurity risks will be assessed using accepted industry and company criteria. A series of measures will then be evaluated that may mitigate these risks, and the cost of these measures compared to the risk reduction benefits (see Step 15 in the PERA Planning Diagram).

As part of evaluation of the corporate IACS Cybersecurity Program, possible costs of IACS security breaches associated with the proposed IACS Cybersecurity Program will be assessed. Note that the likely cost of an IACS breach is typically much more than for an information breach, since in addition to the risk of data loss, actual physical plant operations may be impacted. Thus, loss of production, equipment damage, environmental damage, and injuries or death may result.

These costs are in addition to the likely costs of information security breaches, including:

- Ransoms
- Lawsuits
- Penalties and fines
- Increased insurance premiums
- Loss of revenue do to reputational or brand damage.

Balanced against the risk of losses are the costs of mitigation measures, including staffing and training of Corporate and Plant Personnel.

Other benefits of the IACS Cybersecurity Program may be realized, including

- More efficient use of staff
- Insurance savings
- KPIs and employee awareness (eg., number of attacks vs penetrations, time from attack to detection)
- Benefits of improved asset tracking and IACS architecture documentation
- Improved IT/OT integration

What to do Next

The number of IACS cyber-attacks, and the financial impact of these attacks, are increasing rapidly. Average losses associated with each attack are reaching tens and even hundreds of millions of dollars, particularly in “infrastructure industries” like power generation and distribution, oil and gas processing, petrochemicals, and pipelines. This is increasing the urgency for corporations to establish IACS Cybersecurity Programs to address these risks.

Using ISA/IEC 62443 and the IACS Cybersecurity planning process, companies can apply their existing Control and Automation expertise, rather than hiring new staff, or training consultants on

the operation of their facilities. This is increasingly important, as studies have indicated that over 1.5 million cybersecurity jobs remain unfilled in 2021, and that this is likely to increase in 2022.

It is also true that the risks and costs associated with cyber-attacks on IACS are too high to simply assign technical project and operations personnel to "solve the cybersecurity problem".

The IACS Cybersecurity program should therefore be created and managed by business and technical leadership, via a tiered IACS cybersecurity council. This may include at the first tier, CEO, CTO, COO, CFO, CIO and H/R, as well as at the second tier, senior staff in their organizations who are involved with cybersecurity standards and procedures, such as the CISO (Chief Information Security Officer), and the Corporate Security Manager.

One of these executives should be given the role of "Program Champion". The Chief Technical Officer is a logical choice, as the CTO is responsible for engineering staff who design major projects, and operations staff who operate IACS control systems. The Champion will report progress on the IACS Cybersecurity Program to a review board, that should include major stakeholders including representatives of:

- Plant Operations
- Capital Projects
- IT Operations
- Control and Automation Systems
- Physical Plant Security
- Corporate Risk Management
- Health, Safety and Environmental

Using ISA/IEC 62443 and PERA Master Planning, expenditures for initial phases of IACS Cybersecurity Program Planning are relatively modest, and can probably be funded from existing standards and training budgets. However, creation of the actual corporate program will likely require several months with a dedicated small team.

It should also be noted that the personnel required for an IACS Cybersecurity Program Plan should largely be drawn from existing enterprise resources. It is not possible to create an effective IACS Cybersecurity Program without engineers and technicians who have a deep understanding of the corporation's industrial facilities, IACS, industrial networks, hazards, and organization. Thus, even if "cyber-certified" engineers and specialists were available, the cost to train these new hires or consultants would be excessive, and in any case, would delay implementation of an effective IACS cybersecurity program by many months or years.

The best approach is therefore to support and encourage professional development of current staff, including IACS cybersecurity training and certifications. This may be accomplished in parallel with creation of the IACS Cybersecurity Plan and implementation of the resulting Corporate IACS Cybersecurity Program.

If you would like more information on the above, please contact

Gary Rathwell, President
Enterprise Consultants International Ltd (ECI)
Gary.Rathwell@Entercon.biz, or
Gary.Rathwell@PERA.net

(November 4, 2021 version[109] of this paper used with permission of the author, Gary Rathwell and International Society of Automation)

[109] This document has been updated and may be obtained here: https://www.isa.org/news-press-releases/2022/january/new-white-paper-implementing-an-industrial-cyberse

Appendix 5

About the author

- Vytautas Butrimas has been working in defense and cyber security roles for over 30 years as:
  - Vice-minister at the Ministry of Communications and Informatics, Republic of Lithuania responsible for Information Society programs.
  - Defense Policy and Planning Director, Lithuanian Ministry of National Defense (MoND) responsible for preparing the first Military Defense Strategy.
  - Deputy Director responsible for IT security at the Communications and Information System Service (CISS) responsible for preparing the first National Defense System Cybersecurity Strategy
  - Chief Adviser for the MoND of Lithuania with a focus on cybersecurity policy, including work in the national task force that wrote the Lithuanian Law on Cybersecurity
  - Member (Presidential appointee) of the National Communications Regulatory Service's Council (RTT-Council)
  - Industrial Cybersecurity Subject Matter Expert for the NATO Energy Security Center of Excellence (NATO ENSEC COE) who performed a Cyber Risk Study of the ICS Used in the NATO Central Europe Pipeline System (CEPS) and an Assessment study of Cybersecurity of Smart-grid Technologies Employed in Operational Camps for the French General Staff.
- Mr. Butrimas also contributed to various studies and reports on cyber security and critical infrastructure (for OSCE, EU ENISA, IEA, NATO and other organizations), published articles and made presentations at many conferences and courses on Cyber Security and Defense policy. He has participated in NATO and National exercises including scenarios of cyber-attacks on critical infrastructure. He participated in development of cyberspace confidence and security building measures for the OSCE and supported the Global Commission on Stability of Cyberspace norms proposals.

Vytautas is a member of the International Society for Automation (ISA), Co-chair of ISA99 MLM Work Group 13, and co-moderator of the SCADASEC list. He is currently serving as national representative for industrial cyber security at NATO ENSECCOE and is a member of NATO Science and Technology Board's SAS-163 research task group preparing a report on Energy Security in an Era of Hybrid Warfare.