Cybersecurity Certification Programs Have Matured

White Paper
exida
80 N. Main St.
Sellersville, PA
www.exida.com

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

Copyright exida.com L.L.C. 2018-2020

Abstract

The ISA Security Compliance Institute pioneered the first cybersecurity certification program for automation systems called ISASecure several years ago. A number of automation system products have successfully become certified (www.sael-online.com). Recently new standards in the IEC 62443 series of cybersecurity standards for automation systems have been released and those standards are being used for cybersecurity certification. This presentation shares the experience of a Certification Body and the learned values of cybersecurity certification for products, development processes, integrators, and systems.

Cybersecurity Risk

After a number of cybersecurity attacks on industrial control systems (ICS), most plant owner/operators now consider a cybersecurity attack to be a credible risk. Three of these cybersecurity attacks have received a lot of attention:

1. Stuxnet – an attack on a Siemens PCS7 system where the controller code was changed to cause physical damage to equipment.
2. Industroyer/Crash Override – an attack on the Ukrainian electrical power grid that shutdown a large portion of the city of Kiev.
3. Triton – an attack on a distributed control system (DCS) and a Schneider Triconex safety instrumented system (SIS) believed to be an attempt to cause damage to the plant. The Tricon v10.3 controller did initiate a shutdown of the plant.

It is clear that the ICS owners/operators must improve cyber defenses if we want to even keep up in what has become an arms race of sorts. Fortunately we are learning. There have been enough successful cyberattacks over the years, that many attack patterns have been discovered and documented. In fact, over 500 attack patterns have been documented [1] in Common Attack Pattern Enumeration and Classification (CAPEC). With each attack pattern, a defense against the attack has been developed and these can be found in cybersecurity standards.

ICS Cybersecurity Standards

The ISA S99 standards were the first ICS cybersecurity standards issued starting in the mid 2000s. Those standards were used by the IEC 62443 committee to create a globally recognized set of cybersecurity standards now used by many industries including process control, medical, power generation, and others. The IEC 62443 series of standards includes over ten documents, mostly using the ISA S99 standards. Those documents describe terminology, policies and procedures, system level defense techniques, and device level requirements for product development. Major control system OEMs including Schneider, Honeywell, Yokogawa, Emerson, Siemens, Hitachi, Toshiba, and ABB have selected IEC 62443 as the roadmap to use when hardening their products and systems.

Cybersecurity Certification

An accredited cybersecurity certification program is created to provide technically competent, third party auditing and assessment to attest that the certification target has met the requirements defined in a document called a scheme. In 2007 the ISA Security Compliance Institute (ISCI) was founded and defined the first cybersecurity certification scheme for embedded products, called Embedded Device Security Assurance (EDSA), based on the ISA S99 standards called ISASecure. This group later added a second scheme to certify an OEM product development process, called Security Development Lifecycle Assurance (SDLA), and a third for system level certification called System Security Assurance (SSA).

exida became the first accredited Certification Body for cybersecurity in 2010 and has completed certification projects for Honeywell, RTP, Yokogawa, Schneider, and ABB. Several other OEM companies have completed cybersecurity certification from other CBs including Toshiba, Triconex, Tri-Sen, Hima, and Azbil. Other OEMs will complete their projects shortly. Cybersecurity certification is certainly available or will be available soon in most DCS/SIS product lines.

Since the IEC 62443 standards have been released, new schemes have been defined by the Certification Bodies based on their experience and these new standards. It is expected that the ISASecure scheme documents will be updated per the differences between S99 and ISA/IEC 62443 soon since there are only a few major changes.

Cybersecurity Attack Patterns

Much has been learned about how cyber attackers accomplish their goals. Apparently, there are 508 different ways that they can succeed. But can we classify attack patterns? Fortunately, CAPEC has classified mechanisms of attack and sequences of attack events.

Mechanisms of attack:

- Collect and analyze information – This first step in any attack is usually to try and gather information about a system. There are a number of methods this can be done (118 according to CAPEC), but some examples include looking through a company's web site or user manuals, dumpster diving (literally looking through a company's trash), scanning systems on-line to try and determine technologies used, ports open, etc., and monitoring network communications to better understand format of messages.
- Inject Unexpected Items – An attacker crafts input data to a system in such a manner that causes an application to perform steps unintended by the application. An example would be when a user asked to enter their user name, they instead enter part of a SQL command. If the application uses the user name as part of a SQL query, the user input data could alter the query to meet the attacker's needs.
- Manipulate time and state – An attacker attempts to manipulate state information which is located in a user accessible location (e.g. cookies or URL parameters. Or an attacker attempts to take advantage of timing issues such as race conditions.
- Abuse existing functionality – an attacker takes advantage of existing functionality in a system to use it in a way to adversely affect the system, or to gain privilege for which a user is not authorized. One example would be sending many messages to a system to force the code that processes each message to execute possibly causing a denial of service to other functionality that needs access to system resources. Another example would be to manipulate a system such

that a legitimate display function is used to display information that a user is not authorized to see.

- Employ probabilistic Techniques – an attacker uses probabilistic techniques to explore and overcome security properties of a target system that are based on an assumption of strength due to extremely low mathematical probability that an attacker would be able to exploit very rare conditions required to bypass system security. One example of this would be a brute force attack where, where thousands or millions or billions of possible password combinations are tried until the right one is found.
- Subvert Access Control – The attacker takes advantage of weakness in authentication and access control of a system. This could include accepting messages from unknown devices or users or using weak mechanisms for authorization. One example of this is that many controllers will accept messages from the engineering workstation if they are of the correct format and have a proper CRC. But both of these requirements can be easily imitated by an attacker based on analysis of messages sniffed off of the wire.
- Manipulate Data Structures - Most successful attacks on a system occur by sending unexpected data to that system. For example, if a system is expecting 100 bytes of data and you send it 1000 bytes how does it react? You might expect it so simply reject the data, but there are many known cases where a system accepts this data and overwrites 900 bytes of data in memory. This is essentially how the buffer overflow vulnerability works. The data that you overwrite could be useless information, but it could also be key security data such as the permission level of the attacker. Also, in some cases the data crafted by the attacker is code that can later be executed based on another successful attack.
- Manipulate System Resources – the attack is carried out by manipulating resources in the system that are used by the target program. One example would be to modify a file that will be opened and parsed by the program. By violating assumed structure of the file, the program could be manipulated into doing something unintended

The mechanisms of attack which have been described here can only succeed with the existence of human and system weaknesses. Examples include:

- Users accidentally click on link in phishing e-mail
- Program passes user input directly into SQL query
- Program doesn't check size of data buffer and overwrites buffer when a larger than expected message received
- Controller accepts messages from any source without authenticating source
- System allows six character passwords and does not lockout users after unsuccessful passwords attempted.
- System sends data over untrusted network without encrypting data so attacker can easily view messages and potentially mimic them later.
- User's credentials are not removed from system when user leaves company

An important thing to understand about successful cyberattacks is that they normally use a chain of attack mechanisms to achieve the ultimate goal. For example, one attack might yield a password into one system, while another attack may yield the location in memory of key data, and the third attack may overwrite the data to force the control system into a dangerous state.

Although the details of the attack methods for some events are not known with certainty, expert forensic cyber engineers have made conclusions. In the case of the Stuxnet cyberattack:

- Human mistakes - a staff member carried the malware into the system via a USB stick.
- Knowledge of the control system – Public cyber vulnerabilities, reverse engineering of the system, and testing using a real system are all postulated given the sophistication of the attack.
- System reconnaissance – the malware code scanned target systems looking for specific control configurations.
- Exploitation of known vulnerabilities – four "Zero-Day" vulnerabilities were used in the attack.
- Exploitation of weak security measures – the attack took advantage of the hard coded password for the database code and the read/write I/O image design of the controller.

Preventing and Detecting Cybersecurity Attacks

For every mechanism of attack there are multiple mechanisms that can be put in place to thwart such an attack. These mechanisms are often called compensating controls or risk mitigations. History has shown that attackers are smart and can often find the weakest link to attack a system. So, if a system includes mechanisms to thwart 9 out of 10 possible attack paths, attackers will often find the 10th attack path that has not been mitigated. However, by putting these mechanisms in place, the attackers can increase the time to compromise for the system, meaning essentially that it will take longer for the attacker to break into the system and therefore increase the likelihood that an attacker will give up before an attack is successful. This can decrease the risk of an attack of a system to an acceptable level.

IEC 62443 Requirements

IEC 62443 can essentially be thought of as a catalog of compensating controls and risk mitigations that can be applied to a system. For each attack pattern that exists in the world, there are ideally one or more compensating controls or risk mitigations defined in this standard that will prevent or lower the risk of a successful attack.

At the system level, IEC 62443-3-3 details several categories of cybersecurity requirements including personnel vetting and training, system design rules, data restrictions, network segmentation, patch policies, and the selection of cyber hardened products. Specific requirements include items such as procedures and training that asset owners can put into place. For example, users can be trained to never install email or other applications on engineering workstations. Systems can be designed using network segmentation as a way to limit how much damage an attacker can do when a part of the system is compromised. Intrusion detection and prevention systems can be installed to quickly identify unusual activity. Products can be patched frequently when security vulnerabilities are found. Several good complete references can be found on system level cybersecurity [2].

However, there is no amount of procedures, training and technology can compensate for flaws in the underlying control system. Weaknesses in these underlying systems will always lead to vulnerabilities that can be taken advantage of by attackers unless the cybersecurity strength of the system products are improved. Therefore IEC 62443-4-1 provides a set of requirements for a product development and test process for cyber hardening. IEC 62443-4-2 describes the 3-3 requirements in terms of product features. For example, to prevent against injection attacks, systems should validate any input data received. To protect against attackers sniffing data over the network, the data can be encrypted. To ensure that configurations cannot be downloaded from untrusted sources, user and device

authentication can be implemented. To find other security weaknesses in the devices security testing can be done such as static analysis of source code, fuzz testing, and analysis of binary code.

Sets of cyber protection features are required as a function of security level (1 through 4). Table 1 shows the quantities of requirements as a function of security level. Note that the number of requirements are cumulative and increase with each level. This means that a product certified to level 2 has met more of the cybersecurity requirements and will provide higher levels of cyber hardening than level 1. Level 4 provides the highest number of cybersecurity hardening features.

Table 1: Quantity of Cybersecurity Requirements from IEC 62443-4-2 for each Security Level.

Foundational Requirement	SL-1	SL-2	SL-3	SL-4
FR 1 – Identification and Authentication Control	10	16	22	24
FR-2 Use Control	8	12	21	24
FR-3 System Integrity	5	10	16	19
FR-4 Data Confidentiality	2	4	5	6
FR-5 Restricted Data Flow	4	6	10	11
FR-6 Timely Response To Events	1	2	3	3
FR-7 Resource Availability	7	10	13	13

Many believe that IEC 62443-4-1 provides the strongest future impact for cyber hardened systems. That standard lists the requirements for product development and test, especially software development requirements. Like the functional safety standard IEC 61508 which has been used for decades in safety certified products, IEC 62443-4-1 lists the hardware, firmware and software design requirements needed to provide cyber hardening by design.

Cybersecurity Certification

Applying compensating controls and risk mitigations to a system must occur at multiple levels. The developers of the system must take steps to minimize vulnerabilities in the system components and to ensure that the components include security capabilities that users need to protect their systems. System integrators need to ensure that security mechanisms provided by the underlying components and enabled and used correctly. System operators need to ensure that they are taking the appropriate steps to keep the system secure during operation and maintenance. And when systems are decommissioned or replaced, steps must be taken to ensure that there is no leakage of information that could compromise the security of remaining systems.

As an asset owner trying to protect your system from cyber-attack, how do you ensure that these controls and mitigations have been applied at every layer? The cost of analyzing and auditing each component used in a system and each supplier of services to the system will likely be cost prohibitive and require cybersecurity expertise that simply may not be available. This is where cybersecurity certification enters the picture. It allows for a component or an organization to be audited once by a trusted organization, rather than by each of its users.

Cybersecurity certification clearly makes sense from an economic point of view, but is it too critical of a function for vendor self-certification? Is it too critical to rely on any third party to perform? And if so, how do you ensure that the third-party certification is sufficient? There are several key things to look for in a certification as follows:

- Content of certification – some cybersecurity certifications that are available are what are called “test only certifications”. These certifications are valuable in that they show the supplier has

strengthened their product against vulnerabilities that have been found during this testing. But it is important to realize that this certification does not look at the security capability of the product or the security development process used to create that product so it is far from complete. Ideally a security certification should consist of all relevant IEC 62443 requirements.

- Transparency of the certification – most certifications will include a certificate, which summarizes to what the product is being certified, and a report which defines exactly what was done as part of the certification. In order to ensure that the certification meets your needs, there should be some level of transparency in the report that shows exactly what aspects were considered in the certification. Certificates and Assessment Reports should be public documents.
- Trustworthiness of certification agency. This is such a key item, but also a difficult one to confirm. As a start it is good if the certification agency is itself subject to audit by a third party. This is normally done by having the certification body be accredited by a third party such as American National Standards Institute (ANSI) in the US. Other less concrete factors to consider are reputation of the organization and personal experiences with the organization at conferences, through standards bodies, industry groups, etc.
- Competence of the certification agency. Technical competency is also something that is not always easy to determine. But it is important that the Certification Body be expert in the area that the certification covers. Accreditation by a third party also supports this area since this is generally one of the requirements of IEC 17065 which is the standard to which certification bodies are typically accredited. However, accreditation audits are limited. In addition one should review the CB contributions to the industry. Do they participate in the committees that develop the standards? Do they publish books and papers on topics relevant to the certification? Do they otherwise demonstrate knowledge and expertise on such topics?

Cybersecurity Certification Matures

Significant experience is accumulating with the cybersecurity certification process. Several OEMs have achieved level 1 certification. A few have achieved level 2. Some will achieve higher levels in time. During these certifications experience has shown:

- Some network testing is quite effective while other tests do not seem to detect problems. Focusing on the tests that have proven to be effective saves certification cost and uncovers more vulnerabilities.
- Stronger cyber coding rules are required by the standards and have been defined by various industry groups based on the study of attack patterns. Coding standards such as the CERT and C++ coding standards, developed by the Software Engineering Institute, were created directly in response to this need. In addition, well known safety coding standards, such as the Motor Industry Software Reliability Association (MISRA) C and C++ coding standards have been analyzed and improved for cybersecurity. Secure coding standards for more languages such as Java and Perl have been developed as well.
- Ensuring competency and knowledge of cybersecurity issues has become part of the certification process. As a result, more cybersecurity training has become available for OEM product development teams and integrators.
- Methods of managing the cybersecurity risk of legacy code and third-party components have been developed and put into place. These were previously hidden risks that were often not analyzed.

With maturity comes the clear recognition that the cybersecurity environment is constantly changing. This is because cybersecurity is not like functional safety as the attack agents are increasing not only in numbers but in technical skill. Therefore, cybersecurity certification schemes must constantly monitor attack mechanism reports and change requirements to meet the ever-increasing threats. Results to date have been good but more is needed and that will happen.

References

1. https://capec.mitre.org
2. Gunter, D.G., Medoff, M.D. and O'Brien, P.C., *A Pragmatic Approach to IACS Cybersecurity: Using IEC 62443 Standards,* exida, Sellersville, PA, 2018

Revision History

Authors: Mike Medoff, CFSE, Ted Stewart, CFSP

exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool

- PHAx™ (Process Hazard Analysis)
- LOPAx™ (Layer of Protection Analysis)
- SILAlarm™ (Alarm Management and Rationalization)
- SILect™ (SIL Selection and Layer of Protection Analysis)
- Process SRS (PHA based Safety Requirements Specification definition)
- SILver™ (SIL verification)
- Design SRS (Conceptual Design based Safety Requirements Specification definition)
- Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
- PTG (Proof Test Generator)
- SILstat™ (Life Event Recording and Monitoring)

- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
  - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
  - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com