bsi.

...making excellence a habit.™

ICS Cybersecurity Assessment Framework

Suitable standards supporting a hybrid approach to risk management in ICS

A Whitepaper

Introduction

Companies that have processes controlled by an ICS (Industrial Control System) possess at least two types of networks; the corporate IT network, and a SCADA network, the latter hosting all the control system related items.

The main purpose of this paper is to propose an approach to a Cyber Security Management System (CSMS) based on taking the "best of breed" from several leading ICS influences, such as: IEC 62443, ISO 27001, NIST, CPNI and ENISA.

Each of the above listed standards and security frameworks cover different aspects of cyber security, or are aimed at protecting different types of systems. Some of them are detailed standards, while others are a collection of Cybersecurity best practices. They are influences focusing on IT protection with others aiming for OT security.[1]

The treatment of IT and OT networks from a cybersecurity perspective should be different. They are driven by different priorities, and the standards used to achieve some level of cybersecurity assurance are not applicable between the two types of network.

In the ICS cybersecurity area, the reason for the CSMS assessment is even more important, because of the lack

of cyber risk awareness. Industrial Control Systems were designed to operate in closed environments, isolated from the external world (physically and electronically). Those systems face threats that did not exist 20 years ago, and the system controllers need to understand the risks.

The purpose of the framework depicted in this paper is to define the cybersecurity assessment for Industrial companies with an ICS. The initial step in this path to securing infrastructure is to be audited against ICS dedicated Cybersecurity standards.[2]

1 IT refers to Information technology, and the newer OT stands for "Operation Technology"

2 This paper recommends a subset composed by parts of the standards and best practices listed above for achieving a high standard of cyber-security in the industrial automated systems.

Standards and Influences Overview

ISA/IEC 62443

ISA stands for the International Society of Automation, a non-profit global organization founded in 1945, while IEC

stands for the International Electro-technical Commission, a non-profit organization founded in 1906. The scope of the ISA/IEC 62443 is "to *define the elements necessary to establish a cyber-security management system (CSMS) for industrial automation and control systems (IACS), and to provide guidance on how to develop those elements*"[1] The main strength of using the 62443 standard is that it presents a high level of customization for ICS systems. The standard is able to address many issues that are unique to these particular systems. On the other hand, having a degree of specialization on OT systems could make the standard less accurate when addressing generic IT issues.

ISO 27001

The International Organization for Standardization published this series of standards with the aim of defining a risk management system that is intended to bring information security under explicit management control. This is a mature standard that works perfectly in classic IT systems, but is not designed to define a cybersecurity system for an ICS. Therefore, the strength and weaknesses are similar to the ones that ISA 62443 presents, but the other way around. The standard is excellent for application to IT systems, but not accurate enough by itself to be applied to OT systems.

1 According to IEC 62443-2-1 https://webstore.iec.ch/publication/7030

NIST

The National Institute of Standards and Technology was founded in 1901, and today forms part of the U.S. Department of Commerce. NIST's mission is *"To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life."* [2] Among many other things, NIST supports a cyber-security program that focuses efforts in protecting critical infrastructure. That is translated into large collections of recommendations and methodologies that cover many aspects of IT and OT systems. The main strength of NIST is the wide coverage it provides, being applicable to improve cybersecurity in important parts of IT and OT. NIST does not provide a complete standard, and therefore is not possible to elaborate a complete cyber security system using just NIST recommendations. NIST however, is an excellent supporting tool to help improve risk management and security posture.

CPNI

The Centre for the Protection of National Infrastructure is a U.K. organization which, similar to NIST, is a *"government authority for protective security advice to the UK national infrastructure. Our role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats."*[3]

CPNI covers the Cybersecurity applied to IT and OT with numerous resources freely available. CPNI also covers best practices and implementation recommendations for IoT.[4] The standard covers a wide range of technologies and is updated with the latest cybersecurity trends. Weaknesses identified in CPNI are that it does not provide a complete methodology to build a cybersecurity management system by itself, which can present issues when performing risk management.

ENISA

The European Union Agency for Network andInformation Security is the equivalent of NIST and CPNI but for the European Union. Regarding cybersecurity, it covers many IT and OT aspects, but many new technologies as well such as Blockchain and Big Data. It is a collection of best practices and recommendations, but not a standard, so it has the same strengths and weaknesses as NIST and CPNI.

2 According to NIST https://www.nist.gov/about-nist/our-organization/mission-vision-values
3 According to CPNI https://www.cpni.gov.uk/about-cpni
4 IoT. Internet of Things

The Differences Between Cybersecurity in IT and OT Systems

As is shown in the NIST SP 800-82 Standard, the main differences between the IT and OT systems in the cybersecurity area are described in the below table:

Category	IT System	OT System
Performance Requirements	• Non-Real Time • Response must be consistent • High throughput is demanded • High delay and jitter may be acceptable	• Real Time • Response is Time critical • Modest throughput is acceptable • High delay and/or jitter is not acceptable
Availability Requirements	• Responses such as rebooting are acceptable • Availability deficiencies can often be tolerated, depending on the system operational requirements	• Responses such as rebooting are not acceptable • Availability requirements may necessitate redundant systems • Outages must be planned and scheduled days/weeks in advance • High availability requires exhaustive depolyment testing
Risk Management Requirements	• Data confidentiality and integrity is paramount • Fault tolerance is less important • Momentary downtime is not a major risk • Major risk impact is delay of business operations	• Human safety is paramount, followed by protection of the process • Fault tolerance is essential, even momentary downtime could be unacceptable • Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment or production resulting in major losses
Architecture Security Focus	• Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets • Central server may require more protection	• Primary goal is to protect edge clients (process controllers) • Protection of central server is also critical
Unintended Consequences	• Security solutions are designed around typical IT systems	• Security tools must be tested (before going to production) to ensure that they do not compromise normal ICS operation
Time Critical Operation	• Less critical emergency interaction • Tightly restricted access control can be implemented to the degree necessary for security	• Response to Human and other emergency interaction is critical. • Access to IACS should be strictly controlled, but should not hamper or interfere with Human-machine interaction

Resource Contsraints	• Systems are specified with enough resources to support the addition of third party applications such as security solutions	• Systems are designed to support the intended industrial processes and may not have enough memory and computing resources to support the addition of security capabilities
Communications	• Standard communication protocols • Primarily wired networks with some localized wireless capabilities. • Typical IT networking practices	• Many proprietary and standard communication protocols • Several types of communications media used including dedicated wire and wireless (radio and satellite) • Networks are complex and sometimes require the expertise of control engineers
Change Management	• Software changes are applied in a timely fashion in the presence of good security policy and procedures. • The procedures can be often automated	• Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. IACS outages often must be planned and scheduled days/weeks in advance. IACS may use O.S. that are no longer supported
Managed Support	• Allow for diversified support styles	• Service support is usually via single vendor
Component Lifecycle	• Lifecycle on the order of 3-5 years	• Lifecycle on the order of 15-20 years
Access to Components	• Components are usually local and easy to access	• Components can be isolated, remote, and require extensive physical effort to gain access to them

Framework Overview

The framework proposed in this paper is divided into 8 steps. Each of these steps has been constructed with a set of influences of the mentioned standards and best practices, as is depicted in the following image. Additionally, and in order to address the continuous on-going nature of the process, all the steps encapsulate the Plan-Do-Check-Act (PDCA) methodology.

- **Current State Definition**
  The first step in this framework is to define in the most accurate manner, all the cybersecurity relevant aspects of the ICS to be assessed. Influences: ISO 27001, IEC 62443, NIST and ENISA.
- **Target State Definition**
  After defining the system's present situation, the desired ICS state in the context of cybersecurity, is defined. This is carried out in consensus with management, asset owners and with the assessment of the cybersecurity expert. Influences: ISO 27001, IEC 62443, NIST and CPNI.
- **GAP Analysis**
  Once the current and the desired IACS states are defined, the Gaps between them should be identified and listed, providing a manner to measure the progress of the assets, and a checklist of the desired outcome of it. Influences, IEC 62443, NIST, CPNI and ENISA.
- **Creating Threat Profile**
  As the set of possible threats, threat actors and threat scenarios is enormous and ever-changing. It is important to narrow the group defining a threat profile, identifying the items that the cybersecurity assessment will focus on. Influences: NIST, ENISA and CPNI.
- **Risk Analysis**
  With the outcome of the GAP analysis and the defined threat profile, a multi-level risk analysis may be carried out. All risks derived from the current state of the IACS are used and following a risk prioritization, the remediation order will be determined based on criticality of assets and issues, starting with critical issues on critical assets. Influences: ISO 27001, IEC 62443, NIST, ENISA and CPNI.
- **Remediate**
  With the output of the risk analysis already defined and remediation action prioritized in order of criticality, remediation can be applied to each of the identified assets and risks. Influences: ISO 27001, IEC 62443 and NIST.
- **Benchmarking**
  In order to refine the result of the cyber risk assessment, the outcome of the risk analysis should be compared with a collection of standards and best practices in the cyber security arena. Influences: NIST, ENISA and CPNI.
- **Program Maturity**
  The last step of this framework takes place when the cyber risk assessment has finished. This step covers the elaboration and implementation of an on-going cybersecurity program with periodical updates and revisions. Influences: ISO 27001, IEC 62443 and CPNI.

The framework structure is built following the ISO IT risk assessment principles:

- Risk Assessment methodology
- Risk Assessment implementation
- Risk Treatment implementation
- ISMS Risk assessment report
- Statement of applicability
- Risk Treatment plan

GAP Analysis and Benchmarking steps are included into that structure, in order to increase the accuracy when determining the current and target state of the system.

This enables residual risk analysis to be addressed in the process. Influence of the IEC 62443 helps move the requirements towards ICS alignment.

Framework Steps

We've outlined our framework steps below.

Current State Defintion

The first step in any assessment is to determine the current status of the system to be assessed. The current state of a system is a model that has all the relevant information needed to perform a cyber risk assessment.

Influences Contribution

- **ISO 27001:** The standard provides guidelines under the risk assessment methodology to clearly define the current status of an IT system[1]
- **IEC 62443:** This standard enhances the current state definition, with the system segmentation model[2]
- **NIST:** The institute provides tools for the definition of the current state of an ICS system[3]
- **ENISA:** Additional methods for current state definition are provided with "definition of external and internal environment"[4]

Target State Definition

The Target State Definition sets the expectations for cybersecurity controls, processes, and procedures which should be in place for industrial plants and IT infrastructure. This provides a common reference across the organization.

Target state definition brings IT, OT, Physical Security, and HR together within the organization to agree on a common set of security controls. This process defines interviews with IT, Security, and all applicable operations groups to create and adopt a common set of ICS Security Controls, each tailor made to fit the organization's operational structure and constraints.

Influences Contribution

- **ISO 27001:** Same as in the current status step, ISO status definition methodology can be used to determine the target status to be achieved
- **IEC 62443:** The standard introduces "fundamental requirements" and "security levels", which provide enhancement on the cyber security definition from an ICS perspective[5]
- **NIST:** The institute provides the "Cybersecurity core model", a guideline to address all the cybersecurity goals on an ICS system[6]
- **CPNI:** Provides a collection of "target state" examples in the ICS environment, which can be used as guidelines for each target state

Gap Analysis

Once the current and target states are accurately defined, the GAPs between them have to be listed in order to quantify the differences needed to reduce to arrive at the desired status.[7]

This is an on-going process, as the scope also includes the metrics that should be used to check the degree of fidelity with the desired target state.

The metrics compose a tool that should be used in two scenarios:

- At the cybersecurity assessment
- At the periodical cybersecurity reviews

The cybersecurity reviews should be conducted to update the security degree upon the new threats and threat scenarios, according to a continuous improvement philosophy.

Influences Contribution

- **IEC 62443:** The previously introduced "security levels" are used in the GAP analysis, to address the gaps using a standardized nomenclature
- **NIST:** Vulnerability identification practices[8], provided by the Institute, can be used as an additional method of gap classification, for consistency purposes

1 See Asset inventory, ISO 27001 http://www.iso27001security.com/ISO27k_Roles_-_responsibilities_for_information_asset_management.pdf
2 The system segmentation model methodology enables the division of the ICS systems into simpler "zones" and "conduits" to enable more accuracy
3 NIST "system characterization", under "Risk Management guide for Information technology systems" http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
4 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/activities/risk-management/current-risk/risk-management-inventory/rm-process/rm-process/crm-strategy/scope-framework
5 http://standards.globalspec.com/std/1625784/isa-62443-3-3
6 https://www.nist.gov/cyberframework/csf-reference-tool
7 The current and target state models provide a simplified way to identify and address the gaps between them. Both models will be subdivided into simpler entities that can be compared to get the gap breakdown
8 http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

- **CPNI:** Provides roadmaps to ideal security configuration in ICS[1] that can be followed as a review of the GAP analysis
- **ENISA:** Provides the methodology to perform GAP analysis

Threat Profile

Developing a detailed threat profile provides organizations with a clear illustration of the threats. The current and target state models provide a simplified way to identify and address the gaps between them. Both models will be subdivided into simpler entities that can be compared to get the gap breakdown that they face, enabling them to implement a proactive incident management program that focuses on the threat component of risk.

This framework proposes to conceive the threats not as single events, but as elements in combination with other different threats, which when combined dramatically increase the success rate of attack (penetrating an IACS).

Creating a threat profile is the process which researches the possible threat scenarios that can affect an IACS, and elaborate a collection of them, to focus the cyber risk assessment on them.

Influences Contribution

- **NIST:** NIST provides a large amount of information for threat identification, listing historical cybersecurity threats that the U.S has faced
- **ENISA:** The ENISA Threat Landscape (ETL) provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends[2]
- **CPNI:** It introduced the new terms "threat scenario" and "threat campaign", useful to build more complex and accurate threat profiles

Threat Concept Definition

This glossary, obtained from the ISO 27001 and CPNI, is used by this framework as the initial toolbox for the threat profile construction

- **Vulnerability:** Is a weakness in software or hardware that an attacker could exploit to compromise the confidentiality, availability and integrity of the information
- **Exploit:** Describes any potential means to act on a vulnerability to gain access to an asset
- **Threat:** Any entity with expressed or demonstrated intent to harm an asset or access it in an unauthorized way
- **Threat actor:** Any physical or legal entity that uses a threat to produce an exploit on a vulnerability
- **Threat scenario:** Illustration in which one or more threat actors can mount one or more threat actions in an attempt to compromise the identified target asset by exploiting either or both; vulnerabilities and/or inadequate safeguards
- **Threat Scenario Campaign:** Series of related threat scenarios that are used together as part of an APT (Advanced Persistent Threat) for a common objective
- **Threat Profile:** Includes assets, vulnerabilities, threats, threat actors, threat scenarios, threat scenario campaigns, and presents clear and detailed information of how each

Risk Analysis

At this point of the process, the asset inventory has been populated, the current and the target states are defined, and the threat gathering has been completed. With all of those previous points covered, risk analysis can be undertaken.

Influences Contribution

- **ISO 27001:** The standard provides a methodology to perform a risk analysis in any IT system
- **IEC 62443:** The standard moves the methodology provided by ISO 27001 enhancing it towards the ICS requirements. It also recommends the approach of conducting a first high level risk assessment scoping the whole ICS, and following this, perform a more detailed risk assessment (based on the first part of the assessment) using simpler system models defined in the current and target definition. This two level approach can simplify the risk impact and likelihood classification (using the first high level risk assessment) and then help address the high level risk to a more specific part of the IACS
- **NIST:** Provides good practice for risk analysis (likelihood determination, impact analysis) and heat matrix elaboration (risk determination)
- **ENISA:** Provides good practices in risk criteria selection, which serves to achieve more accuracy determining the risk in each case
- **CPNI:** Establishes the difference in the analysis, between the risks and impact to the HSE[3] as well as those with economic impact. It provides good practices for the likelihood assignation methodology

1 https://www.ncsc.gov.uk/guidance/10-steps-secure-configuration
2 https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
3 Environment, health and safety

Risk Mapping Table

In order to be able to perform analysis on the risks, all risk should be included in a table along with all the needed attributes in order to:

- Identify each risk
- Define briefly each risk
- Indicate the zones of the IACS affected by the risk
- Show the impact degree of the risk. This can be expressed in health and safety, or in economic impact. (Following CPNI principles, HSE impact will always have a higher priority for treatment than the economic impact)
- Show the likelihood of the risk. In consensus with the IACS owners, the probability of the occurrence of each risk has to be estimated
- Define the risk stakeholders. New responsibilities have to be defined in order to cover the discovered risks, for example, if remote SCADA location network security is not properly managed, a stakeholder has to be defined to ensure the network is managed

Risk Impact

The definition of the risk impact can be approached in two different ways. Using a quantitative approach[1], the definition of the risk is objective. This is supportive when prioritizing the risk in order to determine the order of remediation.

Using a quantitative approach poses the problem that it is not always easy to accurately translate the impact of a risk into a numeric expression. A numeric expression can be perceived as an absolute definition of the risk Impact, and used to automate the calculation of controls to be applied, or even the ROSI[2].

This framework considers that as a dangerous procedure, that can lead to situations where the cyber security problems are not only not treated, but also obfuscated.

To avoid the use of what is considered a dangerous procedure a qualitative approach can be used[3].

A qualitative approach will imply a certain degree of consensus with the management and asset owners, and will encourage a continuous process of refining the impact level definition. This process does not stop once acceptable levels of risk are achieved but continuous monitoring of both current risks and new risks is required.

To achieve a level of best practice, a mixed approach, using a quantitative definition of the impact in order to prioritize the risk's treatment order, in conjunction with a qualitative definition to address the controls needed for each of the risks is required. BSI Espion's methodology enables the business to present the risks in both an intuitive way (qualitative classification) and an accurate way (quantitative classification).

Risk Likelihood

The risk likelihood must use a quantitative approach, as it is impossible to establish accurate predictions for future events. A quantitative approach can be taken using historic data to help facilitate future predictions.

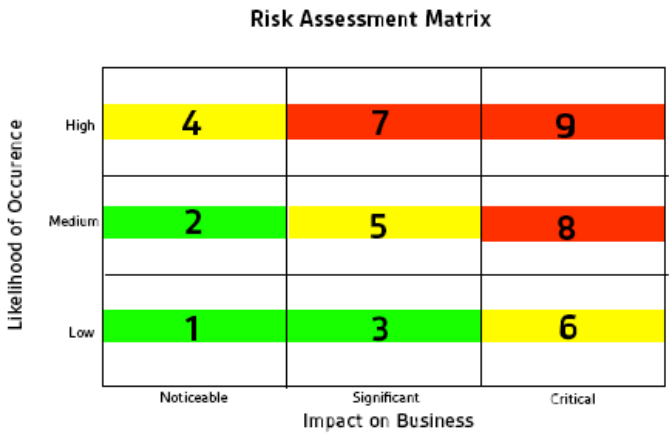
Risk Priority

Using the defined values of the risk impact and the risk likelihood, the risk priority is defined as a combination of the below.

Risk Mapping

After having all the risks in a detailed table and defining the priority and criticality for each of them, a heat map can be built. The heat map is a matrix that shows all the risk with a color code, going from green to red which provides a visual way to distinguish the collection of risks into:

- The ones which need to be treated as soon as possible
- The group that can be added to the midterm treatment plan
- The residual risk group that can be included in a long term treatment plan



1 The quantitative approach uses numeric expressions to express the weight of the risk
2 ROSI: Return on Security Investment
3 The Qualitative approach uses adjectives to define the weight of a risk, adding some degree of subjectivity to the definition

Remediate

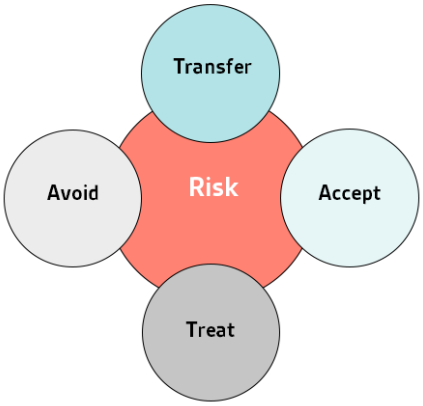
After Risk determination and prioritization, the appropriate remediation has to be designed for each of the risks.

Influences Contribution

ISO 27001

The standard provides a detailed methodology for the risk treatment plan implementation, starting with the remediation classification. In general, all remediation actions fell into one of those four categories:

- **Transfer:** This remediation consists of implementing a strategy that shares or transfers the risk to another party or parties, such as outsourcing the management of physical assets, developing contracts with service providers or insuring against the risk. The third-party accepting the risk should be aware of and agree to accept this obligation
- **Accept:** Accepting a risk consists of making an informed decision, usually at board level, that the risk rating is at an acceptable level or that the cost of the treatment outweighs the benefit. This option may also be relevant in situations where a residual risk remains after other treatment options have been put in place. No further action is taken to treat the risk, however, on-going monitoring is recommended
- **Treat:** This remediation consists of implementing a strategy that is designed to reduce the likelihood or consequence of the risk to an acceptable level, where elimination is considered to be excessive in terms of time or expense
- **Avoid:** This remediation consists of deciding not to proceed with the activity that introduces the unacceptable risk, choosing an alternative more acceptable activity that meets business objectives, or choosing an alternative less risky approach or process



IEC 62443

This standard breaks down remediation (under the threat category) into three element groups:

- **People:** including senior management, staff, contractors and other personnel who develop, follow, implement, enforce and manage all components of the ICS cybersecurity program
- **Processes:** which comprehend the policies, procedures, forms, business processes, and other documentation associated with the ICS Security Management System
- **Technology:** which includes all the technical security controls in place to uphold the system's availability, integrity and confidentialityaccept this obligation

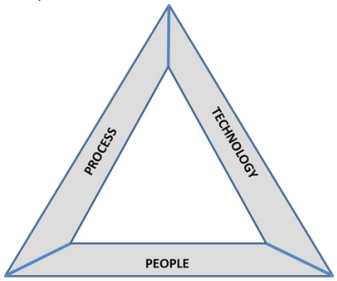
The goal of this sub-classification is to remark the need for balance in those three aspects. The standard presents the three aspects as the three sides of a triangle (see image below). Any remediation has to scope equally the three aspects of the triangle to be effective.

Antivirus software is a typical example to illustrate the importance of the security elements triangle. This remediation will only be effective if the three sides of the remediation triangle are covered:

- **People:** Trained individuals must be assigned the responsibility of managing the antivirus technology, and be accountable for performance
- **Processes:** The appropriate policies must be in place covering the antivirus tool deployment, maintenance, etc.
- **Technology:** The antivirus tool should be properly configured and updated to achieve the optimal performance

If Antivirus remediation covers only technology and processes, it will lose effectiveness quickly, as qualified employees will be accountable. Similar outcomes are obtained when any other aspect is not covered.

NIST: The institute provides control recommendations, which can be used to fit in the remediation framework provided by ISO 27001 and IEC 62443.



Benchmarking

The traditional approach of benchmarking against the matured standards/papers has a Boolean nature. It consist of a checklist, in which the standard/paper recommended controls/remediation have their presence checked.

This paper, however, proposes a new approach to benchmarking. In this new conception of benchmarking not only the standard/paper recommended controls will be check listed, but also, in a second level, a collection of threats and threat scenarios are checked against the existing check listed controls. By performing a second level benchmarking, the residual risk will be also conducted, and as a result, a new level of risk assessment (applied to the residual risk) can be performed if required.

After this first level of the benchmarking has been completed, the second level takes place adding another phase for each of the previously benchmarked controls/ remediation.

At the new depth, controls are benchmarked against a collection of threat scenarios composed by a number of threats. The aim is to show if each of the threats are covered by a control, whilst analyzing the residual risk.

Influences Contribution

- **NIST:** Provides remediation collections in a wide range of applications (IT, OT etc.) which can be used in the control check list
- **ENISA:** Provides methodologies to identify residual risk
- **CPNI:** Provides methods to collect threat vectors, grouping them in to threat campaigns, and further than that, into threat scenarios

Threat scenarios will never cover the full scope of the threats, (as new threats and threat scenarios are being populated constantly) but this kind of approach can reduce the risk significantly, and is designed as part of an on-going process. The process will be updated periodically, benchmarking the controls against new threats and threat scenarios as they are discovered and gathered, further reducing the overall risk.

Program Maturity

A common mistake often made is to address cybersecurity as a project with a start and an end date. When projects have an end date, security levels often decline over time.

Cybersecurity risks constantly change as new threats and vulnerabilities surface along with ever-changing technology implementations and security misconfigurations. A new approach is required to sustain the security gains and keep risks reduced to an acceptable level.

Our framework feeds from ISO 27001 and IEC 62443, both of which recommend developing and implementing an organization-wide cybersecurity management system (CSMS) which will include provisions to reassess risk and take corrective actions to eliminate the tendency for security levels to decline over time, meaning that the security posture is mature and maintained.

Organizations often have different processes and means of arriving at the CSMS. This is defined by the organization's objectives and risk appetite. Often it requires a cultural change that it is not always quick to acquire. Arriving at a fully implemented CSMS can be considered as the necessary evolution process that standardizes the approach to cybersecurity in line with best practice.

The security practices to be implemented must be proportionate to the risk level and will vary from one organization to another. The individual policies and procedures may also be different for each class of system within an organization as levels of risk and security requirements often differ.

Influences Contribution

- **ISO 270001:** Introduces the Plan Do Check Act (PDCA) model to enable an ongoing nature to the cyber security assessment
- **IEC 62443:** Provides a detailed methodology to measure the security life cycles, and to monitor and improve the CSMS as well
- **CPNI:** It provides useful best practices for continuous improvement, such as a constant improvement cycle, which enables the cyber risk assessment loop

Conclusion

There are three main conclusions that can summarize the core principles of this paper:

Best of breed: The framework is influenced by the two most successful cybersecurity standards that can be found today, (ISO 27001 covering IT and IEC 62443 covering OT). The collections of best practices and recommendations of ENISA, CPNI and NIST enrich the framework with updated feedback about the new threats the industry is facing, and the most recommended controls to remediate the first ones. The final result is a framework that scopes IT and OT systems, with updated information about the threats and remediation.

Continuous improvement process: Both ISO 27001 and IEC 62443 understand cybersecurity assessment as a continuous process, which needs to be maintained and monitored in order to obtain the best outcome in the general basis. The framework shares that vision and translates it in its final step "program maturity" which determines the periodicity of it. That is also reflected in the PDCA and security life cycles.

Risk Based Approach: This framework is aware that each potential target of a cybersecurity assessment has different security targets. The definition of the target state comes with the non-treated risk22. The risk appetite of a company (the non-treated risk a company can accept by default) depends greatly on their business type. BSI Espion has found that usually government driven companies have low risk appetite, whereas a private company with intrinsically "risky" involvement (for example, subsea natural gas exploration) will have much higher acceptance for risk. BSI Espion's framework is able to address a wide range of risk appetites, with the very definition of the Target state. The best practices from NIST, CPNI and ENISA provide tools to transform the risk appetite in to more understandable variables (like economic impact); in order to achieve in an accurate manner the risk based approach with a cybersecurity assessment

This paper concludes that the cybersecurity framework is defined as an assessment capable of addressing different system types (IT, OT), with potential customization for risk appetite. Using information feeds from organizations like NIST, ENISA and CPNI to maintain and update this model of the ever-evolving threats and countermeasures means that business can protect their IT and OT networks against actual cybersecurity threats.

References

- **ISA 99. Industrial Automation and control systems security (IEC 62443)** https://www.isa.org/isa99/
- **ISO 27001 Information security management.** http://www.iso.org/iso/iso27001
- **Frost&Sullivan report ICS cyber-security** http://ww2.frost.com/news/press-releases/need-efficient-cybersecurity-innovations-evident-every-sector-says-frost-sullivan/
- **Arc web market analysis on Electric power industry SCADA** https://www.arcweb.com/sites/default/files/Documents/study-brochures/study-scada-electric-power.pdf
- **SANDIA National laboratories. SCADA cyber-security report** http://energy.sandia.gov/energy/ssrei/gridmod/cyber-security-for-electric-infrastructure/scada-systems/
- **Riptech SCADA vulnerabilities White paper.** http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf
- **U.S. Homeland Security presidential directive. Identification and protection of the critical infrastructure** https://www.dhs.gov/homeland-security-presidential-directive-7
- **U.S. Department of energy. Recommendations on SCADA network cyber-security** https://energy.gov/oe/downloads/21-steps-improve-cyber-security-scada-networks
- **U.S. Homeland security. National infrastructure protection plan** https://www.dhs.gov/national-infrastructure-protection-plan
- **U.K. CPNI home page. Critical infrastructure Cyber-security topics** https://www.cpni.gov.uk/
- **White paper on a switch-board tool for authorized secure SSL/TLS connections** https://pdfs.semanticscholar.org/6f84/a63ced725a891bb6ff4352ba96a3731adfdb.pdf
- **IEC 62351 cyber-security Standards for power system information infrastructure h**ttp://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf
- **NIST Industrial control system cyber-security guide** http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- **EADS SCADA threat landscape whitepaper** http://ewic.bcs.org/upload/pdf/ewic_icscsr13_paper4.pdf
- **Eclipse open source SCADA** http://www.eclipse.org/eclipsescada/
- **U.S ICS cyber-emergency response team** https://ics-cert.us-cert.gov/
- **Cyber-X White paper on data exfiltration from ICS using Black Energy malware** http://get.cyberx-labs.com/blackenergy-report
- **Symantec Stuxnet malware White paper** https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- **A review of cyber security risk assessment methods for SCADA Systems.** http://www.sciencedirect.com/science/article/pii/S0167404815001388

Cybersecurity and Information Resilience services

Our Cybersecurity and Information Resilience services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

We can help organizations solve their information challenges through a combination of:

Consulting

Cybersecurity and information resilience strategy, security testing, and specialist support

Training

Specialist training to support personal development

Research

Commercial research and horizon scanning projects

Technical solutions

Managed cloud solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CSA cloud security alliance℠

bsi.

Find out more

Call UK: +44 (0)345 222 1711

Call IE: +353 (0) 1 210 1711

Visit: bsigroup.com