Critical Infrastructures Cybersecurity: recent developments, trends, and challenges *

Henrique Santos[1 [0000−0001−5389−3285]]
André Oliveira[1 [0000−0001−6217−5592]] and Paulo Moniz[2]

[1] Universidade do Minho, Centro Algoritmi, Guimarães, Portugal
https://algoritmi.uminho.pt
{hsantos,asoliveira}@dsi.uminho.pt
[2] Eurodefense, Portugal
moniz.paulo@gmail.com

Abstract. The latest developments in ICT (Information and Communication Technologies) have brought numerous opportunities to improve and increase the efficiency of various systems, including those classified as CI (Critical Infrastructure) systems. But in addition to the benefits, new challenges arise that, if not adequately addressed, can result in catastrophic accidents. One of the biggest challenges is Cybersecurity. In this paper, we seek to identify the best and worst that has been done in this field, seeking to identify the Cybersecurity model(s) that best respond to these challenges.

Keywords: Critical Infrastructures · Cyber security · ATT&CK · Risk Analysis.

1 Introduction

The CI (Critical Infrastructure) acronym refers to a complex, interconnected network of physical and logical components composing systems that are essential for the functioning of our daily lives. These systems provide vital services and support several sectors, including energy, water supply, transportation, communication, healthcare, emergency, and finance. Disruption in any of these services, even if isolated but persistent, can cause considerable damage, which gives this threat a very high-risk level. Different countries assume slightly different definitions, classifications and approaches. But all share the same concern, even if adopting more solo approach strategies than desired, as the impact of incidents in this context can affect several countries when there are shared distribution chains [33].

With no surprise, all nations have some initiatives, legal, regulatory, or standardisation, to control the level of resilience with which CIs are operating. For example, the European Committee created the European Program for Critical Infrastructure Protection (EPCIP)[3], aiming to develop an adequate framework

* Supported by organization x.
[3] https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en

for protecting CIs in all member countries. The USA has an agency dedicated to the sector, CISA (Critical Infrastructure Systems Agency)[4]. For its part, the UK opted for a more ample authority, NPSA (National Protective Security Authority)[5] which works together with its National Cyber Security Center (NCSC)[6] to put into practice CI's protection policies. Given the recent escalation of incidents involving critical infrastructure, even the United Nations decided to include a dimension associated with this problem in its strategic program for sustainable development until 2030 [37]. Overall, the general concern with the resilience of CIs is evident and logical.

Globalisation and recent geopolitical changes have led to an increase in the perception of risk and the consequent adaptation of how CIs are being protected. Clear evidence is the evolution of Europe's 2008 ECI Directive, which focused on identifying, classifying and assessing the level of individual protection, to the 2022 CER Directive, which focused more on the resilience of critical entities. This vision concentrates more on maintaining minimum operating conditions in the face of incidents rather than protecting individual assets [41]. The analysis of this change must be considered within the evolution of ICT in recent decades.

The rise of the Internet of Things (IoT) paradigm and the development of technologies like Artificial Intelligence opened the attack surface on computer-based applications. New ways to access components, including remotely, more complex and obscure software stacks, poor security-by-design practices, market pressures, and demand for new operational scenarios like remote maintenance and twin-based solutions, are among the emerging facts that make systems more vulnerable and exposed [47]. Furthermore, users and operators are frequently not experts missing the skills to operate securely this level of technological evolution and complexity, or even understand the threats systems are exposed to [20].

Unsurprisingly, cybercrime has also emerged as a severe threat in this evolving context. Not only because the range of opportunities is wide and the results obtained are rewording but also because the perception of the risk of being caught is relatively low. From Social Engineering to the so-called Advanced Persistent Threats (APT), which require technical skills and considerable resources, the examples have proven to be harmful and difficult to contain, not least because the imbalance of forces between those who attack and those who defend is very unfavourable for the last [32, 19].

Some relevant aspects are highlighted in this brief introduction to a very complex problem. The context dynamics and, in particular, the speed with which the threat landscape changes require an approach based on risk management. In this process, measuring all aspects of the Information System related to cybersecurity is essential. Only through an appropriate metrics program will it be possible to correctly assess the efficiency and effectiveness of security controls and effectively manage security. But for all of this to be implemented and operated, it is still necessary to resolve the gap created by the need for more knowledge about

[4] https://www.cisa.gov/
[5] https://www.npsa.gov.uk/
[6] https://www.ncsc.gov.uk/

cybersecurity that exists, especially at the operational level and, in particular, in CIs.

In this paper, we aim to contribute to a solution for this challenging problem. In section 2, we present a synthesis of the main cybersecurity concepts, using the most recognised standards, and a survey of the main approaches to cybersecurity in the context of CIs; in section 3, we address the cybersecurity metrics problematic, seeking to characterise what a metrics program for CI can be; in section 4, we address the foremost applicable standards, exploring a continuous certification model appropriate to CIs; finally, in section 5, we conclude with some considerations about the potential application of the models discussed in real environments and the challenges we face.

2 Fundamentals and existing approaches

The ISO/IEC 27000 standard establishes a set of fundamental concepts widely recognised by the community in general. Below, we summarise a small subset of these concepts, essential to frame the work presented in this paper [45]:

Information Security It is a process aiming to preserve a given set of properties or objectives relevant to information security; more specifically, it aims at the "*preservation of confidentiality, integrity and availability of information*" [25, pp. 6]:
- **Integrity**, to ensure information **is not modified** or **created** in an undesirable way;
- **Confidentiality**, to ensure information **is available only** to legitimate subjects;
- **Availability**, to ensure information **is available** whenever we need it; and
- **Others**, which is a placeholder for properties deriving from the above three, whenever **security objectives** are more specific; this is particularly relevant with integrity and confidentiality since the concepts are too abstract (e.g., assuring ownership and authenticity is probably critical for healthcare information, and both are related to integrity).

Threat A **possible cause of damage** in one or more security properties. When analysing threats it is possible not be aware of their origin, or how an accident might occur. Threats are frequently linked to security properties. However, they can also arise from the perception of the existence of an Information System's weaknesses, or even a dangerous contextual situation.

Attack Any malicious action or group of actions, intentional or not, that will **offend one or more security properties**, causing some harm to the Information System. Attacks may be executed by external or internal agents. When analysing possible attacks, we usually start with a relevant threat and in all possible ways it can be came into effect.

Vulnerability Any **flaw** or **weakness** existing in the Information System, which can be explored by a possible attack.

Resource Any asset that has **value** to the organisation. Knowing that value is crucial to define the impact of a total or partial loss. With intangible resources it is a considerable challenge to define it.

Risk Result of **uncertainty on security objectives**, when the Information System faces deviations from the correct behaviour. Uncertainty is related to a deficit of knowledge about events, their consequences or likelihood. Given the nature and variety of the events, that deficit may be impossible to overcome.

Security Controls All the measures we can take to **mitigate the risk**. It includes **policies, guidelines, procedures, and practices**. Their nature can be **administrative, technical, management, or legal**. Frequently, they are also referenced by safeguards or countermeasures. The ISO/IEC Standard 27001 [24] defines a set of security controls' classes, linked to several security objectives and a large number of specific controls. About half of those controls address technical issues, while the other group address organisational issues. Despite the relevance of this standard, there is no general consensus about its benefits. Frameworks like the SP 800-53 [35], or the CIS Critical Security Controls (CIS Controls) [10], among a few others usually promoted by private companies selling security related services, are frequently considered useful alternatives.

In addition to the above generic and standard definitions, the area of Critical Infrastructures has been studied in depth from a scientific point of view. Safeguarding critical resources and their governance, in particular, still requires a great deal of research. From systems theory to entropy phenomena, **resilience** and **reliability**, all related concepts need adjustment when applying them to the complex systems that make up CIs, especially when including their dynamic nature, interactions between systems and rapid technological evolution – CIs are frequently referred to by SoS (Systems of Systems) to rise a focus on complexity. Concerning the interaction between CIs, it is now recognised that the principles of cybersecurity management, which are fundamental to individual survival, must be expanded to governance models that guarantee collective survival. The challenges are increasing in this dimension, given the need to incorporate broader political, economic and social models [21].

2.1 The IT and OT dichotomy

Within the cybersecurity field, the origin of efforts that led to the definition of the above concepts has always been linked to using Information Technologies (IT) in organisations where data is the most critical asset. However, the digital technology revolution also affected industry in general and critical infrastructures in particular regarding Operation Technology (OT). The objective was clear: to increase the efficiency of production processes taking advantage of the IT evolution, a paradigm that became known as Industry 4.0. But from a cybersecurity perspective, and despite the similarities arising from using identical technological stacks, the context is quite different. For example, while in IT the

most critical properties are often integrity and confidentiality, in OT the focus is more on availability and safety [22]. Even the standardisation efforts for both areas follow different paths, highlighting the different perspectives [16] – we will address this topic further in section 4.

Furthermore, in many cases, the OT components (like OPC, Scada, and PLC) were developed with the assumption of using closed systems without security concerns regarding external access, much less via public networks such as the Internet. Suddenly, the technological components that make it possible to promote increased process efficiency imply flexibility in access and interaction, in large due to integration with IT, with a consequent threats increase. Worse still, the OT components cannot be simply redesigned with the same ease as their IT counterpart, as they include legacy components that have operated correctly for many years and whose eventual alteration would endanger the production process itself [4]. Naturally, we began to witness the emergence of a discipline in cybersecurity for OT that is still in development, with numerous challenges of its own [49]. Nevertheless, the main guides and good practices in both domains are clear and aligned when pointing to Risk analysis-based solutions as preferential options.

2.2 Cybersecurity approaches in CI

CI systems have always been the target of intense research. Failures in these systems, both isolated or in cascade mode, can cause considerable damage in general, and safety becomes a primary concern. Making such systems resilient and assessing how that is being accomplished has been a main research goal for a long time. In this context, resilience can be defined as a system's quality that reflects its ability to reduce vulnerabilities and resist to harmful events, ensuring an acceptable level of operation and adapting appropriately to this type of event. Assessing the level of resilience is an ambitious goal that involves several dimensions (e.g., performance, loss, and responsibility), being a fundamental component of trust and certification [43, 11, 36].

We can find various surveys in this area, including the cybersecurity perspective. Most of these studies reveal the main players' perceptions, with strategies usually focusing on giving greater visibility to production control systems indicators, promoting cybersecurity risk management and assessment approaches, and investing in education and awareness programmes for all employees involved in IT, OT and their integration. Employees and related personnel are usually considered the most risky resource [17]. The lack of resources, particularly qualified human resources, compromises other possible cybersecurity controls by limiting their proper use, making education programs a primary concern.

When approaching complex systems (SoS) like CIs [21], we need to use models that reduce complexity to a workable level by simplifying some dimensions. As George Box stated, "*all models are wrong, but some are useful*" [6], meaning that the simplifications introduce errors that can be severe, but sometimes that is all we can get to solve a real problem.

In [2], the authors survey and analyse several modelling techniques used to approach CIs protection from cybersecurity threats. Among other possible classifications, they use one oriented to the nature of the models used, dividing them into (in descending order of frequency of use): empirical, network-based, agent-based, system dynamics, and others. The empirical class encompasses a large number of solutions that follow more holistic specific approaches. The network-based and agent-based solutions are focused on technology and align with a usual model in the IT sector. The solutions oriented by system dynamics focused on the issues related to interactions between different systems that are interdependent on their operation. No matter the relevance of each of the above classes, a real CI usually demand extensive hybrid solutions. Furthermore, the authors acknowledge the importance of risk management-based approaches and point to a very recognised guide that inspires a large number of initiatives: the National Infrastructure Protection Plan (NIPP) plus the CI Risk Management Framework (RMF), which is commonly referred to by NIPP-RMF [13].

The NIPP-RMF model is illustrated in Figure 1. It follows a traditional Plan-Do-Check-Act (PDCA) cycle. The first three phases are typically found in any risk assessment model, corresponding to the analysis and **plan** task. The implementation phase (**Do**) is self-explanatory, and the measure phase aims to **check** the effectiveness of the security controls. Finally, the feedback paths suggest the necessary adjustments (**Act**) in any phases following directions dictated by observing the measurements. But there are some more innovative aspects to this proposal, such as:

- it approaches the cybersecurity objectives in three dimensions: physical, cyber, and human. However, as the crossed lines between phases suggest, there is no clear separation between those dimensions, and the objectives are frequently mixed.
- it proposes continuous monitoring and adjusting operations in the check and act phases to fulfil the real-time safety requirements of CIs (section 4.1 goes deeper into this topic).

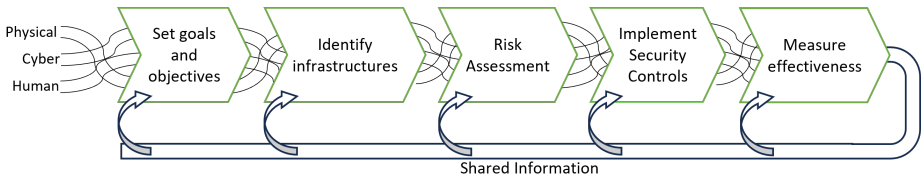

Fig. 1. NIPP-RMF model organisation for CI (based on [13])

There has been a growing interest in model-based safety assessment techniques (MBSA) applied to CIs in recent years. These methods are based on a

single safety model of a system, and analyses are carried out with a high degree of automation, thus reducing the most tedious and error-prone activities that otherwise would be performed manually. Formal verification tools based on model checking have been extended to automate the generation of artefacts, such as Fault Trees and FMEA (Failure Mode and Effect Analysis) tables, which are usually required to certify safety-critical systems. A distinguishing feature of some existing approaches to MBSA is the possibility of automatically injecting faulty behaviours into a behavioural model based on fault specifications taken from a fault library – typically using a computer simulation tool [29].

2.3 Key competencies for CI Cybersecurity

In the previous approach to the problems and solutions associated with CIs, it is clear that organisations need to provide human resources with specific skills. This need is evident in the effective use of tools to analyse and implement specific properties, such as cybersecurity, resilience or safety, and the operation of 'new' production systems that have disruptively integrated ICT. There is a whole ecosystem that forces us to think and act differently. In this section, we will systematise the research work already done on this topic.

Several initiatives have sought to respond to cybersecurity professionals' demands in recent years. Due to their consistency, maturity and scope, some deserve special mention: NICE - coordinated by NIST in the USA -, the Joint Task Force (JTF) on Cybersecurity - involving ACM, IEEE, Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) Education -, CyBOK - an initiative led by universities and companies in the UK -, and the European Cybersecurity Skills Framework (ECSF). All these initiatives developed frameworks that significantly contribute to the curricula coming up worldwide [38]. Those frameworks are different in focus, but they all agree on the multidisciplinary nature of the Cybersecurity discipline and the necessity to complement education and training to accomplish the target of preparing an adequate workforce, particularly when addressing CIs [27].

In [9], the authors present a survey to identify and compare cybersecurity competency models aligned with CI protection requirements. They found a subset of common knowledge, skills and competencies divided into four categories: technical, managerial, implementation, and soft skills. However, there has yet to be an agreement about which ones are more critical. The technical skills include networks, computer architectures and software administration, along with the knowledge about related cyber threads. Soft skills include information sharing and communications, work habits, and situational awareness; the relationship between these skill types and cybersecurity in job performance is evident. Implementation skills are more specific to cybersecurity controls, including vulnerability management and incident response; the level of knowledge and competencies vary according to the possible role, from operator to administrator. Management skills are typically required for chief-related jobs; they are

essential for risk management, workforce management, and evaluating controls' efficiency. Finally, this study points out the gaps between existing cybersecurity educational and academic programs and the industry needs in general and CI protection in particular.

To address the aforementioned education gap, in [8], the authors describe a set of training platforms with practical exercises very close to real-life scenarios. These platforms prove to be more effective in developing the necessary skills. Most of these platforms use simulators. However, once again, there is still no single understanding of the type of exercise to use, especially when we want to achieve different levels of competencies – it is desirable to integrate these exercises into more comprehensive curricula when the necessary background knowledge needs to be guaranteed, and this articulation is not considered yet. On the other hand, given the specificities of each application area, the development effort for these platforms is very high if we have to do it separately for each one.

In conclusion, specific training in platforms is fundamental. Still, since it is not possible to integrate this training into the general cybersecurity academic path, an additional effort is needed to articulate the different education programs in question (e.g. giving practical training in CI Cybersecurity Management only to those who have a postgraduate program in this area).

3 Metrics

Metrics, in general, can be described as quantifiable measurements of any specific and well-identified characteristic of a system or component. When applying the concept to cybersecurity, we expect those characteristics to emerge framed by **well-defined security objectives** [39]. As stated before, metrics are essential to assist the decision-making management process related to cybersecurity in any organisation. Some security experts defend that metrics are vital for monitoring, controlling, and managing security aspects of information systems, which today are the principal support of a broad range of organisational processes [7].

The terms metrics and measurements are frequently used interchangeably within the cybersecurity community. The measurement can be seen as an elementary data item that translates any observation over a given target. In turn, metrics are often derived from one or more correlated measurements, taking some threshold or reference value and aiming to assess and support a related decision-making process. In practice, the difference between metrics and measurements usually has no impact when implementing a security assessment program, and that is why standards devote little attention to that detail. With a much higher impact, we should expect metrics/measurements to exhibit some fundamental properties [3]:

- **Being meaningful** in a given context. It should capture and transmit the target system's relevant attributes.
- **Objective and quantifiable**. Even so, there are situations where qualitative metrics (more subjective) are the only real alternative.

- **Repeatability**. This means different actors will get the same results when doing the same measurements.
- **Sample frequency**, which should be adapted to the expected target modifications.
- **Cost of the metric/measurement** should never exceed the benefit value it produces.

Several works focus on metrics' attributes. The list is extensive and reflects different perspectives, application areas and goals. Even so, it is not difficult to find common aspects among those works, resulting in the above attributes, frequently referred to by the acronym SMART – Specific, Measurable, Attainable, Repeatable, and Time-dependent [46].

Equally intense has been the research into cybersecurity metrics in various fields of application, which reveals the complexity of the problem, starting with the lack of an effective classification [5, 40]. Many research institutions and governmental agencies have been working on developing and cataloguing security metrics in several domains. The Centre for Internet Security and The National Institute of Standards and Technology have proposed a taxonomy based on three high-level dimensions: management, technical and operational. They also highlight the **role of maturity** in the capacity to handle metrics properly [53]. Organisational or management metrics are related to organisational programs and processes, technical metrics are related to computing and networking devices, and operational metrics pertain to production systems in their environments [34].

This type of classification is helpful, but we need further help to find specific and usable detailed metrics. Those fine-grained metrics can be perceived with different levels of detail influencing their interpretation. The maturity level has a crucial role in that job. So, we will only be capable of managing cybersecurity if we get a minimum level of maturity to handle a metrics program properly. But, determining an organisation's level of maturity is, in itself, an equally difficult task. Despite the existence of some standards (such as ISO/IEC 21827) and some proposed models, there are few practical cases, and they are usually in specific contexts [42].

Increasing maturity involves education and training in cybersecurity and a deeper non-functional understanding of the business case and its supporting information systems – a time-consuming, demanding, and almost impossible task to systematise. Many impacting metrics require a high maturity level to handle them properly. In a five-level maturity model, as defined in [7], meaningful security metrics are captured starting at maturity level 3, as depicted in Figure 2. At that maturity level, organisations are usually capable of defining and handling implementation-oriented security metrics in any of the dimensions. Efficiency-oriented and business-oriented security metrics demand higher maturity levels since they require a deeper knowledge of incident effects in all dimensions.

Following the above model and given the critical infrastructure typical context, it is particularly important to focus on the operational and technical met-

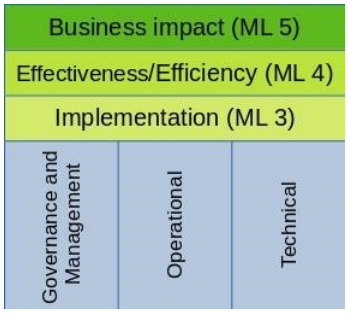

Fig. 2. Metrics taxonomy oriented by function and maturity level

rics. We next describe some possible entries in a hypothetical security metrics program on those dimensions for an illustrative purpose and put it all together.

Examples of security objectives, metrics, and related measurements

- Operational
  - Objective 1: Ensure business continuity
  - Metric 1: Average maintenance time allowed < 10 min
  - Measure 1: Maintenance time

  - Objective 2: Ensure that all devices/systems are supported by the supplier (bugs fixed)
  - Metric 2: Frequency of verification of device systems updates < 15 days
  - Measure 2: List of approved updates

  ==========
- Technical
  - Objective 3: Ensure network integrity and healthy
  - Metric 3: The number of TCP ports used equals the number of TCP ports registered
  - Measure 3: Number of open TCP ports

  - Objective 4: Control the data traffic by a period of time
  - Metric 4: Volume of data transferred by device and by a period of time bellow a given limit
  - Measure 4: Volume of data transferred by device

This simple example illustrates a consistent way to build a metrics program based on where it should be, on security objectives. Still, it also demonstrates the diversity of metrics that can be identified to meet an objective. It would be desirable to have a solid taxonomy of specific metrics, but most of the scientific

papers published on the subject show a great deal of dispersion and mostly holistic approaches. For example, looking at the taxonomy presented in [5] and the metrics used in the previous example, only traffic volume is part of the taxonomy, but the others, which make perfect sense, could easily be integrated into that reference. Therefore, it makes sense to use a more abstract classification, such as the one proposed by NIST (mentioned above) and leave the lower-level definition of metrics to each context. It will always be an iterative exercise, requiring a continuous increase in maturity, but it will guarantee a more effective cybersecurity management process.

Besides the obvious utilisation in monitoring and assessment functions, metrics help in the certification process, as they are devised to support informed statements towards alleged security states. These states should be defined in a meaningful standard. It turns out that related to the industrial sector, there are few certification processes and even less concerning Cybersecurity. Based on our previous research [44, 12], we will follow the ISA / IEC 62443 standard to approach a definition of a certification process, which will be described in the next section.

4 Standardisation efforts

Currently, standardisation efforts are essential to maintain stability and security in Critical Infrastructures. These efforts are characterised by the commitment to a set of requirements and definitions for specific components, systems or services that are expressed and published in a collection of documents and audited by a certified evaluator authority. A standard has the purpose of establishing some rigorous development process according to previously tested and documented requirements to determine a security level [15]. Traditionally, in these documents, the organisation under scrutiny describes their current and desired state, identifying and prioritising opportunities for improvement [12].

The European Telecommunications Standards Institute (ETSI) recognises that "cybersecurity standards are critical to the collective effort to prevent attacks in the first place and reduce the effectiveness of successful incursions" [14, pp. 1]. Therefore, various standard organisations have taken a proactive approach to develop, best practices, guidelines, and other resources to assist organisations in securing their data and systems. Some examples of the results of these approaches include cybersecurity standards like ISO/SAE 21434 [26], ETSI EN 303 645 [51], ISA/IEC 62443 [1], and ISO/IEC 27001 [24]. These standards and regulations promote the development and implementation of security requirements to protect organisations, critical infrastructures and consumers' products [14].

Due to some industrial paradigms, such as the digitalisation phenomenon and Industry 4.0, Information Technology and Operational Technology are now much more aligned than in the past. Specially dedicated to the IT security field, we have the ISO 27001 standard, part of a large series of standards focused on information technology, security techniques, privacy, incident response, and risk management. This standard was developed to manage the cybersecurity princi-

ples for the information technology field and covers organisations of all sizes and sectors focusing on the assessment, mitigation, and certification of cybersecurity [14]. This standard is continuously updated to align with the dynamic nature of cybersecurity, and the threats and vulnerabilities landscape.

Since IT and OT are much more aligned in the industrial sector, the surface of cybersecurity threats and issues increased, and nowadays, ISO 27001 does not provide an adequate response. One emerging standard that can cross both fields is the ISA/IEC 62443. This standard was originally developed by ISA 99 committee initiative to establish an in-depth cybernetic defence benchmark for industrial systems. Today, the joint force of the IEC has the intent to be applied internationally and cross-industry, providing methods to manage risks related to cybersecurity threats in an automation environment being aligned with IoT technologies [30].

ISA/IEC 62443 was developed as a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and Control Systems (IACS) and includes detailed technical control system requirements (SRs) and Requirement Enhancements(REs) for IACS related to seven Foundational Requirements (FRs), which all define the requirements for control system capability Security Levels (SL) and their components. The standard adverts split the IACS architecture into segments of zones and conduits, where this segmentation is a result of a Security Risk Assessment [12]. The 62443 collection is composed of 12 standards arranged into 4 packages that address several aspects or levels of IACS security, including system availability, protection of the industrial plant, and time-critical system response enforced by access control and network security requirements [12]. Given the characteristics of ICS environments, this standard could prove very useful in these contexts, like the Hydro Power Plant use-case described in [23].

4.1 Continuous certification

As stated before, an internationally recognisable security standard is probably the best tool to assign requirements and approach the security of systems, processes or devices that are part of an ICS in a Critical Infrastructure. After the adaptation of guidelines and best practices contained in the chosen international cybersecurity standard, the security level should be certified [50].

Generally, certification can be described as the process of verifying a property value associated with something and providing a certificate that can be used as proof of validity. Frequently, the certification process characterises itself as being complex, time-consuming, and expensive being available essentially to only large corporations. It is also a very slow process becoming difficult to go along with the technological development. The traditional certification schemes are usually "point-in-time" certifications with long periods of validity, and their schemes only require annual or bi-annual audits to obtain or renew a certification [28]. Therefore, aligning the rapid technological evolution to the highly demanding regulatory requirements and the growing trend of vulnerabilities and threats found in the industrial sector is reasonable to accept that a long-term audit is

not enough to testify to the conformity of a device, process or system with an international standard in the industrial sector. Therefore a valid solution, in this case, is to decrease the complexity of the assessments and therefore automate some parts, transforming the process into automatic continuous monitoring or assessment of the certification scheme.

Continuous certification is defined as a method that enables independent auditors to ensure a target quality level, using a series of auditors' reports issued virtually simultaneously with the occurrence of events underlying the target [31]. This concept allows an organisation to pay attention to the certified parameters and maintain the true validity of certification by reacting to changes or events concerning the subject matter. It also has the benefit of facilitating the job of an auditor developing reports to be used in assessing changes and events and in the case of renewing the certification. This model of continuous certification uses and establishes measurements and metrics relevant to assess the fulfilment of requirements needed for the certification process [52]. Through this scheme, organisations can establish an almost "self-certification" mode that captures techniques and procedures to assess whether something remains within the boundaries of its being certified. With proper metrics, it is possible to assess and detect when something either leaves or is in danger of leaving, certified boundaries [18].

Therefore, organisations are capable of maintaining the core concept of Industry 4.0 of developing interconnected adaptable manufacturing systems and securing industrial systems with constant real conformance to internationally accepted standards and regulations, enabling a more flexible and dynamic approach for security along the whole life cycle of industrial systems [15].

Establishing a certification scheme based on ISA/IEC 62443 standards in the industrial sector can help reach the abovementioned goal. The model represented in Figure 3 corresponds to a model to develop a framework of real-time analysis and monitoring, capable of continuously assessing a system, device, or component, improving its security level, and promoting the validity and conformance with an international standard previously certified [12].

Like most risk-based models, this one is based on a PDCA cycle to continuously improve the organisation's posture. If problems are detected, they need to be addressed immediately within the same cycle, by transforming specific information security requirements into something that can be managed and implemented [48]. Under ISA/IEC 62443 orientations, the process begins with a scope definition, which leads to clear demarcation of systems, security zones, and conduits. Next, there is a phase of risk assessment where the security controls and requirements are identified to properly address and mitigate risks. Once the requirements are identified, it is time to establish the desirable security levels, along with actual perceived levels and the necessary metrics to assess that transition. In the final stage, there is the selection of the necessary assessment mechanism(s). Mainly concerning technical and operations security objectives. In this last phase, we find the group of security objectives and metrics that need continuous assessment. Particularly those belonging to the technological and

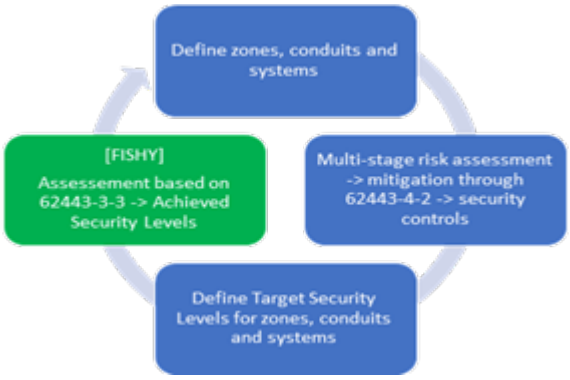

Fig. 3. Model of Certification Cycle

operational dimensions, once the organisational ones, which usually depend on policies, guidelines and regulatory provisions, require re-evaluations with much longer time cycles.

The proposed model is designed to promote a continuous improvement of the security parameters according to the security objectives defined. Implementing this model aligned with the IEC 62443 standard constitutes itself as an action that can empower trust and confidence, in a macro-perspective in organisations and establish trust-ware initiatives within the emerging complex supply chains.

5 Recommendations and challenges

The digital revolution that has taken place over the last few decades has brought enormous advantages to the way we produce, consume, transact and interact. All aspects of life have undergone remarkable transformations. There is no doubt that today, we can enjoy a better quality of life, with digitisation being a determining factor. The so-called Critical Infrastructures, which provide essential services for our way of life, are not excluded from this phenomenon.

But it is not all upside. One of the costs imposed is the need to guarantee cybersecurity, which is challenged by the increase in attack vectors, a considerable number of vulnerabilities created by very complex ITC systems that are not always adequately specified and developed in the context of an intricate cyber threats landscape. Managing cybersecurity risks has become an obligation, all the more relevant given the level of criticality of the systems in question. Devaluing this requirement is like storing critical resources in a cardboard box and hoping that no one will ever find them.

The scientific and professional community has endeavoured to respond to this challenge by creating a wide range of standards and rules to guarantee CI's resilience. However, the standards summarise what we should do, but not so much how we should do it. And in this case, the difference is enormous. In this

article, we identify three of these difficulties and point the way to (even partial) solutions.

One of the most significant barriers is the knowledge deficit. Employees traditionally involved in CI know the processes they work with very well. Still, the change imposed by digitalisation places contextual requirements on them that they must be aware of. These resources cannot simply be replaced, not least because new workers with more digital skills will need to acquire knowledge of the processes inherent in CI. In other words, a training plan needs to be put in place, either for current operational staff to acquire digital skills or for new hires who already have those digital skills but need to learn how to manage critical processes. It's an HR management problem, which will inevitably only bear fruit in the medium term. Worse still, no outsourcing services or equipment will provide a solution, although it may create the illusion.

Another important aspect is the risk management model to use. This paper discussed a possible model that fits the fundamental concepts of the reference standards in this area while providing some agility and simplicity. That is important since the model should be internalised by the organisation and not imposed as a new rule or regulatory provision. Good risk management should be experienced, not forced. One of the difficulties is recognising the most pressing threats, which requires a working knowledge of Cyber Intelligence - a new profile that will need to be incorporated into the organisation's management team and also implies changes to the governance model, which is another significant difficulty in itself. In the case of CI, there is also the need to continuously implement specific security monitoring measures, leading to a continuous certification scheme that can significantly impact the way cybersecurity perception is shared among stakeholders, addressing trust issues.

Finally, a Cybersecurity Management program will only be complete and valuable with the support of a set of appropriate metrics. The identification of these metrics stems from the correct definition of cybersecurity objectives, which, in turn, result from a thorough risk analysis exercise. Some metrics are easily identified (especially those linked to availability). Still, others require a high level of maturity regarding the deployed technologies and the security mechanisms in use or planned. Virtually everything observable can be turned into a metric, but identifying the set of effective metrics in cybersecurity management is a strenuous exercise. It is not expected that the security team, together with the other players, will be able to arrive at an optimal solution in the first iteration. As experience (maturity) with the use of protection mechanisms increases, more appropriate metrics should naturally emerge in subsequent cycles of reviewing the cybersecurity plan.

Acknowledgements This work has been supported by FCT – Fundação para a Ciência e Tecnologia within the R&D Units Project Scope: UIDB/00319/2020.

References

1. 62443, I. Security of industrial automation and control systems. *ISA/IEC 62443 Standard* (2019).
2. Ani, U. D., Watson, J. D. M., Nurse, J. R. C., Cook, A., and Maple, C. A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. In *PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT 2019* (2019).
3. Barabanov, R., Kowalski, S., Yngström, L., and Yngstrom, L. Information security metrics state of the art, 2011. Cit. 2 Scholar 4/2021.
4. Berardi, D., Callegati, F., Giovine, A., Melis, A., Prandini, M., and Rinieri, L. When operation technology meets information technology: Challenges and opportunities. *Future Internet 15* (2 2023), 95.
5. Bhol, S. G., Mohanty, J., and Pattnaik, P. K. Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings 80* (1 2023), 2274–2279.
6. Box, G. E., and Draper, N. R. *Empirical model-building and response surfaces*. John Wiley & Sons, 1987.
7. Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. Nist sp 800-55 revision 1 - performance measurement guide for information security, 2008.
8. Chowdhury, N., and Gkioulos, V. Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review 40* (5 2021), 100361.
9. Chowdhury, N., and Gkioulos, V. Key competencies for critical infrastructure cyber-security: a systematic literature review. *Information and Computer Security 29* (11 2021), 697–723.
10. CIS. Cis controls, 2022.
11. Curt, C., and Tacnet, J. Resilience of critical infrastructures: Review and analysis of current approaches. *Risk Analysis 38* (11 2018), 2441–2458.
12. da Silva Oliveira, A., and Santos, H. Continuous industrial sector cybersecurity assessment paradigm: Proposed model of cybersecurity certification. In *2022 18th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltrú, Spain* (3 2022), IEEE, pp. 1–6.
13. DHS, U. Nipp 2013: Partnering for critical infrastructure security and resilience, 2013.
14. Djebbar, F., and Nordström, K. A comparative analysis of industrial cybersecurity standards. *IEEE Access 11* (2023), 85315–85332.
15. Ehrlich, M., Trsek, H., Wisniewski, L., and Jasperneite, J. Survey of security standards for an automated industrie 4.0 compatible manufacturing. In *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society* (10 2019), IEEE, pp. 2849–2854.
16. Felser, M., Rentschler, M., and Kleineberg, O. Coexistence standardization of operation technology and information technology. *Proceedings of the IEEE 107* (6 2019), 962–976.
17. Filkins, B., Wylie, D., Institute, A. D. S. T., and 2019, U. Sans 2019 state of ot/ics cybersecurity survey, 2019.
18. Fisher, M., Collins, E., Dennis, L., Luckcuck, M., Webster, M., Jump, M., Page, V., Patchett, C., Dinmohammadi, F., Flynn, D., Robu, V.,

and Zhao, X. Verifiable self-certifying autonomous systems. In *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)* (2018), pp. 341–348.

19. Furnell, S., and Dowling, S. Cyber crime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice 5* (3 2019), 13–26.
20. Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., and Baker, T. Security threats to critical infrastructure: the human factor. *Journal of Supercomputing 74* (10 2018), 4986–5002.
21. Grosse, C. A review of the foundations of systems, infrastructure and governance. *Safety Science 160* (4 2023), 106060.
22. Hahn, A. *Operational Technology and Information Technology in Industrial Control Systems*, vol. 66. Springer New York LLC, 2016, pp. 51–68.
23. Heluany, J. B., and Galvão, R. Iec 62443 standard for hydro power plants. *Energies 16* (2 2023), 1452.
24. ISO/IEC. Iso/iec 27001:2013, information technology — security techniques — information security management systems — requirements. Tech. rep., ISO/IEC, 2013.
25. ISO/IEC. Information technology-security techniques-information security management systems-overview and vocabulary (international standard iso/iec 27000). Tech. rep., ISO/IEC, 2016.
26. ISO/SAE. Road vehicles - cybersecurity engineering, 2021.
27. Jaurimaa, J., Saharinen, K., and Kotikoski, S. Critical infrastructure protection: Employer expectations for cyber security education in finland. In *ECCWS 2021 20th European Conference on Cyber Warfare and Security, University of Chester, UK, 24-25 June* (2021), Academic Conferences International, pp. 195–202.
28. Knoblauch, D., and Banse, C. Reducing implementation efforts in continuous auditing certification via an audit api. In *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (2019), pp. 88–92.
29. Krishnan, R., and Bhada, S. V. Integrated system design and safety framework for model-based safety assessment. *IEEE Access 10* (2022), 79311–79334.
30. Leander, B., Causevic, A., and Hansson, H. Applicability of the iec 62443 standard in industry 4.0 / iiot. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (New York, NY, USA, 2019), ARES '19, Association for Computing Machinery.
31. Lins, S., Schneider, S., and Sunyaev, A. Trust is good, control is better: Creating secure clouds by continuous auditing. *IEEE Transactions on Cloud Computing 6*, 3 (2018), 890–903.
32. Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., and Holt, T. Cybercriminal networks in the uk and beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime* (2 2023), 1–24.
33. Mikhalevich, I. F., and Trapeznikov, V. A. Critical infrastructure security: Alignment of views. In *2019 Systems of Signals Generating and Processing in the Field of on Board Communications* (3 2019), IEEE, pp. 1–5.
34. Morrison, P., Moye, D., Pandita, R., and Williams, L. Mapping the field of software life cycle security metrics. *Information and Software Technology 102* (10 2018), 146–159.
35. NIST. Sp 800-53 rev. 5 security and privacy controls for information systems and organizations, 9 2020.

36. Osei-Kyei, R., Almeida, L. M., Ampratwum, G., and Tam, V. Systematic review of critical infrastructure resilience indicators. *Construction Innovation 23* (11 2022), 1210–1231.
37. Painter, C. The united nations' cyberstability processes: surprising progress but much left to do. *Journal of Cyber Policy 6* (9 2021), 271–276.
38. Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., Pereira, T., and Stavrou, E. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (7 2018), ACM, pp. 36–54.
39. Payne, S. C. A guide to security metrics, 2006.
40. Pour, M. S., Nader, C., Friday, K., and Bou-Harb, E. A comprehensive survey of recent internet measurement techniques for cyber security. *Computers & Security 128* (5 2023), 103123.
41. Pursiainen, C., and Kytömaa, E. From european critical infrastructure protection to the resilience of european critical entities: what does it mean? *Sustainable and Resilient Infrastructure 8* (1 2023), 85–101.
42. Rabii, A., Assoul, S., Touhami, K. O., and Roudies, O. Information and cyber security maturity models: a systematic literature review. *Information and Computer Security 28* (10 2020), 627–644. Scholar: 37 cit Dez.2023.
43. Rehak, D., Senovsky, P., Hromada, M., and Lovecek, T. Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection 25* (6 2019), 125–138.
44. Santos, H., Oliveira, A., Soares, L., Satis, A., and Santos, A. Information security assessment and certification within supply chains. In *The 16th International Conference on Availability, Reliability and Security (ARES 21), Vienna, Austria, August 17 - 20, 2021* (8 2021), ACM, pp. 1–6.
45. Santos, H. M. *Cybersecurity: a practical engineering approach.* CRC Press, 2022.
46. Savola, R. M. Towards a taxonomy for information security metrics. *Proceedings of the ACM Conference on Computer and Communications Security* (2007), 28–30. CORE A*Scholar: 92 cit 11/2023.
47. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., and Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials 20*, 4 (2018), 3453–3495.
48. Sun, Z., Zhang, J., Yang, H., and Li, J. Research on the effectiveness analysis of information security controls. In *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (2020), vol. 1, pp. 894–897.
49. Tinnel, L., and Lindqvist, U. *Importance of Cyber Security Analysis in the Operational Technology System Lifecycle*, vol. 666 IFIP. Springer Science and Business Media Deutschland GmbH, 2022, pp. 73–101.
50. Torens, C. Safety versus security in aviation, comparing do-178c with security standards. In *AIAA Scitech 2020 Forum* (2019).
51. v02, E. E. . . Cybersecurity for consumer internet of things. *ETSI* (2020).
52. Yahaya, J. H., Deraman, A., and Hamdan, A. R. The development of pragmatic quality model for software product certification process. In *2006 International Conference on Computing & Informatics* (2006), pp. 1–6.
53. Yusuf, S. E., Hong, J. B., Ge, M., and Kim, D. S. Composite metrics for network security analysis. *Software Networking 2017* (7 2017), 137–160.