Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs

Ludovic Pièrre-Cambacédès, *Member, IEEE*, Marc Tritschler, and Göran N. Ericsson, *Senior Member, IEEE*

***Abstract*—This paper presents and analyzes a selection of 21 "myths" identified from the authors' experience as being the most common in power utilities and the most harmful to their cybersecurity posture. For each one, tangible and referenced elements, typically sparse and dispersed, are presented in this single and up-to-date reference to support their rationalization. This paper also provides generic recommendations supporting power utilities on the ongoing and challenging process of dispelling the identified myths.**

***Index Terms*—Communication system security, computer network security, cybersecurity, power system, supervisory control and data-acquisition (SCADA) systems.**

I. Introduction

THE POWER infrastructure is undergoing profound and rapid evolution, driven by a growing energy demand, governance paradigm shifts, and increased penetration and dependence on Information and Communication Technologies (ICT). The systems in charge of the control and supervision of the power infrastructure reflect and enable these transformations: historically isolated, relatively simple, and proprietary, they are now becoming more complex and interconnected [1]. Real value is created in this process, from enhanced maintenance or faster decisions to completely new capabilities, embodied by smart-grid initiatives [2], [3] and advanced metering infrastructure (AMI) projects [4]. However, these new opportunities have to be considered with their inherent cybersecurity risks (i.e., risks associated with malicious activities on computerized and data assets). Cybersecurity is fortunately now identified as a top issue by most of the critical infrastructure operators and associated regulatory authorities worldwide [5]. Nevertheless, it is still a fairly new domain to power utilities' culture and personnel. People, skills, and behaviors change more slowly than technologies and infrastructures. This allows misconceptions and false beliefs to take root, weaving a web of modern mythology and creating a barrier to considered and appropriate cybersecurity posture.

In this paper, we discuss a selection of 21 "myths" identified from the authors' experience as being both the most common in power utilities, and the most harmful to their cybersecurity posture. The main objective is to provide tangible and referenced elements supporting their rationalization. "Myth-busting" is not a new task in our community (e.g., [6]), but it is of paramount importance, considering the growing gap between factual risks and vivid misconceptions.

This paper contributes to the ongoing process of dispelling these myths by collecting into a single and up-to-date reference, elements which are typically sparse, dispersed, and unverified. In Section II, 21 myths are individually presented and analyzed. Section III provides generic recommendations to foster action with regards to the myths described. In both sections, multiple examples and references are provided to support the message. Section IV concludes this paper.

Manuscript received January 27, 2010; revised June 16, 2010; accepted July 17, 2010. Date of current version December 27, 2010. Paper no. TPWRD-00062-2010.

L. Pièrre-Cambacédès is with the Electricité de France R&D, Clamart F-92141, France (e-mail: ludovic.pietre-cambacedes@edf.fr).

M. Tritschler is with KEMA Ltd., East Kilbride, Glasgow G75 0QD, U.K. (e-mail: marc.tritschler@kema.com).

G. N. Ericsson is with the Svenska Kraftnät (Swedish National Grid), Sundbyberg 17224, Sweden (e-mail: goran.n.ericsson@svk.se).

Digital Object Identifier 10.1109/TPWRD.2010.2061872

II. Twenty-One Cybersecurity Myths

The 21 myths have been grouped into categories, designating more generic issues in which they are rooted. Under each category, the myths can be closely related, and may even reflect different aspects of similar problems. The myths and categories are not presented in any order of priority.

A. Denial of Reality

1) "Industrial Control Systems (ICSs) are Isolated": The architecture of the electricity industry, involving continuous exchanges between generation, transmission, and distribution operations, but also market and planning systems, make claims of isolation very suspect. In fact, isolated systems are now absolute exceptions. Interconnectivity is part of the ICS genome, and the security of these interconnections should be managed instead of denying their existence. Moreover, isolation is not only about networked systems: removable media or laptops connected for maintenance purposes from one domain to another are classic examples, breaking the claimed isolation and opening the door to cybersecurity risks.

Isolation implies not only cautious technical implementation, but also a stringent and respected security policy. However, regular malware-related headlines provide good illustrations of supposedly isolated systems which were not, and suffered: the Davis–Besse nuclear power plant contaminated by the Slammer worm in 2003 [7] is a relevant example. In fact, malware is particularly efficient at discovering unnoticed connections between operational systems. In 2006, 13 Daimler-Chrysler plants were stopped by the Zotob worm [8]. In November 2008, the U.S. Department of Defense (DoD) issued internal directives to stop removable storage media being used, related to the infection of classified systems [9], [10]. The same month, the Conficker worm started one of the widest viral infections, contaminating more than ten million machines [11], including

0885-8977/$26.00 © 2010 IEEE
Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

supposedly isolated ones. Even space-earth distance may not provide sufficient isolation; the U.S. National Aeronautics and Space Administration (NASA) confirmed in 2008 that laptops carried onboard the International Space Station were infected by a virus [12], [13]. Computers, even on military bases, warships, or in orbit, are very rarely isolated.

2) "Nobody Wants to Attack Us": In the last century, despite some minor events (e.g., [14] and [15]), public opinion was not particularly aware of ICS cybersecurity risks. The first widely reported attack was the Maroochy Shire sewage system attack in Australia [16], [17]. Formerly employed as a contractor, the perpetrator attacked the sewage Supervisory Control and Data Acquisition (SCADA) system on several occasions after his job application was rejected. It led to 800 000 liters of raw sewage being spilled into the environment. Having internal and technological knowledge, he managed to disable alarms and interfere with wireless communications between the pumping and central stations [18], [19]. Although over-reported, this event has contributed to raising awareness of real-world consequences of ICS targeted attacks. Section II-A-5 develops this further.

Since 2002, presentations about ICS vulnerabilities are regularly delivered at open hackers events (e.g., [20]–[24]) and demonstrate the increased interest in this issue. Actual attackers' skills and interests are likely to be several years ahead of this work. Also, since 2006, a growing number of ICS vulnerabilities have been officially disclosed by national Computer Emergency Response Teams (CERTs). At the end of 2009, a basic search in the US-CERT vulnerability database [25] resulted in 24 SCADA-related vulnerabilities, all of them giving official status to pre-existing weaknesses. Some have also been integrated into mainstream penetration tools such as the Metasploit Framework [26].

Finally, there have been a number of claims from the U.S. of utilities being hacked with malicious intent [27]–[29]. Most of these claims are lacking in substance; however, even if public disclosure of actual attacks is still rare, a sufficient number of converging elements exist to conclude that ICSs have become attractive targets for various kinds of attackers, from recreational hackers to political activists, disgruntled employees, and criminal organizations. National and international organizations consider computer security as criminal and terrorist threat vectors to critical infrastructures [30]–[32]. A close relationship between the national security agencies, the critical infrastructure operators, and the cybersecurity community, in general, is needed to stay up to date and prepare to face those new risks.

3) "We Only Have Obscure Protocols/systems": Commercial-off-the-shelf (COTS) and classical Internet technologies are already well established in industrial environments. In terms of communication protocols, Ethernet and TCP/IP are now the choice by default, replaced only in case of specific requirements. Regarding operating systems (OS), classical IT systems have become ubiquitous: Microsoft and Linux can be found in all major ICSs, in engineering or monitoring stations and in embedded devices. Microsoft has begun a significant marketing push into the electricity industry by releasing its smart energy reference architecture (SERA) [33], which intends to place Microsoft technology at the heart of the future smart-grid architecture.

While it is difficult to establish statistics for the increasing penetration of COTS components in ICSs, the direction is clear: new projects inevitably replace custom components with COTS, and not vice-versa. Data formats and application layer protocols are no exception to this development, with XML playing a growing role in the industrial environment (e.g., OPC-UA [34]).

Furthermore, even that which seems to be extremely specific or "obscure" is often, in fact, openly documented. The classic power system communications protocols are defined in IEC or IEEE documents (see [35] and [36]). Industrial protocols, such as Modbus, not only have their specifications easily accessible [37], but are also well known by the hacker community [23].

Of course, there is still room for proprietary technologies in industrial environments; however, there is no guarantee regarding their intrinsic security (cf. Section II-C-1).

4) "Anti-Virus and Patching are Useless for ICSs": This common belief is often a consequence of two previously discussed misconceptions, those of "isolated systems" and "obscure protocols/systems." These combine to generate a new myth with respect to patching: believing that patches/updates are relevant only for COTS components. The fact is that security updates are now produced on a regular basis for most of the platforms and applications potentially found in the industrial context. "Patch Tuesday" may not be the best strategy for ICSs, but a thorough and adapted update policy, encompassing all kinds of systems, including ICSs [38], [39], is a fundamental part of an adequate and efficient defense in depth (DiD).

Anti-virus (A/V) is a different issue, as mature solutions exist only for a limited number of platforms. Windows platforms are presently the most targeted, but malware also constitutes a threat for other platforms. In 1988, the first Internet worm was, in fact, tailored for Unix-based systems [40]. Today, major A/V providers maintain signature databases for non-Microsoft OS like Linux: a basic query in such a database provides more than 1150 entries [41], including cross-platform viruses [42]. Finally, proof-of-concept worms especially crafted for SCADA and AMI systems have also been recently demonstrated [24], [43].

Relying on architectures based on various platforms with only partial A/V support should not lead to the decision not to deploy A/V, even in the case where the systems are not typically targeted by viruses. Unprotected vulnerable machines may create denial-of-service (DoS) situations when contaminated, impacting nonvulnerable systems by saturating the media on which they are connected.

5) "Cybersecurity Incidents Will Not Impact Operations": If the Maroochy Shire water station attack (cf. Section II-A-2) raised awareness about real-world consequences of ICS attacks, the Idaho National Laboratory (INL) Aurora experiment has more recently and strongly stressed this. Broadcast by a major TV news channel in 2007 [44], a prototyped cyberattack led to the destruction of a diesel generator, formerly used to supply power to the 13.8-kV distribution grid of the INL testbed.

While Aurora was an experiment, there are also real cases where incidents impacted operations at nuclear power plants. These incidents include malicious (but untargeted) worm attacks, and incidents due to poor management processes. The first of these is the previously mentioned Davis–Besse incident

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

in 2003 [7], where the "Slammer" worm resulted in plant computers being inaccessible for more than six hours (fortunately the plant was shut down for maintenance at the time). The second incident was at Hatch in 2008 [45]. An engineer was testing a software change on a plant data-acquisition server, not realizing that the software synchronized data tags between connected computers running the software. When the local tag values were updated by the engineer's test values, the changes were synchronized with controllers operating part of the plant, resulting in an automatic shutdown. If it is possible for these consequences to occur due to human error and a lack of understanding about the dependencies in the ICS, similar consequences are also possible due to deliberate malicious activity, even if that malicious activity is undertaken without a full understanding of the ICS.

6) "Social Engineering is not an ICS Issue": In the context of cybersecurity, social engineering designates low-technology efforts, aimed at extracting information from or triggering action by individuals [46], [47]. The term is commonly used when discussing criminal activity relating to mainstream ICT, and identity-related crimes. Many Internet users now have an understanding of the basic social engineering techniques and are reasonably well equipped to identify these attempts in Internet and personal ICT contexts; however, they are less likely to successfully identify when these techniques are used outside this context, especially if there is no direct risk to themselves. This is particularly the case when the initiating communication appears to be from a known source, or if a free gift is provided/offered, such as universal-serial-bus (USB) memory sticks [48]. These devices can carry malware and are as much of a risk to ICS as they are to mainstream ICT.

Several of these elements were used in a successful demonstration of a social engineering attack on a power company's SCADA system [49]. The attackers collected e-mail addresses of personnel working at the target power company from Internet user groups and SCADA mailing lists. Then they sent an e-mail (purporting to be an official company e-mail) to each of the harvested addresses, informing them about a plan to cut their benefits. The email included a link to a website where more detailed information was available. On clicking the link, the victims were taken to a website set up by the attackers, which downloaded malware onto the workstations. The attackers claimed that the malware would enable them to take full control of the workstations and the SCADA system.

B. Misplaced Trust in Security Technologies

1) "Our Firewall Protects us Automatically": Firewalls are among the most deployed security solutions. They are complex devices that have to be correctly configured and integrated into specifically designed architectures to turn their filtering capabilities into an efficient security barrier. However, simply having a firewall in place is not enough to ensure proper segmentation between two networks. In 2004, Wool presented the results of a study on corporate firewalls configuration: 80% of them had major misconfigurations [50], mainly due to the rules complexity. Moreover, the specificities of ICSs have to also be taken into account [51].

Even a correctly configured firewall is not enough, as it will never be able to protect against insiders, filter the content of encrypted connections, protect against connections that do not go through it (e.g., dial-up modems), protect against most viruses, or set itself up with a secure configuration.

It is very risky to ignore these basic facts, as a firewall may rapidly create an illusion of security. Also, it has to be part of an approach to security combining technical, organizational, and operational controls in a DiD manner. References [52]–[55] are helpful in this perspective.

2) "One-Way Communication Offers 100% Protection": Connections between highly critical ICSs and other security domains are sometimes acceptable, providing a "one-way communication." Unfortunately, such a requirement is very imprecise and can be implemented with different levels of security. As discussed in [56], communication direction restrictions between two domains can be enforced in three ways, based on the initiation of the communications, the content and useful payload "flow," and a strict one-way communication preventing even a single bit, including data flow control or synchronization signals, from going in the forbidden direction.

The nature and strength of the protection provided by each enforcement policy differs to a great extent. Only the first initiation-restricted policy can be enforced in a straightforward way with a basic firewall. The second needs packet inspection intelligence, while the third can only be realized through specific devices called hardware data diodes, which are radically different from firewalls. A survey of these solutions is provided in [56].

The security difference between the first and second policy is clear. In the first case, it is possible to prevent a direct connection from an attacker toward the protected zone, but the attacker can still piggyback on legitimate communication to cross the barrier. The second case is harder for the attacker, as it prevents him from introducing directly malicious content through regular mechanisms. The difference between the second and third may be less obvious, and a combination of the first two types of policy is sometimes considered to be the maximum security policy. Even if this can provide a high level of protection, network attacks are still possible: control and signaling data are authorized to enter the protected zone, where they are interpreted by devices, allowing potential malicious code execution. This is, for instance, the case for TCP, which is a two-way protocol by nature. An example is given in [56].

3) "It's Encrypted: It's Protected": Cryptography is fundamental in cybersecurity, both in terms of technical solutions and history [57]. Already ubiquitous in mainstream ICT, cryptography is now finding a growing place in ICSs. Nevertheless, the aura of mystery and the mathematics of the "science of secret" should not hide their limitations and prevent an objective view on its usage in the ICS context. Encryption is too often presented by vendors as being synonymous with security, and understood as such by unfamiliar users.

First of all, cryptography encompasses a large number of techniques, which are not equal in functionality or in strength. Only carefully vetted, standardized and up-to-date primitives and algorithms should be used. In general, governmental agencies provide complete and up-to-date recommendations (see, for example, [58] in France, or [59] in the U.S.). Beyond the cryp-

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

tographic primitives and algorithms themselves, secure protocols making use of cryptography [60], [61] should also be objectively considered. They have their own limits and are subject to weaknesses which are regularly disclosed publicly and addressed in new versions (e.g., [62]). Hence, it should not be forgotten that cryptography is just a component of technical architectures which are themselves part of an overall chain of security. Holistically, cryptography may even raise new security concerns, as, for instance, encrypted connections preventing firewalls from exercising their traffic filtering capabilities.

Cryptography is not only about encryption for confidentiality, but is used in techniques for preserving data integrity or addressing nonrepudiation concerns. For all of its applications, the specificities of ICSs pose challenges for cryptographic key management [63]. Finally, even with situations where cryptographic techniques are necessary to protect data, there continues to be requirements for security which cannot be met by these techniques.

4) "Anti-Virus Protection is Sufficient": The overwhelming attention of the media and A/V product vendors is on worms and viruses as the prime cybersecurity concerns. The discussion in Section II-A-2 and the remainder of this paper clearly disqualify this particular myth, as worms and viruses constitute only a part of a much wider threat landscape. Technically speaking, the diversity of the threat landscape implies diversified and independent technical measures, such as firewalls, network segmentation, intrusion detection, and protection systems, or secure channels, among which A/V software is just a component of an overall approach and a holistic security organization.

Also, while well-managed A/V solutions are usually efficient protection against the most common malware (the "Wild List" [64]), they are a far less robust defense against more targeted or less widespread forms of malware. Recently, Devine and Richaud [65] manually tested 12 A/V solutions with regards to home-made malware (i.e., not identified through the A/V signature files but with malicious behavior characteristics, including key-logging, code injection, or network evasion). All products were deficient in at least one area, and some in all areas. In some cases old and well-known techniques were not detected at all, underlining the limits of current A/V technologies outside the mainstream and untargeted threats. Furthermore, a recent contest organized as part of a security conference has shown that six out of seven A/V solutions among the most widely used could be disabled on-the-fly in less than two minutes [66].

The purpose of these statements is not to claim that A/V protections are useless, but rather to demonstrate that they cannot provide an absolute guarantee. In fact, they can only be considered as one layer of defense, to be integrated into a wider DiD approach to security. Finally, the implications of A/V on the overall architecture should be carefully studied in ICS contexts: signature update strategies need specific attention regarding system reliability constraints, configuration management, and distribution.

C. Incorrect Assumptions About Technological Immunity

1) "Obscure Protocols/Systems are Naturally Secure": The reverse-engineering of industrial protocols is usually not difficult: ICS field equipment is prescriptive and minimalist in terms of functionality; the associated communication protocols are similarly designed. Some computer skills and patience are all that are needed to reverse-engineer, at least partially, most industrial protocols that do not have specific security features [67] (which constitute a large majority). Emerging tools may, in some cases, automate the task [68], [69].

It should be mentioned that reverse-engineering is generally not necessary: as stated in II.A.3, the protocols used in the power system may be domain-specific, but they are not always closed and proprietary. Protocol specifications, such as DNP3, ICCP/TASE.2, or IEC 60870-5-104, are publicly available.

History tells us that there is an overestimated benefit in maintaining design secrets when it comes to ensuring security. Cryptography provides famous examples: from Global System for Mobile Communications (GSM) cell phones [70] to radio-frequency tags used for toll payment and car ignition [71], [72], or DVD anticopy protection [73]. They all had secret cryptographic design specifications, which have all been reversed-engineered and broken. For these applications, functionally equivalent open technologies would have been more robust. In 1883, Kerckhoffs stated that ciphers should not be required to be secret and shall be able to fall into the hands of the enemy [74]. The point is not to apply these principles to all security-related information, but to stress that security cannot be only built on the fact that a given design is closed and proprietary. Conversely, an open and standard design is not sufficient. See [75] and [76] for an "open vs. close designs for security" debate.

Finally, precise knowledge of communication protocols might be of no importance. It may not be required for an attacker to succeed in saturating a network: accessing one node where the physical and logical layers do not have the appropriate controls can be sufficient to launch a DoS attack on shared media (cf. Section II-A-4). The Browns Ferry nuclear plant incident [77], although not malicious, has already demonstrated DoS effects in ICS context.

2) "Serial-Link/4–20 mA Wire Communications are Immune": While the use of interoperable networking protocols, such as TCP/IP, has raised new security concerns, other communication technologies do not automatically ensure immunity to cybersecurity attacks. This myth points to related risky assumptions regarding serial links and analog communication channels, such as 4–20 mA current loops. Both types of technology are sometimes erroneously described as inherently secure, providing isolation and protection to critical assets. Although the routable nature of TCP/IP results in a potentially large and reconfigurable attack surface, it is not correct to conclude that serial and 4–20 mA-based links have no attack surface at all. Serial links are digital channels, and like TCP/IP, they make no distinction between malicious and nonmalicious traffic that they carry. The focus should be on the edges of the links, on what elements these edges are connected to, and on what possibilities are offered to an attacker if one edge is compromised. This reasoning can also be used for analog communications links, such as 4–20 mA current loops. Often used to measure physical parameters, such as temperature, pressure, or flow, they can also control output actuators, such as valve positions. If the controlling side is compromised, then

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

the analog nature of the link to the actuator will not prevent the attacker from taking control of the edge device.

3) "ICS Components do not Need to be Security Hardened": One of the distinguishing features of ICSs is that they are often built around a distributed architecture which comprises highly recognizable ICT components at the core (databases, application software, servers, network components, etc.), and much less recognizable ICT components at the edges (sensors, actuators, intelligent electronic devices (IEDs), programmable-logic controllers (PLCs), smart meters, remote terminal units (RTUs), etc.). The need to security-harden the core ICT components is often well understood, as it is common practice in classical ICT, for example, ensuring that a server is only running the services required.

However, as we move out from the core ICT components toward the edges, the devices often become unrecognizable as ICT components, supplied by specialist manufacturers and with prescriptive/limited functionality. Data-communication methods between devices also become more prescriptive, based on industry-specific protocols. This engenders the myth that these devices do not need to be security hardened, because their functionality is so prescriptive, or even because they are not considered as ICT components at all. The truth is often very different, with many of these devices now having built-in Ethernet ports used to connect them to a control local-area network (LAN), through which they communicate using TCP/IP. These devices can also have unnecessary communication services running, which may have been used for debug purposes but have never been disabled. Examples of these include telnet or FTP services.

It is also common to find functionality, such as web servers, running on these devices. These web servers may be included to allow remote users to connect to the device and configure it via a web browser. This may not be required once a device is installed and commissioned, and should be disabled. A specific example known to the authors is an RTU which incorporated a web server to facilitate remote configuration. The web server incorporated an undocumented feature to allow a remote user to reboot the RTU simply by navigating to a specific URL. This example strengthens the argument for hardening field devices; their potential for vulnerabilities which could be easily exploitable has not gone unnoticed in the black hat community (cf. Section II-A-2).

D. Reductive Views on Security

1) "ICS Security is a Technological Problem": The introduction of new technologies, such as firewalls, intrusion detection systems (IDS), and similar security appliances is something which often piques the interest of engineers working with ICSs. It is often assumed that these security appliances alone are the solution. While it is true that these technologies can be very effective as part of the solution, it is important to recognize that the introduction of new security technologies into the ICS environment creates a requirement to develop new skills and technical expertise. Training and development activities must be established in order to ensure appropriate implementation and maintenance of the security technologies. People, process, and policy are of paramount importance for the efficient and effective use of security technologies in ICSs.

Also, introducing additional technical controls has downsides that need to be taken into account. The addition of further components into a system typically increases the overall risk of failure of the system and impacts on maintenance. This is also true for security. Adding components, such as firewalls, may imply maintenance by personnel that have a good understanding of firewalls but not of ICSs and the operational environments that they control. In addition, maintenance of the technical security controls applied to ICSs is often achieved through remote-access facilities. Although these may be protected by authentication and encryption, they do provide additional access points to the ICS and increase the security risks. When considering adding new technical controls, not only does the mitigation of the original security risk need to be assessed, but also a risk assessment should be undertaken to identify any new risks arising from the introduction of the technical control.

Finally, the traditional view of the ICS presupposes a highly controlled environment for human interaction with the system (e.g., a control center), outside of which human interactions with the system are only considered for their safety implications. This view is no longer applicable due to the flexibility of modern systems, and the extent of interaction required with the ICS, both in terms of operator interaction and maintenance interaction. Also, ICS are not immune to risks arising from attempts to compromise them through social engineering attack methods (cf. Section II-A-6). In fact, human factors have become a key aspect in modern ICSs: they should occupy an equally central place in their cybersecurity.

2) "It's Certified, It's Secured": Since the introduction of the Orange Book in the 1980s [78], the concept of certification has accompanied cybersecurity. Formalizing requirements and allowing dedicated entities to verify their fulfillment, certification is a double-edged sword for the security architects: it can be a very valuable tool when clearly understood and appropriately used, but it can also contribute to a dangerous illusion of security if superficially manipulated. Common criteria (CC) [79] provide an excellent illustration of this duality. CC enable the specification of security functional claims and their evaluation along different assurance levels. However, several traps threaten the unfamiliar user: in particular, the seven evaluation assurance levels (EALs) defined in the standard should not be confused with absolute security levels. They only provide a level of confidence in the evaluation of the security functions submitted. In general, to appreciate this certifications and possibly compare them, one should carefully analyze the security claims and the scope of the evaluated products. For example, Windows 2000 has been certified with a fairly high level of assurance $(\mathrm{EAL4+})$: the corresponding security target assumes a nonmalicious environment [80].

The concept of security certification is now entering the ICS arena. This dates back to 2002 and resulted three years later in a CC profile dedicated to ICSs [81], which has never been adopted by solution providers. Present initiatives are distant from the CC and are shaped by two schemes: 1) Achilles certification [82], led by a private company, and 2) ISASecure certification [83], led by an industry-wide consortium. Comparing these is out-

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

side the scope of this paper, but they do share several common points which have led us to raise this issue. They both benefit from an intense promotion by their respective initiators but also by ICS solutions providers; they both appeal to utilities decision makers attracted by the prospect of off-the-shelf security. Even if their approaches differ from the CC, if they are more industry driven and allow more straightforward interpretations, their content and implications should be carefully studied. They may help to differentiate two functionally and technically equivalent solutions. Nevertheless, the security level of a component can only be evaluated in its operational environment, and it has relevance only when considered within the overall architecture. Security certifications will never be able to replace dedicated security analysis and tailored security requirements. Anderson and Fuloria give interesting inputs and analysis on the inherent problems of certification as well as economical and ICS-oriented perspectives on the issue in [84].

3) "Vendors Have a Full Command of Their Products Security": As discussed in Section II-A-3, the last several years have seen a definite trend toward ICSs developed and built around COTS hardware, OS, and software components. Vendors, buyers, and users were initially unconcerned about the security implications of such technology. However, as security has become a more widely held concern over time, buyers and users have, quite naturally, assumed that the ICS vendors have a detailed knowledge of the systems that they are supplying, and particularly of the ICT security features and vulnerabilities of their products. However, this has been proven to be an incorrect assumption in a number of ways. For example, ICS vendors often have very little understanding of the COTS products they assemble beyond the very narrow application that they use them for. The vendors from whom they procure the COTS components carry no liability for the security of their products. Also, ICS vendors have not historically structured their support and maintenance operations to provide a fast reaction to security incidents and are not familiar with disclosure procedures through national CERTs.

A good illustration of this situation was given by the vulnerability discovered by researchers in 2008 in a proprietary ICS data-communications protocol, known as Wonderware SuiteLink [85]. The researchers first attempted to contact Wonderware at the end of January 2008, who took almost one month to even acknowledge the initial contact. Subsequently, the researchers provided support to Wonderware to help them understand the vulnerability in their own product. This resulted in a delay of more than three months in the publication of a security advisory to provide information to SuiteLink users. This event did serve as a wake-up call for Wonderware's developers and for the ICS industry. The result has been that many ICS vendors have become much more knowledgeable about the security of their products and are more proactive in ensuring that customers are kept aware and provided with new patches as required. However, there are still many ICS vendors who have a long way to go.

4) "Compliance With Security Standards Makes You Secure": The introduction of mandatory standards, such as the NERC CIP standards [86], applicable to the North American bulk electric industry, has forced organizations to follow a route toward achieving compliance. While efforts toward compliance with security standards are not normally something that would decrease an organization's security posture *per se*, it can lead to narrow thinking and activities in order to achieve compliance with minimum effort [87]. This can include developing spurious rationale to exclude parts of the organization from scope, or focusing purely on ensuring that the appropriate audit trail is maintained rather than on the quality of the activities undertaken to generate the audit trail. These approaches not only result in suboptimal security posture, but can create the dangerous illusion that actual security posture does not matter as long as compliance is achieved. Similar effects have been formerly observed with regards to safety regulations, when conflicting with the development of a self-promoted safety culture [88], with catastrophic consequences.

Standards can be a powerful means to promote best practices, interoperability of systems, and minimize costs of new developments. Unfortunately, in ICS cybersecurity, we have a confusing situation, where dozens of normative initiatives and documents are available. Each year, surveys and structured comparisons are published (e.g., [89] and [90]), but they deprecate at an impressive speed, due to the pace of evolution of the ICS security standard landscape. As an illustration, let us consider U.S. nuclear power plants operators: as of 2009, they were more or less directly concerned with industry-led documents (NEI-0404 [91]), regulatory documents (including Rule 10CFR73.54 [92], and associated documents such as RG5.71 [93] or NUREG/CR-6847 [94]), but also FERC and NERC documents (cf. [95]); in addition, national standard bodies, such as the National Institute of Standards and Technology (NIST) provide useful reference documents too (mainly [52] and [96, Annex I]); international organizations with a strong U.S. presence, such as the IEEE and the ISA, have their own related guidance and standards documents (e.g., ISA99 [54], and most recently, the ISA-67.15 WG5 initiative [97]). Besides, at the international level, the IAEA is finalizing a reference manual [53] on the topic while the IEC has begun an international standard [98]. Inevitably, their different scopes and their underlying principles lead to incompatibilities, or even counterproductive side effects. In these situations, compliance does not equal security.

5) "ICS Security Assessment Does not Need Full Inventories": The first step in a security assessment is to have a fully detailed and properly maintained asset inventory. It is established practice for ICS inventories to be provided with the handover of the ICS project into production; however, it is common for the inventory not to be maintained after that point. Faulty equipment is replaced with new equipment with different versions of firmware, new equipment is added, software is updated, and the asset inventory continues to reflect the original configuration. In these circumstances, assessing the applicability of disclosed vulnerabilities and their associated patches becomes difficult, because it may not be possible to know if the vulnerable versions of the product are used in the ICS.

6) "Access Points to ICSs are Easily Controlled": There are many examples of undocumented access points to ICS networks [99], or documented but inadequately secured access points, to dispel this myth. Examples include maintenance laptops connected directly to the ICS network, bypassing firewall controls

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

and policy rules, remote access for support and maintenance personnel, dial-up access to equipment that form part of the ICS, undocumented network connections between ICS equipment and non-ICS equipment, dual-homed devices bridging ICS and non-ICS networks, and networking equipment on the ICS network with accessible and enabled ports, facilitating the introduction of new and untrusted equipment onto the ICS network.

Often, the ICS owner has no knowledge of the systems being used in this context, or the personnel using the systems in these ways.

7) "Security is a Problem that Needs to be Solved Only Once": Historically, ICSs existed in an environment where the requirements for functional change over time were very low (or did not exist at all), and the external environment was known and understood. Consequently, the relevance of a solution to a particular problem did not change much over time. Also, field devices had little or no intelligence other than hardwired logic, so other than physical maintenance activities, these devices were "fit-and-forget." This is no longer applicable, but sometimes continues to be applied to modern ICSs with respect to security. This fails to recognize that ICSs are now subject to an ever-changing security landscape, including modern field devices that require being actively configured and maintained. Not only must the ICS and field devices be secured, their ongoing management and maintenance need to be secured as well, and must be capable of managing changes, such as the disclosure of new vulnerabilities or the emergence of new threats.

8) "Cybersecurity can be Handled at the End of the Project": It has become typical over the last few years to see security concerns emerge during ICS projects. However, these projects often span several years, and the general awareness of the security problem has only become prevalent in more recent years, resulting in some projects only addressing security concerns in their later stages. At this point, it is very difficult and/or very expensive to do so. As with any change to a project's requirements or any defect discovered, the later in the project that the change is decided or the defect is discovered, the more expensive it becomes to implement or fix it [100].

A similar situation also exists for more recent projects where security is a known issue from the start of the project. Security commonly manifests itself as a low priority subset of nonfunctional requirements, and the requirements gathering and design processes do not fully integrate security risk assessment and design reviews into the project lifecycle. The result is that security is not fully taken into account during the early stages of a project, resulting in an additional expense (or accepted risk) emerging later.

III. Recommendations

The cybersecurity myths presented in Section II are intended to help the reader recognize them in context. This is the first step before their eradication, which has to be defined in terms of actions toward an appropriate cybersecurity posture. This section provides recommendations which directly support an objective perception of risks as well as an effective cybersecurity posture for utilities. Each recommendation is explained briefly, embedding pointers to more complete guidance. Their respective contributions into fighting the listed myths are summarized in Table I. The recommendations aim neither at covering the whole cybersecurity domain, nor replacing a formal cybersecurity framework. Rather, it is an invitation to take action in a way that is the most likely to prevent the propagation of the identified myths.

1) Stay Tuned With Expert Groups and National Authorities: Cybersecurity is, by essence, a fast-moving discipline: not only coupled with the pace of ICT developments, it is also linked with the evolution of threats in terms of actors, motivations, resources, as well as with the offensive and defensive technological advances. Cybersecurity and critical information infrastructure protection (CIIP) have become national priorities; [5] provides an inventory of national and international CIIP policies: the related organizations are generally first-choice sources for views on the threat landscape and for technical security guidance. Some have dedicated mechanisms allowing trusted exchanges between utilities (e.g., the ISACs in the U.S. or the SCSIE in the U.K. [5]). Other independent cross-utilities organizations can also provide useful forums to exchange good practices and relevant information: CIGRÉ for instance for Transmission System Operators [101]. Finally, among the growing number of dedicated blogs, newsletters, and events, a subset is worth following (for example, the Digital Bond blog [102] and Industrial Defender website news section [103], the SCADASEC mailing list [104], as well as the S4, ACS, as well as SANS SCADA and ICS security events [105]–[107]).

2) Identify and Avoid "FUD": Security-related issues are, by essence, hard to handle at a strictly rational and objective level. They are excellent vectors for "Fear, Uncertainty, and Doubt" (FUD) techniques usually found in public relations but also in marketing strategies, and by which the cybersecurity consulting and vendor community are sometimes tempted. Cybersecurity news, whether highly technical or on a more general level, should always be carefully analyzed, both in terms of credibility and in terms of relevance. Cybersecurity skills and expertise, but also connections to multiple and appropriate channels of information, are necessary ingredients in this analysis. This naturally reinforces the previous recommendation and should feed into a clear and operational risk-management framework.

3) Adopt a Critical and Proactive Posture on Standards: As detailed in Section II-D-4, it is not always simple to navigate through the present profusion of ICS cybersecurity standards [89]. Nevertheless, it would be far more difficult and risky to start the definition of a complete set of security policies, procedures, and controls without taking advantage of the existing material. Thus, a critical and proactive posture on standards is needed. In any case, it is important to realize that none of the existing references have exactly the same scope and address the same aspects. There is no universal standard to rely on, but several pieces to be integrated to build an efficient and consistent organization-wide security posture [89].

4) Deliver an Ongoing Awareness Program: One of the most fundamental recommendations concerning ICS security is to raise awareness of the security issue. It needs to be maintained

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

on an ongoing basis. The literature agrees on making these recommendations a fundamental good practice [54], [108], [109]. Awareness generally works on two levels. The first is management awareness; this brings the issue to the attention of management along with the potential consequences of not addressing it, and is often used as part of the business case for making budget available. The second is user awareness; raising and maintaining awareness of the issue among users so that they use ICSs appropriately and are vigilant with regards to potential security incidents.

5) Establish and Maintain Asset Inventories: All ICS equipment should be integrated in a complete inventory (including ownership information), maintained under configuration control [54], [108], [109]. All changes to the ICS configuration should be recorded, and the need to trigger a risk assessment exercise should also be considered on any update to the inventory. The asset inventory should include all components of the ICS from the control center to the field. Therefore, policies and procedures are required that make configuration management of the assets themselves, and the maintenance of the asset inventory, a "business-as-usual" process. Asset inventories improve the level of control over ICS equipment, and ease the task of assessing the applicability of security patches or updates to a given ICS.

6) Harden Devices at All Levels: All ICS equipment should be covered by a security policy, instantiated in appropriate procedures and technical requirements. Those requirements should, among other things, ensure that the intrinsic technical vulnerability of the systems is minimized, by taking advantage of their configuration options and modularity. Security hardening and associated good practices are now commonly applied in business ICT [110]; equivalent practices should apply to all ICS components: services and communication capabilities set at the minimum, default settings changed, and software versions upgraded. ICS components, such as PLC, IED, RTU, smart sensors, or actuators can no longer be exceptions. References [52], [54], and [109] provide good guidance for this type of process.

7) Adopt a Graded Approach and a DiD Strategy: ICSs have diverse exposures to cybersecurity risks. A graded approach allows these differences to be taken into account and enables optimal use of resources. This may be based on a domain model approach [111] and on the definitions of a limited number of security levels (or degrees), describing hierarchically the security controls required. Several standardization initiatives push in this direction [53], [98] and several references provide examples [91], [112], [113]. The assignment of systems and components to these levels should be based on a clear basis: risk assessments, safety constraints, or regulatory considerations are all valid inputs. In order not to be rapidly outdated, they should not be technology-oriented and stay at a functional level. DiD objectives, through complementary and independent protections [114], should structure their definition. DiD also stresses the importance of nontechnical controls, including human, organizational, and procedural aspects.

8) Follow the KISS Principle: "Keep It Simple Stupid" (KISS) is a well-known acronym and self-descriptive motto, particularly relevant in this case: complexity indubitably leads to weaknesses. Complex codes, functions, and feature-rich software, and, more generally, overengineered systems or architectures are intrinsically fragile and hard to maintain. This applies to ICSs and security solutions. At the organizational level, security policies and procedures need to be understandable and applicable in order to be effective; simplicity is clearly a key factor. As in all risk-oriented disciplines, security is a question of tradeoff, and simplicity should be considered a principle and an objective.

9) Undertake Incident Management and Investigation: Holistic approaches to cybersecurity should cover protection, detection, and response [109]. One of the key areas of detection and response, along with those automated by security appliances, are incident management and investigation. This is still an immature discipline when it comes to ICSs, as many ICSs do not have the capability to record the relevant information for later investigation. However, this is being addressed on newer systems and by research projects (e.g., [115]). Notwithstanding this, cybersecurity should be systematically included in the investigation process as a potential cause of ICS failure.

10) Challenge the Security Posture Regularly: ICSs operate in an environment that is constantly changing: components fail or are upgraded, personnel and third parties are replaced, and networks and requirements evolve. New vulnerabilities are regularly found, and those with malicious intent become interested in ICSs and are able to attack them. In this situation, the only way to maintain an adequate security posture is to regularly challenge it. This implies audits of security-management systems [116], [117]; reviewing risk assessments [118]; checking compliance with procedures; challenging vendors' claims; and performing vulnerability analysis and penetration testing with appropriate care [119], [120].

11) Tailor Security Policies, Procedures and Controls for ICS: Even though the strong tendency for standards and COTS components has been mentioned throughout this paper, ICSs still have their specificities. For instance, communications or actions may have strong time-dependant constraints, or specific reliability and safety requirements may exist. References [52] and [63] provide a good synthetic view of these differences. Besides, nontechnical aspects may also be specific. Organizations, human resources, and associated skills as well as legal and regulatory frameworks also call for specifically tailored policies, procedures, and controls. References [52], [54], [96], [109], and [121] are all useful starting points. This being said, existing and recognized frameworks, such as [96] and [108], should be leveraged and adapted with the help of the previous references.

12) Undertake Security Design Reviews: Security design reviews should be an inbuilt feature of projects, and for any changes proposed to existing systems [108], [109]. This forces the security aspects of a proposed design, or proposed design changes, to be fully considered by appropriately skilled personnel, and helps maintain security as a key requirement in the delivery of new projects and/or changes to existing systems.

13) Ensure Contractual and Formalized Relationships: Most ICS are not stand alone or maintained by a single entity. In most cases, the responsible entity is reliant on third parties to deliver products and services to maintain the ICS operation. These products and services vary from support and maintenance of application software or hardware to services, such as security management (e.g., firewall configuration) or provision of

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

TABLE I
MYTHS AND RECOMMENDATIONS COVERAGE

	1) Stay tuned: expert groups and national authorities	2) Identify and avoid "Fear Uncertainty and Doubt"	3) Adopt a critical/proactive posture on standards	4) Deliver an on-going awareness program	5) Establish and maintain asset inventory	6) Harden devices at all level	7) Adopt a graded approach and a DiD strategy	8) Follow the KISS principle	9) Undertake incident management and investigation	10) Challenge regularly the security posture	11) Tailor security policies, procedures and controls	12) Undertake security design reviews	13) Ensure contractual and formalized relationships
A.1 "Industrial control systems are isolated"					X		X						X
A.2 "Nobody wants to attack us"	X	X							X				
A.3 "We only have obscure protocols /systems"				X	X								
A.4 "Anti-virus and/or patching are useless for ICSs"											X		X
A.5 "Cyber security incidents will not impact operations"	X	X		X					X		X		
A.6 "Social engineering is not an ICS issue"				X			X						
B.1 "Our firewall protects us automatically"							X	X					
B.2 "One-way communication offers 100% protection"							X						
B.3 "It's encrypted: it's protected"												X	
B.4 "Anti-virus protection is sufficient"	X						X				X		
C.1 "Obscure protocols/systems are naturally secure"							X					X	
C.2 "Serial-link/4-20mA wire communications are immune"						X						X	
C.3 "ICS components do not need to be security hardened"					X	X					X	X	
D.1 "ICS security is a technological problem"				X			X	X				X	
D.2 "It's certified, it's secured"			X							X		X	
D.3 "Vendors have a full command of their products security"	X											X	X
D.4 "Compliance with security standards makes you secure"			X							X			
D.5 "ICS security assessment does not need full inventories"			X		X					X		X	
D.6 "Access points to ICSs are easily controlled"							X			X			X
D.7 "Security is a problem that needs to be solved only once"	X				X				X	X			X
D.8 "Cyber security can be handled at the end of the project"			X	X						X		X	X

telecommunication services. These products and services can be provided by other entities within the organization (e.g., corporate IT) or by external entities. In each case, there are risks associated with dealing with third parties. These risks should be assessed and mitigated as necessary [108], [109], which involves having appropriate contractual relationships in place, including service-level agreements (SLAs). Reference [122] provides useful guidance on how requirements on third-party suppliers could be stated.

IV. CONCLUSION

The power system is rapidly evolving, supported by the high-pace of ICS modernization and interconnection. New cybersecurity concerns are emerging, and are still fairly new to the power utilities culture and personnel. As a consequence, many false beliefs and misconceptions distort risk perception and prevent utilities in some cases from adopting an appropriate cybersecurity posture. Discussion of the 21 "myths" in this paper provides rational arguments and concrete references to help identify these pitfalls and contribute to their elimination. However, this paper only gives an instantaneous picture as cybersecurity is permanently changing. It is intended to be a basis for action, to integrate into an ongoing process.

REFERENCES

[1] *Electricity Technology Roadmap -2003 Summary and Synthesis, Product Number 1010929*. Palo Alto, CA: Elect. Power Res. Inst. (EPRI), 2003.
[2] European Comm., "Strategic research agenda for Europe's electricity networks of the future," EUR 22580, 2007.
[3] *NIST Framework and Roadmap for Smart Grid Interoperability Standards NIST Draft Publication, Standards Release 1.0 (Draft)*, NIST Special Publ. 1108, Sep. 2009.
[4] Google map of AMI & smart metering programmes across the world. Maintained by the Energy Retail Association in the UK, Dec. 30, 2009. [Online]. Available: http://tinyurl.com/AMI-projects-worldmap
[5] E. M. Brunner and M. Suter, *International CIIP Handbook 2008/2009*. Zurich, Switzerland: Center for Security Studies, ETH Zurich, 2008.
[6] E. Byres and D. Hoffman, "The myths and facts behind cyber security risks for industrial control systems," presented at the VDE Congr., Berlin, Germany, 2004.
[7] *Potential Vulnerability of Plant Computer Network to Worm Infection, Information Notice 2003-14*. Washington, DC: U.S. Nuclear Regulatory Commission, 2003.
[8] P. F. Roberts, Zotob, PnP Worms Slam 13 DaimlerChrysler Plants Aug. 2008. [Online]. Available: http://www.eweek.com/
[9] N. Shachtman, Under Worm Assault, Military Bans Disks, USB Drives WIRED, Nov. 2008. [Online]. Available: http://www.wired.com
[10] W. H. McMichael and B. Rolfsen, DoD confirms computer virus in networks Air ForceTimes, Nov. 2008. [Online]. Available: http://www.airforcetimes.com
[11] P. Porras, H. Saidi, and V. Yegneswaran, "An analysis of Conficker's logic and rendezvous points," SRI Int., 2009.

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

[12] ISS on-orbit status 09/11/08. international space station (ISS) daily report. NASA. [Online]. Available: http://www.hq.nasa.gov/osf/iss_reports/

[13] Computer viruses make it to orbit. BBC News. Aug. 2008. [Online]. Available: http://news.bbc.co.uk/1/hi/technology/7583805.stm

[14] Juvenile computer hacker cuts off FAA tower at regional airport U.S. Dept. Justice, Mar. 1998. [Online]. Available: http://www.justice.gov/criminal/cybercrime/juvenilepld.htm

[15] P. Oman, E. O. Schweitzer, III, and D. Frincke, "Concerns about intrusions into remotely accessible substation controllers and SCADA systems," presented at the 27th Annu. Protective Relay Conf., Spokane, WA, Oct. 23–26, 2000.

[16] "R v boden QCA 164, Supreme Court of Queensland, Appeal against conviction and sentence," 2002.

[17] T. Smith, "Hacker jailed for revenge sewage attacks," *The Register*, Oct. 2001. [Online]. Available: http://www.theregister.co.uk/

[18] M. Abrams and J. Weiss, Malicious control system cyber security attack case study—Maroochy water services. MITRE, 2008.

[19] J. Slay and M. Miller, *Lessons Learned From the Maroochy Water Breach, IFIP series*. Boston, MA: Springer, 2007, vol. 253, ch. 6, pp. 73–82.

[20] D. Maynor and R. Graham, "SCADA security and terrorism: We're not crying wolf?," presented at the Black Hat Federal Conf., Washington, DC, 2006.

[21] S. Bratus, "Fuzzing proprietary SCADA protocols," presented at the Slides presented at the Black Hat USA Conf., Las Vegas, NV, Aug. 2008.

[22] J. Larsen, "Breakage," presented at the Black Hat DC Conf., Washington, DC, Feb. 2008, slides presented.

[23] M. Bristow, "ModScan: a SCADA Modbus network scanner," presented at the DefCon-16 Conf., Las Vegas, NV, 2008, slides presented.

[24] M. Davis, "Smart grid device security," presented at the Black Hat USA Conf., Las Vegas, NV, Jul. 2009, slides presented.

[25] US-CERT, Search US-CERT Vulnerability Notes. Dec. 2009. [Online]. Available: http://www.kb.cert.org/vuls/html/search

[26] D. Goodin, "Gas refineries at Defcon 1 as SCADA exploit goes wild—At least they should be.," *The Register*, Sep. 2008. [Online]. Available: http://www.theregister.co.uk

[27] E. Nakashima and S. Mufson, "Hackers have attacked foreign utilities, CIA analyst says," *Washington Post*, p. A04, Jan. 8, 2008.

[28] G. Messick, "Sabotaging the system," CBS News 60 Minutes. Nov. 2009. [Online]. Available: http://www.cbsnews.com

[29] S. Gorman, "Electricity grid in U.S. penetrated by spies," *Wall Street J.* Apr. 8, 2009. [Online]. Available: http://online.wsj.com

[30] Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience, Communications SEC(2009)399 and SEC(2009)400 European Comm., 2009.

[31] S. R. Chabinsky, Statement before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security. Nov. 2009. [Online]. Available: http://www.fbi.gov/congress/congress09/chabinsky111709.htm

[32] "Development of policies for the protection of critical information infrastructures," Seoul, Korea, OECD, Ministerial Background Rep. DSTI/ICCP/REG(2007)20/FINAL, 2008.

[33] The Microsoft smart energy reference architecture (SERA), electronic booklet. Oct. 2009. [Online]. Available: http://www.microsoft.com/utilities

[34] OPC unified architecture. 2009. [Online]. Available: http://www.opcfoundation.org/UA/

[35] IEC Technical Committee 57: Power systems management and associated information exchange. [Online]. Available: http://tc57.iec.ch/

[36] IEEE Standards Association, Working Group Areas. [Online]. Available: http://grouper.ieee.org/groups/index.html

[37] Modbus Application Protocol, V1.1b Modbus Org. Std. Dec. 2008.

[38] S. Tom, D. Christiansen, and D. Berrett, "Recommended practice for patch management of control systems," in *DHS Control System Security Program (CSSP) Recommended Practice*, Dec. 2008.

[39] ISA99 Working Group 6, Patch management in the IACS environment (Draft), Tech. Rep. ISA-TR99.02.0, 2009.

[40] T. Eisenberg *et al.*, "The Cornell Commission: On Morris and the Worm," *Commun. ACM*, vol. 32, no. 6, pp. 706–709, 1989.

[41] Virustlist.com Search EngineConsulted Kaspersky Lab Malware Names Database, Jan. 2nd, 2010. [Online]. Available: http://www.viruslist.com/en/find?search_mode=virus&words=linux

[42] BadBunny seen in "The Wild"? OpenOffice multi-platform macro worm discovered. Sophos News. May 2007. [Online]. Available: http://www.sophos.com

[43] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, "An experimental investigation of malware attacks on SCADA systems," *Int. J. Critical Infrastructure Protection*, vol. 2, no. 4, pp. 139–145, Dec. 2009.

[44] J. Meserve, Staged cyber attack reveals vulnerability in power grid, CNN.com/US. Sep. 2007. [Online]. Available: http://www.cnn.com

[45] B. Krebs, "Cyber incident blamed for nuclear power plant shutdown," *The Washington Post*, 2008.

[46] R. Shirey, Internet Security Glossary, Ver. 2, IETF, RFC 4949. Aug. 2007. [Online]. Available: http://tools.ietf.org/html/rfc4949

[47] *Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 2: Glossary of Terms*, IEC Std. 62351-2nd ed. 1.0, Aug. 2008.

[48] S. Stasiukonis, Social engineering, the USB Way. DarkReading Website Jun. 2007. [Online]. Available: http://www.darkreading.com/

[49] I. Winkler, "How to take down the power grid," presented at the RSA Conf., San Francisco, CA, Apr. 2008, slides presented.

[50] A. Wool, "A quantitative study of firewall configuration errors," *Computer*, vol. 37, no. 6, pp. 62–67, Jun. 2004.

[51] NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks (Revision 1.4), U.K. CPNI Guidelines. 2005.

[52] K. Stouffer, J. Falco, and K. Scarfone, *Guide to Industrial Control Systems Security—Final Public Draft*. Gaithersburg, MD: Nat. Inst. Standards Technol. Special Publ. 800-82, 2008.

[53] *Computer Security at Nuclear Facilities (Draft)*. Vienna, Austria: Int. Atomic Energy Agency (IAEA), 2009.

[54] Int. Soc. Autom. Website, The ISA99 committee standards and documents on industrial automation and control system security. [Online]. Available: http://www.isa.org/isa99

[55] A. Bartels, L. Pièrre-Cambacédès, and S. Duckworth, "Security technologies guideline—Practical guidance for deploying cyber security technology within electric utility data networks," *Electra*, no. 244, pp. 11–17, Jun. 2009.

[56] L. Pièrre-Cambacédès and P. Sitbon, "An analysis of two new directions in control system perimeter security," presented at the SCADA Security Scientific Symp., Miami, FL, Jan. 2009.

[57] *The History of Information Security—A Comprehensive Handbook*, K. de Leeuw and J. Bergstra, Eds. New York: Elsevier, 2007.

[58] *Mécanismes Cryptographiques, Règles et Recommandations Standards, Rev. 1.10 The French Network and Information Security Agency*, 2741/SGDN/DCSSI/SDS/LCR, Dec. 2006.

[59] Fact Sheet Suite B Cryptography U.S. National Security Agency (NSA), Sep. 2009. [Online]. Available: http://www.nsa.gov/

[60] S. Kent and K. Seo, Security architecture for the Internet protocol, IETF, RFC 4301. Dec. 2005. [Online]. Available: http://tools.ietf.org/html/rfc4301

[61] T. Dierks and E. Rescorla, The transport layer security (TLS) protocol ver. 1.2, IETF, RFC 5246. Aug. 2008. [Online]. Available: http://tools.ietf.org/html/rfc5246

[62] T. Zoller, TLS and SSLv3 vulnerability explained, Draft v0.98. Nov. 2009. [Online]. Available: http://www.g-sec.lu/practicaltls.pdf

[63] L. Pièrre-Cambacédès and P. Sitbon, "Cryptographic key management for SCADA systems—issues and perspectives," in *Proc. Int. Conf. Information Security and Assurance*, Korea, Apr. 2008, pp. 156–161.

[64] The wild list. Virus bulletin website, resources section consulted. Dec. 7, 2009. [Online]. Available: http://www.virusbtn.com/resources/wildlists/index

[65] C. Devine and N. Richaud, "A study of anti-virus' response to unknown threats," presented at the EICAR 18th Annu. Conf., Paris, France, May 2009.

[66] "Anti-virus "PWN2RM" challenge results," in *1st Int. Alternative Workshop on Aggressive Computing and Security*, Laval, France, Oct. 2009.

[67] R. K. Flink, D. F. Spencer, and R. A. Wells, Lessons learned from cyber security assessments of SCADA and energy management systems. INL, Tech. rep. INL/CON-06-11665, 2006.

[68] G. Wondracek, P. Milani, C. Kruegel, and E. Kirda, "Automatic network protocol analysis," presented at the 15th Annu. Network and Distributed System Security Symp., San Diego, CA, Feb. 2008.

[69] W. Cui, M. Peinado, K. Chen, H. J. Wang, and L. Irun-Briz, "Tupni: Automatic reverse engineering of input formats," in *Proc. 15th ACM Conf. Computer and Communications Security*, 2008, pp. 391–402.

[70] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication," *J. Cryptol.*, vol. 21, no. 3, pp. 392–429, Mar. 2008.

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

[71] S. C. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," presented at the 14th USENIX Security Symp., Baltimore, MD, Aug. 2005.
[72] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel, "A practical attack on KeeLoq," in *Proc. Eurocrypt , Lecture Notes Comput. Sci.*, Istanbul, Turkey, 2008, vol. 4965, pp. 1–18.
[73] F. Stevenson, Cryptanalysis of contents scrambling system, 1999. [Online]. Available: http://insecure.org/news/cryptanalysis_of_contents_scrambling_system.htm
[74] A. Kerckhoffs, "La cryptographie militaire," *J. Sci. Milit.*, vol. IX, pp. 5–38.
[75] B. Schneier, "The nonsecurity of secrecy," *Commun. ACM*, vol. 47, no. 10, pp. 120–120, Oct. 2004.
[76] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ: Wiley, 2001.
[77] *Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations, Information Notice 2007-15*. Washington, DC: U.S. Nuclear Regulatory Commission (NRC), 2007.
[78] *Trusted Computer System Evaluation Criteria*, U.S. Dept. Defense Std. 5200.28-Std., Dec. 1985.
[79] *Information Technology—Security Techniques—Evaluation Criteria for IT Security*, Int. Std., ISO/IEC Std. 15408, 2005.
[80] J. S. Shapiro, "Understanding the Windows EAL4 Evaluation," *Computer*, vol. 36, no. 2, pp. 103–105, Feb. 2003.
[81] ICS-SPP, "Industrial control system," System protection profile, v1.0, NIST. Apr. 2005.
[82] Wurldtech Website, Achilles certifications section. Dec. 7, 2009. [Online]. Available: http://www.wurldtech.com/services/achilles_certification.html
[83] ISA Website, ISASecure certification section. Dec. 7, 2009. [Online]. Available: http://www.isa.org/isasecure/
[84] R. J. Anderson and S. Fuloria, "Certification and evaluation: A security economics perspective," presented at the 14th Int. Conf. Emerging Technologies and Factory Automation, Mallorca, Spain, Sep. 2009.
[85] Wonderware SuiteLink Null Pointer dereference, US-CERT vulnerability note 596268. May 2008. [Online]. Available: http://www.kb.cert.org/
[86] *Cyber Security Standards*, NERC Std. CIP-002-1 through CIP-009-1, North Amer. Elect. Rel. Council , 2006.
[87] J. Weiss, "Are the NERC CIPS making the grid less reliable," *ControlGlobal Magazine.* Dec. 2009. [Online]. Available: http://community.controlglobal.com/content/are-nerc-cips-making-grid-less-reliable
[88] J. N. Sorensen, "Safety culture: A survey of the state-of-the-art," *Rel. Eng. Syst. Safety*, vol. 76, no. 2, pp. 189–204, 2002.
[89] L. Pièrre-Cambacédès, T. Kropp, J. Weiss, and R. Pellizzoni, "Cyber security standards for the electric power industry—A survival kit," presented at the CIGRÉ Paris Session, Paris, France, Aug. 2008, Paper Ref. D2-217.
[90] R. P. Evans, "Process control system cyber security standards—An overview," presented at the INL, Preprint (presented at the 52nd Int. Instrumentation Symp.), INL/CON-06-01317, 2006., Cleveland, OH, May 2006.
[91] Cyber security program for nuclear power reactors, NEI 04-04 Rev. 1, 2006.
[92] Protection of digital computer and communication systems and networks, Title 10, Code of Federal Regulations (CFR) Part 73.54 U.S., National Regulatory Commission (NRC), 2009.
[93] Cyber security programs for nuclear facilities, NRC Regulatory Guide 5.71, 2009.
[94] Cyber security self-assessment method for U.S. Nuclear Power Plants, NRC, NUREG/CR-6847, 2004.
[95] Nuclear plant implementation plan for CIP standards, Cyber Security Order 706B, Federal Energy Regulatory Commission (FERC), 2009.
[96] R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, and G. Rogers, *Recommended Security Controls for Federal Information Systems—Revision 2*. Gaithersburg, MD: NIST Special Publ. 800-53, 2007.
[97] ISA Starts, Cyber security for nuclear plants, Study, ISA InTech. Sep. 2009. [Online]. Available: http://www.isa.org
[98] Nuclear power plants—Instrumentation and control important to safety—Requirements for computer security programmes (NWIP), Ref. 45A/742/NP IEC New Work Item Proposal (NWIP IEC62645), 2009.
[99] T. Nash, "Backdoors and holes in network perimeters—A case study for improving your control system security," *US-CERT Control Systems Security Center, Case Study Series UCRL-MI-215398*, vol. 1.1, Aug. 2005.
[100] B. W. Boehm, *Software Engineering Economics*. Englewood Cliffs, NJ: Prentice-Hall, 1981.
[101] G. N. Ericsson, "Information security for electric power utilities (EPUs)—CIGRÉ developments on frameworks, risk assessment, and technology," *IEEE Trans. Power Del.*, vol. 24, no. 3, pp. 1174–1181, Jul. 2009.
[102] The Digital Bond blog. [Online]. Available: http://www.digitalbond.com/
[103] Industrial defender website. Industry news section. Dec. 2009. [Online]. Available: http://www.industrialdefender.com/news/index.php
[104] The Scadasec mailing list. [Online]. Available: http://news.infracritical.com
[105] Proc. SCADA Security Scientific Symp. Conf. Digital Bond website. [Online]. Available: http://www.digitalbond.com/index.php/s4-proceedings/
[106] Proc. Control Systems Cyber Security Conf. Sections. Applied Control Solutions website. [Online]. Available: http://realtimeacs.com/
[107] SCADA and Process Control Summit sections. The SANS Institute Website. [Online]. Available: http://www.sans.org
[108] *Information Technology—Security Techniques—Code of Practice for Information Security Management ISO/IEC Int. Std.*, ISO/IEC 27002:2005(E),, Jun. 2005.
[109] Process control and SCADA security, Ver. 2 (8 Parts Series) U.K. Centre for the protection of national infrastructure (CPNI), 2008.
[110] J. Hassell, *Hardening Windows*. New York: APress, 2005.
[111] A. Torkilseng and S. Duckworth, "Security frameworks for electric power utilities—Some practical guidelines when developing frameworks including SCADA/control system security domains," *Electra*, no. 241, pp. 18–22, 2008.
[112] M. G. Jaatun, M. B. Line, and T. O. Grotan, "Secure remote access to autonomous safety systems: A good practice approach," *Int. J. Autonom. Adaptive Commun. Syst.*, vol. 2, no. 3, pp. 297–312, 2009.
[113] J.-T. Zerbst, E. Hjelmvik, and I. Rinta-Jouppi, "Zoning principles in electricity distribution and energy production environments," in *Proc. 20th Int. Conf. Electricity Distribution*, Prague, Czech Republic, Jun. 2009.
[114] U.S. NSA, Defense in depth: A practical strategy for achieving information assurance in today's highly networked environments..
[115] Portaledge. Digital bond SCADApedia Wiki pages. [Online]. Available: www.digitalbond.com/wiki/index.php/Portaledge
[116] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, ISO/IEC 27001:2005(E), 2005.
[117] *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program, 1st ed.*, ANSI/ISA Std. ANSI/ISA-99.02.01-2009, Jan. 2009.
[118] *Information Technology—Security Techniques—Information Security Risk Management, 1st ed.*, ISO/IEC 27005:2008(E), Jun. 2008.
[119] M. R. Permann and K. Rohde, "Cyber assessment methods for SCADA security," presented at the 15th Annu. Joint ISA POWID/EPRI Controls and Instrumentation Conf., Nashville, TN, Jun. 5–10, 2005.
[120] D. P. Duggan, "Penetration testing of industrial control systems," Sandia National Lab, SAND 2005-2846P, Tech. Rep., 2005.
[121] "Treatment of information security for electric power utilities (EPUs)," CIGRÉ, Technical Brochure, (Publ. 2010-Q1), 2009.
[122] U.S. Dept. Homeland Security, "Cyber security procurement language for control systems," 2009.

Ludovic Pièrre-Cambacédès (M'05) was born in Clamart, France, in 1979. He received the M.Sc. degree from the National Institute of Applied Sciences (INSA), Lyon, France, in 2001.

Since 2001, he has been a Research Engineer in computer security at Electricité de France (EDF), Clamart. He contributes to communications network architecture design and technical recommendations for the cybersecurity of EDF industrial critical infrastructures. He is a cybersecurity expert in the IEC technical committees on "Nuclear power plants—Instrumentation and control systems important to safety" (SC45A) and "Power system control and associated communications" (TC57). He is actively involved in the CIGRÉ and IAEA cybersecurity initiatives for utilities.

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.

Marc Tritschler was born in Glasgow, U.K., in 1968. He received the B.Eng. degree in electronic systems and microcomputer engineering from the University of Glasgow, Glasgow, U.K., in 1989.

In his early career, he engineered advanced technological solutions for Longwall coal mining automation worldwide. He subsequently moved into the utility industry consulting business and software development, covering control and business systems. Since 2004, he has specialized in ICT-related consulting on critical infrastructure and liberalized market operations with KEMA Ltd.

Mr. Tritschler is a member of the Institution of Engineering and Technology (MIET) in the U.K. He was a member of CIGRÉ Working Group D2.22 from 2007 to 2009, and is an expert reviewer for the European Commission research projects on Critical Infrastructure Dependencies.

Göran N. Ericsson (S'90–M'96–SM'06) was born in Huddinge, Sweden, in 1963. He received the Ph.D. degree from the Royal Institute of Technology (KTH), Stockholm, Sweden, in 1996.

In 1997, he joined Svenska Kraftnät (Swedish National Grid), Sundbyberg, Sweden. During 1997–2006, he held expert and managerial positions within the fields of data communications and telecommunications. From 2007 to 2009, he was the Chief Information and IT Security Officer. He was the convener of CIGRÉ working group D2.22 on information security from 2006 to 2009, and in 2009, he became the Manager of Research and Design.

Dr. Ericsson is actively involved in the IEEE Power & Energy Society PSCC and CIGRÉ SCD2.

Authorized licensed use limited to: Technical University of Denmark DTU Library. Downloaded on December 01,2024 at 15:40:01 UTC from IEEE Xplore. Restrictions apply.