Emerging and Future Cyber Threats to Critical Systems

Edita Djambazova, Magnus Almgren, Kiril Dimitrov, Erland Jonsson

Emerging and Future Cyber Threats to Critical Systems *

Edita Djambazova,[1] Magnus Almgren,[2] Kiril Dimitrov,[1] Erland Jonsson[2]

[1] Institute for Parallel Processing - BAS, Sofia, Bulgaria
{ead,kpd}@iccs.bas.bg
[2] Chalmers University, Göteborg, Sweden
{magnus.almgren,erland.jonsson}@chalmers.se

Abstract. This paper discusses the emerging and future cyber threats to critical systems identified during the EU/FP7 project ICT-FORWARD. Threats were identified after extensive discussions with both domain experts and IT security professionals from academia, industry, and government organizations. The ultimate goal of the work was to identify the areas in which cyber threats could occur and cause serious and undesirable consequences, based on the characteristics of critical systems. A model of a critical system is suggested and used to distill a list of cyber threats specific to such systems. The impact of the identified threats is illustrated by an example scenario in order to stress the risks and consequences that the materialization of such threats could entail. Finally, we discuss possible solutions and security measures that could be developed and implemented to mitigate the situation.

1 Introduction

Critical systems and networks constitute the critical infrastructure of society. The extensive use of Information and Communication Technologies (ICT) and their proliferation in many new areas, such as process control and critical infrastructures, pose substantial challenges to critical systems' security. Modern technologies are used for industrial process control and may introduce new vulnerabilities and even be the cause for incidents. On the other hand, advanced automation is widely used in critical infrastructures through industrial control systems, something that leads to new security problems. Critical infrastructures (CIs) themselves expand the scale of security threats with their complexity, large connectivity, interdependency, and possible cascading effects. The characteristics of critical systems thus highlight the need for security solutions *specific* to those systems and we feel that special attention has to be paid to those specific solutions.

In order to find possible solutions, we first have to identify and understand the emerging cyber threats to critical systems. One of the major objectives of the ICT-FORWARD Project[3] was to outline the critical threat areas where research

* This work was supported by the EU FP7 ICT-FORWARD Project under Grant agreement no. 216331/14.09.2007

[3] http://www.ict-forward.eu

efforts have to be invested and countermeasures have to be devised. After a series of discussions with domain experts from industry, academia, and government organizations, a survey of emerging and future security threats was prepared [1].

This paper summarizes some of the identified security threats to critical systems and discusses the open research problems in applying security mechanisms to such systems and in developing new solutions.

2 Critical System: Modelling and Specifics

In our work, we used the following definition of a threat:

Definition of a threat: *A threat is any indication, circumstance, or event with the potential to cause harm to an ICT infrastructure and the assets that depend on this infrastructure.*

Our version is related to a variety of other definitions that exist in the literature, such as the ones provided by *ISO/IEC* and the *EU Green Paper for Critical Infrastructure Protection* [2]. In both these cases, a threat is described as an event, circumstance or incident that has the potential to cause destruction or, more generally, harm to the system or organization that is exposed to the threat. We adapt our definition to explicitly refer to ICT infrastructures and assets, as this is the scope of the FORWARD project. However, we observe that the definition is reasonably general to accommodate a wide range of possible threats and scenarios.

In order to be able to focus our efforts, we further developed a model of a critical system to help distinguish the most interesting and pressing security threats.

2.1 Modelling a Critical System

In Fig. 1, a generic ICT system is shown. It is defined as any system that delivers service to a group of users. Such a system is subjected to a number of threats, which may influence the service delivery to the users. We could leave the *system* box as a black box in the diagram. A ranking of the most important emerging threats can still be performed on such a black-box system. However, by knowing more about the system box, we can better judge what types of emerging threats will be the most severe and therefore important.

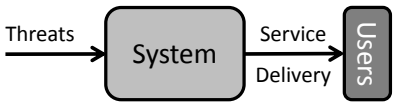

Fig. 1. A model of a generic ICT system.

The paper focuses on the ICT that supports critical infrastructures. Understanding the emerging threats to such systems is important because the consequences can be very dire. In our study, we consider the system from Fig. 1 to be a critical system.

Definition of a critical system: *We define a critical system (CS) to be a system that delivers a critical service to a group of users. A critical system consists of a traditional critical infrastructure or a critical application and supporting Information and Communication Technology.*

More specific definitions of a critical system can be found elsewhere in the literature. Here, we by purpose refrain from a very specific definition. The criterion of criticality may change over time and each professional group that discusses the issue has their own definition. By presenting a general model with the important salient properties found across many critical infrastructures, we can focus on the issues that will remain relevant in the future in our discussions.

In Fig. 2, we have expanded the *system* box shown in Fig. 1. Assuming a critical service delivery, we can further detail the structure of the *system* box based on the model of such critical systems.

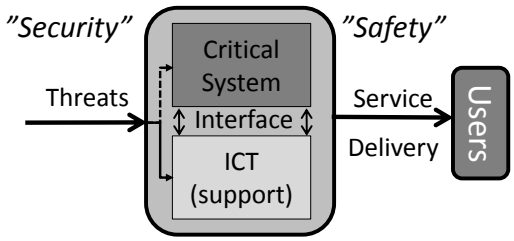

Fig. 2. A model of a specific system for critical services.

We would like to emphasize that there are four boundaries in Fig. 2: the outer system boundary, the two inner boundaries to the critical system (the dashed line) and to the supporting ICT system (the flat line), and the boundary (interface) between the critical system and the ICT system. The threats can then be divided into four groups according to the boundaries shown in Fig. 2.

1. Threats targeting the whole CS–ICT.
2. Threats targeting the interface between the CS and ICT.
3. Threats targeting the ICT part.
4. Threats directly targeting the CS.

We do not consider threats that directly target the critical system (4), in that it is a critical infrastructure. Such threats are already discussed and accounted for in other working groups in the EU and elsewhere. The focus here is on cyber threats, often directly targeting the ICT structure by their very nature. Thus,

the focus is on problems related to the supporting ICT infrastructure, that is (1) – (3) in the list above. We would like to emphasize (2) in the list, as the particulars of this interface may be prone to many security vulnerabilities.

2.2 Specifics of Critical Systems

In order to identify the specific security problems in critical systems we developed the described *model of a system for critical services*. Based on that model we can outline the security specifics of critical systems and why the threats to critical systems and the respective countermeasures need a different approach compared to that of more traditional systems. Even though the emerging and future cyber threats seem common for all ICT applications, there are specific issues regarding the sub-domain of critical systems. There are many differences compared with a regular ICT system. In a regular system, there is no ICT–CS boundary. A regular ICT system is not normally connected to a system governed by physical laws. This implies that a regular ICT system does not have the same constraints in terms of timely input of data or a similar limitation on the types of interfaces available. No critical service is delivered by a regular system.

We divided the *system* box in Fig. 2 into two parts: one part being the actual critical system (or critical infrastructure) and the second part being the supporting ICT infrastructure. In some cases, the critical system is of an ICT nature; in other cases it is a traditional process control system. Some of the specific characteristics of a critical system as shown in Fig. 2 are described in more detail below.

Critical service. A critical system is delivering a critical service to users, which has to be preserved and maintained even in the case of cyber attacks. The disruption of operation of such systems will lead to severe consequences.

Complexity and availability. The complex architecture of critical infrastructures hampers investigation and assessment of the impact of threats. Further complicating the issue is that many of these systems need to run around the clock all days of the year, meaning that a system cannot simply be brought off line for testing or security update.

Many and different interfaces. There are various types of interfaces to a critical system, since it is the result of combining several independent systems and they differ greatly in many ways. This affects the vulnerability of the system as a whole. Critical systems have specific and diverse relations with ICT systems and between internal systems. Further, the system mixes interactions of human operators (slow response) with computer services (fast response) through a variety of interfaces. Many times these interactions are rather complicated in that the access modes vary and the time frames between the parts are widely different.

Interdependency issues (long chains of dependencies). One of the important issues for critical infrastructures is the interdependencies among the infrastructures. There may be long and complex dependency chains. An attack

against any of the services may cascade unpredictably through the system. In [3], the role of ICT in critical infrastructures is defined with the term cyber interdependency. An infrastructure has cyber interdependency if its state depends on information transmitted through the information infrastructure.

Data is important. Almost always, data is important [4]. This is especially true for *financial services*. It is also true for other types of systems, such as air traffic control, where data are underlying even the simplest decisions.

An underlying physical process. Many times, a physical process is underlying the critical system. The system has to observe time constraints which are hard to combine with certain security measures. The critical system may be part of a *control loop* in the physical system. Thus, critical systems have physical and possibly a very complex interaction with the environment. Security functions integrated into the critical system must not be allowed to compromise the normal functionality of the critical system [5].

Real-time constraints. The connection of a CS to the physical world implies that critical systems are often real-time, as they are determined by physical systems. They may also be considered real-time in that they deliver a critical service that should not be interrupted. Depending on the specific system, the term "real time" may imply very different time scales – from seconds to days. Critical systems are generally time-critical and have to respect some acceptable levels of delay and jitter dictated by the individual installation. Some systems require deterministic responses. This may mean that they have to observe time constraints, which are hard to combine with certain security measures. High throughput is typically not essential to CS. In contrast, ICT systems normally require high throughput, and they can typically withstand some level of delay and jitter [5].

Many owners, policies, and domains. Often, a critical system has many owners and this fact is emphasized through the deregulatory nature of policy decisions taken lately. The mixed ownership affects the system as a whole, in that there are artificial interfaces between the parts and each part may be governed by its own security/safety policy. For example, data is often sent over both propriety networks and the Internet.

Trade-off between safety and security. Based on the tradition of safety-critical systems, safety is and has been emphasized over security. For example, passwords are sometimes avoided by intent; it is reasoned that sometimes it is very important to immediately be able to control a process (to stop it from reaching a critical point), and a password would only slow down the operators. Thus, no regards to integrity or access control exists in such a system and such features cannot easily be added later, or added to one part of the system if another part lacks such support.

Mismatch of practices between CS and ICT systems. Operating systems and applications in critical systems may not tolerate typical IT security practices. Legacy systems are especially vulnerable to resource unavailability and

timing disruptions. Control networks are often more complex and require a different level of expertise (e.g., control networks are typically managed by control engineers, not IT personnel). Software and hardware are more difficult to upgrade in an operational control system network. Many systems may not have desired features including encryption capabilities, error logging, and password protection [5].

The human factor plays a pivotal role for proper operation. The human being is considered to be the weakest point in a critical system. The roles include operators in control rooms, engineers taking technical decisions, managers and decision-makers for future strategy development. On the other hand, insiders with experience of and knowledge about the critical system could be a serious threat as seen, for example, in [13].

3 Example Scenario

We illustrate with an example scenario how the specific characteristics of critical systems described above influence information security of these systems. Although the example scenario is completely fictional, it was considered by domain experts as being realistic in that it shows some real or emerging threats for which no ready solutions are available.

The example scenario takes place on an oil platform. That domain, i.e. the oil platform, is specifically chosen because it embodies many of the problems related to critical systems' security highlighted by domain experts, such as the trend to increase efficiency through greater automation and more remote operations. The organizational structures are becoming more complex and there is an increased reliance on computer systems that are vulnerable to malfunctions and malicious attacks. The introduction of ICT opens up the previously isolated critical infrastructures to the information infrastructure and exposes them to threats.

The antagonist in the scenario is a single person with strong environmental ties who wants to make a "statement" about the dangers of the current oil dependency by shutting down an offshore drilling platform. Using his skills and some internal knowledge about the system, he manages to reach the main functionality of the platform. However, instead of stopping the production of oil on the platform, his attack causes a large oil spill with a severe environmental impact. Below, we give a brief overview of the attack, which is further elaborated in [1].

3.1 The Attack and Its Consequences

In order to reduce costs and increase effectiveness, oil platforms are connected in a bigger infrastructure involving remote control centers and a number of expert nodes in case problems occur. The antagonist in the example scenario takes advantage of such a trusted expert node by installing malicious software that does not spread actively, but propagates only when the victim host initiates its

own connection to this server, thus working in much the same way as current malware in the web domain. The malicious server software is tailored towards the victim environment. The antagonist has an insider's view (from his previous work on the oil platform) and knows its weak points, i.e., vulnerable routers that can be corrupted, as well as the means to grant himself sufficient authorization for his goal of shutting down the oil production of the platform (known passwords). He manages to reach the control network and connects to a critical console. At that point, the safety systems on the platform fail and thousands of tons of oil flow into the ocean.

3.2 Related Threats

In Sect. 4, we go through the threats against critical systems in detail. Here, we highlight the threats particularly important to the execution of the attack described in the scenario. Issues related to the *use of commercial-off-the-shelf components*[4] and *retrofitting security to legacy systems* are fundamental to this scenario. Some of the systems are simply vulnerable to "normal" malicious code, and the antagonist uses this fact to download his code onto the offshore platform. The antagonist then uses his detailed knowledge of the system (*the insider threat*) for his next step in the attack. As *safety takes priority over security* in many industrial domains, we emphasize the non-existing password policies at the offshore platform. The domain is complex and issues such as *unforeseen cascading effects* and other problems due to scale also work in favor of the antagonist. Even though not explicitly mentioned, the human factor probably played a role in this scenario, and better designed *user interfaces* might have alerted the operators in time to the failure of the safety system. Finally, we would like to point out that in this story the antagonist was never brought to justice; legacy systems, where security has not permeated the design, seldom have the necessary sophistication for allowing advanced forensic analysis.

3.3 Discussion

Some of the discussed related threats are common to all ICT systems and there are countermeasures developed to overcome them. The problem with critical systems is that the security techniques cannot always be implemented directly. In most cases, they need to be modified according to the timing and performance requirements of the critical system. Even if tailored to the system's constraints, security mechanisms may still not work properly, since it is almost impossible to test them before implementation, because critical systems' operation should not be interrupted.

More interesting for our study, however, are those security threats that are specific to critical systems. Some of them are known to the professional community and there are solutions proposed and implemented. Other threats are just beginning to appear with the introduction of modern technologies in critical

[4] The threat names are printed in italics.

systems and the new, not studied or poorly understood, interactions of the CS and the ICT. We will focus our discussion in the next section on these specific security threats.

4 Emerging and Future Threats to Critical Systems

Based on the characteristics of critical systems discussed in Sect. 2.2, we have identified areas where security threats might grow in the future and where new solutions should be sought for. The identified threats to critical systems summarize the views of many experts both from the domain of information security and industrial automation/critical infrastructure protection, and reflect the general vision that critical systems can become an attractive target for cyber attacks and that the cross area of ICT and CS is an open field for security research. Fortunately, there are not yet many (publicly known and documented) examples of successful attacks to critical systems, but the present experience shows the clear need for effective and specific countermeasures in this domain.

In the following subsections, we describe the identified cyber threats to critical systems and discuss some of the possible solutions. We focus on the ones relevant to the described scenario, but also include other important threats to critical systems. The full list of identified threats can be found in [1].

4.1 Use of Commercial-Off-The-Shelf Components

Threat. The use of Commercial-Off-The-Shelf (COTS) components and systems can make any system, but especially a system connected to a critical infrastructure, vulnerable to a variety of attacks. There are two problems with COTS components. The first problem is related to hidden functionality and outsourcing, as described in Sect. 4.9. The designer has no real control over the product he is introducing into his system. The COTS product is designed (and manufactured) elsewhere and the documentation can be incomplete or even faulty. There is no guarantee that there is no hidden functionality. Nor can its absence be verified, as discussed in Sect. 4.9. The second problem is related to the generality of the COTS systems versus the sometimes very specific requirements of the environments where they are used. It is this second problem we describe below.

To reduce cost and time for design, the use of COTS systems and components in critical applications seems attractive and will thus continue. COTS systems are often used in industrial automation process-control systems because they are cheaper to deploy and may include more functionality than a custom-built system. However, there is a gap between the priorities (safety versus cheap COTS components) and this gap leads to new challenges to security and reliability. For example, COTS systems are prone to "normal" virus infections and attacks, so attackers do not need to specifically tailor their malicious code to these systems. There will be remote access through connections to the Internet, leading to new threats. Response management is needed, coping with incidents – recovery,

isolation, and restoring the system to a working state. Forensics should also be applied to determine the responsibilities.

There are some projects (e.g., DEAR-COTS [22]) where COTS components are applied to design distributed computer-controlled systems. They are organized using redundancy and design diversity to make the system dependable and secure. Some of the issues addressed in DEAR-COTS are the use of emerging information technologies to cope with heterogeneity issues while providing a dependable user-friendly man-machine interface.

Possible solutions. No good solution exists, but various work-arounds, such as using COTS systems with some fault-tolerant approaches (replication, diversity approach); applying COTS components in non-critical areas only; introduce and manage heterogeneity; or use of a compact and trusted application base.

Another possible approach is to introduce semantic technologies, i.e., to take a holistic approach to security with semantic technology (e.g., service-oriented architecture). Physical components should be classified, as they have to be defined from the basis. We have to identify and decide what and how to protect, i.e., an assessment of the assets to be protected has to be done.

4.2 Retrofitting Security to Legacy Systems

Threat. Security can seldom be retrofitted to an existing system, but due to economical constraints this is sometimes considered necessary. Most critical systems are created to provide a certain functionality. Safety and control characteristics are the natural focus of such systems. Thus, applying security measures afterward instead of incorporating them in the original design could constitute a problem. For example, the in-vehicle network has historically been a closed environment responsible for the control and maneuverability and safety of vehicles. The in-vehicle network has been designed to provide this functionality and security has not been part of the design. In the connected car of the future, external communication is allowed to interact with the previously isolated in-vehicle network. Thus, the in-vehicle network is opened up to potential attacks. Designing security solutions for the existing in-vehicle network creates difficulties as real-time constraints, protocol and hardware limitations need to be considered. In addition, security solutions must not interfere with the functionality provided, e.g., by imposing delays as this could have serious consequences from a safety perspective. Due to economical constraints it may not be possible to redesign the entire system with security in mind. Either the best possible security solutions considering the existing system are developed and applied and as a result possibly degrading the system's performance, or good enough solutions are applied to ensure that the existing system's functionality is left unaffected.

Possible solutions. The short-term solution could be a better understanding of how to best adapt security to such systems. Experts recommend [15] to study all connection points in the network, understand what traffic has to flow from the old networks into the business network. The information should be flowed

through a more modern server, which can be better protected and analyze the traffic in real time. In general, analyzing the current architecture in detail and cataloging all software running on the control networks help discovering the weaknesses of the network and strengthening its security.

New architectures can be developed where security permeates all parts of the design for the long term. Migrating to new technologies, however, takes time, while security is needed at the present moment and this reality could influence the process of introducing new and more secure technologies.

4.3 The Insider Threat

Threat. A definition of the "insider threat" is given in [13]. This threat lies in the risk that a trusted employee betrays his employer by conducting some kind of malicious activity. Insider betrayals comprise a broad range of actions, from theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even work place violence. Insider activities cause financial losses to organizations, have negative impacts on their business operations, and damage their reputation.

In [13], it is argued that the nature and seriousness of the threat requires a combined view of physical and IT security systems and policies. Although physical and cyber threats from insiders manifest differently, the concepts are quickly converging as many potential attacks bear characteristics of both physical and IT sabotage, fraud, or theft.

Some interesting results from a study on the insider threat [14] show that a negative work-related event is most likely the trigger to most insiders' attacks. Furthermore, the majority of insiders planned their activities in advance. An observation is that the majority of insiders were granted privileged access when they started work, although less than half of the insiders had authorized access at the time of the incident. An interesting point is that both unsophisticated and relatively sophisticated methods for exploiting a system's vulnerabilities were used. Remote access was used to carry out the majority of the attacks. Many times, the insider attacks were only detected when there was a noticeable irregularity in the information system or when a system became unavailable.

Possible solutions. Effective strategies for discovering an "insider" is an open research question. The recommendations from [13] include low-cost, easily implemented policy solutions for near-term effect: education and awareness, employee screening, technology policy, information sharing. In the long-term aspect, further guidance, findings, samples, and tools are needed. Some solutions for IT systems/cyber security could be the following: to use integrated IT and physical security system tools to identify rule violation patterns for potential insider threat behavior; to use dual protection access technologies (e.g., biometric, key card or encryption key verification); to use dual control access mechanisms to protect high-value systems and processes; to manage access, integrity and availability of computer systems (e.g., identity management system). Control over creation and termination of user and administrator accounts and maintaining

security/access rights should be done by segregation of duties. Using data loss prevention tools could help stopping the leakage of information outside the network and can be a measure to detect an insider activity.

4.4 Safety Takes Priority over Security

Threat. In the domain of critical systems, both safety and security are important but in certain scenarios, safety takes priority. Based on the tradition of safety-critical systems, safety is and has been emphasized over security. Giving priority to safety, however, is not just a traditional vision. It is justified by the potential losses after a safety incident. Safety of critical systems is important because of critical system's interaction with the physical world and the possible risks of that interaction. Security is usually considered being of less importance compared to the major safety issues of the actual CS. With the extensive use of ICT in critical systems, however, security should be considered more seriously, since security and safety are very interrelated. Problems with security can lead to safety issues. Thus, a security attack can lead to a safety problem and endanger lives.

Complicating the issue is the fact that control system professionals are often not aware of security risks, since these are not considered part of the normal system operation. The emphasis in control systems is on safety and availability aspects. On the other hand, IT security specialists use known techniques from a normal ICT system to introduce security, but may be missing important safety and control characteristics of the specific CS, as discussed in Sect. 2.2 and Sect. 4.2. This lack of mutual understanding between the control and security communities makes the overlooking of security a problem. Control specialists and even the management personnel of organizations are security-unaware and tend to neglect security measures and tools. Sometimes people with little experience or with different primary tasks operate the supporting IT system and they are more prone to do mistakes or ignore security alerts.

Possible solutions. As we stated previously, the understanding that safety and security are interrelated is of very high importance and will lead to improvement in overall security and safety policy. A better understanding of the domain for the IT security experts is necessary. On the other hand, the control community should be aware of the important role of security measures to safety. Work should be done on changing the mindset. Some simple technical measures could be to document changes done to the system in order to facilitate the implementation of security tools where they are most needed; keep the control traffic off the business network; document all the software installed on the network, etc.

4.5 Unforeseen Cascading Effects

Threat. Interconnected systems and networks are difficult to model properly and interdependencies between them can lead to cascading effects that are hard to foresee. This is due to the inherent complexity of the connected systems. It is

claimed that nobody *really* understands a network such as the Internet anymore, nor even many smaller interconnected, heterogeneous networks that have been deployed over the past decades. Further, testing is virtually impossible due to the complexity and scale. In particular, testing is often impossible when the system is connected to a critical infrastructure with real-time requirements.

An important class of cascading effects occurs when, e.g., some section of the Internet is attacked or overloaded to the point of service denial and another (perhaps critical) system depends on that section. Even though the attack was not directed against the critical system per se, it is affected indirectly.

It is clear that dependencies are responsible for unforeseen cascading effects. Unfortunately, dependencies in large networks and systems are very difficult to understand due to their complexity. Even though system complexity is an issue in many areas, some factors related to critical systems make the issue of the complexity extra severe in such environments. First, due to the deregulation of markets, critical infrastructures are often run by different organizations that need to cooperate. These organizations are seldom a single unit, but they are comprised by many smaller units as virtual organizations. A complicating issue is then that part of the system may be governed by proprietary protocols while others use open standards. Different system owners may not trust each other, and different parts of the system may be governed by their own safety/security policies.

Possible solutions. What we need are new, more appropriate modelling tools and an overall better, probably structured and hierarchical, architecture with a security baseline. Removing the human from the loop and introducing automation may help. On the other hand, the seemingly intuitive action scripted in automated systems might be completely wrong in certain systems and lead to large problems. For essential services, it is important that dependencies should be tracked from the design phase onwards.

4.6 User Interface

Threat. The human plays various roles in control systems at all levels of their operation. For example, in a real critical system, it has been estimated that in some situations, human reliability can fall from 10^{-4} to 10^{-3}, whereas a system's reliability is maintained at 10^{-9}. Incorrect interactions with the system, handling other operator errors, and complex interdependencies as described above make it difficult to correctly work with the system. For these reasons, the human being is a serious factor when considering overall system security.

It is imperative to wrap new solutions to upcoming and even existing threats in understandable and discreet user interfaces to make sure they are properly used. The user information overload is a constant problem that is very likely to persist for a long time and hinder solutions for security problems to catch, even if they already exist.

Possible solutions. The education and training of personnel working in critical systems is a constant task that can help maintain an up-to-date knowledge on systems and networks. The awareness of security risks should be raised. There are many bad practices (e.g., running un-patched versions of software, using default configurations and passwords, etc.) that could easily be removed by making people understand the role of security measures. A sound and evolving security policy in the organization is needed to mitigate security risks. There are approaches to model the user (cognitive modelling) and user-interactive properties that could be used to improve the interaction of the users with the systems.

Another approach is to model and design the systems in such a way that they are more easily comprehended and understood. This would include, e.g., structural design, encapsulation, intuitive interaction interfaces, etc.

4.7 Sensor Networks

Threat. The convergence of control with communication and computation will make sensor networks the new dominant "computing class." This class will provide the ability for large numbers of interconnected sensors, actuators, and computational units to interact with the physical environment. This computational shift is going to bring a big shift also on computer security issues.

One problem is that small sensors require a means to communicate. This is typically a wireless connection. However, in addition to the security concerns of wireless networks in general (discussed in Sect. 4.8), wireless sensor networks have a number of additional issues. For example, the nodes in sensor networks are in general very limited in terms of battery, storage, and computational power. Therefore, strong cryptography and other general security tools are of limited use, if at all available. An attacker can have much more powerful hardware than the nodes being attacked. Sensor networks also typically reside in unattended environments where an attacker can physically destroy nodes, add malicious nodes or in other ways tamper with the hardware of the network. It is usually hard to distinguish the natural failures of the nodes in a sensor network from a malicious attack where nodes are deliberately destroyed.

There are many venues of attacking sensor networks [6,7], including the following: snooping information, inserting false or misleading information, jamming radio channels, making nodes run out of battery by never letting them sleep, giving the impression of phantom nodes that do not exist, giving the impression of connectivity that does not exist, making messages go through an attacking node that can selectively drop messages from the system.

Possible solutions. In summary, we consider the following three approaches worth further pursuit in the context of sensor devices.

- Autonomic solutions where the system will continuously evolve and control its security.
- Solutions that will mask subsystem takeover.
- Combining sensor information with physical information for verifying certain operations.

4.8 Wireless Communications in Industrial Environments

Threat. Wireless communications offer many convenient advantages compared to traditional wired communications within the industrial domain, such as: operator mobility, safety by enabling remote access to noxious environments, access security for visualization and optimization, and the immediate benefits of their deployment [9].

Today, wireless communications are not yet widely used in practice in industrial environments. Most plants are only considering them for information gathering in the form of measurements, but not for closed-loop control [8]. Based on their advantages, however, a greater adoption of wireless communications in industrial control can be expected, thus with an overall growth in their market share. Experts from WINA and ISA [10] predict that within 10 years, even critical control communications will be wireless.

Recently, following the WirelessHART and ZigBee Alliance announcements and after approving the SP100 standard for industrial wireless communications by ISA, there is already use of wireless communications in industrial and even critical applications. Despite this, the single industrial wireless standard ISA-SP100.11 does not give enough guarantees for dependability and security to critical systems and applications.

One main security aspect of the wireless communications in general follows from the unbounded nature of radio frequency propagation. The perimeter of a wireless network cannot be limited and controlled as can be done with a wired network. There are reflected signals, which find their way out of buildings. These dispersed signals could be detected by motivated attackers that could then attempt to interfere with them if they are in physical proximity of the facility. Thus, traffic can be passively captured and an attempt to penetrate the network could be made with the aim to reach other connected enterprise networks.

Possible solutions. The first and main consideration when addressing security of industrial wireless communications is the conformity to the ISA-SP100 Usage Classes. Many useful and detailed recommendations for securing wireless networks are given in [11].

The IEEE 802.15.4 standard [12] gives some recommendations how to use guaranteed transmission mode and secure mode. It is shown that cryptographic randomization, agility, and diversification, in a game-theoretic context can provide the tools for building resilient wireless networks against both external and internal attacks. Such techniques can even allow the identification of internal attackers.

4.9 Hidden Functionality

Threat. One threat of paramount importance is that of hidden functionality in systems, and in particular, in software. Hidden functionality may comprise almost any functionality, but common examples are back doors, i.e., secret and undocumented entries to a system, and Trojan horses. Such functionality can

be introduced into the system by accident, but the most common reason is that somebody, for example, the designer or maintenance engineer, enters this functionality for his own, in many cases malicious, purposes. In other cases, it is introduced for commercial reasons. Regardless of its purpose, the idea is that this extra hidden functionality is not known by the authorized user and the rightful owner of the system.

It is evident that such functionality presents an enormous threat. Not only is it unknown, but it is also put into the system in such a way that it is very hard to discover. Furthermore, this functionality is uncontrolled and can lead to a large range of very detrimental impacts on the system. As an example, in the U.S., the possibility of malicious hardware used for espionage, or even for terrorist activities is considered an emerging threat. Most hardware fabrication is nowadays outsourced. Circuits can be added on chips at the fabrication plant to offer a back door to potential attackers, or perform some other action. It is technically very hard for vendors to detect whether the produced hardware follows their design to the letter.

Possible solutions. It is very difficult to find solutions to this problem. Any type of remedy would imply the ability to prove, or at least make plausible, that no such functionality exists. Unfortunately, there are significant theoretical obstacles in proving the *absence* of something. It is certainly possible to find and remove such functionality, but to verify that there is none left after removal is extremely hard. Still, the only possible solution would be to develop better validation and verification methods and tools. A methodology for measuring security could be one of them as well as runtime detection of any unknown (malicious) functionality. In the short term, potential solutions to this problem might involve the use of secure and trusted fabs for critical hardware, such as the one used for aviation and military equipment.

4.10 Next Generation Networks

Threat. Recently, there is a general trend for carrying multimedia in the field of electronic communications. Under the pressure of the Internet, on the one hand, and because of the increased service requirements of end users, on the other, some telecommunication companies are migrating to the so-called Next Generation Networking (NGN).

NGN is a broad term describing some key architectural modifications in the telecommunication core and access networks that have been deployed in the last five years. The main goal of NGN is that one network transports all information and services (voice, data, and multimedia) by encapsulating them into packets. NGNs are commonly built around the Internet Protocol and therefore the term *all-IP* is also sometimes used to describe the transformation towards NGN [16].

The openness and easy access and usage of NGN lead to an increased number of vulnerabilities and extreme attention to security measures must be paid. Recently, many security experts bring up the attention to the specific vulnerabilities of the NGNs. The most exploited among them are [17,18]:

- Knowledgeable end users can gain access to the control plane of "all-IP" networks like NGNs.
- Large number of external connectivity points (and from any other point/site of the Internet)
- Shared core network among several NGN operators (the possibility of occurrence and the variety of vulnerabilities is higher)
- Malicious users can manipulate the traffic more easily as no physical access is required.

More than 32 fundamental vulnerabilities in NGNs are described as a result of the systematic assessment of NGN vulnerabilities [19].

Possible solutions. Security mechanisms on open packet networks will be very different from those of legacy telecommunication services in many aspects. In legacy networks, being circuit-oriented vertical networks, much policy management was "built into" the integrated service, comprising all aspects of the network. Security will need to be addressed differently in the NGN. The design and implementation of NGN need to meet complex requirements, which complicates its security architecture. As a consequence, it is difficult to use a single standard to define it [20]. As a present security solution it was recommended in [21] to use *multiprotocol label switching* (MPLS) virtual private networks to construct an NGN virtual private bearer network, and thus logically separate NGN services from traditional data services. As telecommunications companies already deploy NGNs in different forms (e.g., Vivacom in Bulgaria, KPN in the Netherlands, Ireland [16], British Telecom's *21CN*), this is an important problem.

5 Conclusion

Although information security, as a fast developing research direction, offers new solutions to counter cyber threats, there are domains where the existing security techniques cannot be applied directly. In some areas, the necessity to protect systems from cyber attacks is just beginning to be realized. Even though there is a rising interest and concern of the lack of cyber security of critical systems, the research in this area is still scattered and somewhat isolated to particular domains. A more thorough understanding of the risks and the need for new security solutions that focus on the emerging threat areas and the specific characteristics of critical systems is necessary.

The paper demonstrates some of the problems in implementing security in critical systems. The identified and described threats to these systems indicate the research areas where new security solutions are needed. Current practice shows that known IT security measures should be implemented considering the specifics of critical systems. Those measures should respect time constraints, continuous operation mode of these systems, their requirements for availability and safety, their heterogeneity, complexity, and interdependence, etc. New, possibly holistic, solutions should be developed, e.g. building in security at design

level, applying service-oriented architecture, organizing systems according to the "defense-in-depth" strategy, resilience approach to their design and operation.

We have to note that critical systems encounter many different security problems that are a mixture of technological, psychological, and social issues. This calls for interdisciplinary approaches to be adopted to address the diverse threats to critical systems.

References

1. ICT FORWARD Project: Deliverable D3.1: White book: Emerging ICT threats. http://www.ict-forward.eu/media/publications/forward-whitebook.pdf, (2010)
2. Commission of the European Communities: Green Paper On a European Programme for Critical Infrastructure Protection. http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf, (2005)
3. Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 11–25 (2001)
4. G.T.I.S. Center: Emerging cyber threats report for 2009. http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf, (2008)
5. NIST SP800-82: Draft guide to industrial control systems (ICS) security. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf, (2008)
6. Chan, H. and Perrig, A.: Security and privacy in sensor networks. IEEE Computer, 36(10), 103–105 (2003)
7. Perrig, A., Stankovic, J. and Wagner, D.: Security in wireless sensor networks. Commun. ACM, 47(6), 53–57 (2004)
8. Kagan, H.: Interview about wireless devices adoption in the industry and the future trends. Frost & Sullivan, http://www.teknikogviden.dk, (2008)
9. Berra, J.: Emerson first to offer WirelessHART automation products. http://www.controlglobal.com/industrynews/2008/082.html, (2008)
10. Hoske, M. T. and McPherson, I.: Industrial wireless implementation guide. Control Engineering, http://www.controleng.com/article/CA6584939.html, (2008)
11. Masica, K.: Recommended practices guide for securing ZigBee wireless networks in process control system environments, Draft. http://csrp.inl.gov/Documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf, (2007)
12. IEEE 802.15.4 Standard, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs).
13. Noonan, T. and Archuleta, E.: The National Infrastructure Advisory Council's final report and recommendations on the insider threat to critical infrastructures. http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf, (2008)
14. Keeney, M.: Insider threat study: Computer system sabotage in critical infrastructure sectors, Executive summary. http://www.secretservice.gov/ntac/its_report_050516.pdf, (2005)
15. Welander, P.: Securing legacy control systems. http://www.controleng.com/article/307540-Securing_Legacy_Control_Systems.php, (2009)

16. Wikipedia: Next generation networking (NGN all-IP). http://en.wikipedia.org/wiki/NextGenerationNetworking, (2008)
17. Fonash, P.M.: Cybersecurity & Communications (CS&C) overview, Technology trends, & challenges. http://events.sifma.org/uploadedFiles/Events/2008/BCP/Fonash%20presentation.pdf, (2008)
18. Kim, R.-H., Jang, J.-H., Youm, H.-Y.: An efficient IP traceback mechanism for the NGN based on IPv6 Protocol. http://jwis2009.nsysu.edu.tw/location/paper/An%20Efficient%20IP%20Traceback%20mechanism%20for%20the%20NGN%20based%20on%20IPv6%20Protocol.pdf, (2008)
19. NSTAC: Next Generation Networks Task Force, Appendices. http://www.ncs.gov/nstac/reports/2006/NSTAC%20Next%20Generation%20Networks%20Task%20Force%20Report%20-%20Appendices.pdf, (2006)
20. Zhimeng, T., Bo, W., and Yinxing, W.: Security technologies for NGN. http://www.ztebrasil.com.br/pub/endata/magazine/ztecommunications/2007year/no4/articles/200712/t20071224_162457.html, (2008)
21. Yuxi, G.: IP Bearer Network for NGN. http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2005year/no3/articles/200509/t20050921_162351.html, (2005)
22. DEAR-COTS project homepage. http://dear-cots.di.fc.ul.pt, (2001)