On the Protection and Technologies of Critical Information Infrastructures

Javier Lopez, Cristina Alcaraz, and Rodrigo Roman

Computer Science Department
University of Malaga, Spain
{jlm, alcaraz, roman}@lcc.uma.es

Abstract. Critical Infrastructures are complex and highly interconnected systems that are crucial for the well-being of the society. Any type of failure can cause significant damage, affecting one or more sectors due to their inherent interdependency. Not only the infrastructures are critical, but also the information infrastructures that manage, control and supervise them. Due to the seriousness of the consequences, the protection of these critical (information) infrastructures must have the highest priority. It is the purpose of this book chapter to review and discuss about these infrastructures, to explain their elements, and to highlight their research and development issues. This chapter will also discuss the role of Wireless Sensor Network (WSN) technology in the protection of these infrastructures.

1. Introduction

The well-being of the national and international economy, security and quality of life, is becoming increasingly dependent on the safety and the robustness of *Critical Infrastructures* (CI), such as energy, banking, transport, and others. These infrastructures are extremely complex, since they are composed of both physical facilities and highly interconnected national (and international) software-based control systems. These information systems can also be considered critical by themselves, and are commonly called *Critical Information Infrastructures* (CII). Not only the internal elements of critical (information) infrastructures are highly interconnected with each other, but also the infrastructures themselves need other infrastructures in order to function properly.

The notion of criticality in the context of infrastructures is intertwined with the nature of the threats that affect those infrastructures and the possible effects of a single failure. In fact, due to their complexity and their existing interdependences, infrastructures are affected by a diverse number of security risks and vulnerabilities. Such vulnerabilities can be exploited both locally and remotely by a wide range of attackers, like terrorists and malicious/negligent insiders. Lastly, because of those interdependences, any kind of accidental or provoked failure can cascade through and between infrastructures, with unpredictable and extremely damaging consequences.

Protecting CII is an extremely complex task. It is necessary to have clear what the exact meaning of 'infrastructure' is, and what (and why) are the exact sectors that should be considered critical. It is also essential to consider which the differences between CI and CII are in order to effectively discover their specific threats and vulnerabilities. Then it becomes possible to identify who are the different actor groups that need to participate in the protection processes, and what are the challenges that these groups need to overcome in order to adequately protect the infrastructures.

The purpose of this book chapter is to discuss on the previous topics, thus allowing the reader to have a clear understanding of the importance of the protection of critical infrastructures and the existing challenges. The chapter will be mainly focused on CII and will include a discussion on the most important electronic control systems, as well as an introduction to one of its underlying technologies, *wireless sensor networks* (WSN). Moreover, the chapter will provide an overview of the research projects that use such a technology as a foundation.

2. Critical Infrastructures

In order to fully understand what the term Critical Infrastructures refers to, it is necessary to have clear what an infrastructure exactly is. The dictionary definition of the word '*infrastructure*' is "the underlying foundation or basic framework" and "the resources (as personnel, buildings, or equipment) required for an activity" [1]. Such definition is obviously general, and can refer to a broad range of structural elements. Still, it suits to the infrastructures on which we want to focus: civil infrastructures, i.e. the infrastructures that are integral to the social, political, and economic life of a nation. Examples of those infrastructures can be mass transit infrastructures and water treatment systems.

These infrastructure systems have grown in complexity during the course of history: from very simple structures to pervasive, complex, and varied systems. An example can be found in water supply and treatment systems. In ancient towns, citizens had to walk directly to the sources of water, such as rivers or wells. Cities started to grow, and it was necessary to create structures like aqueducts which would carry the water straight from the source. These simple constructions finally evolved into intricate systems that not only transport the water, but also are in charge of treating both the natural water and the wastewater.

The underlying elements of present-day infrastructures are deeply interconnected, and they depend heavily from each other. There are three major elements in an infrastructure: Administration, Physical, and Information System. Administration includes the human aspects (both decision-makers and workforce), and economic, regulatory, and organizational aspects. Physical corresponds to the material aspect of the resource supply system. Finally, the Information System corresponds to the underlying Information and Communications Technologies (such as SCADA, Distributed Control Systems, and others) that manage the infrastructure.

The infrastructures themselves are not the only thing that has evolved over time. During the last 20 years, the actual definition of the word infrastructure in policy terms has evolved as well. Many sectors have been included or excluded from being public infrastructure depending on the definition used at that time. A possible reason is their inherent heterogeneity: each sector is different historically and technically, as well as in their professional practices, financing problems, and public attitudes towards them [2].

Nowadays, the concept of infrastructure in policy terms is more or less stable. In the EU, an Infrastructure is considered as a "framework of (inter)dependent networks and systems comprising identifiable industries, institutions (including people and procedures), and/or distribution capabilities that provide a reliable flow of products, supplies and/or services, for the smooth functioning of governments at all levels, the economy, the society as a whole, and of other infrastructures" [3]. Note that a comprehension of infrastructure may span also their operating procedures, management practices, and development policies [2].

Once the concept of infrastructure is clear, it is possible to apply the concept of critical in this specific context. The word '*critical*' can be seen as the combination of two words: *important* ("marked by or indicative of significant worth or consequence") and *indispensable* ("not subject to being set aside or neglected") [4]. As a consequence, formally speaking, an infrastructure can be considered critical if it has a strong influence over its environment, so strong that if it is not available for a period of time the possible effects are not negligible.

Moving on to the definition of Critical Infrastructures, we realize that such definition is no unique. According to the European Commission, Critical Infrastructures consist of "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States" [5]. On the other hand, the United States consider Critical Infrastructures as "those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [6].

Regardless of their definition, most CI share four key properties: interdependencies, private ownership, ICT dependence, and global boundaries [7].

- Exhibit strong and mutual dependences. A failure in one single infrastructure will cascade and affect others. Due to the inherent complexity of the infrastructures and their relationships, it is extremely difficult to anticipate the scope of such interdependences.
- Mostly (but not only) owned and operated by the private sector due to privatization processes. Note that the private sector is not the only actor group that has influence over these infrastructures (cf. Section 4.1).

- Becoming increasingly dependent on Information Systems, since they basically depend on highly interconnected national (and even international) electronic control systems for their smooth, reliable, and continuous operation.
- Becoming increasingly more international. This is a logical consequence of the increasing globalisation of commerce. As a result, it is not enough to simply develop a purely national methodology for protecting the critical infrastructures.

Differences among between countries can be observed not only in the definition of the term CI, but also in the definition of which are the critical sectors. The conceptualization of whether an infrastructure is critical or not depends on their strategic position within the whole system and the socio-political context, and it is also influenced by specific geographical and historical preconditions. There are also two differing, but interrelated perceptions of criticality: Systemic and Symbolic [8]. In the systemic approach, an infrastructure is critical due to its structural position and its interdependences with other systems. On the other hand, in the symbolic approach the importance of an infrastructure mainly depends on its role or function in society.

The most frequently mentioned critical sectors in all countries are the following: Banking and Finance, Central Government / Government Services, Information and Communication Technologies, Emergency / Rescue Services, Energy / Electricity, Health Services, Transportation / Logistics, and Water management systems. Other important sectors are Food / Agriculture, Information Services / Media, Military Defence, Oil and Gas Supply, and Public Administration. Note, however, that it is broadly acknowledged that the focus on sectors is far too artificial to represent the realities of complex infrastructure systems, thus it is deemed necessary to evolve beyond the conventional “sector”-based focus and to look at the services, the physical and electronic (information) flows, their role and function for society, and especially the core values that are delivered by the infrastructures [9].

All these infrastructures are menaced by certain threats that may hinder their functionality or render them temporarily or permanently useless. Precisely, it is the existence and the possible consequences of these threats what drives the need of considering the criticality of an infrastructure. From a global perspective, threats can be organized into three distinct categories: natural threats (in the form of disasters such as floods, fires, and landslides), environmental threats (e.g. long-term power failure, pollution, infrastructure decay, and others), and human threats. Note that human threats, which are originated from human sources, can be accidental or intentional, and may come from inside or outside the infrastructure [10][11].

One of the key human threats against the security of infrastructures is terrorism. A large number of factors, like regional conflicts and the proliferation of Weapons of Mass Destruction, can fuel the existence of terrorist groups. Such groups can act worldwide, with dramatic consequences both in human and financial terms. Note that there are still other relevant human threats, like corporate espionage and malicious/negligent insiders [10]. Although the probability of the occurrence of these threats is different for a certain socio-economical context, any of the previously

presented type of threats can be able to hinder the provisioning of the infrastructures' services, thus there is a need of quantifying the potential risk of any threat.

Not only the potential risk of existing threats is of importance, it is also significant to measure whether a certain infrastructure is more critical than others. For the EU, the selection criteria of what infrastructures are critical and their different degrees of criticality depends on the following three factors [5]:

- *Scope*: The loss of a critical infrastructure element is rated by the extent of the geographic area, which could be affected by its loss or unavailability.
- *Magnitude*: The degree of the impact or loss can be assessed according to the following criteria: public impact (population affected), economic (significance of economic loss, present and future), environmental (impact on the location), interdependency (between other critical infrastructures), and political (regarding the confidence on the government).
- *Time*: This criterion ascertains at what point the loss of an element could have a serious impact, and at what point it would be possible to recover the functionality of that element.

2.1 Dependencies and Interconnectivity

Generally speaking, a CI is based on a set of collaborative and adaptive components [12], with capability to learn of past experiences. These components communicate with each other in a certain context, and receive as inputs the outputs corresponding from other components. Moreover, a specific input could produce a certain effect on the state of a component. This way of establishing connexions between components can also be applied to the relationships between complex entities such as infrastructures. In other words, most infrastructures depend on other infrastructures. As explained before, this is one of the key properties of critical infrastructures.

Connectivity of infrastructures can be done through dependent or interdependent connections. When the relation between two infrastructures is individual and unidirectional, it is considered a simple dependency connection. This can be seen as a linkage between two points *i*, *j*, where *i* depends on *j*, but *j* does not depend on *i*, and any problem in *j* affects on *i*, but not on the contrary. However, in the real life the connections of infrastructures are much more complex. Every infrastructure is connected to other by means of bidirectional links (*j* depends on *i*, and *i* depends on *j*), known as interdependency connection. This relation implicates that any state of each infrastructure influences on the behaviour of other and vice versa, involving an inter-block between them.

There are four main types of interdependencies that are not mutually exclusive: physical, cyber, geographic, and logical. When an infrastructure depends on the material output (commodities or resources) of other, then the interdependency is *physical*. In this case, any change in the state of an infrastructure could affect upon the other. Other kind of interdependency is the *cyber*, which appeared with the pervasive

computing and the need of automating the infrastructures. It is related to the information transmitted through the information infrastructure by means of electronic or communications lines. In this type of interdependency, the states of the next infrastructures will depend on the output of the current information infrastructure. For large systems, the operation is based on computerized or specialized systems, as for example *supervisory control and data acquisition systems* (SCADA). A *geographic* interdependency occurs when the infrastructures are spatially distributed and close to each other. This proximity could implicate devastating consequences if an unexpected event (fired or explosion) takes place in a determined point of the environmental. Finally, a *logical* interdependency consists of control mechanisms or regulations used to interlink components of different infrastructures without requiring of physical, cyber or geographic connections. Also the human decisions and actions may play an important role in the logic interdependency because any incorrect decision or action could involve serious problems in a system.

3. Critical Information Infrastructures

As previously noted, a CI is highly dependent on ICT because information systems are one of the three major components. The principal task of ICT is to manage, control and supervise the infrastructures, thus allowing their smooth, reliable and continuous operation. However, ICT can be considered as critical infrastructures themselves, because in most cases they are indispensable for the operation of the infrastructures [13]. Thus, the concept of CII arises.

For example, the power industry relies heavily on information technology to regulate power generation, optimize power production, and control demands and power distribution, amongst other things. Such monitoring is carried out by electronic control systems such as SCADA, which are also used to integrate electric companies into regional or national power grids for optimization and redundancy purposes. Another specific example is the Internet because it is used to manage essential services such as financial transactions, emergency community alerts, and military communications [14].

There is no exact definition of the term CII, probably because the information systems can be considered just as an essential part of CI. This is backed up by the definition given in the CI2RCO FP6 project, where CII are “Information processes supported by Information and Communication Technology (ICT) which form critical infrastructures for themselves or that are critical for the operation of other critical infrastructures” [3]. Nevertheless, even if CI and CII cannot and should not be discussed as completely separate concepts due to their interrelationship, it is necessary to distinguish them, at least in conceptual terms.

The need to separate both ideas primarily comes from the specific threats inherent to the information infrastructures, which are specialized in targeting its immaterial contents: the information that flows through the infrastructure, the knowledge that is

created from such information, and the services that are provided. Those attacks can be launched simultaneously from anywhere by unknown actors, resulting on great damage not only to the logical infrastructure but to the physical infrastructure as well [15]. By separating CII from CI, it is possible to have a clear view of the challenges that the CII have to overcome and to be more precise in the development of programs and activities that pursue their overall protection.

Although nature and environmental threats are important to CII, most specialized attacks against these information infrastructures come from humans. A successful attack can disclose sensitive data from an infrastructure, falsify or corrupt its information flow, hinder the functionality of its services, or provide an unlimited – and unauthorized – access to the monitoring and control mechanisms that could be exploited later. Most of these attacks are carried out using ICT (e.g. system penetration and tampering), although attackers can use other non-technological methods, such as social engineering and blackmail, to obtain information that could be used in future attacks.

4. Critical Information Infrastructure Protection

It is necessary to admit the criticality of the information infrastructures and locate the most important threats against their normal operation. However, these are not sufficient conditions for assuring their proper behaviour. Using that knowledge as a foundation, it is indispensable to create and establish certain procedures that efficiently protect the CII against the attacks that may come, anytime, anywhere, from those threats. *Critical Information Infrastructure Protection* (CIIP) can be formally defined as follows: "The programs and activities of infrastructure owners, manufacturers, users, operators, R&D institutions, governments, and regulatory authorities which aim at keeping the performance of critical (information) infrastructures in case of failures, attacks, or accidents above a defined minimum level of service and aim at minimising the recovery time and damage" [3].

The importance of any protection mechanism is dependent on the nature of the existing threats and their possible harmful effects. And in case of these infrastructures, there is no room for discussions. The threats are numerous, and due to cascading effects, the effects of a simple failure can be devastating in both economic and human terms. For example, in 2002, a remote intrusion into a SCADA system of a sewage plant resulted in the dispersion of around 1,2 million litres of sewage into the environment. Also, in 2004, a fault in the air-conditioning system of an important Telco node near Rome affected most of the check-in desks of the Fiumicino airport at Rome. These and other episodes [16] are just a small subset of the possible situations that justify the significance of the protection mechanisms for CII.

Similarly to the previous case, there is a narrow line between CIP and CIIP. Nevertheless, the key focus of CIIP is relatively clear: the protection of the information systems and its services on which the infrastructures depend. Also, due to

the existent and future challenges within the CIIP context, to consider CIIP as a separate issue from CIP is becoming increasingly important. Those challenges are the following [17]:

- The protection of the CII has generally become more important due to the increasing role of the ICT in the management of infrastructures and their interlinking position between various infrastructure sectors.
- The number of computer and network vulnerabilities is expected to remain high, mainly due to the ongoing technological evolution and the unbelievable low priority of security as a design factor. Therefore, future infrastructures will have many critical points of failure due to an ill-understood behaviour of the underlying systems and hidden vulnerabilities.
- The threats targeting CII are evolving rapidly both in terms of their nature (e.g. becoming highly distributed) and of their capability to cause harm (e.g. affecting a physical element with a simple operation).

As this book chapter is mainly focused on CII, the remainder of this section will focus on the protection of such infrastructures. Nevertheless, since CII can be considered as an essential part of CI, the following contents can be also of relevance for the protection of these ones. As an example, the actor groups that have a large influence on CIIP also retain that influence regarding CIP.

4.1 Protection Requirements and Actor Groups

The creation of protection mechanisms for critical information infrastructures is a daunting task. Not only are those protection mechanisms extremely important, but also especially complex. There must be different layers of protection that are in charge of ensuring the safety of the infrastructures before, during and after attacks occur. The existence of these layers is consistent with the special operational requirements of these infrastructures: the main purpose of a certain protection mechanism is to assure that the protected system is operating as it should, and a CII must provide its services at all times. Moreover, there are many different actor groups, such as the public/private sector, the academic community, and the individual consumers that affect or are affected by the protection policies and measures; hence, they must be involved in the creation and maintenance of these mechanisms.

It is possible to divide the protection requirements of CII into four groups [18]: dependability, survivability, law enforcement, and national security. Regarding *dependability*, the existence of basic information security services that provide confidentiality, integrity and authentication to the elements of the infrastructure and their information flow are not enough to consider that the dependability properties are preserved. There should be other methods that assure the availability and reliability of the system, alongside with procedures that analyze the existing interdependences between infrastructures and their inherent risks. Concerning *survivability*, the protection mechanisms that must keep the system safe against abnormal situations should recognize the attacks and the extent of their damage, react automatically to

mitigate the effects of those attacks, and maintain a certain level of service in the most critical *processes*. After those abnormal situations take place, the system must recover their essential services as soon as possible and provide an output about the situation that could help on improving the robustness of the system against future attacks.

The existence of the other two groups, *law enforcement* and *national security*, is justified by the interdisciplinary nature of the CII: there must be a legal framework and a policy framework working beyond the scope of a single infrastructure or set of infrastructures. In particular, for law enforcement, policies are needed that facilitate the cooperation between the different actors, allowing the existence of mutual agreements. Also, through that cooperation, the private sector must be capable of identifying and localizing the infrastructures with the highest priority in their socio/economical context. Beyond law enforcement, all relevant actors must have the necessary procedures to prevent and react against any problematic situation of relevance at a (inter)national level. Those procedures include building awareness about a certain problem, providing information in case of emergency, and reacting/mitigating against the emergency scenarios.

As previously noted, there are many actor groups dealing with CIIP. The public sector consists of governments and their different agencies. They are responsible of the economy of their countries and the well-being of their citizens, and have a strategic role due to their global point of view and capacity to provide assessment, coordination, and leadership. The private sector owns and administers most infrastructures due to the privatization processes (since the 1980's in Europe and much before in US) [19], thus has the task of actually implementing the protection policies. The third actor group is the academic community, that is capable of undertake medium and long-term research on many fields related to infrastructure protection, ranging from the technical issues to the socio-economical dimensions of the topic. Finally, the individual users or consumers can be considered as the final actor group. The existence of efficient protection mechanisms is difficult to achieve without the participation and cooperation of all the actor groups involved.

All these actors do not have a single perspective on CIIP since all consider the topic from different perspectives and with different motivations. As a result, there can be different, yet equally valid, viewpoints that discuss about what needs to be protected, by whom, with which measures, and so on. The answers may vary depending on the scenario, and are linked to the question of which protection efforts, goals, strategies, and instruments are appropriated for problem solution in a certain context [20]. Such viewpoints are observed below:

- The system-level, technical viewpoint: CIIP is approached as an IT-security or information assurance issue, with a strong focus on internet security. Threats to the information infrastructure are to be confronted just by technical means such as firewalls, anti-virus software, or intrusion and detection software. The establishment of early warning approaches such as Computer Emergency Response Teams (CERTs) is an example of this perspective.

- The business viewpoint: here, CIIP is seen as an issue of "business continuity", especially in the context of e-business. This requires not only permanent access to IT infrastructures, but also permanently available business processes to ensure satisfactory business performance. Protection mechanisms used in this perspective include the ideas used on the technical viewpoint, but also includes organizational and human activities. This perspective is also reflected in some countries' protection approaches that mainly aim to support the information society.
- The law-enforcement viewpoint: CIIP is seen as an issue for protecting the networked society against technology-enabled crimes of major and minor scale. This type of protection involves more or less traditional law-enforcement strategies and is assisted by adopting appropriate legislation and fostering international co-operation.
- The national-security viewpoint: this is a very comprehensive view of CIIP where the whole society is perceived as being endangered, so action must be taken at a variety of levels (e.g., at the technical, legislative, organizational, or international levels). Actors involved in protection efforts include government officials from different agencies, as well as representatives of the private sector and of the general public.

4.2 Research and Development Issues

Once the protection requirements and the different actor groups are known, it is possible to enumerate which are the most important Research and Development topics that pursue the fulfilment of such requirements. Those topics can be divided into eight categories, and are presented below. Each category have been gathered from the different research communities and government agencies and then verified by relevant actor groups [3].

1. *Holistic system security*. This research topic considers the security of the CII as a whole, rather than the security of its individual parts. Therefore, research efforts in this area deal with the discovery and analysis of interdependences between infrastructures. In addition, it is also necessary to create realistic simulation models that could both serve as a testbed and provide an insight on the effects of future attacks. This research topic mainly comprises (inter)dependency and complexity theory and cascading theory, alongside with simulation and modelling of complex systems.
2. *Risk management and vulnerability analysis*. In order to know how to effectively protect a particular infrastructure, there should be certain procedures that evaluate their inherent risks, analysing the impact on CII of attack scenarios and the present or future reaction of the elements of the infrastructures under such circumstances. It mainly comprises risk and vulnerability awareness, assessment, and management, as well as information security and scenario management.
3. *Prevention and Detection.* Security on CII must be proactive rather than reactive, i.e. it has to act in advance to deal with an expected difficulty. Therefore, both the human and computer elements of the system should be warned against any possible or ongoing abnormal situation that is taking place. This research topic mainly

comprises *Early Warning Systems* and *Intrusion/Malware detection*, plus setting up information sharing networks.

4. *Incident Response and Recovery*. Just as CII must function properly and provide their services anytime, unforeseen events and attacks can also happen anytime. As a result, these complex networks must be designed to rapidly respond to any adverse situation and recover their functionality as soon as possible. It comprises the existence of support tools for Computer *Emergency Response Teams (CERTs)* and incident analysis, response, and recovery.
5. *Survivability of Systems*. Detecting and Reacting against external or internal malicious events is not enough for a CII. The protection mechanisms must concentrate all their efforts on allowing the business continuity by means of adequate optimisation strategies and survivable systems and architectures. Mainly, it comprises security and resilience of hardware components, operating systems, and the process of software engineering, along with procedures for redundancy and service continuity.
6. *Policies and legal environment*. As many actor groups participate and are affected by the CII, it is necessary to provide a set of legal frameworks where the protection of the infrastructures can be effectively negotiated and enforced. Due to the (inter)national nature of CIIP and the different actor groups motivations, the creation of these frameworks and cooperation networks is really challenging. This topic mainly comprises (cyber) crime legal frameworks and development of CIIP policy and information sharing frameworks.
7. *Fundamental research and development*. There are some fundamental problems that the underlying elements of CII must deal with in order to provide a strong foundation for secure infrastructures. These problems are mostly of technical nature, and their overall objective is to build secure, scalable, and reliable systems. It comprises secure protocols and architectures, standardisation, fault tolerant systems, and management of trust and resilience.
8. *Non-technology issues compromising CIIP*. There are a number of non-technological factors, such as human and organisational aspects, that can affect positively or negatively the performance of the system. This research topic mainly comprises training programmes for increasing public awareness, treating humans as another element of the CIIP, planning common concept developments, and tools for cost/benefit analysis of investments on CIIP.

5. Electronic Control Systems

5.1 SCADA and PLC

Supervisory control and data acquisition systems, or SCADA [21], can be seen as a complex system comprised by a set of hardware (for instance, controllers) and software (for instance, database or programmes) components that are interconnected. The main goal of this type of systems is to control and supervise the state and/or condition of every element (products, machines, materials, and even the staff) of an

infrastructure, as well as to carry out in real time a set of operations. SCADA systems can monitor large infrastructures, thus it requires long and secure communication networks to send and receive the control packets and measurements obtained from its components. In fact, depending on the overall dimensions of the infrastructure, it may be necessary to establish connectivity with outside networks.

A SCADA system is basically composed of five fundamental elements, which are represented in the figure 1. The infrastructure is supervised and monitored by an operator using a central system known as *Human Machine Interface* (*HMI*). The HMI works like a mediator between the system and operator, and shows all the data obtained from every part of the system by means of graphical interfaces (schemes, windows, graphics, and so on). All the information is recollected by a *Master Terminal Unit* (*MTU*), which also retransmits the operator's control signals to remote parts of the system. Both the recollected data and the control signals are sent out using a *communication infrastructure*, such as Internet, wired networks, wireless network, or public telephone network. Finally, the control signals are received by *Remote Terminal Units* (*RTU*), which retransmit them to the individual devices of the system. The measurements coming from those devices, such as flow or voltage, are also gathered by the RTU and sent to the MTU. Note that a RTU may be a Programmable Logic Controller (PLC).

A PLC is a small computer used for automation of real-world processes, such as control of machinery on factory assembly lines. More specifically, the PLC is a microprocessor based device with the specific purpose of reading data from sensors connected to its input ports and controlling actuators through its output ports. These sensors can read limit switches, dual-level devices, temperature indicators, and others. Also, the actuators can drive any kind of electric motor, pneumatic or hydraulic cylinders or diaphragms, magnetic relays or solenoids, and so on.

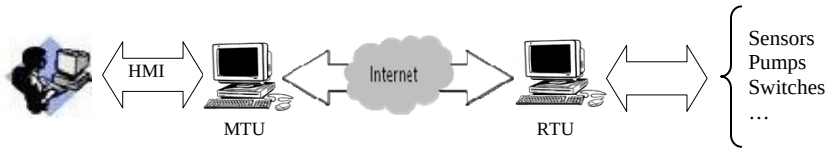

Fig. 1. General representation of SCADA system architecture.

Traditional systems consisted of hard-wired relay logic, which had virtually no control system and applications. As a result, the design engineers had to manually monitor the processes in order to prepare specifications and reports for the contractor. On the contrary, SCADA systems allow the engineers to design the appropriated functionality that the system should have, facilitating the operation of the whole system. A concrete example of the applicability of SCADA systems are water treatment or wastewater treatment infrastructures [22], which are composed of a set of applications, programmable controllers, distributed control systems, and computer-based operator interface stations to control all the facilities. The applications must be unique for each facility because they have to manage specific processes at every individual plant, such as pump control algorithms, equipment control, and so on.

5.3 Vulnerabilities in Electronic Control Systems

The *Electronic Control Systems (ECS)* are very vulnerable to threats mostly because of two reasons. Firstly, the communication infrastructure is based on wired or wireless networks, and sometimes, depending on the distance between its elements, it requires to keep connectivity with outside networks such as the Internet. Secondly, these ECS are essential parts of critical infrastructures, and any failure (logical or physical) in a component could bring severe and devastating consequences. If an attacker penetrates in an ECS, for example a SCADA system of a refinery, he could access, manipulate, control and change all its behaviour – from passwords to measurements and devices (HMI, MTU and RTU).

The specific threats that may affect ECS are physical and logical in nature. For example, a ECS could be targeted by a cyberattack (e.g. autonomous worms, denial of service attacks, viruses), a failure or attack in the communication infrastructure (e.g. lack of connectivity, vulnerability in subnetworks, lack of authentication, confidentiality and privacy methods in the underlying protocols), a natural disaster (e.g. hurricanes, tornadoes, flooding, earthquakes), a deliberate action (e.g. terrorism, organized crime), a human or technical error (e.g. radio interferences, unsuitable applications software) or an accident.

Therefore, ECS must be able to detect and warn of the type of threat and its localization to the human operator as soon as possible, and also automatically respond in real-time to reach a stable and reliable system. However, including methods of detection, alerting and protection in such complex systems is not an easy task, since it requires of secure and specialized mechanisms (for instance, specially designed *Intrusion Detection Systems*), as well as extremely robust and reliable secure communication protocols. Still, it is mandatory to apply security primitives to protect the information, and to provide confidentiality, authentication and privacy to all the elements and services of the ECS.

6. Wireless Sensor Networks in CIP/CIIP

The protection of Critical Information Infrastructures faces numerous challenges, for example managing the secure interaction between peers, assuring the resilience and robustness of the overall system, or deploying warning and alert systems. For carrying out such proposals, suitable and intelligent technologies (for instance, Wireless Sensor Networks) are required for providing support to such protection. Indeed, Wireless Sensor Networks technology possesses appropriate properties and capabilities to control and work in diverse scenarios. Therefore, the main focus of this section is to justify why Wireless Sensor Networks technology is suitable for providing security in determined critical scenarios, describing its structure, behavior, advantages, disadvantages, and its role in the overall scheme of protecting the Critical Information Infrastructures

6.1 Wireless Sensor Networks

A *Wireless Sensor Network* (WSN) [23] is composed of small and autonomous devices, deployed over a certain region, that cooperate with each other in order to achieve the same objective. These devices, called sensor nodes, make use of different types of sensors to monitor the physical state of a specific object or to examine the environmental conditions of its surroundings. Thanks to these attractive features, this technology is increasingly being applied in diverse scenarios and applications (from simple, complex to critical) of very different sectors (such as agricultural, business, environment, health care, homeland security, industry, and so on).

Sensor nodes can measure a wide range on environmental conditions, like temperature, humidity, lighting, radiation, noise, and others. Such information must be transmitted to the end user (a human being or computer) with the purpose of obtaining, evaluating, and studying relevant samples. However, there is no direct link between the real world, where dozens, hundreds and thousands of sensor nodes are deployed, and the end user. Between both points, there should exist devices whose resources and capabilities have to be more powerful than sensor nodes. Those devices are known as B*ase Stations*. Any device with enough capabilities to manage the services offered by the sensor network, such as a laptop or a PDA handed by a user, can become a base station.

Regarding the services offered by a WSN, sensor nodes not only can monitor the environment, but also can issue warnings and receive queries about the state of the network or a certain property. Indeed, all measurements perceived (e.g. radiation) and processed by the nodes must be sent to the closest base station, being later retransmitted to the end user. Besides, nodes must be able to detect any kind of anomalous activity of the environment (e.g. high levels of radiation) and alert the end users. Finally, the base stations can request to the nodes information about a specific feature of the network or environment, which is provided “on-demand”. Note that base stations can also send control packets in order to reconfigure the network without using an additional infrastructure, since the nodes have the capability of self-configuring themselves. Therefore, the channel of communication between the sensor nodes and base station is totally bidirectional.

It must be noted that there are two types of architectures in WSN, which are represented in the figure 2: hierarchical (HWSN) and distributed (DWSN). In a hierarchical network, the sensor nodes are organized into groups, known as clusters. In every cluster there exists a special node, called “cluster head”, entrusted to manage certain tasks in the cluster, as for example data aggregation. In contrast, in a distributed network the sensor nodes are completely independent, making their own decisions and determining which their next actions are by themselves. Note that it is possible to have both architectures in a sensor network at the same time (i.e. hybrid), thus improving the resilience and robustness of the network in case the “spinal cord” (i.e. the “cluster heads”) fails.

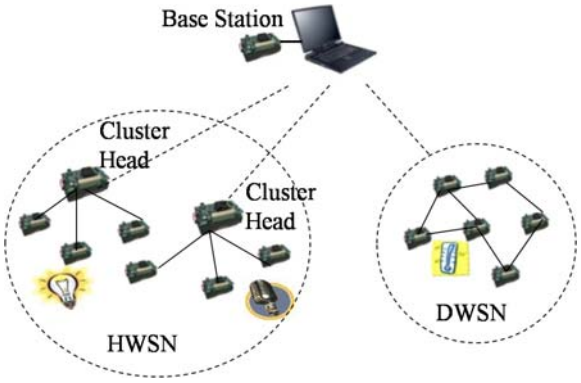

Fig. 2. General representation of a Wireless Sensor Network architecture.

6.2 Sensor Node Hardware

A sensor node has four principal components: processor unit, sensing unit, power unit, and transceiver. Concretely speaking, the *processing unit*, also known as microcontroller, is a highly-constrained computer integrated on a chip. This unit also has memory and input/output interfaces. The *sensing unit* is composed of a set of sensors such as temperature, humidity, vibration, light, air, radiation, and so on. The power unit, which in most cases consists of batteries, is the responsible for supplying energy to every element of the system. With a finite energy source a node can subsist long periods of time, even a year with an optimal configuration. Finally, the *transceiver* is the responsible of sending and receiving messages through a wireless antenna, allowing the nodes to support multiple communication paths and providing routing capabilities.

In the design of a wireless sensor network is important to take into account the possible computational and communicational capabilities of sensor nodes, with the purpose of analyzing whether they are suitable for carrying out a determined application. Actually, it is possible to classify sensor nodes into three categories according to the features of their microcontrollers: “weak”, “normal”, and “heavy duty”. Additionally, there are two major types of transceivers: wideband radios and narrowband radios. Note that any type of node category is able to support both narrowband and wideband radios.

The class “weak” represents those sensor nodes whose capabilities are extremely constrained (i.e. less than 2kB of instruction memory and 64B of RAM), but still enough to execute very simple applications (such as monitoring the temperature in a region). Conversely, the class “normal” represents those nodes that are able to fulfill any kind of sensing and collaborative applications. A node belonging to this class usually has a microcontroller of 4-8Mhz, with 48kB-128kB of instruction memory

and 4kB-10kB of RAM. Finally, nodes belonging to the "heavy-duty" class are expensive PDA-like devices that are able to execute any kind of application, from simple, complex to critical. Their microprocessors are quite powerful, with around 180Mhz, 4MB-32MB of instruction memory and 256kB-512kB of RAM.

On the other hand, regarding the type of transceivers, wideband radios are faster and more robust, working at frequencies such as 2.4Ghz, but are also power-demanding and slower to wake up. Narrowband radios have less throughput (i.e. work at lower frequencies, such as 868Mhz) and are more susceptible to noise, but they have less power consumption and faster wakeup times. Note that most nodes use wideband-based transceivers that follow the IEEE 802.15.4 standard.

A question that may surface at this point is what nodes are suitable for being used on a critical infrastructure. The answer is simple: it depends on the tasks assigned to those nodes: "weak" nodes can behave as mere data collectors, forwarding the data to a node of higher capabilities; "normal" nodes can both obtain data from their surroundings and preprocess them, or even more, make organizational decisions in pure distributed or hybrid networks; "heavy-duty" nodes can behave as "cluster heads" in hierarchical networks, or act as surrogated base stations in control of one section of the network.

6.3 Role of Sensor Networks in CIP/CIIP

The scientific community and national governments consider WSN technology as a fundamental part in CIP and CIIP, since the sensors can be embedded into systems and provide attractive operations such as monitoring, tracking, detecting, reporting and collecting. For these reasons, in 2004 the U.S Department for Homeland Security [24] declared as one of their strategic goals "to provide a *National Common Operating Picture* (COP)" for Critical Infrastructures, where the core of the systems would be an intelligent, self-monitoring, and self-healing sensor network. Also, the Australian government suggested sensor network technology as part of their new R&D proposals to develop several topics based on research and commercialization of CIP in Australia, known as "*Cooperative Research Center for Security* (CRC-SAFE)".

From an academic point of view, the scientific community is interested in applying the WSN technology in many critical applications. In fact, at present there are several applications running, or even finished. An example is the CoBIs project [25] developed by BP in a petrochemical plant in Hull (UK) [26]), where sensor nodes are attached on chemical containers and storage facilities to control both the nearness of incompatible dangerous products and their safety during their storage or transportation. Intel [27] also led an experiment in a plant of Oregon to control the vibrations of its semiconductor fabrication equipments. Another project associated to industry infrastructures is SMEPP project [28], which aims to supervise the radiation levels of nuclear power plants. Moreover, the U.K. (EPSRC) is involved in other specific projects (Underground M3 and Smart Infrastructure - WINES II project [29])

related to ageing of civil infrastructures (bridges, tunnels, water supplies and sewer systems).

Finally, other sector that is also critical is the quality and treatment of water. On this matter, the DISCOVERY project [30], also known as Distributed Intelligence, Sensing and Coordination in Variable Environment, consists of the deployment of an underwater sensor network to control oil spills, and in extreme cases, to respond and seal off a perimeter containing contaminated water. In the same way, the University of California is leading two projects [31] to measure the amount of arsenic in Bangladesh groundwater, and the nitrate propagation in soils and ground water in California.

As already mentioned, WSN are also appropriated to secure the protection and safety of the information in critical infrastructures. For that purpose, it would be advisable to have available and configured an *Early Warning System* (EWS) and a *Dynamic Reconfiguration Systems* (DRS) in order to detect anomalous events, specify the exact location of a problem, alert and attend the problem as soon as possible, and in certain situations, to re-configure the different components of the CII taking as input the output of EWS.

6.4 Research Challenges and Security

As already seen in previous sections, there are many scenarios where sensor networks play a major role. However, this type of technology has some research issues that need to be solved, and the security is one of the most relevant. Sensor nodes are highly vulnerable to attacks, due to their constrained nature in terms of computational and memory capabilities, and also due to the wireless nature of the communication channel [32]. Hence, it is necessary to discover and design secure, robust and effective architectures, protocols (such as routing, aggregation and time synchronization) and applications.

In the WSN context there are two major types of attacks: physical and logical. A malicious adversary can carry out any of them in order to compromise and manipulate the network (locally or globally) for its own convenience. Generally, physical attacks are caused by the implicit and explicit nature of the nodes, that is, most of them are not tamper-resistant and can be easily accessible by intruders, respectively. As a consequence of physical attacks, the sensitive information of the node can be retrieved, but also the node itself can be reprogrammed. However, it is also important to know that there are some mechanisms to protect a node against data stealing, such as *data and code obfuscation* schemes, which generate new software version of the sensor nodes [33]. Even more, a node could check the state of another one simply calling to the procedure *code attestation* [34].

On the other hand, logical attacks are caused by the weaknesses inherent to the communication channel. Any device, equipped with a wireless antenna and located in the vicinity of the network, can easily access the information exchange. Therefore, a

minimal protection is required to assure the confidentiality and authenticity between peers, and the integrity in the communication channel and the messages. Such protection mechanisms are necessary, but not sufficient conditions for guaranteeing the viability of the services offered. These services are based on certain "core" protocols, such as *data aggregation* (to filter all the information collected in a single message), *routing* (to route a message from a source to a target node) and *time synchronization* (to synchronize the clocks of each sensor node). At present, there are many specific implementations of these protocols, but any of them guarantees neither the correct functionality of the network nor its robustness against any kind of threat or failure.

The nodes must have integrated and implemented the basic security primitives to assure a minimal protection of the information flow in the communication channel. Those primitives are *Symmetric Key Cryptography* schemes (SKC), *Message Authentication Codes* (MAC), and even *Public Key Cryptography* (PKC). There are many existing implementations of software-based SKC primitives for sensor networks (cf. [35]). Regarding MAC, it is possible to implement that primitive using SKC operations (e.g. by using CB-MAC). Finally, until 2004 the PKC implementations for sensor networks were considered technically "impossible", since they required very high computational capabilities. However, that idea was changed by, among others, Gura et. al. [36]. They introduced the possibility of using *Elliptic Curve Cryptography* (ECC) as a efficient PKC primitive, with keys of 163 bit and point multiplications.

Primitives are the foundation for the protection of the information flow, but they need of security credentials such as secret keys in order to work properly. At the moment, there are many *Key Management System* (KMS) proposed for sensor networks, and every one is oriented for a specific context with certain properties. As these properties are associated to the requirements of every scenario, it is necessary to use a tool that identifies [37] the Key Management System more suitable for a specific application domain. Aside from all these advances in security, it is important to research other areas such as *Intrusion Detection Systems* (IDS) for network monitoring and self-configuration, trust management, delegation of privileges, secure management of mobile nodes, and so on.

As a final note, it can be pointed out that there are some similarities between a SCADA system and a wireless sensor network, since both offer special services that can be useful for the management of the infrastructure, such as monitoring, and both also present vulnerabilities of internal and external attacks against the system. However, the SCADA system is more complex, and its elements have higher processing capacity, memory and energy, than a sensor node.

7. Research Projects

As of 2007, the protection of CII is one of the priority areas for research in the context of the European Community. For instance, in the *VII Framework Programme* (FP7),

this topic is part of the first ICT challenge, "Pervasive and Trusted Network and Service Infrastructures". CIIP has been also considered as an important area in the previous European research programmes. There have been more than 20 projects in the last years mainly oriented to solve the interdisciplinary challenges of European infrastructures [38]. In this section we present some of those projects, alongside with other non-European projects that have used sensor network technology.

7.1 VITUS

VITUS (*Video Image analysis for TUnnel Safety*) project [39] is included in the Program I2 "Intelligence Infrastructure" (2002-2006), and supported by the Austrian Federal Ministry of Transport, Innovation and Technology. The objective of VITUS is to provide automatic safety in tunnel roads of Europe using automated visual video surveillance systems. Analogue CCTV-systems have been used in the past to monitor traffic incidents, but they are not very robust and reliable. The need to develop such intelligent system arises from the concrete measures issued by the EU in 2001 [40] aimed to prevent serious disasters such as the Mont Blanc tunnel incident.

This project was divided in two subprojects, known as VITUS-1 [41] and VITUS-2 [39]. Specifically, VITUS-1 has been the responsible of analyzing the viability part of the project, with the partial tasks of identifying the appropriated mechanisms and sensors to detect abnormal and dangerous events, as well as of mechanisms to alert to the tunnel operators in serious situations. On the other hand, VITUS-2 was the responsible of developing and evaluating the prototype defined in VITUS-1. VITUS-2 has been organized in several partial tasks, such as the installation of electronic components and calibrated digital cameras, recording of scenes for the video database, development of algorithms for detecting and tracking static or dynamic objects in the tunnel, classification of objects, detection of unexpected events or irregular behaviors, the development of framework and interfaces prototypes, evaluations, documentation and dissemination, and management of documents.

7.2 CoBIS

CoBIS (*Collaborative Business Items*) is a 6th European Framework Programme (FP6) project [25]. This project was finalized on 2007, and its objective was to develop a platform to embed business logic in physical entities, such as materials, machine parts, modules, clothing, and so on. These items had to be able to provide services and to adequately solve problematic situations, by cooperating and communicating with each other. In this platform, every item must have associated an unique RFID tag to be identified, and a sensor node to monitor both its current state and the environmental conditions. This way of handle services provides more reliability and scalability than traditional systems, since the intelligent objects can help in reducing manual data collection.
Partial tasks of this project were identification and classification of services, development of collaborative and technology frameworks, design and implementation

of management services, and evaluation in an oil and gas industry. Indeed, and as mentioned in previous sections, a BP petrochemical plant in Hull in the United Kingdom [26] carried out the first evaluations, attaching sensor nodes on chemical containers and storage facilities. As a result, it was possible to control the proximity of incompatible dangerous products and both their state and environmental conditions during their storage or transportation. On the other hand, CoBIS also intended to guarantee workplace safety using smart clothing. Note that although evaluations had been made in oil and gas industries, this project could be extended and applied in other sectors whose products (for example, food, pharmaceuticals or healthcare) could suffer severe damage by environmental conditions.

7.3 CenSCIR projects

The *Center for Sensed Critical Infrastructure Research* (CenSCIR) [42] is housed in Carnegie Mellon University's College of Engineering (CIT) Institute for Complex Engineered Systems (ICES). This center runs several projects whose objectives are to monitor and supervise infrastructures of critical importance, such as decaying road systems, oil and gas pipelines, unstable electric power grids, leaking water distribution systems, water treatment plants, telecommunications networks systems, and commercial and industrial facilities. Specific objectives are the development of data interpretation techniques, data models, decision support frameworks, sensor data driven decision support, and so on.

Examples of projects carried out inside CenSCIR are the projects led by Akinci et. al. [43] and Singhvi et. al. [44]. The first one supervises the construction deviations of buildings, with the goal of reducing unexpected impacts or undesired damages, and even minimizes the maintenance costs. Indeed, most constructions suffer deviations by quality or ageing of materials, lack of inspection of construction work or unskilled workers. All of these cause an increase of 12% in construction costs. The second one aims to optimize the user comfort by minimizing the energy costs in intelligent homes. For that purpose, they used wireless sensor network to create a intelligent lighting control system.

7.4 WINES II

WINES II (*Wireless Intelligent Networked Systems - Smart Infrastructure*) project [29], is funded by the EPSRC (Engineering and Physical Sciences Research Council), with a duration of three years (2006-2009). In this project, specialists of very different areas are involved with the aim of investigating the best way of controlling the ageing of civil infrastructures of United Kingdom (such as bridges, tunnels, and water supply and sewer systems), primarily by using wireless sensor networks. In fact, most of the research challenges suggested for this project, such as maximizing scalability and resolve the problems related to security and power supply, are associated with WSN.

The foundations of this project were based on the problematic of maintaining the civil infrastructures in UK, which are around a hundred years old. This is the case of tunnels in the London underground (LUL) and pipelines of Thames Water. On the other hand, there are around 150,000 bridges in the UK which are related to critical links corresponding both roads and rail infrastructures. The use of WSN technology allows the autonomous control of every previously mentioned infrastructure, and it is important to note that all the information retrieved from those networks is sent to a same common system by means of wireless systems or the Internet.

8. Future Directions

It has been clear during the course of this chapter that CIIP is a very young and interdisciplinary research topic that needs to be addressed by many actors with different points of view. There is, however, a sense of emergency attached to this topic. The nature of its threats and the possible effects of a single failure demand for a fast and coordinated action from all stakeholders involved. If no solutions are devised soon, the chances of problematic incidents that can globally affect the safety of a nation will grow steadily. While it is not possible to completely eliminate the possibility of such events taking place, it is necessary to keep them under control.

The statements presented in the previous paragraph could be perceived as catastrophic, in the sense that the actual risk of a certain critical infrastructure failing and the influence of such failure on its socio-economical surroundings are mostly unknown. Nevertheless, there are some global and infrastructure-related trends that clearly will affect the well-being CII [45]. From a global point of view privatization and outsourcing are growing, thus it will be more difficult to coordinate all interested parties, amongst other things. Also, globalization is growing, so the already complex interdependences between infrastructures will become even more transnational.

Infrastructure-specific trends range from social ones to technological ones. Our society is becoming more and more dependent on the unfailing operation of critical infrastructures: it is difficult to picture life as we live it now without the services provided by such infrastructures. The increasing complexity of their underlying systems and computer networks multiply the chances of a single failure, failure that can be provoked anywhere, anyhow, anytime. These problems in a single component of an infrastructure could easily cascade to other infrastructures, due to their inherent interdependences.

There are many challenges that all actor groups have to overcome so as to provide an appropriate protection to the actual and future CII. As of 2007, the major challenges on the area of CIIP are the following [3]:

- Design and development of integrated protection architectures and technologies for the pervasive and ubiquitous secure computing environment that become part of the CII (resilient and secure hardware/software architectures).

- Tools and platforms for dependencies and inter-dependencies analysis and anti-cascading protection measures.
- Tools for intrusion detection.
- Tools and platforms for trusted sharing of sensitive information.
- Tools for dealing with uncertain dynamic threats to CII and the preparation for proper and efficient and effective incident management including optimization strategies in risk reduction.
- Organizational, technical and operational policies and good practices for intra-sector, cross-sector, cross-border and public-private partnership establishment and conditioning.
- Forensics tools for critical infrastructures (Network Forensics)

9. References

1. Definition of the word *Infrastructure*. Merriam Webster's Collegiate Dictionary (11th ed.), Springfield, MA (2003).
2. National Research Council, Dahms, L.: Infrastructure for the 21st century - framework for a research agenda. National Academy Press, Washington, D.C. (1987).
3. Critical Information Infrastructure Research Co-ordination (CI2RCO). Deliverable D12, ICT R&D for CIIP: Towards a European Research Agenda. April 13th, 2007.
4. Definition of the word *Critical*. Merriam Webster's Collegiate Dictionary (11th ed.), Springfield, MA (2003).
5. Commission of the European Communities: Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism, COM (2004) 702 final, Brussels (2004).
6. Congress of the United States of America: USA PATRIOT ACT. Public Law 107-56, Washington D.C., (2001).
7. Analysis and Assessment for Critical Infrastructure Protection (ACIP). Deliverable D1.1, August 31st 2002.
8. Metzger, J.: The Concept of Critical Infrastructure Protection (CIP). In: Business and Security: Public-Private Sector Relationships in a New Security Environment. Oxford University Press, pp. 197--209 (2004).
9. Dunn, M., Abele-Wigert, I.: The International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations (Vol. I) (Zurich, Center for Security Studies, 2006).
10. Stoneburner, G., Goguen, A., Feringa, A.: Risk Management Guide for Information Technology Systems. In: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30, WashingtonD.C. (2002).
11. Radvanovksy, R.: Critical Infrastructure: Homeland Security and Emergency Preparedness. CRC Press, Boca Raton (2006).
12. Rinaldi, S., Peerenboom, J., Kelly , T.: Identifying, understanding, and analyzing Critical infrastructure interdependencies. IEEE Control Systems Magazine, v21, pp 11-25, (2001).
13. President's Commission on Critical Infrastructure Protection (PCCIP): Critical Foundations: Protecting America's Infrastructures. Washington D.C., (1997).
14. Landau, S., Stytz, M. R., Landwehr, C. E., Schneider, F. B.: Overview of Cyber Security: A Crisis of Prioritization. In: IEEE Security and Privacy, vol. 03, no. 3, pp. 9--11 (2005).
15. Dunn, M.: Threat Frames in the US Cyber-Terror Discourse. In: Paper presentation at the 2004 British International Studies Association (BISA) Conference, Warwick, (2004).

16. Bologna, S, Setola, R.: The need to improve local self-awareness in CIP/CIIP. In: Proceedings of First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), pp 84--89. Darmstadt, Germany (2005).
17. Dunn, M.: Understanding Critical Information Infrastructures: An Elusive Quest. In: Myriam Dunn and Victor Mauer (eds.); The International CIIP Handbook 2006: Analyzing Issues, Challenges, and Prospects (Vol. II) (Zürich, Forschungsstelle für Sicherheitspolitik, 2006), pp. 27-53.
18. Critical Information Infrastructure Research Co-ordination (CI2RCO). Deliverable D1, Common Understanding of CI2RCO-Basics. March 1st, 2005.
19. Henriksen, S.: The Shift of Responsibilities within Government and Society. CRN Workshop Report. Societal Security and Crisis Management in the 21st Century, pp. 60–63, Stockholm (2004).
20. Dunn, M.: The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP). In: International Journal for Critical Infrastructure Protection, Vol. 1, No. 2/3, pp. 258–68 (2005).
21. Krutz, R. L.: Securing SCADA Systems. Wiley Publishing (2005).
22. Malcolm Pirnie: Why Malcolm Pirnie Can your Configuration Needs. White Paper. http://www.pirniecentral.com/Docs/MPI_Configure.html (2000).
23. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. In: Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 38, no. 4, pp. 393-422 (2002).
24. The Department of Homeland Security, Science and Technology Directorate. The National Plan for Research and Development in Support of Critical Infrastructure Protection. Washington, D.C. (2005).
25. Collaborative Business Items project (CoBIS), http://www.cobis-online.de, 2004-2007.
26. Collin, J.: BP Tests RFID Sensor Network at U.K. Plant. http://www.rfidjournal.com/article/articleview/2443/ (2006).
27. Sensor Nets / RFID. Intel Corporation. http://www.intel.com/research/exploratory/wirelesssensors.htm.
28. SMEPP "Secure Middleware for Embedded Peer-to-Peer Systems" (FP6-2005-IST-5). http://www.smepp.org (2007)
29. WINES II – Smart Infrastructure, http://www.winesinfrastructure.org, University of Cambridge and Imperial College London (2006).
30. Distributed Intelligence, Sensing and Coordination in Variable Environments. CSIRO. http://www.ict.csiro.au/page.php?cid=97 (2006).
31. Ramanathan, N., Balzano, L., Estrin, D., Hansen, M., Harmon, T., Jay, J., Kaiser, W.J., Sukhatme, G.: Designing Wireless Sensor Networks as a Shared Resource for Sustainable Development. In: Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD 2006), Berkeley, USA (2006).
32. Walters, J. P., Liang, Z., Shi, W., Chaudhary, V.: Wireless Sensor Network Security: A Survey. In: Security in Distributed, Grid, and Pervasive Computing, Editor: Yang Xiao, Auerbach Publications, CRC Press, Boca Raton (2006).
33. Alarifi, A., Du, W.: Diversifying Sensor Nodes to Improve Resilience Against Node Compromise. In: Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2006), Alexandria, USA (2006).
34. Park, T., Shin, K.G.: Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks. In: IEEE Transactions on Mobile Computing, pp. 297-309, vol. 4, no. 3 (2005).
35. Law, Y. W., Doumen J., Hartel, P.: Survey and Benchmark of Block Ciphers for Wireless Sensor Networks. In: ACM Transactions on Sensor Networks, vol. 2, no. 1, pp 65-93, February 2006.

36. Gura, N., Patel, A., Wander, A.: Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In: Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Cambridge, USA (2004).
37. Alcaraz, C., Roman, R.: Applying Key Infrastructures for Sensor Networks in CIP/CIIP Scenarios. In: 1st International Workshop on Critical Information Infrastructures Security (CRITIS 2006), Samos, Greece (2006).
38. Critical Information Infrastructure Research Co-ordination (CI2RCO). Deliverable D10, Gap analysis of existing CIIP R&D programmes at regional, national and EU level. September 29th, 2006.
39. Schwabach, H., Harrer, M., Waltl, A., Horst, B., Tacke, A., Zoffmann, G., Beleznai, C., Strobl, B., Helmut, G., Fernández, G.: VITUS: Video based Image analysis for Tunnel Safety. In: International Conference on Tunnel Safety and Ventilation (2006).
40. Commission of the European Communities. European transport policy for 2010: Time to decide. White Paper 370 (2001).
41. Schwabach, H., Harrer, M., Holzmann, W., Bischof, Fernández Domínguez, H., G., Nölle, M., Pflugfelder, R., Strobl, B., Tacke, A., Waltl, A.: Video Based Image Analysis for Tunnel Safety – VITUS-1: A Tunnel Video Surveillance and Traffic Control System. In: 12th World Congress on Intelligent Transport Systems (2005).
42. Center for Sensed Critical Infrastructure Research (CenSCIR), http://www.ices.cmu.edu/censcir/ (2006).
43. Akinci, B., Boukamp, F., Gordon, C., Huber, D., Lyons, C., Park, K.: A formalism for utilization of sensor systems and integrated project models for active construction quality control. Carnegie Mellon University, Pittsburgh, United States, ScienceDirect, (2005).
44. Singhvi, V., Krause, A., Guestrin, C., Matthews, H. S., Garrett, J. H., Matthews, H.: Intelligent Lighting Control using Sensor Networks. In: Proceedings of SenSys'05, San Diego, California, USA (2005).
45. Critical Information Infrastructure Research Co-ordination (CI2RCO). Deliverable D6, Report on the analysis and evaluation of CIIP R&D programmes. June 2nd, 2006.