Security of Industrial Sensor Network-based Remote Substations in the context of the Internet of Things

Cristina Alcaraz[1], Rodrigo Roman[2], Pablo Najera[1] and Javier Lopez[1]

[1]Computer Science Department, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
[2]Institute for Infocomm Research, 1 Fusionopolis Way,
#19-01 Connexis, South Tower, Singapore 138632
[1]{alcaraz,najera,lopez}@lcc.uma.es, [2]rroman@i2r.a-star.edu.sg

October 27, 2015

Abstract

The main objective of remote substations is to provide the central system with sensitive information from critical infrastructures, such as generation, distribution or transmission power systems. Wireless sensor networks have been recently applied in this particular context due to their attractive services and inherent benefits, such as simplicity, reliability and cost savings. However, as the number of control and data acquisition systems that use the Internet infrastructure to connect to substations increases, it is necessary to consider what connectivity model the sensor infrastructure should follow: either completely isolated from the Internet or integrated with it as part of the Internet of Things paradigm. This paper therefore addresses this question by providing a thorough analysis of both security requirements and infrastructural requirements corresponding to all those TCP/IP integration strategies that can be applicable to networks with constrained computational resources.

Keywords: the Internet, Supervisory Control and Data Acquisition (SCADA) Systems, Industrial Control Networks, Wireless Sensor Networks, Internet of Things

1 Introduction

The introduction of new technologies and different types of communication systems (Information and Communication Technologies, ICT) in industrial control networks have given rise to new and important advances in the automation and control processes. A particular case is the Supervisory Control and Data

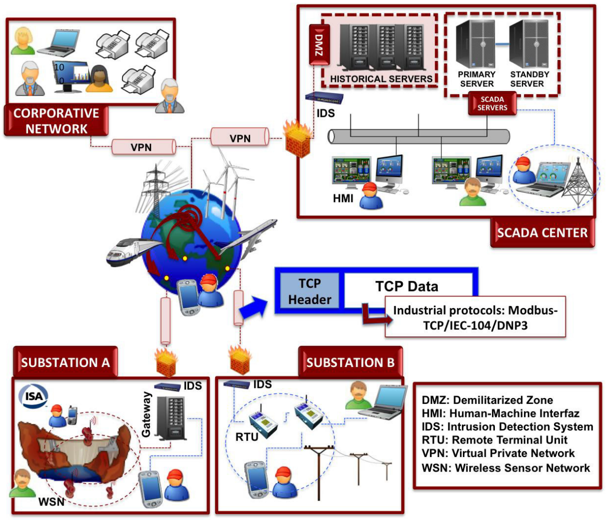

Figure 1: A Current SCADA Network Architecture

Acquisition (SCADA) system, which uses new technologies to monitor in real-time many of the Critical Infrastructures (CIs) deployed in our society, such as energy systems, transport systems or oil/water distribution systems. In particular, Internet connectivity is in high demand as it offers global connectivity and communication, irrespective of the physical location of devices; either industrial engineering devices or communication components.

Figure 1 depicts a current SCADA system [1, 2], where authenticated human operators are authorized to read and manage data streams transmitted by substations. A remote substation is composed of automated electronic devices, known as Remote Terminal Units (RTUs), which are able to collect, manage and resend sensitive data (e.g. temperature, pressure or voltage) received from their sensors to the central system. On the other hand, Figure 1 also shows how the substations have evolved quickly, trying to adapt new technologies; standing out from among them, Wireless Sensor Networks (WSNs), which are based on industrial sensor nodes and are able to offer control services as an RTU but with a low installation and maintenance cost. Said sensor nodes can be configured in remote substations to supervise, at first level, the natural state of deployed CIs, such as industrial pipelines with water, oil or fuel, as well as electricity pylons or generators. However, current communication standards for this type of technology only contemplate local connectivity, significantly reducing its functionalities out in the field. For this reason, both industry and scientific communities are trying to offer remote control and data acquisition through different types of ICTs. As a result, a new paradigm starts to emerge in the context of CI, the Internet of Things (IoT).

The IoT consists of large heterogeneous and interconnected ICT infrastructures, where the Internet, services and physical objects ('Things') play an important role in the control and automation processes. For example, in an industrial context, these things could be industrial sensor nodes, actuators, smart meters, pole-top devices, Radio-Frequency Identification (RFID) tags, Personal Digital Assistants (PDAs), and any other automation devices, such as RTUs [3]. Focusing on WSNs, their sensor nodes will create an autonomous and intelligent virtual layer over the physical environment of remote substations, providing information about the state of the real world that can be accessed from anywhere at any-time. This interaction can be achieved by using many different types of integration strategies: From sensor nodes implementing the TCP/IP stack and becoming fully-fledged citizens of the Internet to capillary networks that maintain their independence, while using Internet servers as interfaces to external entities.

However, it is necessary to study whether the security requirements of critical systems can be fulfilled in this upcoming networks or not. In fact, there are no studies in the literature that provide a systematic analysis of which strategies should be used in the integration of industrial WSNs in the IoT. The purpose of this paper is to provide a basis to try and respond to all these questions; analyzing the security and infrastructural requirements of industrial WSNs connected to the Internet, and discussing the suitability of the integration strategies that will realize the vision of ubiquitous management in the area of control and industrial networks.

The paper is organized as follows. In Section 2, we introduce the advances in remote substation technologies in terms of hardware devices and TCP/IP connectivity. Section 3 explains how the Internet and Wireless connectivity is changing the landscape of industrial control networks. Section 4 describes both the integration strategies and the requirements that have to be considered for achieving a secure integration. Finally, Section 5 provides an analysis of the integration between WSNs and the Internet in the context of control networks taking into account the previously mentioned requirements. Section 6 concludes the paper and outlines future work.

2 Advances in Remote Substations and communication protocols

The hardware and software (HW/SW) capabilities of RTUs in remote substations have significantly evolved in recent times [4]. In 1970, RTUs used 8-bit microprocessors with limited memory (e.g. 4-16 KB) and processing power. Later, faster microprocessors, math co-processors and larger memories increased their intelligence and autonomy. By the 1980's, serial interfaces with advanced I/O functions and operational software were supported; and from the end of the 1990's to the present, RTUs have advanced to offer web services, wired and wireless communication interfaces, standard protocols and Application Program Interfaces (APIs). In addition, they are also able to carry out several tasks for data management and acquisition. For example, they can behave as a concentrator to collect data streams from any field device; or an access controller to remotely reconfigure the system and gain access to other devices.

The migration to IP for monitoring and automation is becoming increasingly popular in the industry, as the TCP/IP connections offer real-time monitoring and maintenance processes, peer-to-peer communication between RTUs, multiple sessions, concurrency and security services. The RFC-6272 [5] presents how to best profile the Internet Protocol Suite for use in Smart Grids (i.e. electrical energy control systems controlled by SCADA systems). In addition, such migration allows systems to design hybrid networks using a multitude of communication technologies including Bluetooth, GSM, GPRS, WiMax, WiFi, ZigBee, Ultra-Wideband (UWB), microwave or WSNs. Within this set, industrial WSNs and their sensors offer attractive services for control (e.g., monitoring, tracking, detection and alert); and their communication protocols are able to provide specialized services for coexistence with other systems, reliability in communication channels and security [6]. Currently, there are three chief wireless communication standards for critical industrial networks: ZigBee PRO [7], WirelessHART [8] and ISA100.11a [9]. Given their importance in the industrial control context, we are going to focus part of our analysis on these standards.

The advances in control and automation activities using TCP/IP also have obliged engineers and industries to use IP-based SCADA protocols, such as Modbus/TCP [10], DNP3 [11] or IEC-104 [12]. Both DNP3 and Modbus/TCP are the most used utility automation protocols in United States; whereas IEC-104 is the most used in Europe. The main problem related to these SCADA protocols is that they lack authentication and encryption mechanisms. For this reason, new standards have recently been specified, such as the IEC-62351 standard [13] and the DNP Secure Authentication (SA) proposed by the DNP Users Group [14]. IEC-62351 provides confidentiality (using Secure Sockets Layer/-Transport Layer Security - SSL/TLS), authentication and integrity; whereas the DNP SA ensures authentication with Hash-based Message Authentication Codes (HMAC) and challenge-response. This advance has allowed the DNP SA protocol to be considered by the International Organization for Standardization (ISO) to be integrated in applications of Smart Grids [15].

Another essential part of a Smart Grid infrastructure is the inter-connectivity of physical elements (e.g. smart meters, sensors, pole-top sensors and intelligent electrical devices) using the Internet as a suitable medium of communication. However, this type of communication based on TCP/IP together with wireless communication needs special attention from the scientific community to resolve some pending challenges. In particular, there are two important aspects to highlight. First of all, most industrial scenarios only provide human operators with local access to nearby parts of the system, limiting, for example, the remote operational maintenance and performance [16]. Second, it is necessary to offer a suitable trade-off between (near) real-time performance of the system and security [17]. Some research about global connectivity using the Internet is ongoing, where some web-based solutions are being offered. All of these aspects will be discussed in-detail in the following section.

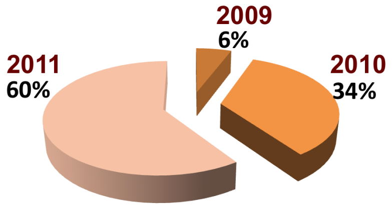

Figure 2: Incidents and Cyber-Attacks in the Energy Sector and its Control Systems Between 2009 and 20011 Reported by the ICS-CERT

3 New Challenges: Internet Access and Wireless Platforms

3.1 Internet as a Global Solution

The adaptation of ICTs and their application for CIs are bringing new and interesting challenges to the industrial sector. Researchers and engineers in particular are actively working in this field in order to analyze and develop constructive Internet-based or web-based SCADA solutions, and in doing this improve automation processes in terms of operational time [18]. This improvement includes monitoring and supervision at all times irrespective of geographic locations, in addition to guaranteeing real-time performance, flexibility in acquisition and management, dissemination of information, visualization of data streams and resources as well as maintenance and diagnostic processes. Thus authorized human operators could remotely access a substation from anywhere and at any time in order to (i) transmit commands (e.g., open/close pump), (ii) manage measurements (i.e., $\{r_i, r_j, ..., r_n\}$), (iii) respond to alarms (i.e., $\{a_i, a_j, ..., a_n\}$), and (iv) check normal or anomalous states. In order to validate such states, behavior patterns are required to delimit states such as $r_i \in / \notin [V_{min}, V_{max}]$, where V_{min} and V_{max} represent the behavior thresholds.

Moreover, recent advances in cloud-computing have encouraged researchers to continue the integration of the Internet into the operational tasks [19]. Individual operational objects (e.g., sensors, RTUs,...) could for example provide their interfaces through a Service-Oriented Architecture (SOA) interface to share their information and offer backup instances inside the cloud. This way, the system can ensure information recovery in emergency situations. Security experts also consider the Internet as a suitable way of reinforcing and controlling the security of existing engineering systems, maintenance and safety. This is the case of [20], which introduces the concept of a P2P overlay to interconnect different critical infrastructures and thereby improving and ensuring the resilience and trustworthiness of the overall infrastructure. From a commercial point of view, it is also important to stress the existence of companies investing on web-based SCADA solutions like Exemy SCADA Web [21].

Unfortunately, the integration of the Internet in control and automation tasks could bring about numerous security problems which may be associated with new threats and vulnerabilities, data reliability and service availability [17]. According to the last report of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the number of incidents and threats in critical sectors have become more and more relevant in the last few years (2009-2011) with particular relevance in the energy sector and its control systems [22, 23] (See Figure 2). Generally in these types of critical contexts, malicious outsiders or insiders of the system try to lead (single or multiple) attacks to compromise the availability, integrity or confidentiality of the entire system, its information and users' identity [24]. Namely, adversaries may take advantage of the nature of the communication infrastructure so as to explore and target vulnerabilities (e.g., unused and prohibited active ports), penetrate the system, intercept and/or alter the critical signals transmitted/stored, disrupt services and/or isolate any part of the system. For example, if remote control accesses are carried out through security credential databases and insecure protocols such as Hypertext Transfer Protocol (HTML) without encryption or tunneling, an attacker may exploit such databases using Structured Query Language (SQL) techniques. These techniques include remote reading, manipulation of content, replication of information or execution of modified code.

There are several ways of protecting the underlying system from threats coming from external networks such as the Internet. For example, the control of unused services and ports, hard cryptographic primitives, TCP/IP security services (e.g., SSL/TLS), key management systems (preferably based on Public Key Cryptography (PKC)) [13], or the use of security mechanisms such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), diode systems with unidirectional communication, antivirus, Virtual Private Networks (VPNs) based on the Internet Protocol security (IPsec) protocol under the tunnel mode (see Figure 1), as well as other existing mechanisms and approaches [25]. In addition to this, authentication from any connection point (e.g., a HMI or any electrical device) over the Internet must also be considered properly. This means that access control and authentication mechanisms have to be configured to restrict unauthorized access to HW/SW resources. Authorization mechanisms must be equally installed to prove the entity's identity and rights to manage critical signals and commands. Additionally, data redundancy mechanisms to ensure data availability at all times, accountability of incidents or anomalous events, security policies, training, testing, maintenance and auditing should be considered [16, 2].

3.2 WSN as a Wireless Solution

WSNs have evolved considerably in the last few years growing from a promising research field into an efficient and profitable technology, meaning traditional RTUs and their sensors are being displaced in favor of this lower cost and flexible technology. In particular, this technology is composed of two types of entities: (i) low-powered sensor nodes with constrained computational and storage resources (i.e., typical specs could be 8 KB - 128 KB RAM, 128 KB -

192 KB flash memory, 80 KB ROM and 4 MHz - 32 MHz micro-controllers), and (ii) powerful base stations. Sensor nodes are autonomous devices capable of retrieving information from their surroundings (i.e., r_i). They can process such data and communicate with other network nodes. The base station acts as an interface between the real world (close to human operators) and the data acquisition world (i.e., the sensor nodes). This is able to collect, process, store and transmit any information generated by sensors as well as issue control orders to these entities. Regarding the network architecture, it does not have to be centralized. Sensor nodes can operate in a distributed way without accessing the base station, participating in both the routing and decision making processes.

Other features of this technology is its capability for self-configuration, which allows sensor nodes to adapt by themselves to network topology, and its ability for self-healing to cope with unforeseen events. Additionally, the autonomous nature of the sensors enables them to offer easy deployment, maintenance and collaboration with other devices so as to achieve common goals. As a result, WSNs can provide a wide area coverage by merging the limited area observed by each individual node. Data aggregation from different sensor sources also increases the accuracy of the observed parameters. Intelligent sensing is performed in each sensor by processing the raw data prior to transmission, thus reducing the communication overhead and providing an efficient use of resources [26]. Last but not least, the low cost of sensor nodes, despite being a non functional feature, may tip the balance in favor of WSN technology. Moreover, WSNs can be used for monitoring and surveillance applications with support for offering warning services by checking the state of specific conditions and trigger alarms under anomalous circumstances. Finally, they can provide on-demand information services associated with states of the observed system ($r_i \in [V_{min}, V_{max}]$ or $r_i \notin [V_{min}, V_{max}]$) or states of their surroundings for diagnostic purposes. All of these aspects have made WSNs a promising technology for CIs, where governments, industry, scientific community [27] and market are interested in extending the applicability of WSNs in real environments.

Most of the wireless communication standards applicable to WSNs, such as ZigBee PRO, WirelessHart and ISA100.11a, are based on the IEEE 802.15.4-2006 standard [28]. The main goal of these standards is to provide secure connectivity assuring energy saving, coexistence with other systems and data reliability [29]. To this end, the network design is typically based on a specific network topology; i.e., a wireless mesh network. For example, ZigBee PRO supports mesh and many-to-one networks using a coordinator (a trustworthy node), routers and sensor nodes. WirelessHART was defined to provide industrial solutions through wireless mesh networks composed of sensor nodes, routers, handheld devices, gateway using a network manager (a trustworthy node), and existing industrial devices. Similarly, ISA100.11a provides industrial solutions under a mesh and star network composed of node sensors, routers, handheld devices, gateways (one or several), and two managers: a system manager, in charge of allocating resources and providing communication, and a security manager, in charge of offering security services. It is important to point out that these standards have been mainly designed for carrying out local activities in field, substations or subsystems, such as local access to sensor nodes.

4 Industrial WSN Requirements and Integration Strategies

In order to provide their services, industrial wireless sensors could greatly benefit from being integrated into the envisioned IoT. Collaboration and critical data aggregation between geographically dispersed sensors could be enhanced providing more reliable and accurate information. Moreover, system operators and also end-users (with restricted privileges) could benefit from anywhere real-time access to infrastructure data with reduced system costs. However, as there are many integration strategies that can be used to connect WSNs to the Internet, it is necessary to know which one is more suitable given the requirements of the scenario. The purpose of this section is therefore to introduce both the specific requirements of industrial WSNs and the different integration strategies that can be used to connect this technology to the Internet.

4.1 Control and Automation Requirements

In order to study the security of industrial WSNs in the context of the Internet, it is essential to consider not only security requirements, but also the requirements that such control networks must satisfy, like maintenance, system performance and reliability of the resources/services [17]. The reason is simple. Some of these requirements have a direct influence on the security requirements of the network, and vice versa. For example, if we use an end-to-end secure channel to open a communication channel between a sensor node and a central system, we will increase the overhead associated with the node, not only in terms of response time, but also in terms of the memory available to the node. Consequently, this subsection introduces the basic requirements (including security) that both control systems and industrial systems must consider.

4.1.1 Maintenance

One important aspect of the management of any substation system is the maintenance of its SW and HW resources. To prevent the appearance of errors, every device must be properly configured at all times, and periodical tests should be performed either from the control center or at a local level; i.e., at the substation itself. Moreover, the software components included within the devices should be up-to-date (after such components have been properly tested in a controlled testbed) and new hardware devices should be added to the substation if needed. Consequently, the properties associated with maintenance are:

- *Addressing.* It is necessary to specify some kind of unique identification (e.g., network address) for every RTU present in the substation in order to access the stream of data each one produces. This property is related to how the different identifications of the devices are accessed and who is responsible for storing those Identities (IDs).

- *Internal Access.* The services offered by the devices found inside the substation should be accessed locally by substation operators, either for testing purposes or for redundancy purposes. This property is concerned with the actual complexity of accessing the devices of the substation locally (e.g., either using IP connectivity or using specialized protocols and devices).

- *Maintainability.* As with any device, the software included within the RTUs will need to be updated for many reasons, such as upgrades, optimizations, security patches, and so on. This property refers to the number of devices that must be changed in order to fix or update the functionality of the substation.

- *Extensibility.* The number of RTUs that can be found in a given substation will certainly change during the lifetime of the infrastructure. As a property, extensibility is related to the overall changes that must be made in the substation in order to include new hardware devices.

4.1.2 Reliability

As one of the major purposes of a substation is to examine and control the state of CIs, the functionality provided by the substation must be reliable enough to offer its services within certain quality levels. The data streams provided by the RTUs should be available at all times, and any query regarding the actual content of a given data stream should arrive at the central system as fast as possible in order to react to critical situations. Consequently, the properties associated with reliability are:

- *Availability*[1]. As the infrastructures monitored by the substations are usually critical, the data produced by the RTUs must be available at all times in order to react to problematic situations and ensure the integrity of the whole system. As a property, there are in fact two dimensions of availability: one related to reliability (using the redundancy of the system to avoid single points of failure) and one related to security (existence of denial of service attacks and use of self-healing mechanisms to provide the services even in the case of attacks/system failures).

- *Performance.* Not only must the data be available at all times, but it must also be retrieved from the RTUs at an acceptable speed. As a property, performance is related to the hardware capabilities of the devices of the substation, in addition to the actual speed of the substation network infrastructure, and the number of hops between the RTU and the data

[1] Note that availability can be considered as a security requirement, but it has been classified as a reliability requirement due to its close relationship with the functional dimension of a substation.

repository. Note that this property is classified into the “Reliability” category because poor performance under challenging situations can hinder the reliability of the overall system.

4.1.3 Overhead

As pointed out in sections 2 and 3.2, the computational resources available to substation devices are increasing. Nevertheless, it is necessary to achieve a balance between the number of resources available to a device and its overall cost. A device should not be encumbered by an excess of workload, but it should not have any unnecessary resources. Additionally, those resources should be optimized to work in the substation environment. Consequently, the properties associated with the overhead are:

- *Device Resources.* In order to implement the different protocols that provide the core functionality of substations, such as DNP3 or WirelessHART, the devices must use some of their HW and SW resources. This property refers to the amount of resources (e.g., RAM, CPU) that are needed within a node to implement those protocols.

- *Communication Overhead.* The bandwidth available inside the substation for local communications between devices might be restricted due to limitations in the wireless channel. For example, most sensor nodes introduced in Section 3.2 make use of the IEEE 802.15.4 standard, which only provides a maximum transfer rate of 250 kbit/s. As the size of the packets are highly dependent on the header size of the protocols used inside the network, this property deals with the overhead produced by such protocols. For example, if a combination of protocols waste too much header space, the amount of bytes available for the transmission of data will be limited.

- *Optimization.* There are some specific protocols that are optimized to provide the best possible functionality in a particular environment. This property is related to the existence of network-specific protocols (such as WirelessHART or ISA100.11a), which are aware of the specific features of the network environment and use them to provide better services. Some of these services are network redundancy, link robustness, industrial noise or obstacle control (using frequency hopping and blacklisting methods), collision control through a specific TDMA (Time Division Multiple Access) based on fixed time-slots, diagnostic mechanisms, routing discovery, low-duty cycle, maintenance tasks through handheld devices, or even alarm management based on priorities [30]. For example, ISA100.11a uses up to five priority levels (journal (0-2), low (3-5), medium (6-8), high (9-11) and urgent (12-15)) for four kinds of diagnosis subcategories: a device diagnostic, a communication diagnostic, a security alert and a process alarm [29].

4.1.4 Security

Ensuring the security in the different processes of a substation is a matter of utmost importance. If security is not fully considered, any problem that causes an impact on the integrity of the elements of a substation will potentially affect the real world as well, harming not only physical infrastructures, but also human lives and money. Therefore, only authorized users should have the right to modify the state of the elements of a substation, and only trusted users should be able to access the streams of data produced by the substations. In addition, there should be some mechanisms that store the interactions between the different elements of the substations. Such mechanisms not only facilitate the analysis of the behavior of the system and the detection of possible security breaches, but also help to control the uncertainty in the interactions between entities. Consequently, the properties associated with security are:

- *Attacker Impact.* Adversaries usually target those subsystems that provide the biggest payoff. Therefore, it is necessary not only to identify the potential weak points, but also to understand the extent to which an attacker can manipulate the infrastructure once these weak points are subverted. As a property, it refers to the actual impact caused by an adversary that takes control of a section of the network.

- *Secure Channel.* Whenever two devices that belong to the same SCADA system (e.g., a machine from the central system and an RTU from a substation) communicate, it is important to set up a secure channel that supports end-to-end integrity and confidentiality services. If the integrity of the data stream is protected, attacks will not be able to falsify any reading $(\{r_i, r_j, ..., r_n\})$/alarm $(\{a_i, a_j, ..., a_n\})$. In addition, once the confidentiality of the information flow is assured, adversaries will be unable to read any sensitive information. As a property, it refers to the type of machines and mechanisms (e.g., end-to-end secure channels) that are involved in the creation of a communication channel that support confidentiality and integrity.

- *Authentication.* As for user authentication, the devices should be confident about the identity of the user that is requesting a certain operation. As a property, authentication is also concerned with the location and the nature of the mechanisms and elements that can be used to prove the identity of a human user (e.g., whether the mechanisms are distributed or centralized).

- *Authorization.* Once any user of the network (be it either a human user or a machine) proves their identity, it may be necessary to check whether that user has the rights to access the information. Not only should the access to the data be controlled, but also the granularity of the data. Beyond data, it is also necessary to monitor control operations (e.g., devices must only be reprogrammed by authorized users). As a property, authorization deals with the types of mechanisms, credentials and tools that can be used to check whether a certain entity is authorized to perform an operation.

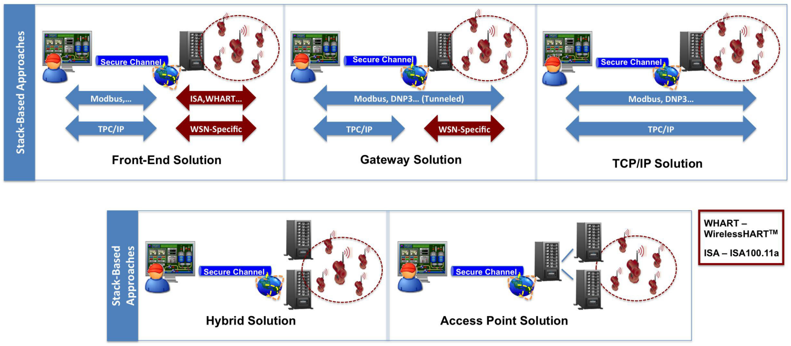

Figure 3: Integration Strategies

- *Accountability and Detection.* Since a heterogeneous set of users will be accessing the services of a substation, it is important to record the interactions with those users. By storing all interactions, we can recreate security incidents and abnormal situations. In addition, we can detect specific attacks in real time. As a property, accountability and detection refers to the structure of the accountability subsystems (e.g., detection rules) and the mechanisms that can be used to analyze them.

- *Trust Management.* Within a substation, there can be several nodes that provide the same services for redundancy purposes. Moreover, various nodes can also collaborate with each other. However, in this situation, we have to solve the problem of uncertainty (i.e., Which is the best data source? Whom should I collaborate?). This task is usually fulfilled by a trust management system. As a property, trust management is related to the nature of the mechanisms that are used to (i) measure and share the reputation of the different elements of a substation, and (ii) use those values as input when determining specific trust values.

4.2 Integration Strategies

It is possible to classify the integration approaches between the Internet and WSNs in two different ways: stack-based [31] and topology-based [32]. In stack-based classification, the level of integration between the Internet and a WSN depends on the similarities between their network stacks. A WSN can be completely independent from the Internet (*Front-End*), be able to exchange information with Internet hosts (*Gateway*), or share a compatible network-layer protocol (*TCP/IP*). On the other hand, in topology-based classification the level of integration depends on the actual location of the nodes that provide access to the Internet. These nodes can be a few dual sensor nodes (e.g., base stations) located in the root of the WSN (*Hybrid*), or a fully-fledged backbone of devices that allow sensing nodes to access the Internet in one hop (*Access Point*). For the sake of clarity, the different approaches (which are shown in Figure 3) will be explained in the following paragraphs.

In **stack-based classification**, the first approach is the *'Front-End' solution*. In this solution, the external control systems (e.g., the central SCADA system) and the WSNs of the substations never communicate directly with each other. In fact, the sensor network is completely independent from the Internet, so it can implement its own set of protocols (e.g., ZigBee PRO, ISA 100.11a, or WirelessHART). All interactions between the outside world and the sensor network will be managed by an concentrator device (e.g., an RTU). This type of device is able to store all the data streams coming from the WSN, and it can also provide control systems with field information through well-known interfaces (e.g., DNP3 or web services). In addition, any queries coming from the control systems will always traverse the concentrator device. Most academic and commercial control systems that use the Internet (cf. Section 3.1) use this type of solution.

The second approach, the *'Gateway' solution*, considers the existence of a device (e.g., an RTU) that acts as an application layer gateway, in charge of translating the lower layer protocols from both networks (e.g., TCP/IP and proprietary) and routing the information from one point to another. As a result, Internet hosts and sensor nodes are able to exchange information without establishing a direct connection. For example, nodes will be able to answer specific protocol queries (e.g., DNP3, WirelessHART) from external control systems. In this solution, the sensor network is still independent from the Internet, and all queries still need to traverse a gateway device. As of 2012, this solution is technically possible with standards like ISA100.11a that support protocol tunneling (e.g., using a "tunnel" object).

As for the third approach, the *'TCP/IP' solution*, sensor nodes implement the TCP/IP stack (or a compatible set of protocols such as 6LoWPAN [33] in 802.15.4 networks), thus they can be considered as fully-fledged elements of the Internet. Any Internet host (e.g., the elements of a control system) can open a direct connection with them, and vice versa. The connection with the Internet is usually done through a concentrator point, which can provide translation services (e.g., 6LowPAN ↔ IPv6). Moreover, using other IETF protocols such as the Constrained Application Protocol (CoAP, a generic web protocol definition) and the Constrained RESTful Environments (CoRE, a lightweight REST web service architecture), even constrained nodes can provide web services to external hosts. In fact, such combination of protocols enables the integration of industrial WSNs with the IoT. However, using this approach, it is not possible to use specific substation protocols like WirelessHART in the WSN, as these protocols define their own stacks. Still, we can use other protocols that support TCP networks, such as DNP3/IP or Modbus/TCP.

Regarding the **topology-based classification**, the *Hybrid solution* approach considers that there is a set of nodes within the WSN, usually located on the edge of the network, that is able to access the Internet directly. In fact, these nodes can be easily mapped to base stations, since every sensor within the WSN needs to traverse them in order to connect to the central system, and vice versa. The specific features of this type of approach are redundancy and network intelligence. By default, this approach considers that it is possible to provide more than one base station to access the functionality of the network. In addition, as those base stations have the capability to connect to the Internet, it means that the intelligence of the network (i.e., the implementation of the different substation protocols) is pushed onto a subset of the WSN.

This delegation of capabilities is further developed in the *Access Point solution* approach. Here, WSNs become unbalanced trees with multiple roots, where leaves are normal sensor nodes and all other elements of the tree are Internet-enabled nodes. As a result, all sensor nodes are able to access the Internet in just one hop. One of the main features of this approach is the possibility to increase the capabilities of nodes that belong to the backbone network. For example, backbone nodes can have more resources than normal nodes, and can implement faster network standards (e.g., 802.11 vs. 802.15.4).

It is important to note that the previously shown topology-based networks are usually combined with the approaches from the stack-based classification. For example, in a backbone-type network, the Internet-enabled nodes can behave i) as a front-end, effectively isolating the WSN sensors from the Internet, or ii) as gateways, allowing direct data exchange between sensors and the central system. There is an exception, though: it is essentially irrelevant to combine the 'TCP/IP' solution with the hybrid and backbone solutions, as every node is able to connect to the Internet. In fact, the only task of the nodes that connect to the Internet with the local network will be to behave as translators (e.g., between 6LoWPAN and IPv6).

5 Analysis of Integration Mechanisms

Once we have introduced the integration strategies and the requirements of industrial WSNs, we should be able to tackle these two questions: (i) *What are the specific advantages and disadvantages of every integration strategy in the context of industrial WSNs?*; and (ii) *Which strategy should I choose for a particular deployment?* In the following paragraphs we will answer the first question by discussing the influence of the integration strategies over the requirements presented in Section 4.1. For the sake of clarity, this is summarized in Table 1. We will make use of this discussion for answering the second question in the next section.

5.1 Analysis

5.1.1 Maintenance

The properties associated with maintenance that have to be analyzed are addressing, internal access, maintainability, and extensibility.

In terms of *addressing*, the 'Front-End' and 'Gateway' solutions require translating the identity of the node (e.g. Metering Pump A, DNP3 Address 65519) to the actual address of the node (e.g., WirelessHART EUI-64 Address).

Remote Substations		*TCP/IP*	*Front-End*	*Gateway*
Maintenance	*Addressing*	Translation at central system	Translation at substation	
	Internal Access	Use IP address	Use local services	
	Maintainability	Update all nodes	Update 1+ device	Update all nodes
	Extensibility	Add row to translation table	Add row to translation table and local management	
Reliability	*Availability*	Vulnerable due to constraints	Single point of failure, "store and forward", "cache"	
	Performance	May need of 'Access Point' solution. Extra penalty if packet processing		
Overhead	*Device Resources*	More mechanisms inside nodes	Less mechanisms	More mechanisms inside nodes
	Communication	Extra 6LowPAN headers	Choice: extra and local headers	
	Optimization	Use only IP and MAC layer services	Take advantage of WSN-specific optimizations	
Security	*Attacker Impact*	Covert attacks	Single point of failure	Covert attacks
	Secure channel	End-to-end	Bridged at base station	End-to-end
	Authentication	Distributed mechanism	Centralized mechanism	Distributed mechanism
	Authorization	Distributed mechanism	Centralized mechanism	Distributed mechanism
	Accountability	Limited by storage / Hybrid	Centralized	Centralized, only statistics
	Detection	Efficient detection rules	Lightweight detection rules	Efficient detection rules
	Trust Mgmt.	Local and Global, drawbacks depending on solution		

Table 1: Detailed Analysis of Properties and Integration Strategies

The translation table should be located within the remote substation, as the conversion between identity and WSN address will be performed there. On the other hand, the 'TCP/IP' solution requires the translation table to be located in the central system (e.g., Metering Pump A → a.b.c.d), as such a system must use the IP addresses of the WSN nodes to open a direct connection. For this particular property, the suitability of the approaches depends on the kind of management preferred (decentralized or centralized). Note that the complexity of the addressing management increases if we take into account the 'Hybrid' and 'Access Point' solutions, as we need either to replicate the translation tables among the Internet-enabled nodes or to create a centralized service that provides a translation interface.

Internal access is not an issue for most solutions. In all solutions, the human operators performing maintenance processes within the remote substation can use the substation network to connect to the data retrieval services (e.g., through an RTU, using TCP/IP direct connection with the sensor nodes, etc). If the operators are in the field where the sensor nodes are deployed, they can also use the local services of the WSN-specific protocols. For example, in solutions where the WSN is independent of the Internet ('Front-End' and 'Gateway'), an operator can use the features offered by internal protocols like WirelessHART to access the data stream of a sensor node in a direct manner. As for the 'TCP/IP' solution, direct local access is also possible, although operators should know the IP addresses of the nodes they want to access beforehand. The 'Access Point' solution may add a small amount of complexity to this process, as operators need to be physically near the node they want to read data from if they want to use the internal protocols of the WSN.

Maintainability is directly related to the number of devices that need to be upgraded when a SW update is tested and accepted by the central management. In every solution, upgrading the protocol used in the WSN (e.g., ISA100.11a, TCP/IP) means upgrading all sensor nodes. Therefore, we will focus on the upgrades that target the control protocols that interface with the central system (e.g., DNP3). For control protocols, the 'Front-End' solution is the most simple to maintain: there is only one device (the concentrator device) that needs to be upgraded. On the 'Gateway' and 'TCP/IP' solutions, we need to change the control protocols in all sensor nodes. Nevertheless, in the 'Front-End' solution the whole WSN will not be available during the upgrade (i.e., the concentrator device is the only entry point to the network), while for the other two solutions it is possible to perform a gradual upgrade. Note that the 'Hybrid' solution is also able to provide support for gradual upgrades due to its inherent redundancy, while the 'Access Point' solution can not provide full support for gradual upgrades as every sensor node is usually connected to one single backbone node.

Finally, regarding the *extensibility* property, adding a new node is not a very cumbersome task. In the 'Front-End' and 'Gateway' solutions, we need to include a new entry in the translation table and run the specific mechanisms of the WSN protocols. The process in the 'TCP/IP' solution is simpler, as the only change that needs to be made is to add a new entry to the translation table. The task is similar for the 'Hybrid' and 'Access Point' solutions, although, if the translation table is distributed then all changes must be stored in all devices (or in a centralized service if a translation interface is available).

5.1.2 Reliability

The properties associated with reliability that have to be analyzed are availability and performance.

In terms of the *availability* property, the 'Front-End' solution is weak against failures or attacks (e.g., Denial of Service attacks). As there is only one single point of entrance to the WSN, any problem will bring the whole system down. Still, this solution can be improved if combined with the 'Hybrid' solution, as redundancy improves availability. Additionally, the 'Front-End' solution can make use of the lack of integration with the WSN to transparently implement self-healing mechanisms. For example, the concentrator device can use store and forward mechanisms, and can also know whether a certain sensor of the WSN is unreachable and try to obtain information from another sensor if the WSN is redundant enough. The 'Gateway' solution has the same advantages and disadvantages of the 'Front-End' solution, although the self-healing mechanisms will be less transparent since data messages will arrive "as is" to the sensor nodes. It also must take into account attacks that target the application layer. Finally, the 'TCP/IP' solution is very vulnerable against attacks that target the availability of the network, mainly due to the limited capabilities of the sensor nodes (i.e., an attacker will need less resources to perform a DoS to a node with just 128 KB of memory), so it will be indispensable to implement protection mechanisms in the remote substation access points. This particular problem is shared by the 'Access Point' approach, as the backbone will use TCP/IP to transmit information to the sensor nodes.

In contrast, the 'Access Point' approach has some advantages in terms of *Performance*. If the backbone nodes use high-speed communication technologies (and have a reliable power supply), the data streams can be provided to the substation network at a very fast speed. To put this assertion into context, the maximum data rate of the 802.15.4-based WirelessHART and ISA100.11a protocols is 250 Kbit/s, while the maximum data rate of 802.11b-based networks is 11 Mbit/s. Of course, as the link between the backbone nodes and the sensor nodes has a low data rate, all the other solutions can have a similar performance if there is only one hop between the sensor node and the substation network. Performance can be also improved if the central system does not want to access real-time data, as the 'Front-End' and 'Gateway' solutions can prefetch data streams and store them in a cache. Observe that packet processing may also harm the overall performance of the WSN, thus all solutions that impose any extra packet processing (e.g., 'Front-End' solution) may have a performance penalty.

5.1.3 Overhead

The properties associated with overhead that have to be analyzed are device resources and optimization.

In terms of *device resources*, all solutions that push the intelligence to the sensor nodes (e.g., the 'Hybrid' and 'Access Point' solutions, the 'TCP/IP' solution) require that sensor nodes have enough capabilities to implement the application protocols, including any security protocols. As pointed out in section 3.2, the sensor nodes that are used in SCADA systems are only slightly better than the sensors used in the academic world. Therefore, most results regarding the feasibility of implementing a complete IP-stack in sensor nodes, as well as issues related to computational and memory constraints available in the literature, can be extrapolated to current industrial nodes. Analyzing the capabilities of industrial sensor nodes, it would seem difficult to implement a TCP/IP or WSN-specific stack, a control protocol parser, and all the necessary security mechanisms (cryptography primitives, link-layer security, end-to-end security) inside the same node. However, recent research results (e.g., IPsec [34]) show that this restriction might be lifted in the future.

Regarding the *communication overhead* property, the 'TCP/IP' solution seems to impose an extra overhead due to the size of the 6LowPAN headers, in comparison to the simpler headers that are used by protocols optimized for local communications. Nevertheless, this assumption is challenged by various factors. For example, 6LowPAN makes use of diverse header compression mechanisms, which provide support for various compression modes (e.g., address compression, option compression, multicast address compression). Moreover, some protocols such as ISA100.11a not only make use of simple header mechanisms, but also can choose to make use of 6LowPAN as their underlying network infrastructure. As a consequence, the overhead of all solutions (either Internet-based or local-based) largely depends on the design of the network.

As for the *optimization* property, all solutions that make extensive use of WSN-specific protocols ('Front-End', 'Gateway', 'Hybrid') can benefit from their optimizations. For example, WirelessHART uses a TDMA data-link layer to provide Quality of Service, supports mechanisms such as channel hopping to maximize coexistence with other ISM band equipment, and also implements a self healing, redundant path mesh routing protocol. Some of these benefits cannot be found in pure TCP/IP networks, and others (e.g., the use of an underlying data-link layer that provides certain properties) are usually not explicitly considered. Nevertheless, the 'Access Point' solution can also benefit somewhat from these optimizations, since the connection between the sensor nodes and the backbone nodes uses the WSN-specific protocols.

5.1.4 Security

The properties associated with security that have to be analyzed are: attacker impact, secure channel, authentication, authorization, accountability / detection, and trust management.

The *attacker impact* is highly dependent on the importance of the different elements of the substation. In the solutions where concentrator devices behave as an interface between the external control systems and the sensors (e.g., 'Front-End', 'Hybrid', 'Access Point'), such devices become the most attractive target for attackers. By controlling a concentrator point, an adversary can disrupt the functionality of a large section of the sensor network: all information flows can be eavesdropped, and all operations can be manipulated – even in a subtle way. This problem is attenuated in the 'Gateway' and 'TCP/IP' solutions, as the services are provided directly by the nodes. Attackers can still hinder the provisioning of services (e.g., by attacking the availability of the concentrator, cf. Section 5.1.2), but data tampering attacks become much more difficult due to the possibility of implementing end-to-end secure channels. It is important to note that, in all solutions, attackers can directly take control of specific nodes within the network, so as to covertly affect its services. This type of attack can principally be carried out by exploiting vulnerabilities in the nodes' services. While the 'Front-End' solution becomes more complicated (i.e., the adversary must first gain access to the internal sensor network), this task is easier whenever the 'Gateway' and 'TCP/IP' solutions are implemented (i.e., any external attacker can try to perform this attack).

In order to comply with the *secure channel* property, it is necessary to protect the confidentiality and integrity of all communications between the central system and the sensor nodes. The 'TCP/IP' solution is able to provide an end-to-end secure channel between these entities, as every device located in the routing path will use the TCP/IP stack. Still, IPsec is not officially supported due to resource constraints [35], although novel research results are trying to solve this issue [34]. In addition, it might be possible to use other mechanisms such as SSL/TLS at the transport layer or WS-SecureConversation (for security contexts in web services) at the application layer. These security mechanisms at the application layer can also be used by the 'Gateway' solution due to its forwarding capabilities. Note that even if Internet protocols are supported in the near future, it is still necessary to tackle the problem of key management: nodes need to store certain devices credentials (e.g., the certificates of all external control systems from all operators), but the storage available for sensor nodes might be limited. Moreover, the management of all these credentials becomes more complicated in this distributed environment.

As for the creation of secure channels in the 'Front-End' solution, in this approach it is not possible to create an end-to-end secure channel: operators do not contact sensor nodes directly. Still, the information exchange can be easily protected from external eavesdroppers: one part of the connection will make use of TCP/IP security mechanisms and the other part of the connection will employ the WSN-specific protection mechanisms. Key management is also easier, as the nodes only need to store the credentials of the concentrator devices. As a final note, for both the 'Front-End' solution and the 'Gateway' solution, it is also possible to create a VPN between the central system and the concentrator (e.g., gateway, front-end) located in the remote substation.

Regarding user *authentication*, one of the major challenges to solve is the location of both the authentication service and the storage of the user credentials (e.g., user/password pairs). In the 'Front-End' solution, where all traffic must traverse one single device (e.g., the concentrator), all processes and user data can be stored in that device. The other solutions ('Gateway', 'Hybrid', 'Access Point', 'TCP/IP') have multiple points where the service can be provided. As a result, it is necessary to integrate either an authentication server or other protocols and mechanisms such as Kerberos in order to centralize the authentication information and avoid replication. However, it should be pointed out that in the 'TCP/IP' solution these centralized approaches can become energy-consuming if the service providers (i.e., the sensor nodes) must use an external service to test the user credentials. Consequently, it can be also possible to replicate the user databases if needed, although this configuration increases the complexity of the maintenance processes. Moreover, this replication strategy might not work if the authentication mechanisms are complex and too cumbersome for the sensor nodes. Note, however, that this approach has a specific benefit: in case the authentication servers are not available, operators (e.g., employees located within the substation) can still perform some operations in case of emergency. Another approach that can be used for the 'Gateway' solution, which also forces all traffic to traverse one single device, is to implement a mechanism where an user can obtain a dedicated secure channel between himself and the gateway after the authentication process.

Authorization is very similar to authentication. Its main challenge is the location of the authorization service and the permissions of users. The same solutions explained as authentication apply for authorization, although it should be noted that the maintenance of a distributed authorization database is more complex: user permissions change more frequently than user identities. Note, however, that certain mechanisms such as Role-Based Access Control (RBAC) can be implemented in a distributed-friendly way. While RBAC is a complex approach, it is possible to implement it using Attribute Certificates (AC) [36], where the sensor nodes check whether the roles contained within these AC have the right to perform an action. Still, it is necessary to consider that such mechanisms require not only enough computational power within the nodes, but also an infrastructure in charge of defining roles and policies.

As for *accountability*, one possible approach is to use a single entity to store all the interactions between the central system and the sensor nodes. This approach is quite optimal for centralized solutions such as 'Front-End' and 'Gateway', because in other solutions any interaction information must be collected from the different entities and sensor nodes. Note that if end-to-end security mechanisms are used (e.g., in the 'Gateway' solution), the gateway devices can only extract statistical data from the information flow. As for pure decentralized solutions, where the interactions are stored in all sensor nodes, the actual amount of information that can be stored is limited by the nodes' storage. Nevertheless, it might be possible to use an hybrid approach if the sensor nodes are able to collaborate with each other or with other devices. For example, in the case of overflow, the historic data can be moved to a specialized system or even to more powerful devices (e.g., powerful nodes in the 'Access Point' solution).

Regarding *detection*, decentralized solutions that push intelligence to the sensor nodes ('Access Point', 'TCP/IP') need to implement various detection rules within all the sensor nodes, because any node can become a target of attacks. Note that firewalls and other mechanisms can (and should) be used, but as mentioned, the existence of end-to-end mechanisms makes the implementation of some rules within the nodes necessary. Nevertheless, for all solutions, the creation of lightweight detection rules within the WSN that can detect possible malfunctions and internal attacks should be recommended: these detection rules can uncover not only external attacks, but also internal attacks caused by malicious or malfunctioning nodes. In fact, the field of intrusion detection in WSNs is advancing steadily, and various simple yet usable mechanisms can be integrated as of 2012 [37].

Finally, all solutions can benefit from a local *trust management* system implemented in the sensor network. The nodes of the network can analyze the behaviour of other nodes in order to evaluate their reputation; later trust values can later be derived from this reputation. In fact, there are already various trust management systems specifically designed for sensor networks, which might be applicable in this particular context (cf. [38]). However, the 'TCP/IP' and 'Gateway' solutions have some additional challenges that need to be considered. The amount of information available to the local nodes is lower: not only the communication layers cannot be extended with specific WSN information due to the use of Internet protocols, but also end-to-end secure channels can reduce the amount of information available to neighbour nodes. In addition, the concentrator in the 'Front End' solution can become another element in the trust management system (due to its holistic point of view of the sensor network state), transparently selecting the most adequate sensor services according to the available data. This transparency cannot be used in the 'TCP/IP' solution: external control systems must first query the trust values of specific nodes before making a decision. Obviously, it is also possible to develop a trust management system at the SCADA level. In this case, various control systems share their interactions with the different sensor nodes of a substation, so as to make informed decisions regarding whom to trust for a particular service.

Solutions	*Advantages*	*Disadvantages*
TCP/IP	Full integration with the Internet Support for gradual updates Resilience to node failure *(Future:)* Nodes can directly access external services	More complex security mechanisms Highly vulnerable service providers Cannot use optimizations from specific industrial WSN protocols No "store and forward", no data stream caches
Front-End	Standards for security mechanisms Can use specific industrial WSN protocols Network is simpler to maintain Support for "store and forward", data stream caches	Concentrator becomes a "single point of failure" Complex upgrade procedure
Gateway	Standards for certain security mechanisms Can use specific industrial WSN protocols Support for "store and forward", data stream caches Support for gradual updates	More complex security mechanisms Vulnerable service providers (direct data connection) Maintenance becomes more complex Complex upgrade procedure

Table 2: Summary of Major Advantages and Disadvantages of the Integration Strategies

5.2 Discussions

Once the features of the different integration strategies have been analyzed, it is time to discuss their suitability for industrial environments. Due to the importance of the 'TCP/IP' solution for the IoT paradigm, this solution will be discussed first, followed by the 'Front-End' solution and the 'Gateway' solution. For the sake of clarity, these discussions are summarized in Table 2.

The 'TCP/IP' solution guarantees that the WSN located in remote substations are fully integrated with the Internet, but it is not clear whether this can be considered as an advantage or not. In terms of security, it is necessary to protect the WSN from any kind of intrusion, as even an increase in the network traffic can become problematic for the sensor nodes due to their limited capabilities. Obviously, firewalls and other mechanisms can help to alleviate this problem, but new rules and algorithms must be specifically created for these networks. Other security aspects such as user authentication and authorization have no established solution (although mechanisms such as authentication servers can be applied), and the topic of key management is quite complex. Moreover, the implementation of trust management systems presents various additional challenges in comparison with other solutions. In addition to these security issues there are other aspects in the 'TCP/IP' solution that need to be considered. In particular, a TCP/IP-based WSN will not benefit from the specific optimizations of protocols like ISA100.11a, and will have no native support for "store and forward" mechanisms and data stream caches. Additionally, the capabilities of the sensor nodes may not be enough to implement the required protocols. Nevertheless, the 'TCP/IP' solution also has some specific advantages, such as support for gradual updates (i.e., updating one node will not bring the entire system down) and resilience to device failure (i.e., a failure in one node will probably not endanger the whole network).

In contrast, the 'Front-End' solution solves some of the problems of the 'TCP/IP' solution, although it also has issues of its own. Existing standards can be used to implement the security mechanisms, although the existence of a concentrator as an entry point of the network makes this solution quite vulnerable against several types of attacks (e.g., availability, tampering, controlling). This problem can be lessened by using the 'Hybrid' and 'Access Point' solutions, but these solutions have their own specific problems (mainly due to the replication of resources). Another important benefit of the ‘Front-End’ solution is the use of the WSN-specific optimizations, and the ability to include self-healing mechanisms (e.g., if one node is not available we can access another one if the WSN is redundant enough). Finally, the maintenance of the network is quite simple (e.g., only one device needs to be upgraded), but this is a doubled-edged sword, as the network will not be available during the upgrade process. This issue can be solved through replication and the ‘Hybrid’ and ‘Access Point’ solutions.

The ‘Gateway’ solution provides a middle ground between the ‘TCP/IP’ solution and the ‘Front-End’ solution. It has some of the ‘Front-End’ solution benefits (e.g., use of WSN-specific optimizations, implementation of “store and forward” mechanisms), and it allows the central system to query the sensor nodes directly. Nevertheless, it also pushes some complexity to the sensor nodes, and it also needs to solve certain security details, such as the implementation of the authentication, authorization, and trust management mechanisms. Moreover, the gateway device should parse all incoming messages in order to analyze the queries and to avoid application-specific attacks, and other aspects (such as maintainability) getting more complex as well. Note that this solution can also be combined with the ‘Hybrid’ and ‘Access Point’ solutions to obtain benefits such as redundancy, although the specific problems of these solutions (e.g., distribution of tables and resources) need to be taken into account.

From the previous discussions, *it would seem that the actual benefits of using a pure ‘TCP/IP’ solution for remote substations are not enough to warrant a total integration between WSN and the Internet in industrial networks.* As control systems simply want to access data streams and to issue control commands, other solutions (e.g., ‘Front-End’) combined with approaches that provide extra redundancy may be good enough for the present needs of the industry. Nevertheless, the complete integration of the WSN and the Internet may bring one specific benefit that needs to be further analyzed, sensor nodes evolve from mere passive devices to fully-fledged citizens of a networking society, able to access any web service in the world if they need to do so. In the future, it will be necessary to analyze this particular feature in order to make breakthrough discoveries that may benefit the industry as a whole.

6 Conclusions

As sensor nodes have become part of the IoT, new challenges and research horizons have emerged. This paper is a clear example of these challenges. Here, an analysis has been presented of the secure integration of sensor nodes in the Internet, with a clear focus on the industrial environment. As a conclusion of this analysis, it can be stated that for the existing needs of the industry, it is not necessary to fully integrate the industrial WSNs with in the Internet, and a simple capillary network [39] with enough redundancy can provide all the desired functionality. However, for future work, it will be necessary to check how bringing all the functionality of the Internet to an industrial sensor node may enable new and exciting applications.

Acknowledgments

This work has been partially supported by PISCIS (P10-TIC-06334), ARES (CSD2007-00004) and SPRINT (TIN2009-09237) projects. This last one is cofunded by the FEDER Program.

References

[1] C. Alcaraz, G. Fernandez, F. Carvajal, *Security aspects of SCADA and DCS environments*, Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense, LNCS 7130, pp. 120-149, Springer-Verlag, September 2012.

[2] B. Reaves, and T. Morris, *An open virtual testbed for industrial control system security research*, International Journal of Information Security (IJIS), Springer Berlin/Heidelberg, vol. 11, no. 4, pp. 215-229, ISSN: 1615-5262, 2012.

[3] M. Botterman, *Internet of Things: an early reality of the Future Internet*, Information Society and Media Directorate General, Networked Enterprise & RFID, European Commission, 2009.

[4] W. Shaw, *Cybersecurity for SCADA systems*, PennWell Corp, Tulsa, ISBN: 978-1-59370-068-3, 2006.

[5] F. Baker and D. Meyer, *RFC 6272-Internet protocols for the smart grid*, Internet Engineering Task Force (IETF), June 2011.

[6] G. Irwin, J. Colandairaj and W. Scanlon, *An overview of wireless networks in control and monitoring*, In Proceedings of the 2006 International Conference on Intelligent Computing (ICIC'06), LNCS, vol. 4114, pp 1061-1072, 2006.

[7] ZigBee Alliance, `http://www.zigbee.org/`, accessed on October, 2012.

[8] HART Communication Foundation, `http://www.hartcomm.org/`, accessed on October, 2012.

[9] ISA100, *Wireless Systems for Automation*, `http://www.isa.org/`, accessed on October, 2012.

[10] *Modbus-IDA the architecture for distributed automation*, `http://www.modbus.org/`, accessed on October, 2012.

[11] DNP3, *DNP Users Group*, `http://www.dnp.org`, accessed on October, 2012.

[12] IEC 60870-5-104, *Part 5-104: Transmission protocols - network access for IEC 60870-5-101 using standard transport profiles*, Second edition, 2006-06.

[13] IEC-62351, *Power systems management and associated information exchange - data and communication security*, International Electro-technical Commission, `http://www.iec.ch`, accessed on October, 2012.

[14] EPRI, *DNP security development, evaluation and testing project opportunity*, Electric Power Research Institute, `https://www.controlsystemsroadmap.net/ResourceCenter/2008RoadmapWorkshop/Presentations/06\%20DNP\%20Security\%20Development.pdf`, accessed on October, 2012.

[15] ISO New England, *DRI Project: DNP Secure Authentication*, `http://www.iso-ne.com/committees/comm_wkgrps/othr/dritwg/mtrls/iso-ne_dri_project_-_dnp_secure_authentication_recommendation.pdf`, accessed on October, 2012.

[16] NISTIR 7628, *Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-Level requirements*, The smart grid interoperability panel – cyber security working group, August 2010.

[17] C. Alcaraz, and J. Lopez, *Analysis of requirements for Critical Control Systems*, International Journal of Critical Infrastructure Protection (IJCIP), Elsevier, ISSN: 1874-5482, 2012.

[18] M. Jain, A. Jain and M. Srinivas, *A web based expert system shell for fault diagnosis and control of power system equipment*, In Proceedings of International Conference on Condition Monitoring and Diagnosis (CMD'08), pp. 1310-1313, 2008.

[19] C. Alcaraz, I. Agudo, D. Nuñez, and J. Lopez, *Managing incidents in smart grids à la cloud*, In Proceedings of IEEE CloudCom 2011, pp. 527-531, 2011.

[20] H. Ghani, A. Khelil, N. Suri, G. Csertan, L. Gonczy, G. Urbanics, and J. Clarke, *Assessing the security of internet-connected critical infrastructures*, Security and Communication Networks, in press, ISSN: 1939-0122, 2012.

[21] Exemys, *SCADA WEB, embedded web server*, `http://www.exemys.com.ar/beta/english/news/campanias/WEB_SCADA/index.html`, accessed on October, 2012.

[22] ICS-CERT, *ICS-CERT incident response summary report*, pp. 1-17, 2001-2009, `http://www.us-cert.gov`, accessed on October, 2012

[23] B. Miller, B. Young, *A survey of SCADA and critical infrastructure incidents*, Conference on Information Technology Education (SIGITE/RIIT), pp. 1-6, Canada , October, 2012.

[24] B. Zhu, A. Joseph, and S. Sastry, *A taxonomy of cyber attacks on SCADA Systems*, In Proceedings of The 2011 IEEE International Conference on Internet of Things (iThings'11), pp. 380-388, 2011.

[25] D. Hadziosmanovic, D. Bolzoni, and P. Hartel, *A log mining approach for process monitoring in SCADA*, International Journal of Information Security (IJIS), Springer Berlin/Heidelberg, vol. 11, no. 4, pp. 231-251, ISSN: 1615-5262, 2012.

[26] M. Qureshi, A. Raza, D. Kumar, S.-S. Kim, U.-S. Song, M.-W. Park, H.-S. Jang, H.-S. Yang, and B.-S. Park, *A survey of communication network paradigms for substation automation*, In Proceedings of IEEE International Symposium on Power Line Communications and Its Applications (ISPLC 2008), pp. 310-315, 2008.

[27] A. Das, *A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks*, International Journal of Information Security (IJIS), Springer Berlin/Heidelberg, vol. 11, no. 3, pp. 189-211, ISSN: 1615-5262, 2012.

[28] IEEE Standard, 802.15.4-2006. *Wireless medium access control and physical layer specifications for low-rate wireless personal area networks.* ISBN 0-7381-4997-7, 2006.

[29] C. Alcaraz and J. Lopez, *A security analysis for wireless sensor mesh networks in highly critical systems*, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 40, no. 4, pp. 419-428, ISSN: 1094-6977, 2010.

[30] S. Petersen, *WirelessHART Versus ISA100.11a: the format war hits the factory floor*, IEEE Industrial Electronics Magazine, vol. 5, no. 4, pp. 23-34, ISSN: 1932-4529, 2011.

[31] R. Roman and J. Lopez, *Integrating wireless sensor networks and the Internet: a security analysis*, Internet Research, vol. 19, no. 2, pp. 246-259, ISSN: 1066-2243, 2009.

[32] D. Christin, A. Reinhardt, P.S. Mogre and R. Steinmetz, *Wireless sensor networks and the Internet of things: selected challenges*, Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze, 2009.

[33] G. Montenegro, N. Kushalnagar, J. Hui and D. Culler. *RFC 4944: transmission of IPv6 packets over IEEE 802.15.4 networks*, Request for Comments, September 2007.

[34] S. Raza, S. Duquennoy, J. Hoglund, U. Roedig, and T. Voigt, *Secure communication for the Internet of things - a comparison of link-layer security and IPsec for 6LoWPAN*, Journal of Security and Communication Networks, in press, ISSN: 1939-0122, 2012.

[35] N. Kushalnagar, G. Montenegro and C. Schumacher, *RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*, Request for Comments, August 2007.

[36] Z. Wei, and C. Meinel, *Implement role based access control with attribute certificates*, In Proceedings of the 6th International Conference on Advanced Communication Technology (ICACT'04), pp. 536-540, 2004.

[37] T. Bhattasali, and R. Chaki, *A survey of recent intrusion detection systems for wireless sensor network*, In Proceedings of the 4th International Conference on Network Security and Applications (CNSA-2011), pp. 268-280, 2011.

[38] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, *Trust management systems for wireless sensor networks: best practices*, Computer Communications, vol. 33, no. 9, pp. 1086-1093, ISSN: 0140-3664, 2010.

[39] G. Privat, *From smart devices to ambient communication*, Workshop 'From RFID to the Internet of Things', Brussels, Belgium, `http://cordis.europa.eu/ist/audiovisual/neweve/e/conf6-70306/conf6-70306.htm`, accessed on October, 2012.