Enabling Secure Information Exchange from a Less Secure Zone to a Control System Zone in a Critical Infrastructure

Pascal Sitbon, Arnaud Tarrago, Pierre Nguyen
Electricité de France
Paris France
{pascal.sitbon, arnaud.tarrago, pierre.nguyen}@edf.fr

Abstract: Critical industrial infrastructures face two contradictory requirements. On one hand, operators are responsible and sometimes liable for their security. The cyber-security requirements and regulatory context lead the operators to define strict security levels and ensure information system segmentation. On the other hand, operators need more information exchange in order to be able to take advantage of the sophistication of new digital systems thereby improving the overall safety and performance of the industrial process.

The solutions available today don't meet these needs in a convenient way. Electricité de France (EDF) R&D work on a new kind of security device called "DESIIR", designed to overcome this dilemma and favourably exchange information in a more secure way with built-in defence-in-depth. This innovative device makes it possible to transfer data from a lower security level, e.g. corporate network, to a higher security level, e.g. SCADA network, while remaining compliant with an operator's highest security policy level. This paper discusses the security principles, presents the prototype, and proposes use cases showing what could be the benefits of the solution provided by DESIIR.

Keywords: DESIIR, DMZ, One-way Data Diode, Security Zones

1 Introduction

The features and performance brought by network interconnections in information systems are vital for many businesses. These interconnections allow better use of many digital systems in order to improve quality and operation.

However, in some cases, in particular for critical infrastructure such as power utilities, operators are responsible and sometimes liable for their level of computer security. Many regulations try to strengthen the cyber-security requirements for critical industrial infrastructures, leading to information system segmentation. The need for information exchange between different zones, each dealing with a particular function such as safety, operation, or supervision and having a different security level, is therefore complicated if not forbidden by the operator's security policy and best practices. In particular, transfer of information from a less secure zone to a higher one such as a control system zone is usually forbidden because there is no solution able to ensure a high security level.

Another constraint is that industrial sites have difficulties attracting workers skilled in computing network and security skills for many reasons. Architectures that need these skills for administration or supervision are therefore unusable in the field. Simple solutions addressing the requirements of industrial sites are therefore needed. These needs fall roughly into two categories:

- Need 1 – publish information from a control system zone to a less secure zone protecting against flow of information in the opposite direction
- Need 2 – transfer information from a less secure zone to a control system zone, with constraints on the data transferred, such as expected structured data with a validated format

If there are some well known solutions for the first need, there are no solutions on the market addressing the second need. In this paper, we describe a new type of device designed to address the second need, and also improve the solution for the first need. More formally, we defined three main requirements for such a device in Table 1.

Requirement	Description
R1	Need for high security level
R1a	Ensure that the security level is assured even in case of software flaw or configuration error
R1b	Protect the more sensitive zone from content attacks. In particular, malformed files, automatic execution and viruses must at least be sanitized so they become innocuous.
R2	Ensure reliable data transfer. The sender should be able to know if the transfer is successful.
R3	Regular application interactions must be usable
R3a	Must work on different operating systems without impact and preferably be interoperable without any specific software installation on both sides
R3b	Basic knowledge should be sufficient to install and use (plug & play). No administration skills should be required.

Table 1 – Security Requirements for Information Exchange Between Zones

2 Analysis of Current Solutions

According to the requirements in Table 1, we can state the main features that a solution should ensure:

1. "physical isolation", no end-to-end network flow
2. validation of the data format, content, length before data transfer
3. defense-in-depth
4. ease of use

5. possibility to acknowledge the transfer of information
6. ease of installation, no/minimum supervision

There are already some solutions available today that can address Need 1, even if not necessary optimally, see Table 2 for an overview of these solutions.

Solution	Advantages	Disadvantages	Requirements		
			R1 – Security	R2 – Reliability	R3 – Usability
Classical DMZ architecture	Proven and widespread architecture	Security level insufficient for industrial needs	No	Yes	Partial
Data diode	High security (physical one-way)	No acknowledgement of transfers	Yes	No	Partial
Removable media	No physical connectivity	Difficult to use on field, exposed to malware content	Partial	Partial	No

Table 2 – Available Solutions for Need 1: Publish Information from ICS

Even if there is a lack of reliability, the data diode appears to be a suitable solution for industrial needs, ensuring the high security level and still being usable in the field. We will see later in the paper how we can improve on this solution.

For the need 2 "transfer information from a less secure zone to a control system zone", the available solutions are presented in Table 3.

Solutions	Advantages	Disadvantages	Requirements		
			R1 – Security	R2 – Reliability	R3 – Usability
Classical DMZ architecture	Proven and spread architecture	Security level insufficient for industrial needs	No	Yes	Partial
Data diode	N/A				
Removable media	No physical connectivity	Difficult to use in the field, exposed to malware content	Partial	Partial	No
Paper transfer	No physical connectivity, no digital data (no malware)	Difficult to use in the field, not reliable (input & transcription errors)	Yes	No	No

Table 3 - Available Solutions for Need 2: Transfer Information to ICS

Usually security is provided by devices with security mechanisms implemented in software, like segmentation tools such as stateful firewalls, proxies, and switches. Vulnerabilities have been found in these devices [1][2][3], due to their programmable nature, leading to the network they were supposed to protect being compromised. These software vulnerabilities can also be found in inspection mechanisms, for example in layer-7 protocol inspection through the use of external libraries such as XML or ASN.1, [4][5]. Moreover, a poor configuration can lead to total exposure of the network. Thus, these tools must be configured and supervised with extra care, and need to be audited on a regular basis.

Some solutions exist and address this security issue but are not sufficiently usable and reliable in an industrial context. As shown in Table 3 and Figure 1, a data diode is not a solution suitable for data transfer from a lower security zone to a control system zone because it doesn't protect the control system zone from threats on integrity and availability. Moreover, a data diode works using specific software or hardware on both sides, and, by definition a data diode is not able to acknowledge the transfer of information.

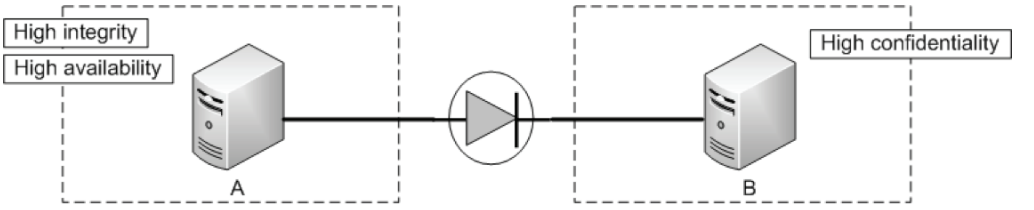

Figure 1 - Data Diode and Security Services, Flow of Information A -> B

The last 2 solutions described in Table 3 are based on physical separation. The solution using removable media seems to be a suitable solution at first glance, but in fact it doesn't meet the industrial needs and brings new risks. Indeed, this solution is usually implemented using a removable storage device such as a USB key, which can be used to propagate viruses and malware. Indeed, this solution, which appears to have been chosen in some critical infrastructures, could lead to their control systems being compromised. It is widely assumed that such removable media is responsible for the infection on control systems in the French Navy [6], UK Ministry of Defence [7] and a hospital in the city of Sheffield (UK) [8].

3 DESIIR: Concepts and Security Mechanisms

As we have seen, there is no existing solution for transferring data from a lower security zone to a control system zone and answering the requirements posited in this paper. The authors propose a new solution based on the work at EDF R&D, named "DESIIR".

3.1 Concept

DESIIR is a device connected to two hosts, each through a dedicated physical port (USB, Firewire, S-ATA, etc.) enabling the transfer of information without a network connection. The security is based on the nature of the device and not only on the implementation or the configuration. Conceptually it behaves like a double door system without direct interaction between the two hosts, and even without the two hosts being aware of the existence of the other host. As shown in Figure 2, each host is acting like there was an external storage disk drive directly connected through a USB port. In fact the real storage is inside the DESIIR device itself.

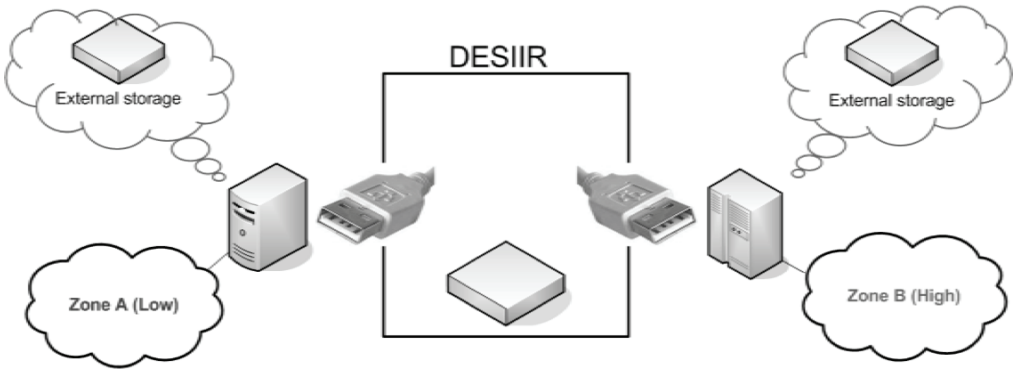

Figure 2 – General Concept of DESIIR

DESIIR has been designed to overcome the situation described in Section 1, meeting both "more secure" and "more information exchange" requirements, making it possible to transfer data from a lower security level (Zone A on Figure 2) to a higher security level like a control systems zone (Zone B).

In Figure 3, we see the principle of operation of DESIIR. The host in Zone A is able to transfer information to DESIIR. This information, if compliant with predefined rules contained inside DESIIR, is then available for access from Zone B. Thus, we ensure that non-compliant information will not be passed to the other side.

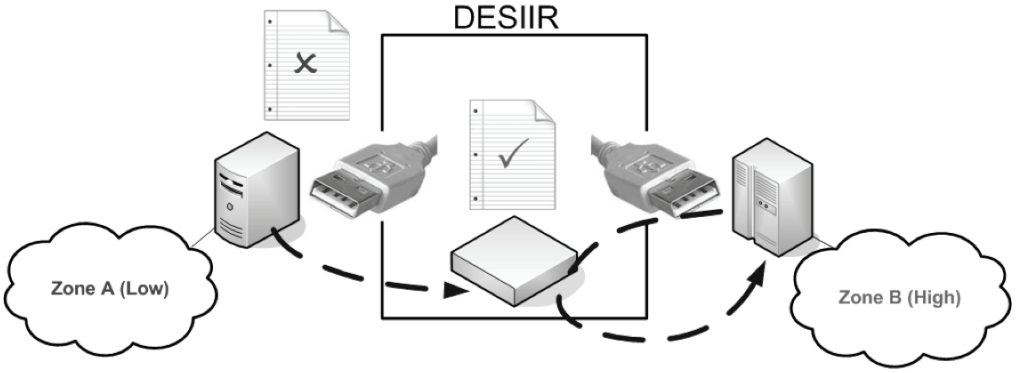

Figure 3 – Principle of Operation of DESIIR

3.2 Internal View and Security Considerations

In this section, we present the main mechanisms implemented in the DESIIR device. This paper is not intended to be exhaustive about what has been implemented but rather what can be done.

The internal architecture of DESIIR is designed as defense-in-depth with redundant access controls, various implementations of filters on different electronic components. Each component is not aware of the existence of the other components and doesn't trust them.

In the Figure 4, we see the main components of DESIIR. The component $C1_A$ (resp. $C1_B$) is in direct interaction with the host of zone A (resp. B). The component C2 is a central component which, among other responsibilities, manages the internal storage C3. C1 and C2 are implemented using microcontrollers or FPGA's while C3 is a regular storage resource.

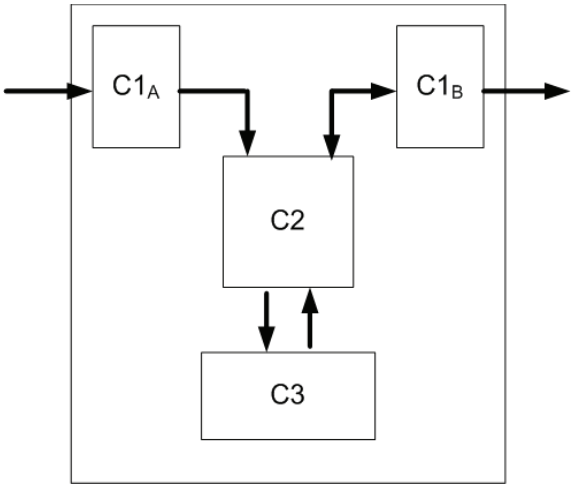

Figure 4 – View of Internal Components of DESIIR

3.2.1 Physical Segregation, No End-to-End Flow of Information

DESIIR is acting like a proxy, using different protocols. The device is seen from the hosts as an external storage unit and behaves like that. Information is transferred through USB/SCSI to and from DESIIR. This mode of operation avoids the need to install specific software on the hosts, and is independent of the operating systems, as long as they support USB/SCSI mass storage devices.

The internal storage unit (C3, Figure 4) is mandatory and ensures that no information is exchanged directly end-to-end. Each host is not aware of the existence of the other host. Thus, DESIIR is acting similarly to an application proxy. This is also true for the internal design of the device, where each component is not aware of the existence of the others. This is done by simulating a memory bus at each interface between components.

This also ensures that hosts connected to DESIIR must actively request information stored by DESIIR, knowing exactly what file they are looking for.

Each host is still in control of its security, independent from the security brought by the DESIIR device itself, and should implement further security mechanisms such as filtering the content and verifying the consistency of the data.

3.2.2 Redundant Security Controls, Based on Various Implementations

We have re-implemented every component, and for each component, only the necessary functions have been implemented. Most of the components are not re-programmable, making it impossible to modify the components behavior after the fact. In our implementation, the components C1 are performing a first level of filtering, rejecting every character which is not ASCII (0 – 127). As the components C1 do not understand the file structure, they are not exposed to attacks trying to take advantage of the file

structure or content. The component C2 is performing smarter filtering, based on meta-data of the files (file name including extension, file size) and on the content (length of the lines, authorized grammar).

3.2.3 Restrict the Operations Available on Each Component

Each component only possesses the operations that are necessary. For example, if the host in Zone B is not permitted to write a file, the component C1B will not have the corresponding "write" function. Thus, if requested to write a file it is incapable of doing so by its nature as it doesn't know what "write" means, and there is no corresponding instructions implementing the "write" function.

3.2.4 Content Filtering

Content filtering ensure that the files are consistent and data is safe, and sanitized if necessary. In particular, executable files cannot be transferred through the DESIIR device. For example each character might be filtered to ensure there are no unwanted characters (e.g. outside of [0, 127] ASCII), but equally to ensure that the file respects a certain "grammar".

3.2.5 Virtualization

The resources are shown to he hosts only after validation. This is a sort of virtualization, the visible resources shown being different to the real resources on the C3 internal storage unit.

3.2.6 Summary of the Security Mechanisms

The DESIIR device comes with defense-in-depth built-in. In accordance with the best practices, the security of DESIIR depends on the conception and the implementation of the device and not on keeping the internal architecture secret. Even with all the details of the internal components, it should not be possible to break through the device that is to attack the zone B from the zone A.

If the internal storage unit inside DESIIR is full, there is no further data transfer possible, but the zone B is not impacted in any way. Its integrity, confidentiality, and availability are ensured.

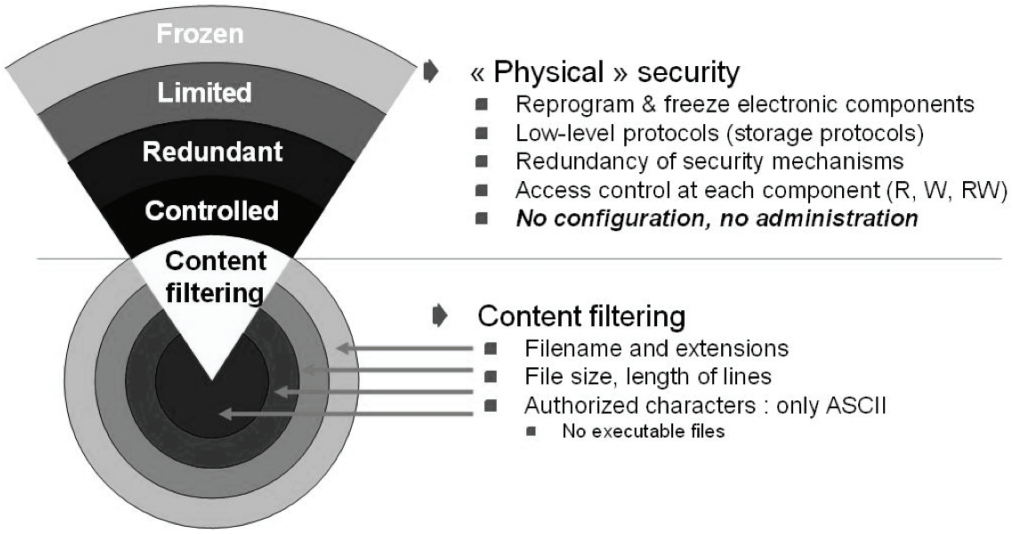

Figure 5 – Summary of Security Mechanisms Implemented by DESIIR Device

4 DESIIR Security Compared to DMZ Architectures

DESIIR could be integrated in complex and existing architectures. It is designed to go beyond the best practices in security already used in classical DMZ architectures in order to be able to provide services for critical information systems like industrial control systems and SCADA.

4.1 Best Practices in Classical DMZ Architectures

A DMZ architecture should be able to protect information systems while at the same time providing the necessary information exchange with the outside world. Best practices used in classical DMZ architectures are explained in the following paragraphs, some being directly based on the defense-in-depth principle.

4.1.1 Limited Access to IT Rooms

The different devices and equipments must be kept in a secure IT room with limited access. Racks must be locked for the most sensitive equipments. Following this practice, DESIIR considers its environment as physically secure.

4.1.2 Use Two Different Security Devices, At Least

It is recommended to use at least two different security devices based on different technological designs in order to limit the risk of a single vulnerability being able to impact the overall architecture. DESIIR implements this recommendation.

4.1.3 No Direct Access on Security Devices

It is recommended that the security devices should not be directly visible from the Internet in order to make the exploitation of a vulnerability more complex. DESIIR implements this recommendation; in particular the internal file system and configuration parameters are not accessible from outside.

4.1.4 Application Proxies

It is recommended to use application proxies which are able to hide the internal network and control the information flow in an application specific way. DESIIR implements this recommendation; in particular the internal storage unit acts as a proxy.

4.1.5 Hosting Based on Levels with Inter-layer Filtering

Typical system architectures are based on different layers, for example multi-tier architectures (presentation, logic and data). Each layer performs specific information flow filtering. DESIIR implements this recommendation with different electronic components and different implementations.

4.1.6 Hosting Zone Segregation

Hosting zones are usually segregated from one and other in order that the compromise of a zone doesn't weaken the overall architecture. DESIIR implements this recommendation, each component not being aware of the existence of the others.

4.1.7 Routing Barrier

This important recommendation ensures that the routes to the internal networks are not known from the Internet but only by some specific components in the architecture. If there is no known route, the information flow cannot access sensitive components. DESIIR, by design, respects this practice.

4.2 Concepts of Security Improved by DESIIR

Many problems still remain with the classical DMZ architecture. In particular, configuration, administration and maintenance are of paramount importance. The major weaknesses found in security audits and testing come from inconsistent filters, poorly maintained administration rules, or poor administration.

DESIIR is designed with simplicity in mind and to make the lives of users easier, and at the same time offering a more secure interconnection.

4.2.1 Administration and Configuration Rules Non-modifiable

During the fabrication, the authors intentionally introduce a step where we freeze physically the main electronic components. It is not possible to modify the configuration parameters during the lifetime of the device. Administration, supervision and audit of configuration are therefore not necessary.

4.2.2 Administration skills

Classical DMZ architectures require the local administrator to be highly skilled due to the complexity of the security components that suppose a practical and everyday knowledge of the equipment and its configuration. Also, monitoring of the equipment must be permanent in order to react quickly if necessary. Such administration skills could exist only in a dedicated team.

DESIIR permits an owner/operator to do without such skills, thus being congruent with the fact that those skills are still rare on industrial sites.

4.2.3 Architecture Backup

The DESIIR device could be replace by another with the same configuration very easily. There is no need to backup configuration or time to restore it, relieving the burden of a complex and costly backup architecture.

4.2.4 Service Continuity

High availability could be ensured by using two DESIIR devices in parallel.

4.2.5 Versions, Operating Systems Hotfixes and Pre-production Architectures

As a general best practice, it is recommended to use the latest version of an operating system, drivers and software available. Also, new patches and hotfixes must be applied in the equipment as soon as possible. Of course, it is necessary to test patches and new versions beforehand on a pre-production architecture to ensure that it will not cause any problem when deployed. Usually this leads to complex procedures describing the steps that should be followed and also the steps in order to get back to the original situation if something goes wrong.

If an evolution is necessary with DESIIR, it can easily be done with replacing the device by another differently configured device. In case of problems with the newly installed device, a rollback is accomplished by simply replacing the new device with the old one.

4.2.6 Best Practices on Operating Systems

It is recommended to follow the best practices on operating system security for example from NIST SP800-123 on securing servers [9], e.g. only the necessary services should be installed and running on the equipments. DESIIR itself respects this recommendation. Also the security of the interconnection is not based on the security of the hosts (Zone A and Zone B).

4.2.7 Best Practices on Application Development

There are best practices for secure development and on application usage. For example, in UNIX systems, using chroot to isolate the execution environment of one application from another and being careful with SUID/SGID are part of those best practices [10].

Using DESIIR could avoid the need to follow these requirements. DESIIR can also be used along with proprietary industrial protocols inside each zone.

4.3 Supplementary Concepts of Security Brought by DESIIR

4.3.1 Protocol Segregation

This concept is quite simple: using the same protocol end-to-end weakens the chain, one end being able to directly attack the other. To avoid such a situation, it is recommended to use protocol segregation through proxies, gateways, multi-tier architectures, etc. Thus it is more complex to exploit a vulnerability in the first protocol and get through the other layers, as shown in Figure 6 [11].

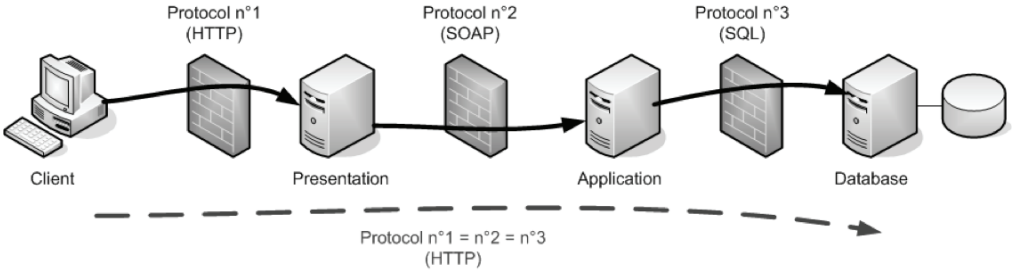

Figure 6 – Multi-tier Architecture and Protocol Segregation Concept

DESIIR doesn't use network protocols. There is a segregation between the different protocols used outside and inside DESIIR. The protocols used inside DESIIR itself are memory read or write functions on storage devices like SCSI or flash memory

4.3.2 Non-implementation

Most of security devices forbid some actions based on a feature or a configuration. DESIIR has been design to perform specific operations, thus it can implement only the needed functions. For example, the code handling the "write" function will not be implemented if there is no need. Thus, this function will not be accessible, independently of the level of security of the architecture or the device itself.

5 Ensuring the Level of Security of the Device

Of course the level of security of a device cannot be achieved by decree. That is the reason why we have started an evaluation process to ensure it in real world conditions combining internal EDF reviews and external evaluations.

The objective is to provide the closest possible security to an air gap with no interconnection adding some filtering features. The most crucial part is that it should not be possible to take control from one side to the other side through the device.

The DESIIR device is currently under evaluation by an independent body, potentially leading to an official certification by the French National Government, called CSPN [12] (First-Level Security Certification), an alternative to Common Criteria. This evaluation is currently under way at the time this paper was written.

6 Use Cases

6.1 Use Case 1: Sensor Network

The first use case involves the transfer of information processed by sensors. In an industrial context, sensors often reside in zones that are physically less secure than an operation centre or that use wireless communications. Thus, using direct information transfer could expose the supervisory network to the risks of intrusion.

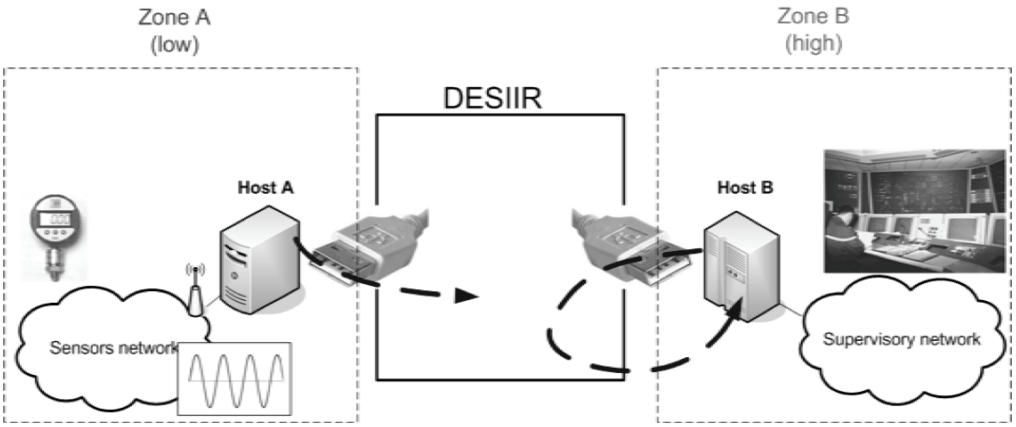

Figure 7 – Transferring Data from Sensor Network to Supervisory Network

Using a DESIIR device advantageously as shown in Figure 7 could allow an owner/operator to get input from sensors, even wireless sensors, without bringing unacceptable risks to the supervisory network.

6.2 Use Case 2: Combined Use with Data Diode

When dealing with high volumes of data, we can combine the use of a one-way diode for throughput and security, and DESIIR for acknowledge that the data was received.

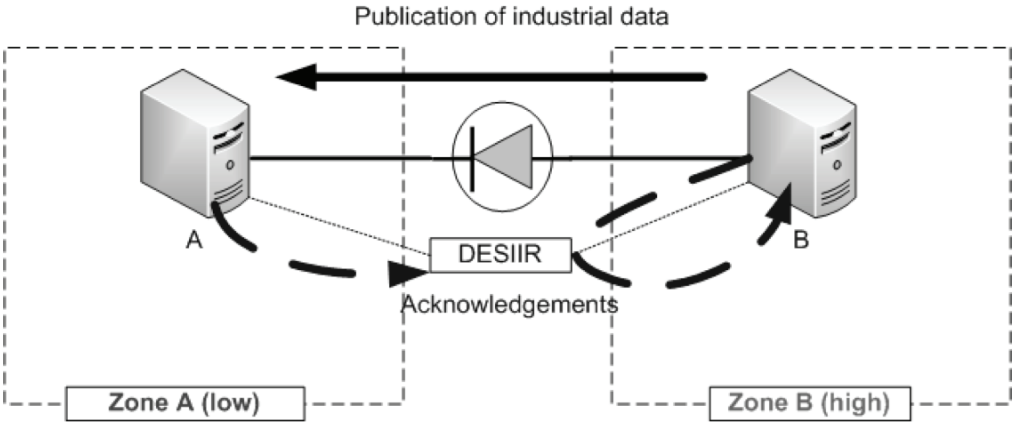

Figure 8 – Combined Use with Data Diode

In the Figure 8, the DESIIR device is used only to transfer the acknowledgments from Zone A (typically the corporate network) to Zone B (typically the industrial control systems zone).

Figure 9 – The DESIIR Device

7 Conclusion and Perspectives

In this paper, we have described a new approach to overcome the collision of two trends: the need to increase the security level of the critical infrastructure while at the same time being able to take advantage of available data for a better operation of industrial process.

We have developed our approach and built a prototype, which is the first generation of a new class of security devices. In order to have an independent measure of the level of security of the work, this device is currently being examined for certification by the French Government.

This device is answering real concerns of industrial control systems, and the paper discussed some use cases in which the added value is significant, allowing interconnections that are impossible with current critical infrastructure security policies. This of course leads to a new kind of perspective of use for industrial context.

About the Author – Pascal Sitbon, CISSP, ISO27001 Lead Auditor, graduated from ENSIMAG Engineering School in 1997 with an MS in Computer Science. Joining EDF in 1998, he has specialized in IT security since 2001. His main interests are IT security, including technical, organizational as well as managerial themes. He is currently working at EDF R&D as a cybersecurity expert, research engineer, and project manager on EDF Industrial Control Systems Security issues. He takes part in different working groups at International, European or National level (IEC TC57, EuroSCSIE, etc.).

Arnaud Tarrago, graduated from LIP6 (University Pierre et Marie Curie Paris VI) in 1995, Arnaud is a research engineer in security of information systems at EDF R&D since 1995. Project leader of Security Studies of the information system of EDF, he has worked since 2003 in the areas of security for the industrial and science computing of EDF.

Pierre Nguyen graduated in Advanced Systems from Ecole Centrale Paris, France. After a year in CEA (Atomic Energy Commission), he joined EDF Research & Development in 2001 as a Wireless Communications Expert and since then, he was involved in evangelizing these emerging technologies and worked on several projects in Production, Distribution or Commercialization area : remote control solutions, smart metering, smart home automation… In 2008, he took the leadership of a project called SESAME whose goal is to deploy wireless networks in nuclear power plants for new mobility applications.

References:

[1] A Stateful Inspection of FireWall-1 , Thomas Lopatic, John McDonald TÜV data protect GmbH, http://www.monkey.org/~dugsong/talks/blackhat.pdf

[2] Anatomy of an IP Fragmentation Vulnerability in Linux IPChains: Investigating Common Vulnerabilities and Exposures (CVE) Candidate Vulnerability CAN-1999-1018, http://www.sans.org/reading_room/whitepapers/threats/anatomy_of_an_ip_fragmentation_vulnerability_in_linux_ipchains_investigating_common_vulnerabilities_and_exposures_cve_candidate_vulnerability_can1_1110

[3] VLAN Security White Paper by CISCO, http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

[4] Researchers find large-scale XML library flaws, http://www.securecomputing.net.au/News/152193,researchers-find-largescale-xml-library-flaws.aspx

[5] Microsoft Windows ASN.1 Library Integer Overflow Vulnerabilities, http://secunia.com/advisories/10759

[6] French fighter planes grounded by computer virus, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/, French-fighter-planes-grounded-by-computer-virus.html

[7] MoD networks still malware-plagued after two weeks, http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/

[8] Conficker seizes city's hospital network, http://www.theregister.co.uk/2009/01/20/sheffield_conficker/

[9] NIST SP800-123 Guide to General Server Security, http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

[10] Best Practices for UNIX chroot() Operations, http://unixwiz.net/techtips/chroot-practices.html

[11] "Deconstruction of Some Industrial Control Systems Cybersecurity Myths"; Piètre-Cambacédès L. & Sitbon P.; Sixth American Nuclear Society International Topic Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, Knoxville (USA), April 2009

[12] First Level Security Certification (Certification de Sécurité de Premier Niveau), French Network and Information Security Agency, in French, http://www.ssi.gouv.fr/site_article80.html