DECONSTRUCTION OF SOME INDUSTRIAL CONTROL SYSTEMS
CYBERSECURITY MYTHS

Ludovic Piêtre-Cambacédès and Pascal Sitbon
Electricité de France R&D
1 Avenue du Général de Gaulle, 92141 Clamart, France
ludovic.pietre-cambacedes@edf.fr; pascal.sitbon@edf.fr

ABSTRACT

This paper presents a selection of technical issues to address to secure sensitive control systems. The selected issues were chosen because they all suffer from misconceptions and a mythology that needs to be rationalized. The paper first presents and deconstructs a selection of these modern myths. A particular stress is placed on the over-estimated “magical powers” of firewalls, and the belief that proprietary systems are “closed thus invincible” sometimes found in our industrial environments. Technical considerations and solutions are then given to face the reality. The use of firewalls, physical data-diodes and intrusion detection for industrial control systems are discussed.

Key Words: security, firewall, intrusions, data-diodes, IDS (Intrusion Detection System).

1 INTRODUCTION

Industrial Control Systems (ICS) is a generic term covering a wide range of components, systems and architectures [1]: from SCADA (Supervisory, Control and Data Acquisition) systems to DCS (Distributed Control Systems), from digital instrumentation to supervision systems in control rooms, from PLCs (Programmable Logical Controllers) to data historians and engineering stations. All of these are used to supervise and control industrial processes in a broad range of sectors such as energy, transportation, manufacturing, water, oil or chemical, including of course the nuclear industry. ICS are evolving tremendously: from closed and proprietary technologies, they’re now getting more and more interconnected; they use or integrate with regular IT technologies, and regularly add new functionalities and possibilities to the asset owners. In the meantime, the threat and risk landscape is evolving at the same pace, turning ICS cybersecurity into a permanent and high priority challenge. In this daunting task, awareness-raising and training are essential components to cope with the incredibly fast evolutions just mentioned; in particular, some cultural and historical beliefs, which are a legacy from past situations where ICS were not as exposed and vulnerable as today, can make the job even harder.

This paper deals with a selection of technical aspects that suffer from this persistent mythology. In section 2, some of these modern myths are recalled and deconstructed. After a quick review, a particular stress is put on two of them: the over-estimated “magical powers” of firewalls, and the belief that proprietary systems are “closed thus invincible”. In section 3, related technical considerations and defensive solutions are discussed, especially concerning firewalls, physical data-diodes and intrusion detection for industrial control systems.
2 BREAKING SOME MYTHS

2.1 Some cybersecurity myths are already fading…hopefully

Some cybersecurity myths that used to contribute to an inappropriate security posture in the industrial control systems community have started to fade away. Recent facts and awareness efforts have lead to real progress on different issues, making cases like complete risk denial or blind trust on technologies less common. Below, a selection of such issues is given. Some associated facts and arguments that have contributed to weaken them are also recalled; they may still prove useful as such beliefs are still alive and should be rationalized as often as possible.

2.1.1 “Nobody wants to attack me/is interested”

Public opinion has not been aware of ICS cybersecurity risks for years. The first widely commented attack was probably the Vitek Boden’s case, in Australia, sentenced to 2 years of prison for having attacked the Maroochy Shire water sewerage SCADA system [2,3]. Mr. Boden, formerly employed as a contractor for two years as the site supervisor, attacked on several occasions the system after resignation when his job application to the area’s Council was refused. It led to 800,000 liters of raw sewage being spilled into the environment. Having internal and technological knowledge, he managed to disable alarms and interfere with wireless communications between the pumping and central stations (Ref. [4,5] give a complete analysis of the attack). Although over-commented, this event has nevertheless contributed to raising the awareness of possible real-world consequences of ICS failures. Another recent case that stresses the real-world consequences concerns the DHS Aurora experiment, conducted at the Idaho National Lab (INL). Commented by CNN in 2007 [6], a prototyped cyberattack led to the destruction of a diesel generator, formerly used to supply power to the 13.8 kV distribution grid of the INL test-bed.

The observation that since 2002/03, presentations about ICS vulnerability are regularly found at open hackers events (see [7-10] for recent examples) shows the increase in interest on this issue. Of course, actual attackers’ skills and interests are several years ahead of the presented work in such events. In parallel, since 2006, a growing number of ICS software vulnerabilities has started to be officially published by national CERTs (Computer Emergency Response Teams). For example in the US by the US-CERT control system security program [11], giving official existence to preexisting weaknesses that have sometimes been present for years. Some of them have already been integrated in mainstream security tools like the Metasploit Framework [12,13]. Like in traditional IT Security, this constitutes only the tip of the vulnerabilities iceberg.

ICS vulnerabilities are known, easy-to-use tools are coming, but does anyone want actually to use them? In January 2008, a CIA senior analyst announced that several utility companies outside the United States had been hacked and subjected to extortion, leading in at least one case to a power outage that affected multiple cities [14]. In fact, even if public disclosure of actual attacks are still rare, a sufficient number of converging elements can be assembled to consider that ICS have become attractive targets for different kinds of attackers, from recreational hackers to political activists and criminal organizations. National and international organizations indeed consider computer security as criminal and terrorist threat vectors to critical infrastructures [15-17]. A close relationship between the national security agencies and the cybersecurity community in general are needed to stay up-to-date and prepared to face rationally those new risks.
2.1.2 “I’m not connected / My systems are isolated”

For a long time, industrial control systems used to live their own life with dedicated and isolated closed-loop infrastructures. Cyber-security could at least rely on physical isolation. For a vast and growing majority, these times are over. For many good reasons, from operation or maintenance improvement to cost-effectiveness, interconnection has turned into the general rule. This generic statement is of course true for nuclear facilities [18]. In fact, even the global electric system call for such connectivity: planning, market and dispatching entities need near real-time status information on every generation asset.

Such connectivity can of course take different forms and serve different objectives: from targeted remote-maintenance, historically based on unsecured dial-up modem connections [19], to specific gateways or DMZ connecting corporate networks with operation ones, allowing real-time monitoring and reporting from the desktop. Whatever the situation, the “no-connection” argument has to be systematically challenged. In particular, the connectivity may change depending on the operational phase of the considered facility. Of course, automatically spreading malware may be the first to discover unmanaged bridges to operational systems; famous examples like the Davis-Besse nuclear power plant infected by the Slammer work in 2003 [20] or the thirteen Daimler-Chrysler plants stopped by the Zotob worm in 2006 [21] are here to recall this fact, but they also may be silently used by attackers, actively looking for remote access that potentially circumvents the traditional security protections.

Finally, if network connectivity is an important vector for cyber attacks, non-networked data exchange constitutes also a major issue: in particular, USB sticks and other forms of removable media are ideal but often ignored vectors for malwares. Highly protected systems, or even supposedly completely isolated ones, may be exposed. In November 2008, the US DoD issued several internal directives ordering that flash media stopped being used [21]. The exact perimeter and reasons were at the time uncertain; it was allegedly related to a wide infection of critical classified systems by a malware [21]. A few months before, NASA had confirmed that laptops, with no critical role, carried on board of the International Space Station were infected by a computer virus [22]… Computers, even on military bases or in orbit, are in fact rarely isolated, and always vulnerable.

2.1.3 “The anti-virus and patching are not my problems”

The previous discussion has hopefully already presented some good reason to question such a statement. Often built on the previous myth, it also stems from the belief that ICS specific technologies are immune to viruses and other forms of common malwares. ICS are nowadays in fact based for a large part on the same technological blocks found in IT environments: Microsoft OS, market-dominant database servers and so on. Specificities may still exist of course, but are getting concentrated on sub-systems, on the PLC level and for highly targeted application (e.g. SIS). Almost all the biggest solution providers such as Emerson, Alstom, GE or ABB now have Microsoft-based control system offers. As a matter of consequence, anti-virus software and the application of security patches should be put in place, even if specific procedures are of course to be observed [23,1].

2.1.4 “I use a firewall, my systems are automatically protected”

Firewalls are among the most known and deployed security technologies. They are also complex devices that have to be correctly configured and integrated in a specifically designed
architecture and organization to turn their filtering capabilities into efficient security barrier. It may sound obvious, but “having a firewall in place” is definitely not enough to ensure proper segmentation between two networks. Configuration and maintenance are of course fundamental, they may have specificities for ICS environments [24]. But even configured and maintained, there are things that a firewall will never be able to do: they can’t protect against insiders, they don’t protect against connections that don’t go through them (e.g. dial-up modems), they don’t protect against malwares, and once again, they don’t set-up themselves magically. Nothing is more dangerous than ignoring these basic facts, as a firewall may create a simple illusion of security. It has in any case to be included in a multi-layer approach to security, combining other technical, but also organizational and operational controls. Numerous references are helpful in this perspective (cf. for example [15,1,25,26]).

2.2 Focus on two myths still to deconstruct

In this part, two “myths” are examined more closely than the ones discussed in §2.1, as they appear, at least in the authors’ perception, even more commonly encountered. The objective is to contribute in creating the right conditions to establish a balanced cybersecurity posture.

2.2.1 “I only have obscure protocols/systems in there, it’s secure”

This avatar of the recurrent paradigm “Security by obscurity” is still encountered frequently among the industrial control system community [27], and deserves more effort to raise awareness. In fact, each part of the statement is questionable. To start with, as already stated, COTS and IT technologies are finding their way into industrial environments more than is commonly thought. Of course, there is still room for very specific or proprietary technologies in our environments; however it does not bring any guarantee about their intrinsic security. Several reasons and simple facts can be given to support this.

First of all, reverse-engineering of industrial protocols is usually not difficult: typical field equipments are simple machines, with targeted functions, and the communication protocols with such devices are typically also simple. Some computer skills and patience are the only ingredients needed to reverse-engineer, at least partially, most of the closed industrial protocols that don’t have specific security features [28], which constitutes a large majority. In certain cases, reverse-engineering is even not necessary: the protocols in use may be very domain-specific, it does not mean that they are necessary closed and proprietary: typical industrial protocols like Modbus, DNP3, ICCP/TASE.2 or IEC 60870-5 Part-104, just to give a few examples, are extensively documented, with publically available specifications. In any case, a wider look at the history of communication security gives very little credit to secret design when it comes to ensuring security. Cryptography or DRM systems history provides numerous examples: from GSM phones encryption [29] to RFID systems, like Speedpass [30] or Keeloq [31] used for toll payment and car ignition, or DVD anti-copy protection [32], they all had a secret design specifications, they have all been reversed-engineered and broken whereas functionally equivalent open technologies would have been much more robust. More than one century ago, in 1883, Kerckhoffs had already stated in its security design principles for military ciphers that they should not be required to be secret and shall be able to fall into the hands of the enemy [33]… Of course, the idea is not to apply such a principle to all security-related information, it is only that security cannot be built on the fact that a given design is closed and proprietary. Conversely,
open and standard design is of course not sufficient. Several references give good insights on the open vs. close designs for security (e.g. \[34,35\]).

Beyond this discussion, even if we assume that some closed protocols are indeed hard to reverse-engineer, it’s not sufficient to protect the nodes from attacks: precise knowledge of communication protocols is not required for an attacker to saturate the media used by such protocols, from the moment he could gain access to one node of the network and that the physical and logical layers do not embed adapted counter-measures. Denial of service is often an easy card for an attacker to play, the Browns Ferry Incident should be taken as a warning \[36\].

2.2.2 “My firewall is configured as a logical diode, I’m 100% protected”

Many misconceptions are associated with firewalls; some of them have already been discussed previously in this paper, but a particular one deserves more efforts to be tackled: “the diode syndrome”. In fact, specifically critical ICS (e.g., for safety instrument systems) connection to other security domains are often accepted providing a “one-way communication”. Unfortunately, such a requirement is very imprecise and can be implemented with very different levels of security. Communication direction restrictions between two domains can broadly speaking be enforced in three ways:

(i) based on the initiative of the communications (channel establishment direction),
(ii) based on the content and useful payload “flow” (content direction), in addition to (i)
(iii) on a strict one-way communication basis, preventing even a single bit, including signalization, from going in the forbidden direction (bits direction).

The nature and strength of the protection provided by each of them differ to a great extent. Only the first, initiative-restricted policy can be enforced in a straightforward fashion with a regular firewall. The second one needs packet inspection intelligence while the third one can only be realized through specific techniques, out of reach for a firewall (cf. §3).

The security difference between (i) and (ii) is clear. In the first case, it’s possible to prevent a direct connection from an attacker towards the protected zone, but the attacker can still wait to piggyback on a legitimate communication to get across the barrier. The second case makes attacker’s life much harder, as it prevents him from introducing directly malicious content through regular mechanisms. Nevertheless, the difference between (ii) and (iii) may be less obvious, and (i) + (ii) is sometimes considered to be the maximum security policy. Even if it can indeed provide a high level of protection, network attacks are in fact still possible: control and signaling data are authorized to enter the protected zone, they are interpreted into it; this simple fact allows potential malicious code execution. This is the case for TCP connections in particular, TCP being a non one-way protocol by nature.

For example, Figure 1 represents a firewall controlling an outgoing FTP connection with content restrictions:

- only FTP “push” from the client to the server outside the protected zone is allowed,
- FTP is in passive mode, the data and control connections flow in the same direction
- inward TCP connections are not permitted.
FTP control data can still enter the zone, and will be interpreted by the client (Step 1 in Fig. 1). This could be enough to gain access to the client. In step 2, the malicious server crafts malicious control messages as a reply to the client to exploit a buffer-overflow vulnerability in the remote client. The policy is respected but the client is compromised. Of course, all of this requires the attacker to have knowledge of an exploitable vulnerability in the client software.

Previous work from the authors [37], on which is largely based §2.2.2 and §3.1 of the present paper, gives a detailed analysis of these aspects.

Finally, only strict one-way implementations should be called diodes and can pretend to the implied level of protection. All TCP-related or more broadly all protocols implying bi-directional signalization, including acknowledgements, cannot enforce strict one-way policy. Of course, non-connected/unidirectional protocols such as UDP filtered by a firewall could be considered as data diode. However, firewalls maybe vulnerable or misconfigured; in critical environments, the one-wayness may have to be ensured physically, by dedicated hardware called physical data diodes, presented in the following section.
3 SOME DEFENSIVE PERSPECTIVES

3.1 Physical data diodes

3.1.1 General and historical considerations on physical data diodes

Physical data diodes are currently gaining interest in the ICS security community for their integrity protection capabilities. However, they have been used by the military to protect classified environments for a long period of time (cf. [37] for history of the concept).

Grounded in this history, physical data diodes have first been used mainly for confidentiality protection, and are used for integrity protection in a sort of reversed way. In the first case, traditionally found in military and governmental environments, the diode ensures that data can only be sent from a network with a higher classification level to a lower one, whereas in the second case, more typical of control systems, the diode prevents data from being sent from a lower security zone to a higher security zone. In fact, physical data diodes can play a role in addressing each of the “CIA Triad” of information security:

- Confidentiality, preventing data to be sent from a system with a higher classification level to a system with a lower classification level. In figure 2, the system B is physically unable to spread out its own information.
- Integrity, preventing data to be sent from a less protected system to a more protected system. In figure 2, the data in system A cannot be infected or polluted by information coming from system B.
- Availability, preventing flooding and other denial of service events, malicious or not. In figure 2, the system A can’t be disturbed by system B.

![Figure 2 – Physical data diode and CIA Triad](image)

3.1.2 Technical approaches

- RS232: Customized RS232 serial links have been used over the years to implement physical diodes in a simple fashion, despite their limited bandwidth. Report [16] presents details of several alternatives that can be used to realize such data diodes, explaining cabling and necessary modifications.
- AUI Ethernet: Another approach to implementing strict one-way communications on a physical basis is to modify a point-to-point Ethernet link at the physical layer. The deprecated AUI standard provides a very simple way to realize such a diode by modifying pins.
• Optical Fiber: The most common design relies on Ethernet optical fiber-based standard connectivity. A simple design involves two dedicated transceivers connected as in Figure 3.

![Diagram of optical fiber connection](image)

**Figure 3 – A classical optical diode design [37]**

On Figure 3, the receive interface (RX) of the controller attached to system A is not connected (the C device is only used because the optical controller need to see an “up” link but it is a dead end), while the transmit interface (TX) of the system B’s controller is not connected. Thus, system B is physically unable to transmit information to system A while system A can.

3.1.3 Solutions and functionalities

Several providers propose solutions based on optical fiber point-to-point links, such as the link described earlier. Table 1 gives a non-exhaustive overview of some commercially-available solutions. Most of them implement file transfer, email transfer, and raw data forwarding.

**Table I. Physical Data Diode commercial solutions**

<table>
<thead>
<tr>
<th>Provider (country)</th>
<th>Core Product</th>
<th>Some characteristics &amp; functions</th>
<th>Certification</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owl (USA) [38,39]</td>
<td>Data Diode Network Interface Cards (DDNIC)</td>
<td>55, 155 MB/s or 2.5 Gb/s (ATM)</td>
<td>Common Criteria EAL4</td>
<td>Based on modified ATM, not Ethernet (from Sandia Labs) Claimed as widely deployed (&gt;650) in US agencies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File Transfer, raw UDP forwarding, multiplexing, TCP handling (proxy).</td>
<td>“Approved-to-Operate” in the US DoD and Intelligence community</td>
<td></td>
</tr>
<tr>
<td>Tenix (Australia) [40,41]</td>
<td>Interactive Link Data Diode (IL-DD)</td>
<td>1Gb/s or 100Mb/s</td>
<td>ITSEC E6</td>
<td>From the DSTO Starlight products (&gt; 5000 units), widely deployed in Australian gov.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File Transfer, raw UDP forwarding, SMTP, keyboard switches</td>
<td>Common Criteria EAL7+</td>
<td></td>
</tr>
<tr>
<td>Thales (France) [42]</td>
<td>ELIPS-SD</td>
<td>100 Mb/s (20 Mb/s user throughput)</td>
<td>Secret-Défense approval for use in French Defense/State environments.</td>
<td>Claimed as widely used in French military environments.</td>
</tr>
</tbody>
</table>
### 3.1.4 Specific reliability issues

As physical data diodes prevent the use of acknowledgements and other connection-oriented mechanisms, the question of transfer reliability naturally arises. First of all, physical data diode solutions use one-way protocols in ideal conditions: dedicated point-to-point link, no collisions, no or limited interferences. Therefore, non-connection-oriented protocol like UDP can be quite reliable [49]. Nevertheless, other aspects have to be considered: for instance, the receiving and the transmitting processes have to be managed specifically because of the feedback of information from the receiver to the emitter is impossible. There is no obvious solution for the emitting process to be sure that the receiving side is ready to handle the transmitted data: the buffers or CPU may be overloaded, the receiving side may simply not run fast enough to treat the flow. To avoid such situations, the network buffer sizes and the priority of the treatment process must be specifically dimensioned on the receiving side. The sender might also adjust the delay between packets to allow for the constraints in the receiver. As losses can still happen, complementary mechanisms are put in place to compensate: data is divided, numbered, and sent several times, potentially in different order of transmission; CRC and equivalent mechanisms are added at different levels; status messages are sent to the receiver. In fact, specific headers and/or footers are typically used to pass such information from the emitter to the receiver in order for it to undertake the appropriate actions. If the emitter is blind, the receiver can still use these mechanisms to obtain a clear view of the status of the communication. Overall, an excellent level of reliability can be achieved.

### 3.1.5 Architectural discussion

As discussed before, a physical data diode can be used to protect highly sensitive networks from lower security zones. This implies that such a division is clearly established in the considered environment. Guidance such as ISA99 [25], but also Cigré’s works [50,26] for power utilities or the future IAEA reference manual on computer security for nuclear facilities [15] can help in this task, as they all discuss zone distinction and graded approaches to security. Note that such diodes can protect a complete zone but can also be considered in specific cases for single systems; in any case, the diode should of course be a choke point. Considering the diversity of industrial architectures and systems, there is no one-fits-all position. However, three generic “principles” may be useful for the security architect:
• The “security Ockham’s razor”: if two situations provide the same level of security, choose the simplest. In our case, when considering strict one-way communications between two entities, the designer should always check if the two communicating entities could and should not be put into the same security zone. The simpler the better.

• The “One-way vs. zero-way debate”: is one-way connectivity absolutely needed for highly sensitive systems? Would no communications at all (“Air Gap”) and non-networked solutions (with human operators) be acceptable?

• The “Maginot line syndrome”: physical diodes provide such a high level of assurance regarding network connectivity that one could be tempted to give them magical powers… and forget that other communications exist (e.g. removable storage). More generally, the use of a diode should not prevent the enforcement of other complementary security measures.

3.2 Real multiple-stages demilitarized zones (DMZ)

A commonly accepted best practice when crossing two domains of trust is to insert multiple stages as DMZ. An example is a multi-tier architecture consisting of logically separate processes for presentation, application processing, and data management [51]. This concept is valuable in a security context only if the services, and systems used are based on different technologies and protocols. It means that if we queue the same type of technologies or controls (for example allowing only HTTP at each step with the same type of firewall device), there is no additional security over a single layer. An attacker finding a way to compromise the first layer will also be able to use the same way in order to compromise the others.

![Figure 3 – Real multiple-stages DMZ](image)

In order to avoid putting all our eggs in one basket, we need to use successively different measures. In the case of a multi-tier architecture, this is can be achieved by using a first step based on the HTTP protocol, then on SOAP encoded messages, and finally on SQL requests. This implementation of the defense-in-depth principle requires an attacker to compromise the whole chain in order to reach the last step, making his work much more difficult (cf. Figure 3).

To make this strategy efficient, we need specific firewalls, dealing with application layer attributes and constraints specific to industrial protocols.
3.3 Specific Firewalls (going up the stack)

The evolution of firewalls to protect network communication has been to ascend the layers of the OSI protocol stack [57]. Original basic routing functionality was used to limit who might communicate through Access Control Lists (ACL), we have moved to stateful firewalls capable of keeping track of the state of network connections. Finally, inspection of packets content at layer 7 is available using application proxy software for common protocols like HTTP or FTP.

The use of firewalls in the industrial world has recently caught with their use with classical IT. There are products emerging on the market capable of supplying the same firewall functionality for Modbus protocol, one of the major industrial protocols. The challenge here is to take a security decision based on attributes related to the application layer. Products like MTL and Byres Security Tofino [52] or Checkpoint UTM-1 Edge [53] can perform content inspection for Modbus/TCP, for example filter requests based on static commands, authorized memory spaces or data. This could be applied to put in place global decisions to restrict communication between zones, for example allowing read-only action coming from supervisory zone, excluding any possible action.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Device</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Router with ACL</td>
<td>permit tcp any 502&lt;br&gt;permit tcp any 502 established</td>
</tr>
<tr>
<td>4</td>
<td>Stateful firewall</td>
<td>iptables -A OUTPUT -p tcp -dport 502 -j ACCEPT&lt;br&gt;iptables -A INPUT -m state - state ESTABLISHED -j ACCEPT</td>
</tr>
<tr>
<td>7</td>
<td>Application firewall</td>
<td>Permit specific Modbus functions, like “read register”, eventually only on a specific range, for specifics values</td>
</tr>
</tbody>
</table>

Of course such tools must carefully implement the desired filtering decisions, as they could have impact on the correct operation of the industrial process. Well defined process behavior is mandatory and the priorities of safety and performance of the industrial process must not be disrupted when introducing such devices.

3.4 Intrusion Detection and Prevention

The basis of intruder detection is the inspection and identification of malicious content. Content inspection can be performed using either an active or passive approach. Active devices include firewalls [52,53] and Intrusion Prevention Systems. Passive devices include Intrusion Detection Systems used in stealth mode (without blocking traffic) [58].

As we have seen, ICS protocols content inspection is emerging as commercial products and represents the actual state-of-the-art of Industrial Control System protection. In the content inspection process, along with the restriction on industrial protocol commands (usually read, write, and diagnose), some protocol compliance checks can be performed, taking advantage of SCADA Intrusion Detection Systems signatures [54]. This is done by vendors coming from classical IT like Tipping Point ([55]) or vendors of more industrially targeted equipment like Industrial Defender ([56]).
The industrial process is globally well-known, fixed and, predictive. Thus, it should be possible to make the security tools aware of the underlying industrial process and logic. This introduces the possibility to make security decisions based on the understanding and mastery of the industrial process.

Such an approach has been taken by the authors [37]: after having developed a library handling Modbus/TCP requests and responses, we have set up a proof-of-concept (PoC) layer-7 firewall for Modbus/TCP interacting with Netfilter [59]. This PoC enables the filtering based on layer 7 attributes but can also be used to develop a “layer 8” approach, as presented in [37]. The layer 8 deals with the applications logic, including data and industrial process logic. In this approach, security decisions are based on industrial process awareness (operation mode, other measures or states) and application dynamic (consistency of the timeline of actions and observations).

<table>
<thead>
<tr>
<th>Layer</th>
<th>Function</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Data range checking protecting from fuzzing on layer 7</td>
<td>-50°C &lt; t° &lt; +50°C</td>
</tr>
<tr>
<td>“8”</td>
<td>Protecting from actions outside the industrial process logic. Using heuristics to decide if an action is dangerous.</td>
<td>open_a_valve_allowed = depends of (pressure, historic, temperature, context) if pressure and temperature are normal and we are in operation mode “running state”, then accept the “open the valve” command</td>
</tr>
</tbody>
</table>

This ongoing work is described in [37]. In particular, further work is needed to generate automatically an industrial process security model from existing configuration data available at engineering level. Moreover, advances in behavioral and anomaly-based intrusion detection techniques [60], might be used in the development of smart tools to assist an operator to decide if an unexpected situation requires further investigations.
4 CONCLUSION

This paper has presented a non-exhaustive list of “myths” based on wrong beliefs about security. Hopefully, it will contribute to rationalize them, helping to find a balanced security posture for ICS. Industry best practices for ICS security are emerging (e.g., [1,15,25,26,50]) and should be followed. In particular, defense-in-depth should structure the global approach. Moreover, simple solutions should be promoted, complexity being almost always orthogonal with security.

We have mentioned in §3 some new technical solutions. Some of them are still under development or currently only tested with a research and development perspective (it is the case of our “layer 8” approach to content filtering). Some commercial solutions are already available and due care must be followed to ensure that their integration with legacy systems goes smoothly and without any unwanted counterproductive effects. In all cases, the discussed solutions are not sufficient per se and have to be integrated in a complete security architecture and organization.

Security being a process, a global and consistent approach of risk management must be applied, taking into account that technical solutions can not alone be the answer. Human factors and organizational issues are paramount in a global security posture.
5 REFERENCE


[13] Dan Goodin, “Gas refineries at Defcon 1 as SCADA exploit goes wild - At least they should be,” The Register, Sep. 2008; http://www.theregister.co.uk/2008/09/08/scada_exploit_released/


[34] Bruce Schneier, “The nonsecurity of secrecy,” *Communications of the ACM*, vol. 47, October, 2004, p. 120.


[48] “The Fort Fox Data Diode - 100% guaranteed one-way (version 3)”;
http://www.datadiode.eu.


[53] Checkpoint upgrade to UTM-1 Edge Appliances announce,

[54] SCADA Network Intrusion Detection Systems (IDS) signatures,

[55] “TippingPoint expands security coverage for critical infrastructure – TippingPoint Augments IPS with SCADA (…)”,


[58] “Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS)”; Jared Verba and Michael Milvich

[59] Userspace library to handle packets queued by the kernel packet filter;