IST-152 Workshop on **Intelligent Autonomous Agents for Cyber Defence and Resilience**

Industrial Control System: Comprehensive Security Approach

SUPPORT PAPER

AUTHORS

PANICO, AGOSTINO – "LA SAPIENZA" UNIVERISTY OF ROME
CERULLO, LUCIO – JOINT OPERATIONAL CYBER COMMAND - JOCC
DELAURENTIS, VITO – JOINT OPERATIONAL CYBER COMMAND - JOCC
MURINO, GIUSEPPINA – UNIVERSITY OF GENOVA
VESTITO, GEN. FRANCESCO – JOINT OPERATIONAL CYBER COMMAND - JOCC

Summary

1. DESCRIPTION OF THE CYBER THREAT

The switch to the "*Digital Era*", characterized by profound dependence on computer systems, expose the current society to threats that were unthinkable a few decades ago.
While smartphones, tablets, personal computers are tools that allow us to live in an interconnected global network, changing the concept of time and space and to benefit from entirely new forms of communications, om the other end these are the breeding ground for attackers that are designed to steal data, spy on, disrupt and hit their "*target*" (1).
The threat in cyberspace is becoming an increasingly significant relief and directly proportional to those countries, including ours, the most technologically advanced basing much of its economy on Information Technology (2).
For this reason as just said, developing new capabilities and new tools to improve the cyber security of the country system is a challenge nationally important for growth , well-being and the security of citizens. The correlation between the economic prosperity of a nation and the quality of its cyber infrastructure will be getting tighter and a country to stay in the group of the most developed and advanced nations, will need to improve cyber security, in the industrial system, in public administration and most important in the sensibility of the people.
The cyber-attacks can be conducted by a variety of actors - such as states, organized crime, political activists, entities without identity - who are able to act in different ways to achieve their interests and objectives in the most important areas of the country such as political, economic, social and military.
The events of recent years are showing us that many systems, among which are those defined as "*legacy*", designed and implemented mainly to ensure service availability and at the expense of the safety aspects, have been and are the subject of cyber-attacks daily through the exploitation of vulnerabilities in the setup procedures, management systems and implementation (3).
In this context, the cyber threat is increasingly evolving: hackers, using sophisticated and persistent attack techniques, are targeting, not just the most common communication services, such as web servers and mail servers, but also the most complex industrial systems such as power plants and energy distribution, whose failure has a significant impact on both the economic structure of the country system and the daily lives of its citizens.

2. IT & OT

Nowadays the circumstances force us to make a fundamental distinction, from the technological and doctrinal point of view, into two areas: Information Technology (*IT*) and Operational Technology (*OT*).
The *IT*, Information Technology, is defined as the set of communications, networks and networking that ensures the management of information between users so they are securely sent, received and stored.
Information Technology devices are chiefly placed in office spaces or enterprise data center that are clean and temperature- and humidity-controlled, with either failover systems and/or local support staff available to respond quickly to performance issues, or both. (4)
The *OT*, Operational Technology, is instead defined as the set of communications hardware and software systems, with which can be controlled and supervised the industrial systems, causing or detecting changes made on these physical systems in real-time or near-real -time. One example is an energy management system of a dam or a wind power production system.
Operational Technology devices are designed to perform a very limited number of functions, often only one, according to exceedingly high reliability metrics. For example, a temperature monitoring sensor in a boiler may not be improved by the installation of powerful processor, but the unfailing performance of its one duty, to consistently and accurately report the temperature, is

an essential link in the chain that keeps the boiler from overheating and exploding. Understanding this distinction, that reliability and integrity are absolutely the primary considerations, is key to comprehending the divide between OT and IT, whether we are discussing their cultures, their organizations, or their technologies. (4)

This distinction immediately highlights the different purpose of these two families of devices, and consequently their difficult integration, which represents in the modern information warfare one of the main vectors of attack against these infrastructures.

3. REFERENCE STANDARDS

3.1 Italian National Framework of Reference

Based on the above definition, the *Operation Technology Critical Infrastructure* can be defined, in accordance with Legislative Decree 61 of April 11, 2011, as: "*An infrastructure, located in an EU Member State who are essential for the maintenance of vital societal functions, health, safety and economic and social welfare of the population, and the disruption or destruction of which would have a significant impact in that State because of inability to maintain those functions.*"

This definition, based on the aforementioned legislation itself, has expanded through the introduction of "*European Critical Infrastructure* (*ECI*)" defined as critical infrastructure located in the EU Member States the disruption or destruction of which would have a significant impact on at least two Member states. The importance of this impact is assessed in terms of cross-sector in relation to the involvement of different types of infrastructure.

In this context, in Italy, the Ministry of Defence and other ministries such as Interior and Economic Development, within their respective competences, put in place all the actions and measures necessary to ensure the protection of *ECI* located in national territory without prejudice to the responsibility at the local level the protection of the individual installations, the *ECI* constituents are attributed to the territorially competent prefect (5).

The Legislative Decree 61 also establishes the *Inter-Ministerial Nucleus Situation Planning* (*NISP*) and contains the definition of the Security Plan for operators of European Critical Infrastructures. At *NISP* (at the Prime Minister's Office in collaboration with the relevant ministries) entrusted with the identification and designation of *ECI*, the head structure (Secretariat for Critical Infrastructure, "*SIC*") for the technical and scientific work necessary for *NISP* functions and relations with the Commission and other Member States affected by the *ECI* that Italy intends to designate.

The Critical Infrastructure has been identified by the European Commission, after much debate, with the promulgation of the European Commission Directive COM (2006) 787 which identified 11 critical areas ranging from energy to communications, from transport to food.

3.2 Outline of the international regulatory framework

The Legislative Decree 61 of April 11, 2011, was accepted by the Italian implementing Directive 2008/114 / EC on the identification and designation of European critical infrastructures and aims to evaluate the need to improve their protection.

Therefore, the definitions of *CI* and *ECI* are consistent among all the EU member states with those illustrated in the preceding paragraph.

In the UK Cabinet Office defines *Critical National Infrastructure* (*CNI*) those "infrastructure, physical and electronic that are vital to ensure the integrity and availability of essential services and the disruption or impairment may result in economic or social damage or loss of lives. " The *CNI* spanning nine areas ranging from energy to communications, from transport to financial services.

Britain has set up a "*Center for the Protection of National infrastructure"* (*CPNI*), which represents the structure of government that oversees the protection and security of the *CI*.

Across the Atlantic, the US has identified 16 types of critical infrastructure in those sectors whose structures, systems and networks, physical or virtual are considered vital because if destroyed or altered may cause effects on national security. In this regard has been issued a directive, the Presidential Policy Directive 21 (6) where there are the guidelines aimed to maintain safe, functional and resilient critical infrastructure.

Below is a comparative diagram of the IC identified within the EU, UK and USA.

EU	GB	USA
ICT	Communications	Information Technology Communications +
Water	Water	Water + DAMS
Energy	Energy	Energy
Nuclear		Nuclear
Food	Food	Agriculture and food
Health	Health care	Public health care
Financial	Financial services	Banking and Finance
Transport	Transportation	Transportation system + Postal and shipping
Chemical industry		Chemical
Space		
		Monuments and icons
	Government	Government facilities
		Defence industrial base
		Commercial facilities
	Emergency services	Emergency services
		critical manufacturing

Figure 1: Comparative diagram main IC identified by regulations EU, UK and US

4. THE ICS AND SCADA SYSTEMS

4.1 Definition

The production processes are managed through *Critical Infrastructure Industrial Control System* (*ICS*) which generally consist of different types of systems for electronic monitoring of the physical plant, including that of supervision and data acquisition (*SCADA- Supervisory Control and Data Acquisition*).
Distributed Control Systems (*DCSs*) are typically used within a single process or generating plant, or used over a smaller geographic area or even a single-site location.
Supervisory Control and Data Acquisition (*SCADA*) systems are typically used for large-scale environments that may be geographically dispersed in an enterprise wide distribution operation. (7)
An *ICS \ SCADA* is, therefore a system that monitors in real time one or more industrial plants in order to reduce the costs of monitoring of machinery and increase automation and productivity.
The peculiarity of a *SCADA* other than *ICS* is that it monitors and controls systems over large geographical areas through communication infrastructure such as radio, satellite, telephone networks; It is composed of sensors associated with "*remote terminal units*" (*RTU)* that collect data and verify the condition of machinery and industrial processes, and that subsequently, after processing, send them to the plant or "*master terminal unit*" (*MTU*) control station.
The *ICS \ SCADA* systems allow to monitor in real time situations and so that the data obtained are used by third-party systems.
In the area of defence oversee *ICS* systems, for example, the energy management of a base, or a naval vessel but also the management of weapons systems of a tactical vehicle. Even the latter can be understood as an *ICS* as it controls a process and monitors the operation.
This overview aims to depict how the *ICS* systems are not peculiar to certain industrial processes, but rather permeate our daily lives, managing many aspects.

4.2 From 2010 to nowadays: a rapidly changing cyber security environment

The nature of the *ICS*, mainly oriented to the operation and the provision of seamless services 24h / 365, often makes it difficult to ensure the safety of the infrastructure in accordance with the same philosophy of Information Technology apparatuses.
In recent years, *ICS*, for economic reasons linked to the development and maintenance, they are directed to the use of hardware and software business and the use of common communication protocols, yet the ICS world still looks still varied and bound not to standardized protocols but implemented and customized protocols by market leaders.
As for *IT* systems, it is essential a support management that guarantees "*as soon as possible*" to install updates of application, minimizing user impact, and an improvement of the system security, for *ICS* instead the regular patch installation and implementation of software security measures, if not properly checked, could result in impacts on functionality.
Consider also that in some cases the management systems employed in these types of systems are at the end of life and therefore no longer supported by the parent with patching security.
In this regard, by way of example, consider that most of the *SCADA* software is based on operating system "*Windows Millennium Edition*" whose safety support has ended in 2006.
Also, and this is an aspect far from negligible, to be competitive in the market companies need to produce systems with lower costs and eventually functionality similar to or better than their competitors.
This simple statement, linked to the realization that develops and design safely is a significant cost, means that many of the currently available systems not only represent a risk to the cyber environment but also for the physical, given the implications that they may have.

4.3 A recent example of attack: Black Energy 3

On December 23, 2015, in Ukraine, (8) an electricity distribution company, Kyivoblenergo, interrupted the service to about 225,000 clients, declaring that the blockage was caused by the illegal entry of third parties in the company's control system and the *ICS \ SCADA* systems.
Later it was stated that the cyber-attack had been so pervasive as to affect most sections of the network and push the central administrators to switch to the manual operation mode.
The cyber defences, despite being highly structured, have been bypassed by using a wide range of vectors including aggressive spear phishing emails, malware variants BlackEnergy 3 and handling of Microsoft Office files.
It is evident that such an action, the high level and the amount of force put in place, was conducted by an entity able to:

- conduct intelligence activities to get to know the target system;
- shape the central bank, at least through the use of similar technology as turbines, PLC, power grid;
- production malware 0-day.

From a technical point of view the probable attack sequence can be described as follows:

- a spear phishing email in which was contained malware "BlackEnergy 3" that exploited 0-day vulnerabilities;
- the theft of passwords in enterprise networks;
- using *Virtual Private Networks* (*VPN*) to access the *ICS* network;
- remote access from intruder with full control of the *SCADA* control systems;
- access to serial devices and Ethernet as well as communication through the firmware;
- using a "*KillDisk*" software to erase in a targeted number of useful instructions and backup to prevent the restart system automatically in the event of failure;
- using the *UPS* system load systems for interruption of service;
- denial-of-service attack against the call center to prevent communication.

5. CURRENT ISSUES: NEED FOR A COMPREHENSIVE POLICY

One of the biggest obstacles is the lack of accurate data and information relating to cyber incidents that flock to the *SCADA*. Often companies concerned, mainly for not undermine the trust placed in them by investors and customer, don't state when and if they were interested in the attacks.
Also consider that in a world so interconnected, and the case of *Stuxnet* (9) teaches, no one can be considered immune to this type of threat, even air-gapped networks systems can be the object of attack.
With this background, it is necessary to provide a method to ensure the continuity of services provided by *ICS* and policies to define how their cyber security needs to be addressed and guaranteed.
This continuity can be ensured by developing, on one hand, the static and dynamic security policies, in fact the recent trend speaks of defence activities and proactive activities, on the lines of those already implemented and constantly developing in *IT* and, on 'other, providing integrated policies to ensure a longer life to the *OT* system (through for example the retrofit) and a resilience to attacks.

This policy, which we like to call "*comprehensive*", can be decomposed into several macro-activities:

- *risk assessment;*
- *static protection*;
- *proactive defence*;
- *resilience*;
- *retrofit*;
- *transportation vectors*;
- *security by design*;
- *safety culture and cyber teams*.

5.1 Risk assessment

The first consideration to be made in order to have an effective security policy for enterprise *IT* and *OT*, and in particular for the *ICS* system, is on the implementation of risk analysis designed to identify which are the most sensitive parts exposed to a possible attack. The risk analysis allows a census of the system components as a function of the threat, the level of vulnerability and the probability that it will be attacked. This allows to produce a list with the priorities of the system components to be protected by the appropriate security policy.

The Morgan's formula allows to summarize what was said:
R = t * v * fourteenth
Where R = risk, threat = t, v = vulnerability and fourteenth = probability that the vulnerability being exploited (10).

From 2004 to date it was produced numerous documents and papers with the objective of defining security standards for ICS.

There are different methods that could be applied to ICS systems (10), but few of these have specifically been studied for such systems, and even fewer of these are supported by tests in real environments. This situation is a constant in the ICS, where very often considerations and aspects of the IT world are borrow forgetting that the main

specifications of the OT systems require more detailed analysis, because as we noted above, despite the technology can be very similarly, the objectives are different, and therefore the relative risk should be supported by different evaluations.
Therefore, the need to develop, after the analysis of the uniqueness of the environment *OT*, a risk assessment methodology both quantitative and qualitative, which can be applied to those specific cases.
To this end, we propose the use of two different frameworks as a starting point, as it may represent the proper mix of qualitative analysis and quantitative necessary.
We will discuss primarily the framework "*OCTAVE Allegro*" (11) and then we will pass to an analysis of the "*Italian National Framework*" (12).

a. OCTAVE Allegro

This method consists of 8 steps, arranged in turn in 4 stages, as shown below.

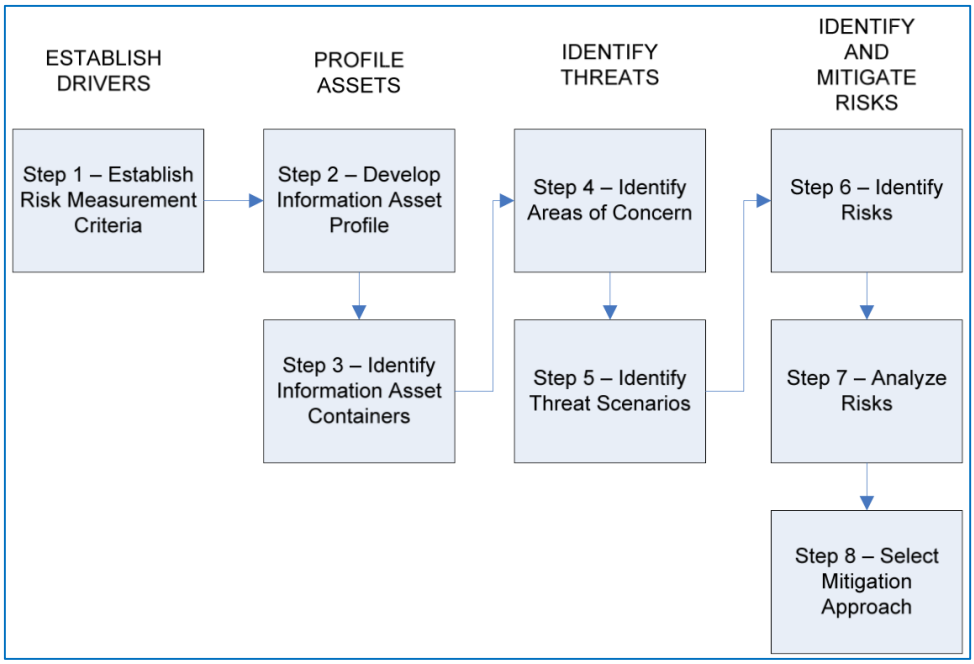

Figure 2: G8 of them step OCTAVE Allegro

In the first phase, the organization is asked to identify the drivers of the audit and general criteria, such as the activity guidelines. In the second stage, we are witnessing the definition of the analysis scope, through the formalization of the assets exposed to risk, with their specific detail, and which are subject to audit.
In the third and fourth phase the focus is moved to the concept of risk: identifies the dangers that may insist on asset previously surveyed, are analysed, evaluated and finally developed the response of the same solutions and risk mitigation.
Every step, in turn, is divided into a series of activities (in fact the standard controls), which guide the Auditor in the activity.
Unlike other approaches to risk analysis - as the case of *NIST* and the "*Italian National Framework"* treated more forward whole family *OCTAVE* outlines a roadmap through the various steps, activities, and related controls, the auditor has to follow, through maximum ease of use.

b. National Framework for cyber security

In Italy has been presented the "*National Cyber Security Framework"* (12) that comes "*with the aim to offer organizations a voluntary, uniform approach to dealing with cyber security in order to reduce the risk linked to the cyber threat*".
The National Framework was founded on the basis of the "*Framework for Improving Critical Infrastructure Cybersecurity*" developed by the *National Institute of Standards and Technology* (*NIST*), in the US, from which it inherits much of the central components, but adapting to the Italian production, it made up mostly of Small and Medium Industry (SMEs).
Choosing the NIST as the reference standard was made on the one hand to ensure full integration with the international contexts and, for another, despite being born in the field of critical infrastructure, it can effectively adapt even in contexts less complex and highly developed.
Indeed, the structure is divided into a main component (Core) and introduces two fundamental notions, Profile and Implementation Tier.
Compared to the structure of NIST, the National Framework varies with the introduction of the concepts of priority levels and maturity levels needed to make their own controls and indications more closely reflecting the national economic environment.
The effectiveness of the National Framework is given from being able to keep that enough abstraction that allows adapting the audit in reality very different size, joints, business and risk profiles, but at the same time specifically, have integrated indicators created in support of SMEs.

c. ICS Risk Assessment

One of the objectives with regard to the risk assessment is to define a basic framework, agile and functional, can be used effectively and efficiently towards the ICS \ SCADA systems. Such a framework will have as its starting point the methodology OCTAVE Allegro, previously defined, and making a detailed evaluation of the controls implemented in the national framework for cybersecurity, in particular, mapping these controls to reality and to the OT goals. This evaluation will be described in detail as a result of the case study planned as future works, in which will be evaluated the benefits and costs of the exposed approaches.
In this regard, it also highlights the need for sharing among agencies of the results of the various risk assessment. Such sharing, carried out anonymously and based on the same type and risk assessment methods would have an overall picture of the country's system risk and would focus investment and security initiatives.
Therefore, the proposal of a shared framework for OT systems may have a significance not only for the company but also for the country system.

5.2 Static Protection

At the approach light-encompassing, as a result of the risk assessment, which is the guideline for the implementation and evaluation of the state of the *ICS* system, it is essential to ensure the security of the implementation of "*static*" security measures, which contributes to reducing the areas of physical and logical attacks.
In particular, in relation to the threats that can target an ICS system, it is necessary to establish certain physical security criteria, personnel, software and hardware used, detailed described in this paragraph.

a. Physics Safety Requirements and physical access

It includes all the necessary countermeasures to make a secure environment and to prevent the physical damage of the equipment caused by unintentional, intentional or accidental actions.
These measures relate to the infrastructure, the access control and technological systems used.
Below is presented a comprehensive of the measures that are important to ensure the physical security of the entire structure from the overall system functionality up to the individual PLC:

- hardening of the infrastructure that host terminal and the sensors through the gratings installation, armoured doors, video surveillance mechanisms;
- access management and control lists (for example, with an access list of authorized personnel in a specific area/sensor);
- supervision, registration and accompaniment of unauthorized personnel;
- physical access control (locks on the doors, keys, magnetic cards, guards, access lists);
- physical security of servers, terminals, peripherals, MTU, RTU, PLC;
- physical protection of facilities and utilities (air conditioning, power supply) for critical and essential systems;
- procedures for media labelling, their protection and destruction;
- physical security of communications in the WAN (if feasible);
- control of electromagnetic compromising emanations with the definition of "bubbles" (if feasible);
- the discussion of procedures for the hardcopy output of the system depending on the sensitivity of the same level;
- for the scattered sensors / PLC along with the network, wherever possible, to provide physical burglar tools type that prevent access or that the marker occurred burglary.

b. Safety Requirements of personnel

The staff employed in areas and on the part of the more sensitive system must be if permitted and to the extent possible, subjected to reliability verification, through a sort of "*Security Clearance*" for operators.
It also needs to implement the policies on a model of "dual key" system that would prohibit unaccompanied staff to be able to compromise the functionality of the system.

c. Security of the "source"

One of the main point of failure, because skipped in most cases, is the need to "*validate the source*" the hardware components and software used. In other words, a fingerprint must be able to ensure that part of the code and/or hardware component that I am going to implement, must have been previously tested and validated according to the reference standards.
In this regard, it is also important to note the tendency to use as well as validated and certified technology, the domestic technology for critical systems, this trend is amplified if we consider also modern "*Internet of Things*" devices.

d. Limitations of physical and logical access to the ICS network

In order to reduce the risk of impairment of networks that are usually air-gapped, it is necessary to implement access restrictions that must provide at least the following measures for both physical and logical:

- use of unidirectional gateway;

- demilitarized zone (*DMZ*);
- a separate corporate network from the *ICS* and creating separate *VLANs* logically;
- the use of *VPN* and "*jump server*";
- safety of transport carriers such as encrypting communication in the *WAN* (if feasible) to ensure the safety of transport carriers, satellite, radio networks through the use of cryptographic devices and deployment of *VPN*;
- allow access to the corporate network and *ICS* defined only by authorized devices and certificates;
- creation of dedicated management stations;
- network access control;
- separate mechanisms and authentication credentials for users of corporate networks and *ICS* networks.

The *ICS* systems should also use a network topology that has multiple layers, depending on the sensitivity of the information level, the most critical communications that occur in the most secure and reliable layer.

In order to make clearer, the discussion is presented in the following figures, merely by way of example and not however completely explanatory, two of the possible network architectures.

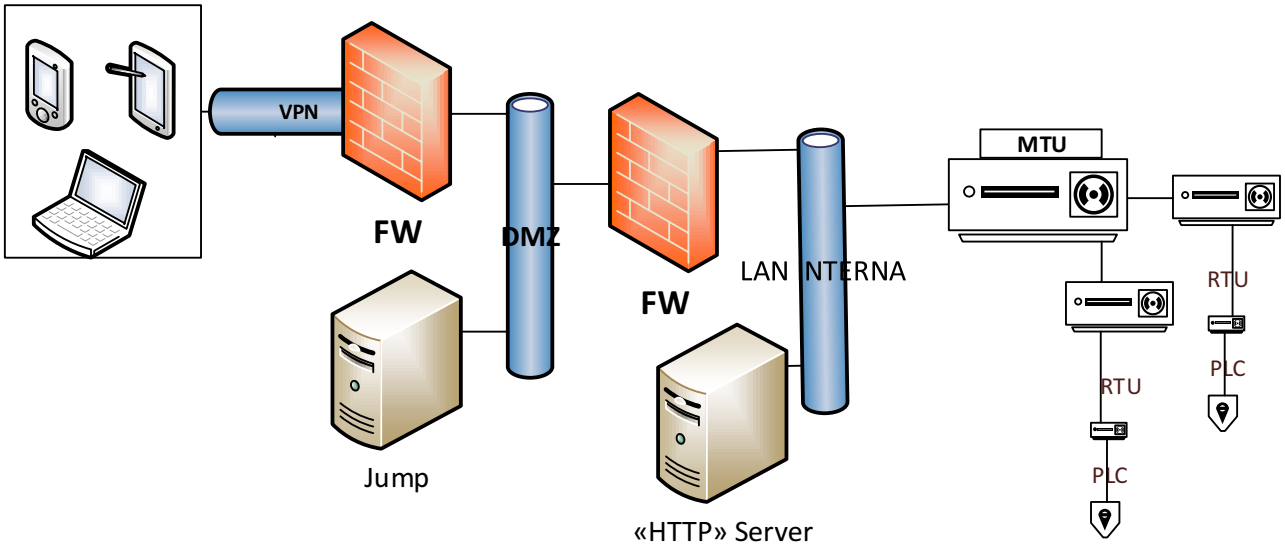

Figure 3: Solution Server Protection WEB "external"

Figure 1 is a network diagram with a *VPN* which allows connection to external devices, double Firewall protection, a *DMZ*, the presence of a "*jump server*" and an external web server the ICS network for the management of the actuators.

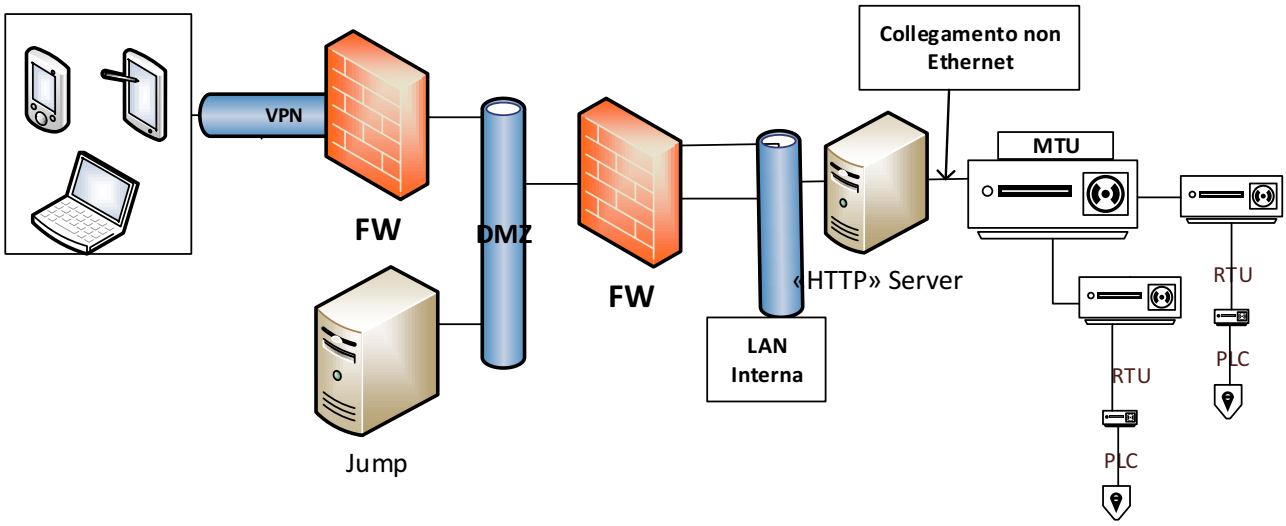

Figure 4: Solution Web Server Protection "Internal"

Figure 2 is a network diagram with a *VPN* which allows connection to external devices, double firewall protection, a *DMZ*, the presence of a "Jump Server" and a web server for the management of the internal actuators to the *ICS* management network not "*Ethernet*" connected.

Management Station: These positions will have to be configured to discriminate access to administrators and will be inserted in the site VPN management. Only such a station will be enabled to make changes to the configuration of the network management apparatus and the information logical structure.

Network Access Control: In the context of a considerable increase in the overall security level, you must take the "*Network Access Control*" policy to prevent malicious access by unauthorized devices. Such control makes it possible to associate a particular authentication policy to the devices within the network, by limiting access to unauthorized devices. This criterion may be the *MAC* address of the association of the device in the simplest systems or the association of the authentication device behaviour, evaluated continuously done by performing a continuous authentication. The absence of such control could allow an attacker to connect in a relatively simple manner to the network equipment if there is the physical availability of access to the area.

e. ICS Software Protection

In critical environments such as the *ICS* there is a need to provide for a series of measures for the protection of software, such as:

- implementation of policies for managing devices and locations of "*scrub*";
- the anticipation of a test environment for the functionality of these security patches and anti-virus;
- predict the distribution of security patches, after having suitably tested in field conditions;
- predict the dynamic implementation of measures that will underpin the perimeter security;
- implementing centralized antivirus and *IPS / IDS* to detect the malware and malicious traffic and mitigate risks;

- implementation of systems that allow certain operations (e.g. change of configuration) through the generation of an "*OTP – One-time password*" or implementation of biometric control systems;
- implementation of security policies, if possible but that provide centralized access to the stations in question according to the principle of "least privilege";
- implementation of BIOS password, the definition of a baseline software configuration as well as boot configuration so as to allow the starting of the operating system only from the hard disk;
- expiration of the "*work session*" from the outside after a defined period of time;
- disabling all unused ports and services and ensuring that they remain deactivated;
- monitoring and log management relating to the activities of interest defined on the basis of the risk assessment;
- implementation of virtual environments in order to put in place policies backup and restore;
- policies for the inclusion of new users and managing the account lifecycle;
- the control of the hardware configuration and software of the system;
- implementation of the complexity of the access password policies.

f. Near real-time monitoring activity

One of the main activities to be performed for the safety of OT in a distributed environment, is the ability to monitor sensors constituents of the system itself. For the implementation of such a system reference is made to a more general architecture of analytics data, known as "Kappa Architecture". It is illustrated in the following figure:

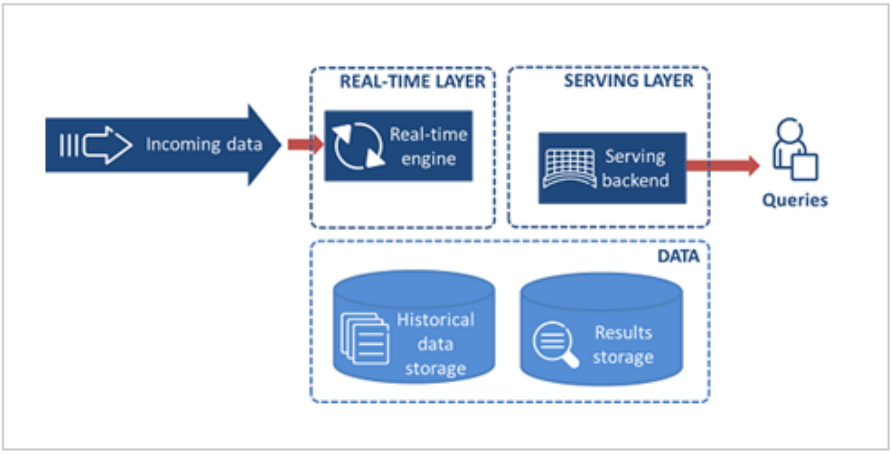

Figure 5: Type architecture diagram "Kappa"

The architecture Kappa, Lambda Architecture evolution, is characterized by the characteristic of being able to carry out, through same application code (within the Real-time Layer represented in the figure) either batch processing that type of Real-time type, reducing so much time and cost of development of analytics capabilities.
In this architecture, the object of analysis input data is taken typically by accessing an Event Bus ("Incoming Data"), which guarantees an asynchronous behaviour between the various manufacturers of such data and the functionality of Data Analytics which uses them; the bus also has characteristics of fault-tolerance.
The acquired data are persisted (and unchanging - append only) and constitute the archive called "Historical data storage" in the figure above. The results of computations performed by the Real-Time Engine are kept instead in a file called "Results Storage."
A detail of the architecture is shown in the following figure:

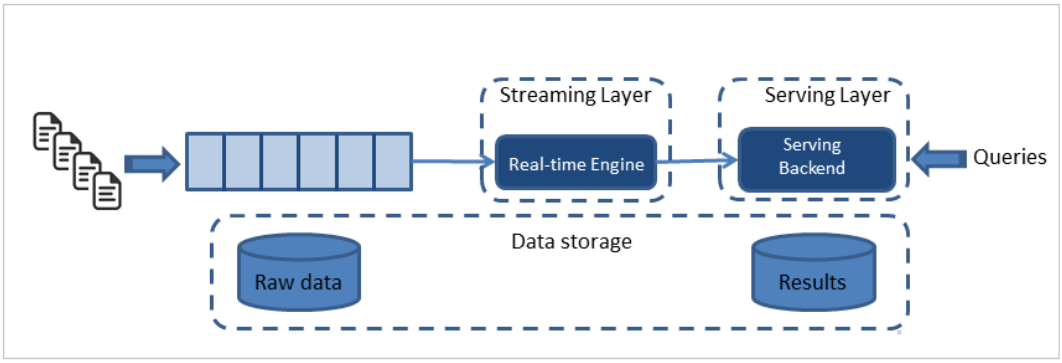

Figure 6: Architecture "Kappa" - detailed data flow

The Kappa architecture lends itself to be carried out by using different technological platforms, for the modules that constitute it. As part of this project, it was identified as the optimal selection of the following platforms.

a) ***Apache Kafka*** for the acquisition functionality and data buffering and acquired events;

b) ***Flink Apache / Apache Storm***, for real-time analysis of the simulation events or deferred as provided in Architecture Kappa;

c) ***Elasticsearch,*** for the data storage (indexing events of interest collected during an exercise and results of operations analytics);

d) ***Kibana and Grafana,*** for access to the results of the analysis (in real time or delayed), the creation of dashboards, scheduling of reports.

The target architecture of the analysis system is then represented in the following figure:

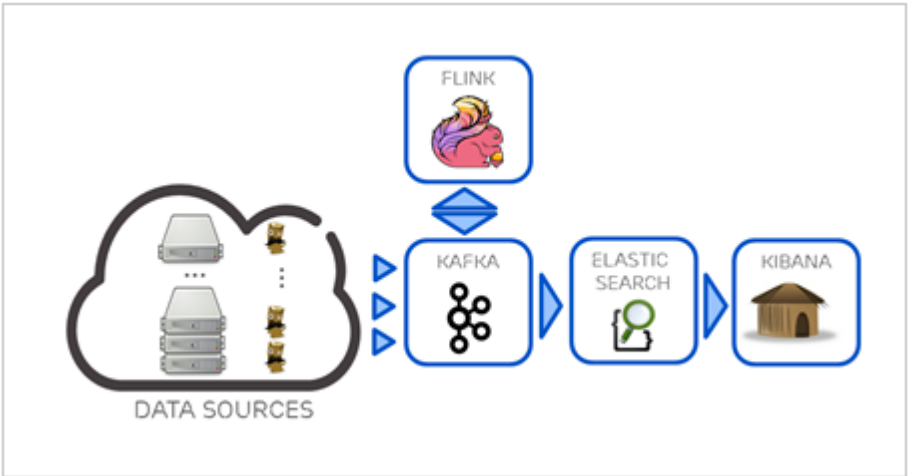

Figure 7: Architecture Analysis System

Such a monitoring system, efficient and effective for the management of numerous flows of varied and heterogeneous data, as often happens in *ICS* environments, leads to the creation of what in the military sphere is defined *COP* (*Common Operational Picture*) generated representing a situation in real time defined homogeneous joints of the installations monitored and fed by similar sensors.

It is possible through the use of dashboards to represent the state of health of all the air conditioning systems of the examined systems. Such evaluation may be more or less extended according to the needs and according to relevance. A *COP*, by monitoring the

functionality of the components, services not available and resources in the process of saturation, allow developing policies that will ensure the *ICS* operation and management.

g. Detection of events and security incidents

Defined in the previous paragraph the necessary monitoring capabilities, this must be linked to a detection and response capacity.
As evidenced by different field studies, time-to-detection for very virtuous companies is estimated at about 50 days (1). For this purpose it is necessary to emphasize the importance of having a set of tools that not only allow the detection but will allow the management of the incident in all its phases, from remote analysis tools used to analyse presumably infected workstations, to subsequent mitigation, containment and eradication, to reduce the risk of further impairment. For this purpose, tools with dedicated signatures for research in memory of particular behaviours associated with malware can be especially useful associated with all directions given above.
The detection and response should enable studies of the events in order to avoid future incidents.

5.3 Proactive Protection

In recent years the trend of attacks and subsequent breach led to the realization that security cannot be limited to the static protection, but must have a holistic approach based on the detection.
This awareness led to the use in a more or less distributed platforms of Active Defence and Threat Intelligence capabilities.
Active defence is the use of a range of tools and techniques aimed to achieve the following capabilities:

- *annoyance;*
- *attribution;*
- *attack.*

As "*annoyance*" is meant the ability to disturb the intruder during the phases of the attack in order to achieve the dual purpose of slowing it down and generate a "noise" that can be detected by monitoring systems.
As "*attribution*", can be considered the ability to define, above any reasonable doubt, the attack source.
As "*attack*", however, it is the counter-attack capabilities and quick response to threats.
In the *ICS / SCADA* ecosystem, these techniques are not adopted uniformly to both a lack of sensitivity to the Active Defence, primarily due to an "old" legacy from those who manage them and for the age of some of the systems, that prevent the compatibility with such tools.
In this regard, should be made clear the precise assumptions aimed at defining the threat model to use in this context. In particular, we can assume that:

- the attacker knows the services offered, the network infrastructure and applications in a comprehensive manner but not as well as the defender. This assumption is reasonable because the attacker has been enough time in the network to know whether or not the smallest details as the defender;
- the defender must implement measures of active defence, such as the range of services ports, the names of critical files and so on. In essence, he must be put in place all those Active Defence actions aimed to slow the attacker down, to reduce his knowledge of the infrastructure and forcing to carry out a new assessment of the system.

With a threat as relevant, the goal to be achieved by those who defend in a "proactive" is to slow down as much as possible forcing the attacker to increase the time required to gain a

detailed understanding of the network; this can be done through the use in a combined or individual of skills and techniques.
To achieve Annoyance and Attribution, for example, often are implemented honeypot or honey-net aimed at addressing the attacker towards non-critical objectives in order to have more chances to perform the detection.
This must go through the use and development of a series of specific tools aimed at 'active defence, better if easily deployable and usable.
A fairly recent trend leads to the development of a honeypot "adaptive" system comprising the combined use of monitoring techniques, proactive defence and threat intelligence. Such security infrastructure designed to detect behaviour outside the "norm", where normally means all the behaviours common to all users.

Penetration Testing

Another key option to achieve proactive defence is perform periodically penetration testing activities, from both internal team and external teams, to analyse the attack surface and evaluate the real risk exposure of the infrastructure.
The penetration testing is the set of activities aimed at identifying through the use of expert operators, such as an *ICS* to respond to an intelligent and dynamic cyber-attack how and whether it can be violated and what information can be gained from it. The penetration testing includes, in principle, a number of activities that are listed below:

Information Gathering: phase of information regarding the target collection. Of fundamental importance are the identification of sources, their number and subsequent correlation and exploitation of the resulting data. The Gathering information can also be classified into "passive" and "active" depending on the direct involvement of the infrastructure of the target placed in the analysis.

Vulnerability: refers to individuals, groups of individuals, software and SCADA protocols. They are such exposures to threats that endanger the survival of the systems, integrity and confidentiality of the data they contain and the services provided.

Exploit: the tools (scripts, viruses or worms or binary), exploiting a specific vulnerability in a computer system, allow the execution of malicious code aimed at obtaining administrative privileges or not. They can be implanted in an ICS through the use of any vector appropriately identified.
An exploit in turn can be divided into different components such as payload, shellcode, encoder

System & Privilege Escalation: it means the exploitation of project errors, application configuration, or holes in order to acquire the control of system resources normally precluded to a user or application.

Post-Exploitation: once within the system, the attacker sets up activities aimed at maintaining the access to exploitation system level (persistence). It may be actually included all activities for collecting data (packet sniffing, pivoting, patching level, network settings, etc.) in preparation for future activities related to further exploiting, pivoting and privilege escalation. It is the highest stage of system compromise.

Vulnerability Assessment

The process aimed at assessing the effectiveness of the systems and the security level acquired. The aim of this research is to identify the loopholes in the system analysed so that it can improve and prevent attacks based on specific vulnerabilities. Given the number of

new vulnerabilities discovered every day is crucial perform the VA with the right frequency in order to ensure that the system configurations are correct and appropriate security patches applied.

5.4 Resilience

Resilience involves the *ICS* design so that every critical component is redundant and that, in the case of failure, will be excluded from the network and does not generate unnecessary traffic on the network causing the cascading events. This expresses the need to find, in the case of attack, the methods that allow not to turn off "tout court" but the system that allow me to predict the extent to which an *ICS* if attacked is able to resist (the concept of resilience classes).

The resilience must allow a degradation "attenuated" passing by "normal operation" of the *ICS* to "emergency operations" through automated procedures or able manuals, this will be addressed in the future works in which a specific case study will be analysed.

When *ICSs* are part of the so-called critical infrastructure (*CI*), then Their correct behaviour Becomes essential for the maintenance of vital societal functions. This is Because the damage to a critical infrastructure, its destruction or disruption by terrorism, criminal activity or malicious behaviour, may have a significant negative impact on the security of the *EU* and the well-being of its citizens.

Reducing the vulnerabilities of critical infrastructure and increasing time Their resilience is one of the major objectives of the *EU*. In Particular, analysing the resilience of a system is of paramount Importance from a system maintainer's standpoint. This is Because, in spite of all the prevention and detection policies That might be applied to protect a specific *ICS*, the risk of an undetected intruder That penetrates the system and tampers with its parameters cannot be eliminated completely. Systems with a high built-in resilience are less prone to service disruption Because it is harder for the intruder to bring the system outside the boundaries of correct action, and this leaves to the maintainers more time to identify, isolate and defy the menace without causing major service disruption. It is expected That resilience analysis Should Provide the maintainers with a concise quantitative measure of resilience Obtained, e.g., by comparing the system boundaries stability under normal working conditions with the same boundaries considering various attack scenarios. Under this perspective, a highly-resilient system is one in which the overall stability is maintained even in the face of large modifications Affecting one or will more regulation parameters. In order to evaluate resilience, outline as before, one could consider various approaches including state-of-the-art control theory, simulation and AI techniques. In Particular, it is possible to devise systems whereby the *ICS* under test is attacked by intruders simulating intelligent programs, or, alternatively.

5.5 Retrofit

One of the major issues related to the implementation and development of *ICS* systems is the difference between the life cycle of *ICS* systems and the life cycle of their hardware and software. This is particularly reflected in those installations where the cost of construction and installation take several decades to be depreciated, while the component becomes obsolete and obsolescence is also accompanied by the risk related to the impairment of the equipment.

To address this risk is important to know that the maximum evaluations linked to technological life of some *ICS* systems, linking them to data with those derived from the quantitative risk assessment of obsolescence for *IT* systems.

For this purpose, we take as a reference, purely by example, the life cycles of Microsoft systems; this assessment is dictated primarily by the availability of documentation (13) and

the presence of important agreements of partnership between leading companies *ICS* and Microsoft field.

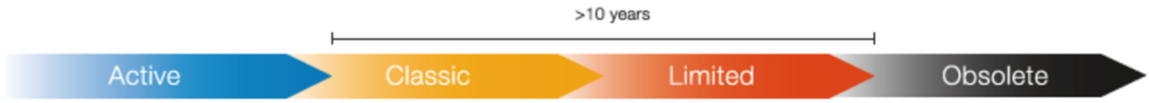

Figure8: End-of-Life Product ICS

Sistemi operativi client	Service Pack o aggiornamento più recente	Fine del supporto Mainstream	Fine del supporto Extended
Windows Vista	Service Pack 2	10 aprile 2012	11 aprile 2017
Windows 7 *	Service Pack 1	13 gennaio 2015	14 gennaio 2020
Windows 8	Windows 8.1	9 gennaio 2018	10 gennaio 2023
Windows 10 **	Versione 1703	13 ottobre 2020	14 ottobre 2025

Figure 9: End-of-Life Products Microsoft

A considerable discrepancy is detected between Figures 8 and 9, in fact, while the average life of an *IT* system is about 7-8 years before becoming obsolete, for *OT* systems this value is at least 10 years.
In the light of this assessment, it has in the best possible condition a lack of quantifiable in about 2 years. In the best-case scenario, considering the number of vulnerabilities found and resolved during the year it has very high exposure to critical systems without the possibility of having a resolution of the problem.
From this qualitative risk assessment, it is considered that even the best-case scenario is minimally acceptable for an *ICS*.
To this regard it is important the introduction of the concept of "*Evolution without obsolescence*", i.e. a process in which both the purely *OT* part both the portion *IT* to support must converge to a correct management of the lifecycle of systems. This development, safeguarding security, can be continuously carried out without too many and heavy charges.
To achieve this goal, which turns out to be the primary for the effective mitigation of the risk during the life cycle, it is necessary to adopt lines of development according to the principles of the "*secure development lifecycle*", in order to have systems which in their phases will follow a process replicable and quantifiable, and whose management, upgrades, disposal does not require a continuous design "ex novo" but vice versa are considered parts of a constant development process.
This phase must be preceded by a risk assessment that highlights the most critical obsolete components for the industrial plant operation: interruptions in service and upgrades of legacy systems should be planned with a reasonable period in advance.

5.6 Security by Design

As indicated in Section 5.5, one of the major risks arising from *ICS* systems is related to the different life cycle of the various components that constitute them. In this context, it is necessary that both a supportable and resilient system then comprising a security process by design for the development and testing of the *ICS*.
Therefore this suggest a guideline to follow for the development of *ICS* systems, named *Security Development Lifecycle* (*SDLC*).

The *SDLC* process has been thoroughly discussed in the literature, in particular by leading companies in the software development industry. Rarely it was used for the development of complete hardware and software but it is certainly one of the methods that allow part of the security implementation right from the design part.
The *SDLC* can be divided into 7 different phases, which are described below:

- *Training*
- *requirements*
- *Design*
- *Implementation*
- *Verification*
- *Release*
- *Response*

Accompanied by the part of *SDLC* there is the necessary capacity to understand and shape the threat as more realistic and exhaustive as possible, especially with the application of what is considered "*Threat Modelling*". In this regard, can be indicates as one of the most reliable for making threat modelling and related mitigation the *STRIDE* model:

- *spoofing*
- *tampering*
- *repudiation*
- *information disclosure*
- *denial of service*
- *elevation of privilege*

To which we associate the following mitigations:

- *authentication*
- *integrity*
- *non-repudiation*
- *confidentiality*
- *availability*
- *authorization*

This adds specific best practices:

- all software developed must not consist of software or parts of it open source;
- they must be provided for laboratory environments able to verify the patching in order to ensure that the integrity of the system is maintained.

5.7 Safety culture and cyber team

Safety culture

Violations / IT impairments are often favoured in unintended ways by users. The tools and next generation security policies become more sophisticated and efficient but their effectiveness can be attenuated by users' improper conduct. This demonstrates that computer security is a shared responsibility throughout the organization. In this context, it considers it necessary to resort periodic indoctrination programs for staff as well as the drafting of specific regulations that contain the basic rules of good behaviour.
It is also necessary to provide cybersecurity team and those elements of the organization created specifically to ensure the information security infrastructure. They must be composed by different professionalism. In principle must consist of managers and system administrators are responsible for the network configuration, security experts and a manager to the physical security. Also, a member of the cyber component must be part of the management board in order to represent the cyber security issues at the highest levels.

Education and training

It is necessary to realize an integrated platform for the training bench, in the field of cyber-security and to the testing of cyber technologies of *ICS* in a highly dynamic and evolving environment.
This platform, aimed at the education and training of specialist staff, must be:

- ***dynamic*** with the ability to adapt and extend its modelling capabilities, virtualization and simulation of real-life contexts in terms of environments and *IT* technologies and strategies and cyber-security techniques;
- ***flexible*** with the ability to adapt to environments and contexts of use different and varied with different cultures, differing practices, specific operational methodologies;

In addition, if the orientation was open to operational cooperation with other national and international entities and the sharing of tools, components and common good results, the platform must be interoperable.
This training platform will provide:

- operator training through introductory and specialized courses;
- training through the design of contexts and scenarios to emulate environments and configurations cyber-attack as realistic as possible through to use *ICS* bench "*modelled*",

Research, Testing and Development

The primary requirements are added, through a constant evolution as:

- experimentally validating the research of new cyber solutions for *OT*;
- providing an environment where testing the software, hardware, actuators and sensors by verifying and validating new solutions in the field of cyber security;
- enabling the development of "*techniques, tactics and procedures*" (*TTPs*) targeted both response to hostile activities and the conduct of offensive activities.

6. CONCLUSIONS

These days, the "*time to detection*" of a malicious activity on traditional *IT* systems (1) (14) is stood over an average of more than 50 days, even considering the most virtuous environments.
The threat level in recent years and the evolution of asymmetric warfare oriented towards the use of cyber-attack against *ICS* systems also reminds us that the trend for the future involves more sophisticated and advanced attacks, involving not only the cyber but also the physical world.
While it is undeniable that *ICS* systems are normally designed to withstand the technical failure through redundancy it is also true that redundancy, and the case of black energy proves it, may not be enough to deal with structured malicious attacks.
It is therefore necessary to implement measures so as to enable the integrity of the system both during normal operations and during the cyber-attack. Such measures must not only be of a technical nature but must take into account, the bulk point of vulnerability is represented by man. For instance, the case Stuxnet (9) teaches that the malware has been introduced into the plant control network by a little zeal technician.
Also attacks on *ICS* systems have so far been conducted by organizations technologically and logistically advanced which means that only those who are structured and has significant resources can think of a successfully attack an industrial plant (15) (16).
Hence the need to provide a 360-degree policy, which is not to omit any aspect and consider all aspects of the man-machine combination.
The current trend shows that all the major industrial powers, primarily in the United States, are working on *ICS* environment to make them as security compliance as possible. Only the escalation into more damaging hostile acts against *ICS* enabled the cyber security in this particular area, and recently, to become a priority.
The conclusion of this paper is to raise awareness of the need to develop and consolidate a culture of cyber security for *ICS / SCADA* starting a path that takes into account all aspects that contribute to ensuring genuine cyber protection to *OT*.
Therefore, the comprehensive approach can be summarised as follow: borrow and adopt best practices and concepts already employed or developing in the industrial, military and academia making them viable for reality *ICS / SCADA*.
As future work, and a natural follow-up activities based on this paper, the practical implementation will be consider, applying the indicated requirements in a real world scenario, than will be considered as initial use case of *ICS* security in a military environment.

7. BIBLIOGRAPHY

1. **FireEye.** *M-Trends Reports 2017.* s.l. : FireEye, 2017. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.
2. **Gen Graziano, CaSMD - Intervento Commissione Difesa Camera.** www.camera.it. [Online] 2017 gennaio 25. http://documenti.camera.it/leg17/resoconti/commissioni/stenografici/pdf/04/indag/c04_cibernetico/2017/01/25/leg.17.stencomm.data20170125.U1.com04.indag.c04_cibernetico.0009.pdf.
3. *CYBER WAR, CYBER SECURITY.* **Gen Vestito, CIOC.** 2017, Rivista Aeronautica.
4. **Dereck, Harp.** *Bridging the Divide.* s.l. : Next Defence.
5. **Parlamento Italiano.** *Decreto Legislativo 61.* Roma : s.n., 11 Aprile 2011.
6. **21, Presidential Policy Directive.** *Critical Infrastructure Security and Resilience* . 2013.
7. **Robert, Radvanosky.** *Handbook of SCADA/Control Systems.* s.l. : CRC Press, 2016.
8. **Zetter, Kim.** Inside the cunning, unprecedented hack ukraine's power grid. *Wired.* [Online] 03 Marzo 2016. [Cited: 10 Luglio 2017.] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
9. *Cyber threats to critical information infrastructure.* **Wilson, C.** s.l. : Springer, 2014, Cyberterrorism: Understanding, Assessment, and Response.
10. *A review of cyber security risk assessment methods for SCADA systems.* **Cherdantseva, Yulia Burnap, Pete Blyth, Andrew Eden, Peter Jones, Kevin Soulsby, Hugh Stoddart, Kristan.** s.l. : Elsavier, 2016, Computers & Security, pp. 1-27.
11. **Carnegie Mellon University.** Octave Allegro. *US-CERT.* [Online] [Cited: 10 Luglio 2017.] https://www.cert.org/resilience/products-services/octave/.
12. **CIS Sapienza.** Framework Nazionale. *Framework Nazionale CyberSecurity.* [Online] [Cited: 10 Luglio 2017.] http://www.cybersecurityframework.it/.
13. **Microsoft.** Lifecycle. *Microsoft Support.* [Online] [Cited: 10 Luglio 2017.] https://support.microsoft.com/it-it/lifecycle.
14. **NIST.** *NIST Special Publication 800-82 Revision 2 - A guide to Industrial Control System (ICS) Security.* s.l. : NIST, 2015.
15. **AAVV.** A review of cyber security risk assessment methods for SCADA systems. 10 2015.
16. —. Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali. *Informazioni Difesa.* 2014.
17. **Franchina, Luisa.** [Online] http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/OSN/Documents/05_Franchina.pdf.

LIST OF FIGURES