Cyber Risk in Aeronautic and Naval sectors, comparison with Industrial Cybersecurity

By Gerico Security Srl (www.gerico-sec.it)

The year 2021 will see new obligations concerning Cyber security in the Naval and Avionic sectors. The specificity of the aeronautic sector has determined dedicated rules for Cybersecurity risk treatment and mitigation, aimed at protecting Airworthiness and thus Safety (the so-called Security for Safety). The standards at issue will be applied internationally[1]. On the contrary, the naval sector is still far from setting binding rules for a worldwide standardization, it is limited to the resolution of International Maritime Organization (IMO)[2], and non-binding guidelines[3]. In any case, it is wise to bear in mind that Cyber Risk management, which is connected to Safety, will be a binding factor within the Compliance activities in the naval sector from 2021 onwards.

Avionics and naval systems traditionally have not been affected by the Cyber threat pressure likewise to the industrial control systems (ICS e/o SCADA) on the grounds that the critical environments were naturally isolated from the outside world and based on proprietary technology within which it was difficult to conceive the exploitation of vulnerabilities for attacking by using malware or malicious intrusions. Technology develops slowly in sectors in which extreme reliability and absence of project errors, which could put safety in jeopardy, are required. Nevertheless, it evolves and nowadays, computer products, derived from "general purpose" commercial systems or interconnected systems, which directly or indirectly have interfaces to the "large network" or simply threat sources such as USBs, are used more and more often in Avionic and Naval sectors. The industrial sector has likewise dealt with and is likewise dealing with a significant change of approach, in which the process control systems are connected more and more to enterprise networks and from there, even unexpectedly, to the outside world.

When we usually talk about cybersecurity governance we mean ISO/IEC 27001 and the related controls as specified in ISO/IEC 27002, NIST SP800-171 or NST SP800-53 within the USA while, as far as risk analysis is concerned, ISO/IEC 27005 or NIST SP800-30 are meant. On the other hand, ISA 62443 (which is a set of standards) or NIST SP800-82 for the USA are indicated for the control system sector

In spite of the peculiarity of each sector, we can nevertheless see that the approach of the risk management is the same and, as proof of this, the risk approach of the Naval[4] sector and of the "traditional" IT sector covered by ISO/IEC 27005 is shown below :

[1] Here we refer to ED202A of Eurocae and its homologous RTCA DO-326A, and other connected rules.
[2] Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS) adopted on 16/06/2017
[33] The article refers to "The Guidelines on Cyber Security on Board Ships" version 3, Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL
[4] "The Guidelines on Cyber Security on Board Ships" version 3

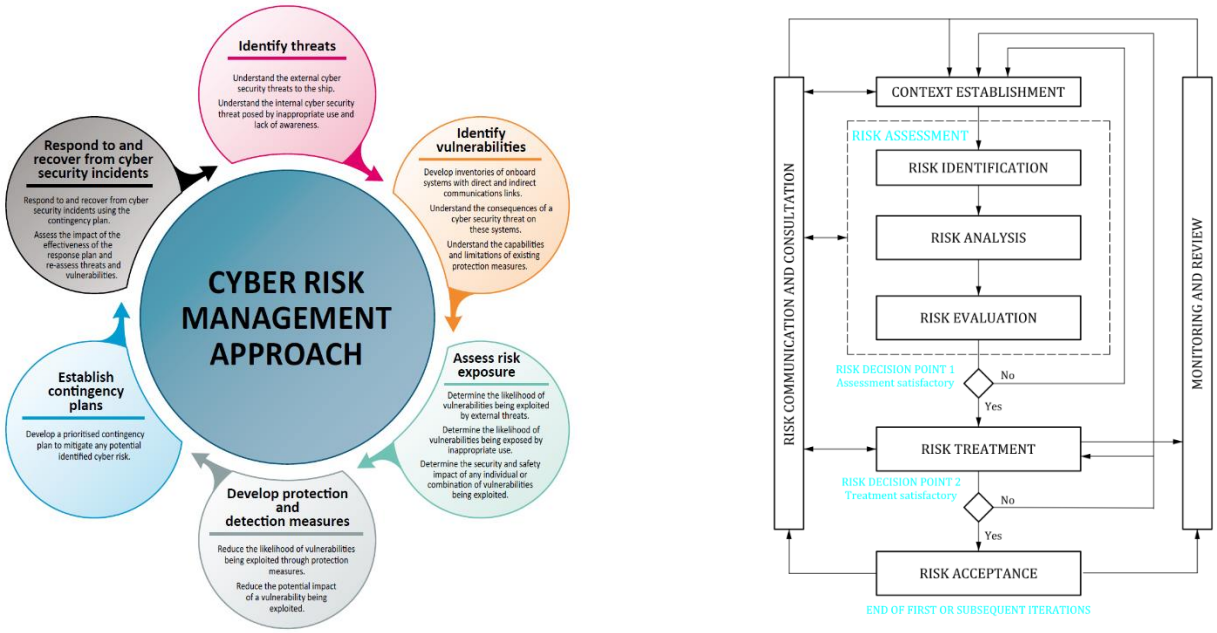


Figure 1: Risk Management

The industrial, aeronautic and naval worlds have in common similar architectures and criticalities in terms of operational response. Looking at the figure below, we can abstractly depict architectures or operational needs for all the three sectors, based on 5 levels with the most critical systems in the centre and those that progressively increase the risk area outside:

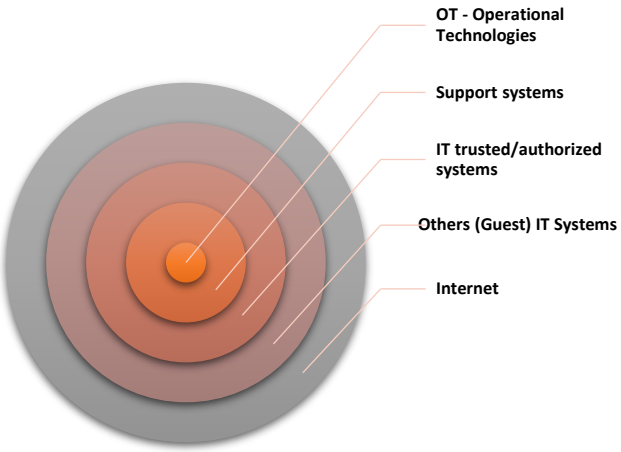


Figure 2: Information System Levels

Industrial control levels, operational naval systems and avionics have in common the same features that are summarized in the right-hand column of the figure 3 (OT Systems). The features are compared to the classic IT[5]:

[5] NIST SP800-82 source

Category	IT system	OT system
Performance requirements	■ non-real-time ■ response must be consistent ■ less critical emergency interaction ■ tightly restricted access control can be implemented to the degree necessary for security	■ real-time ■ response is time-critical ■ response to human and any other emergency interaction is critical ■ access to OT should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (reliability) requirements	■ responses such as rebooting are acceptable ■ availability deficiencies may be tolerated, depending on the system's operational requirements	■ responses such as rebooting may not be acceptable because of operational requirements ■ availability requirements may necessitate back-up systems
Risk management requirements	■ manage data ■ data confidentiality and integrity is paramount ■ fault tolerance may be less important. ■ risk impacts may cause delay of: ship's clearance, commencement of loading/ unloading, and commercial and business operations	■ control physical world ■ safety is paramount, followed by protection of the process ■ fault tolerance is essential, even momentary downtime may not be acceptable ■ risk impacts are regulatory non-compliance, as well as harm to the personnel onboard, the environment, equipment and/or cargo
System operation	■ systems are designed for use with commonly known operating systems ■ upgrades are straightforward with the availability of automated deployment tools	■ differing and possibly proprietary operating systems, often without built in security capabilities ■ software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and possible involvement of modified hardware and software
Resource constraints	■ systems are specified with enough resources to support the addition of third-party applications such as security solutions	■ systems are designed to support the intended operational process and may not have enough memory and computing resources to support the addition of security capabilities

Figure 3: IT VS OT

The industrial world teaches us to delimit and segregate correctly the different levels of systems so as to avoid the propagation of possible "contaminations" throughout more critical levels. A typical architectural solution for the segregation of "mission critical" systems from the traditional ones is the network[6] architecture. It is shown on the left below. Then, comparing it with the one on the right, which is suggested for the naval[7]world, we see that the approach at issue is the same and based on the segregation and the appropriate protection of the OT part from the support systems to the mission and from the rest of the world:

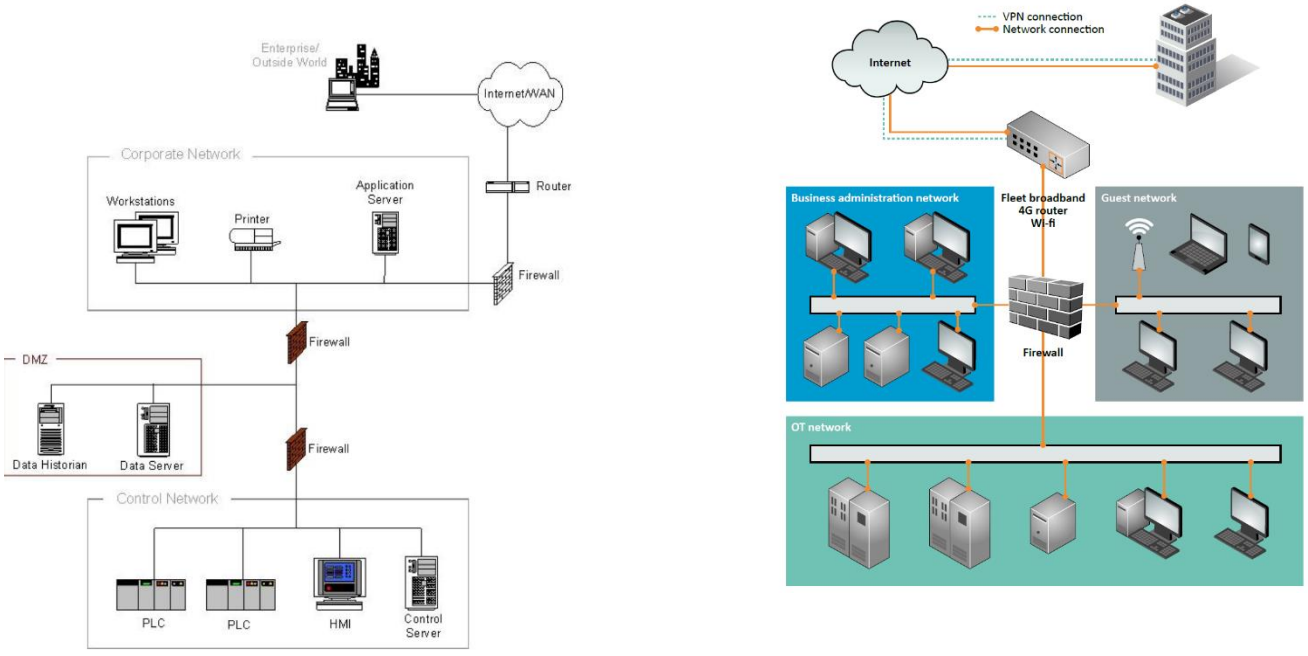
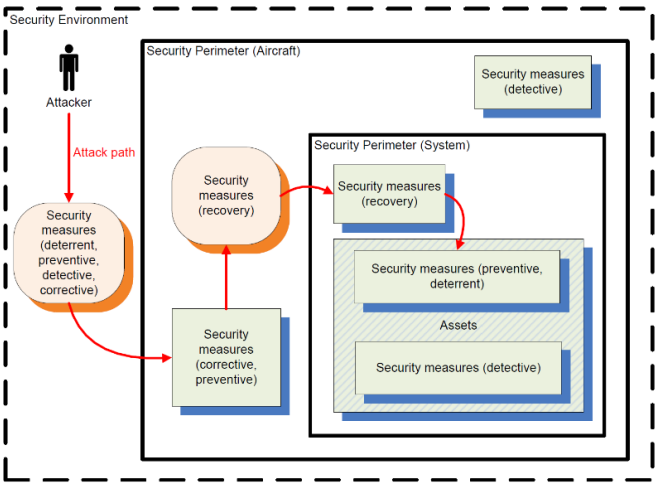


Figure 4: Typical network architecture

[6] Figure taken from NIST SP800-82
[7] From "The Guidelines on Cyber Security on Board Ships" version 3

The evaluation and management of the Cyber risk should be alike, both the industrial, naval and avionic systems are to be evaluated by delimiting the different parameters[8], the critical systems from those for the support and then, those from the rest of the world to effectively identify:

- Threats
- Attack Paths
- Attack surfaces
- Attack containment measures and recovery for each level



Adopting the principles of ISO/IEC27001 for security airworthiness, ED202A has divided the environment of the analysis into 3 elements (that can be analysed within more levels, from the aircraft to single element of a subsystem:

- The critical asset (it can be the whole aircraft or a system/subsystem from the analysis point of view) at risk of Security
- The Security perimeter, which is the set of elements composing the critical asset to be protected and therefore, represents the interfaces exposed to the outside environment
- The outside environment, actors and systems that can interact (authorized or not) with our asset by using the existing interfaces

This approach enables an accurate identification of each perimeter levels, regardless of the asset features (physical and logical ones), exposed to greater criticality and vulnerability, to intentional attacks or malware, the attack impacts on security and thus, the results can be combined with the safety requirements. The analysis of the context throughout concentric circles enables the comparison of both the bottom-up and top-down "Attack paths" with the possible impacts on safety then, picturing the possible "Security Scenarios affecting Safety".

Although different worlds are involved, it is clear that air and sea can benefit from the existing Best Practice provided for land (Industrial sector), aimed at counteracting the Cyber Risks and ensuring the necessary Safety features. The industrial world can also benefit from rules and standards set for other technological worlds for the improvement of the risk analysis and its defensive capability against Cyber attacks. In a simple matrix, we see therefore as the existing rules, set for the Information security and Industrial Security world, can support and be complementary to the Aeronautics[9] and naval Sector rules.

Perimeter	**Aeronautic sector**	**Naval sector**
OT	ISA 62443 / NIST SP800-82	ISA 62443 / NIST SP800-82
Support Systems	ISA 62443 / NIST SP800-82	ISA 62443 / NIST SP800-82
IT trusted/Authorized systems	NIST SP800-171 NIST SP800-172	ISO/IEC 27001/27002
Others IT Systems	ISO/IEC 27001/27002 NIST SP800-171	ISO/IEC 27001/27002
Internet	ISO/IEC 27001/27002	ISO/IEC 27001/27002

[8] Figure taken from ED-202A EUROCAE
[9] The rules indicated in the table can be an important starting point to effectively implement the requirements as provided in ED202A, ED203A ed ED204.

Gerico Security Srl **(**www.gerico-sec.it**)**

It is a consulting and business-integrated services company on risk management Information & Cyber Security and Business Continuity. It has been set up by specialists of the sector to satisfy the demand for security. The expertise has been acquired by and based on the activity of design and development of real-time systems, carried out over the years (Space and Telecommunications) together with a supporting activity to major critical infrastructures (Telecommunication and gas transportation and storage) in the sector of Information Security and business Continuity and to large and small-sized enterprises within financial, insurance and value-added fields.

Gerico Security Srl is following the "Security for Safety" Cybersecurity evolutions in the Naval and Aeronautic market, helping companies to be compliant with sector specific rules, such as ED202A, ED203A and ED204 related to the Airworthiness Security. Moreover, Gerico supports Organizations in obtaining new CMMC – Cybersecurity maturity Model Certification required by USA DoD to all Defence supplier.

The company is ISO27001 certified (Certification n. 57112, issued by CSQA, expire date 26/11/2022), it provides specialist consulting services, assessment, internal and third-party audit activities, personnel training, support for business process certifications and key-in- hand project services of Governance Risk & Compliance.