Cyber Risk aeronautico e navale: una comparazione con la Industrial Cybersecurity

Author : Giustino Fumagalli

Date : 7 Settembre 2020

Il 2021 vedrà l'avvio di obblighi relativi alla sicurezza cyber nel settore navale e aeronautico. La specificità del mondo aeronautico ha richiesto la formulazione di norme dedicate al trattamento e mitigazione dei rischi di *Cybersecurity* al fine di garantire l'aeronavigabilità e quindi tutelare la *Safety* (la cosiddetta ***Security for Safety***), che hanno valore internazionale[1].

Al contrario il mondo navale, ancora lontano dal trovare norme vincolanti valide uniformemente a livello globale, si limita a una risoluzione dell'International Marittime Organization (IMO)[2] e a linee guida non vincolanti[3], anche se - è bene ricordare - la gestione dei *Cyber Risks* in relazione alla *Safety* sarà elemento vincolante nelle attività di *Compliance* navale dal 2021.

Come per i sistemi di controllo industriale (ICS e/o SCADA), l'avionica e i sistemi navali tradizionalmente non hanno sentito la pressione della minaccia Cyber, in quanto gli **ambienti critici** in genere erano naturalmente isolati dal mondo esterno e basati su tecnologie proprietarie in cui era difficile immaginare vulnerabilità adatte ad essere sfruttare per attacchi tramite *malware* o intrusioni malevole. La tecnologia evolve lentamente in settori in cui è principalmente richiesta affidabilità estrema e l'assenza di errori progettuali che possano mettere a repentaglio la *safety*. Tuttavia, evolve; e ora sempre più spesso si utilizzano, anche in campo navale e aeronautico, prodotti informatici derivati da sistemi commerciali *"general purpose"*, o sistemi interconnessi, che, direttamente o indirettamente, presentano interfacce verso la "grande rete" o più semplicemente **sorgenti di minacce** quali le USB. Esattamente come nel mondo industriale, il quale ha visto e sta vedendo un forte cambiamento di impostazione, dove i sistemi di controllo di processo si collegano sempre di più a reti *enterprise* e da lì, anche quando non previsto, al mondo esterno.

Normalmente, quando parliamo di governare la *cybersecurity* pensiamo alla ISO/IEC 27001 e agli annessi controlli specificati all'interno della ISO/IEC 27002, o nel mondo USA alla NIST SP800-171 o la NST SP800-53, mentre per l'analisi dei rischi si pensa alla ISO/IEC 27005 o alla NIST SP800-30. Se guardiamo al mondo dei sistemi di controllo si parla, invece, di ISA 62443 (che è una famiglia di norme) o della NIST SP800-82, tipica del mondo statunitense.

Tenuto conto delle peculiarità di ogni settore, possiamo però vedere che l'approccio alla

gestione del rischio è il medesimo, e a riprova si riporta qua nel seguito l’approccio al rischio suggerito nel mondo navale[4] da quello della ISO/IEC 27005 per il mondo IT “tradizionale”:

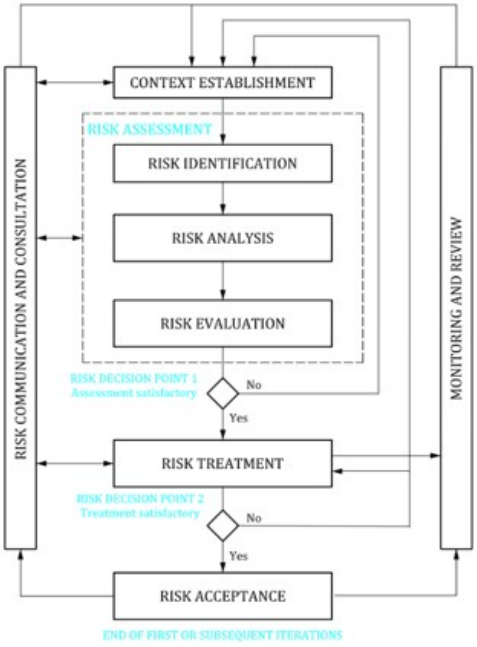


Figura 1: Risk Management

Il mondo industriale, quello aeronautico e quello navale sono accumunati da architetture similari, con criticità analoghe in termini di risposta operativa e di *safety:* se guardiamo alla figura sottostante possiamo astrattamente raffigurare, per tutte e tre i settori, architetture o necessità operative basate su 5 livelli, con al centro i sistemi più critici e all’esterno quelli che ne aumentano progressivamente la superficie di rischio:

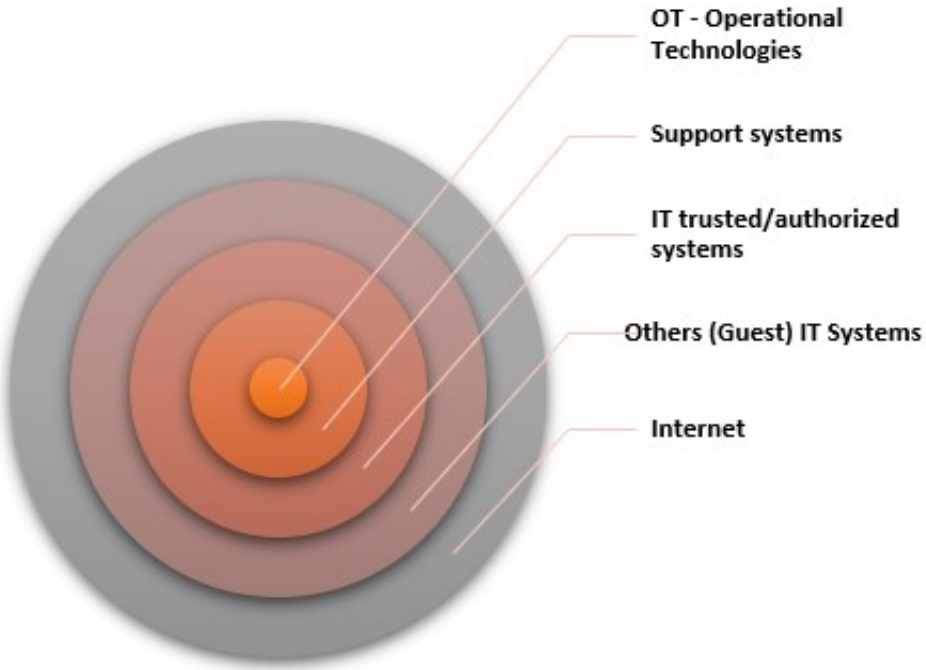


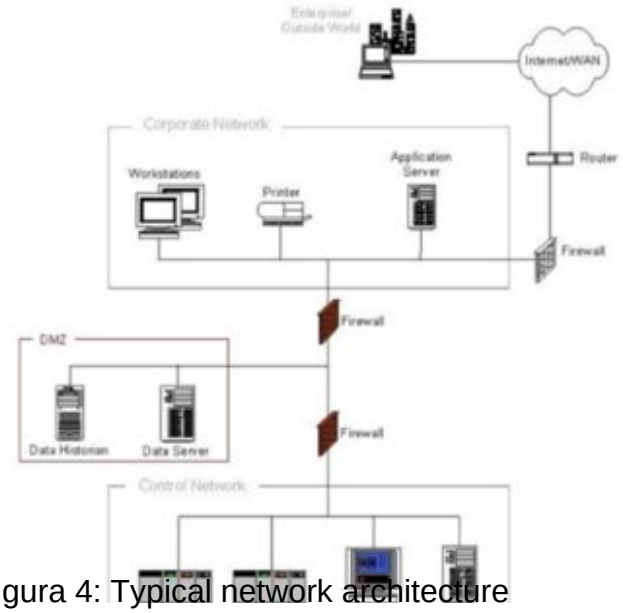
Figura 2: Information System Levels

I sistemi di controllo industriale, i sistemi navali operativi e l’avionica hanno in sostanza le medesime caratteristiche che troviamo sintetizzate nella colonna a destra della figura 3 (*OT Systems*), caratteristiche che sono messe a confronto con il classico IT[5]:

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

Figura 3: IT vs OT

Il mondo industriale ci insegna a delimitare e separare correttamente i diversi livelli dei sistemi, in modo da evitare che eventuali "contaminazioni" riescano a propagarsi all'interno dei livelli più critici. Una classica soluzione architetturale per la separazione dei sistemi *"mission critical"* da quelli tradizionali, prevede l'architettura di rete[6] mostrata a sinistra qua sotto e, se la compariamo con quella di destra, che è suggerita per il mondo navale[7], ci accorgiamo che l'approccio è il medesimo, basato sul separare e proteggere adeguatamente la parte OT da quella dei sistemi di *support* alla missione e da tutto il resto del mondo:



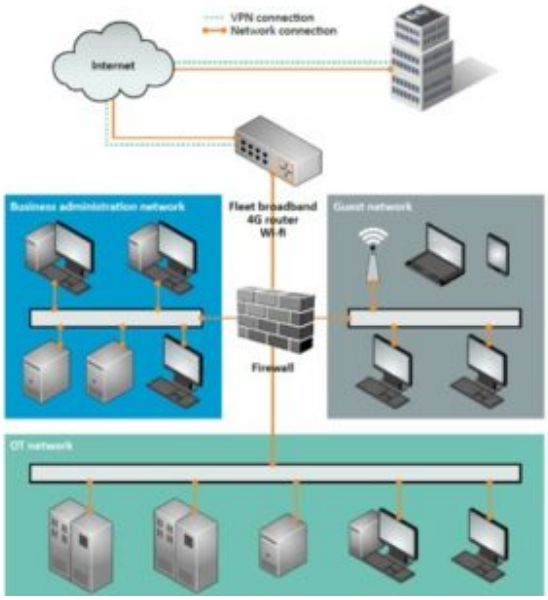
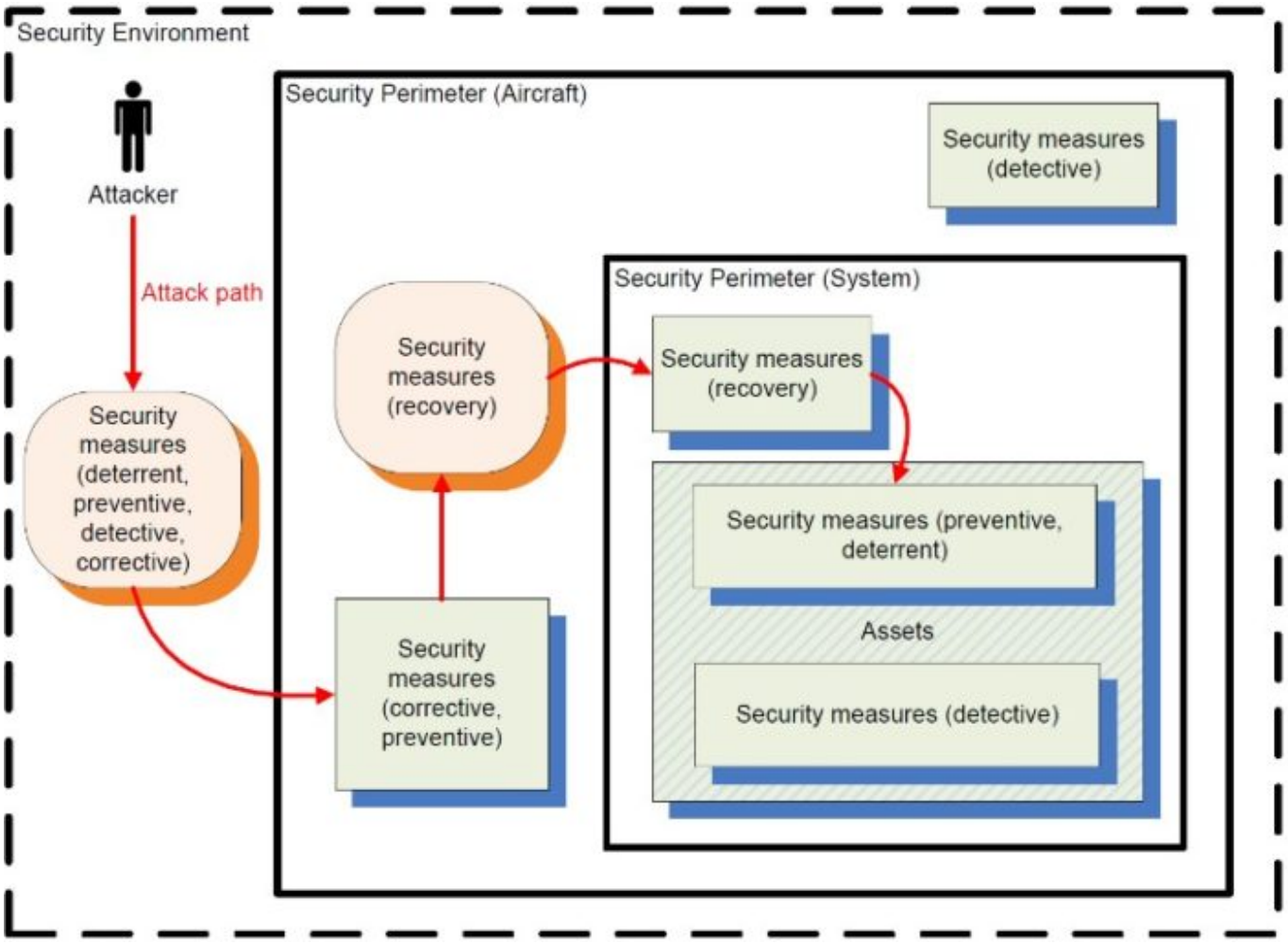


Figura 4: Typical network architecture

Analogamente i rischi cyber, sia per i sistemi industriali, sia navali e avionici, dovrebbero essere valutati e gestiti delimitando i diversi perimetri[8], in particolare i sistemi critici, da quelli di supporto e poi dal resto del mondo, in modo da identificare efficacemente per ogni livello:

- minacce;
- *Attack Paths;*
- superfici di attacco;
- misure di contenimento dell’attacco e *recovery.*



La ED202A per la sicurezza dell'aeronavigabilità, facendo propri i principi della ISO/IEC27001, ha suddiviso l'ambiente d'analisi in 3 elementi (analizzabile su più livelli, dal velivolo al singolo componente di un sottosistema):

- l'Asset critico (in base al punto di vista dell'analisi può essere anche il velivolo intero o un sistema/ sottosistema) a rischio *Security;*
- il *Security perimeter*, che è l'insieme degli elementi che compongono l'Asset Critico, e di conseguenza le interfacce esposte all'*Environment* esterno;
- l'*Environment* esterno, ovvero gli attori e i sistemi che possono (autorizzati o meno) interagire con il nostro asset tramite le interfacce presenti.

Un siffatto approccio permette di identificare in modo preciso, per ogni livello del perimetro, quali siano gli asset (fisici e logici) a maggiore criticità e vulnerabilità ad attacchi intenzionali o *malware*, gli effetti dell'attacco in termini di *security* e conseguentemente associare tali effetti ai requisiti di *safety*. Analizzando il contesto a cerchi concentrici si ha inoltre la possibilità di verificare e confrontare, sia *bottom-up* sia *top-down,* gli *"Attack paths"* e le potenziali conseguenze in termini di *safety*, disegnando così i possibili *"Security Scenario affecting the Safety"*.

Benché in presenza di mondi diversi, è chiaro quindi che aria e mare possono sfruttare le

esistenti *Best Practice* di terra (*Industrial*) al fine di contrastare i *Cyber Risks* e garantire la necessaria *Safety;* e il mondo *Industrial* può anch'esso attingere alle norme e pratiche di altri mondi tecnologici per migliorare la capacità di analizzare i rischi e la sua capacità difensiva dai *Cyber attacks*. Vediamo quindi, in una semplice matrice, come le norme esistenti nel mondo dell'*Information security* e nel mondo dell'*Industrial security* possano essere di aiuto e complementari alle norme di settore, sia nel campo aeronautico[9] e sia navale.

Perimetro	**Aeronautico**	**Navale**
OT	ISA 62443 / NISP SP800-82	ISA 62443 / NISP SP800-82
Support Systems	ISA 62443 / NISP SP800-82	ISA 62443 / NISP SP800-82
IT trusted/Authorized systems		