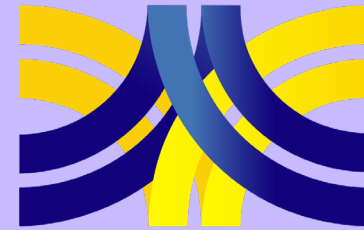


# 49<sup>th</sup> ASECAP DAYS

*Decarbonizing Road Infrastructure : Challenges,  
Perspectives and Actions in Tough Economy*

**ASECAP DAYS**



**BRUSSELS 2022**



Hotel Marriott Grand Place, Brussels  
24 – 25 November 2022



***ASECAP DAYS***



**BRUSSELS 2022**

# A Cybersecurity Strategy For the Motorway Operators

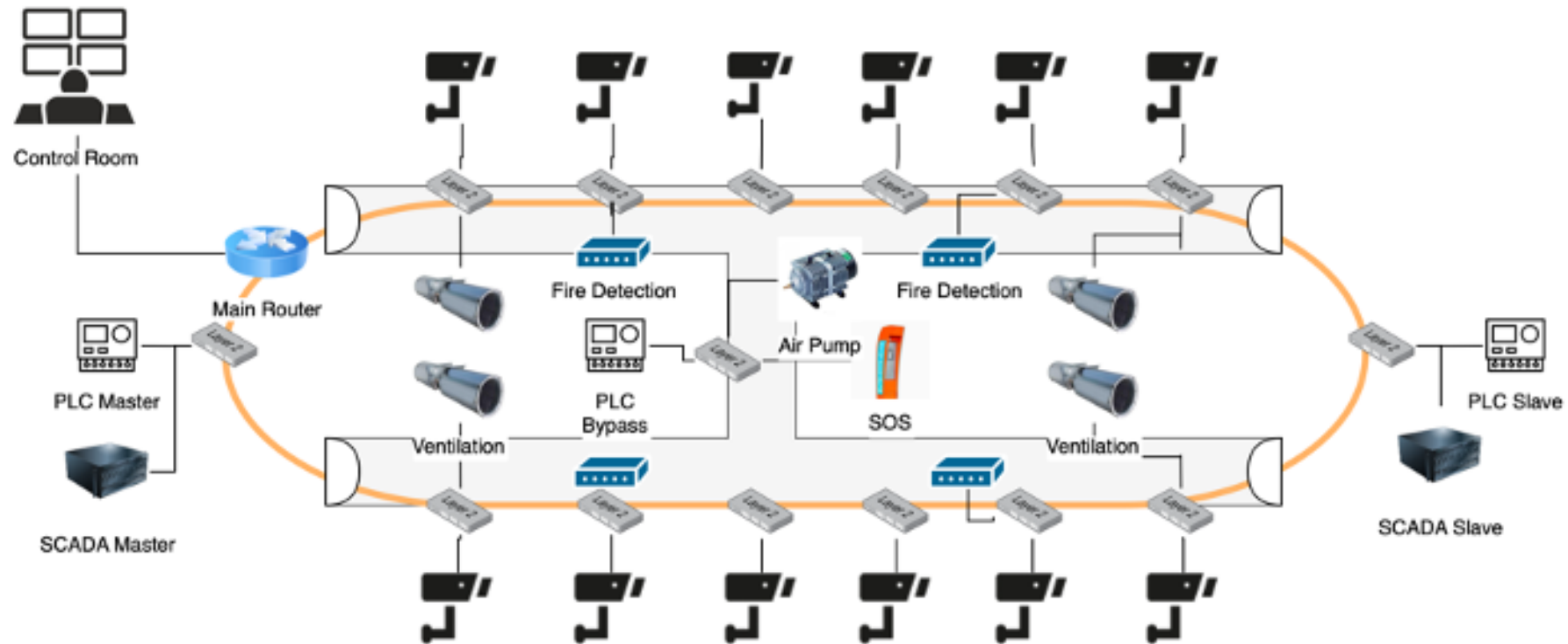
Massimiliano Masi  
Autostrade Per L'Italia

Logo

# Cybersecurity for a Motorway Operator

- Cybersecurity is an important issue, in terms of Availability, Integrity, Confidentiality
- Threat Landscape: are we specific?
- IT/OT/IoT: different cybersecurity, domains, or *zones*. C-ITS, Tunnels, Electronic Fee Collection, Sensors Actuators, Vehicles as sensors
- NISv1 categorizes road transport as essential service (Annex 2, 2(d)). Updated recently
- *Cybersecurity is a scarce resource. We shall cooperate.*

# A Tunnel Use Case



- A cyber attack could result in injuries or death
- No norm exists
- No typical IT Security

# Operators are all interconnected

- Interpol, ENISA, raised the need to perform multi sector assessments to evaluate the posture as a entire sector
- Services, SRTI, RTTI, Traffic Regulations, are shared between motorway operators
- A security incident could stem in a motorway operator and move laterally to others, even in different domain: **cascading effects.**

- **Regulate ourselves before someone will regulate us**
- Need for an harmonization of the field
- Abide to common concepts such as:
  - Risk assessment methodologies
  - Common vocabulary for cybersecurity incidents
  - Common practice for incident response
  - ISAC
  - Cyber Ranges
- Cooperate with ENISA in defining the threat landscape

# Governance models

- ISO 27001 is not enough: we have Industrial Automation and Control Systems
- IEC 62443 is the de-facto norm for Cybersecurity Management Systems, technical, and supply chain aspects
- Too broad: we lose specificity
- ***Engage the SDOs for a new work item!***

# And others?

## IEC 62443 in other verticals

**IEC TR 60601-4-5**  
Edition 1.0 2021-01

**TECHNICAL REPORT**

---

**IEC ISO 81001-5-1**  
Edition 1.0 2021-12

**INTERNATIONAL STANDARD**  
**NORME INTERNATIONALE**

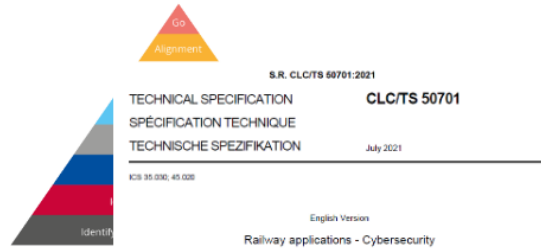
**MEDICAL DEVICES**

Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle  
Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé – Partie 5-1: Sécurité – Activités du cycle de vie du produit



ZONING AND CONDUITS

Figure 1 Zoning and conduit methodology



**RAILWAY SYSTEMS**

The overall process for CLC/TS 60701:2021 is split for easier explanation

The Technical Specification was approved by CENELEC on 2021-06-11.

CENELEC members are required to announce the endorsement of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

**E26 Cyber resilience of ships**  
(Apr 2022)

1. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

---

**E27 Cyber resilience of on-board systems and equipment**  
(Apr 2022)

1. General

1.1 Introduction

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stages. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

The document specifies unified requirements for cyber resilience of on-board systems and equipment.

1.2 Limitations

The UR does not cover environmental performance for the system hardware and the functionality of the software. The URs shall be applied:

- UR E10 for environmental performance for the system hardware
- UR E22 for safety of equipment for the functionality of the software

1.3 Scope

The requirements specified in this UR are applicable to computer based systems as defined in UR E26.

Navigation and radiocommunication systems may follow IEC 61162-460 instead of the requirements in this UR. See IACS UR E26 section 1.3.

Note:

- This Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024 and may be used for other ships as non-mandatory guidance. In order to allow sufficient time for non-mandatory pilot application of this UR, the application date of 1 January 2024 has been selected.
- The 'contracted for construction' date means the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. For further details regarding the date of 'contract for construction', refer to IACS Procedural Requirement (PR) No. 29.

**SHIPS**  
**SHIP COMPONENTS**

News and Press Releases / ISASecure Announces ISA/IEC 62443 IIoT Component Security Assurance (ICSA) Certification Launch

### ISASecure Announces ISA/IEC 62443 IIoT Component Security Assurance (ICSA) Certification Launch

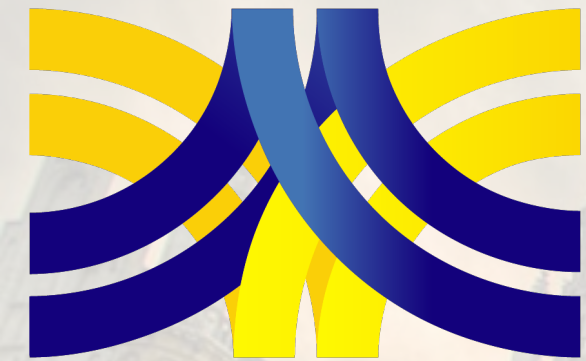
September 01, 2022 | Location: North Carolina

## INDUSTRIAL IOT DEVICES

The ISASecure program is announcing the new ISASecure certification offering for industrial internet of things (IIoT) components based on the ISA/IEC 62443 series of standards.



**ASECAP DAYS**



**BRUSSELS 2022**

**THANK YOU FOR  
YOUR ATTENTION**

Massimiliano Masi <[mmasi@autostrade.it](mailto:mmasi@autostrade.it)>