CYBERSECURITY

SYSTRA

Resilient transport infrastructure
No trust without cybersecurity

PROTECT YOUR ESSENTIAL SERVICES

Transport systems are complex, highly interconnected and the impact of a cybersecurity attack is potentially major at operational, safety, reputational and financial levels.

For brownfield projects, it is up to the transport authorities and operators to identify existing assets, assess the risks (e.g. safety critical incident, loss of operations control, data leak...), then put in place organisational and technical measures to mitigate them. Main challenges are:

- Wide geographic distribution of assets along the railway line;
- Increasing mix of legacy systems (e.g. bespoke stand-alone systems) with new connected technologies (e.g. standardised COTS, open-source platforms, remotely accessible ICS and other IoT);
- Tough patch management and protection of outdated components due to systems warranty conditions;
- Eligibility to both cybersecurity and safety requirements.

For the construction of new lines, it is a matter of integrating cybersecurity issues into design and conception choices and setting up processes to adapt systems to the changing threat.

Cybersecurity becomes essential to deliver more connected and resilient transport services. Many transport infrastructures are considered as critical by national authorities, and submitted to security regulations such as NIS Directive in Europe or LPM in France.

SECURITY LEVEL TARGET

IEC 62443 standard "Security for Industrial Automation and Control Systems" defines four Security Levels.

SL1 ($)

Relevant protection against opportunistic threats

› *as a minimum*

SL2 ($$)

Relevant protection against hackers & cybercriminals

› *recommended for non-critical systems*

SL3 ($$$)

Relevant protection against hacktivist & terrorist organisations

› *recommended for critical systems with potential impacts on operations*

SL4 ($$$$)

Relevant protection against most Advanced Persistent Threats and governmental organisations

› *recommended for critical systems with potential impacts on safety*

Railway infrastructure managers and operators are quite vulnerable to cyber threats: governance and protection measures are partly implemented whereas detection and response measures are rarely implemented.

Majority of known cyberattacks on railway systems are opportunistic, but logging and detection means are lacking to investigate this further.

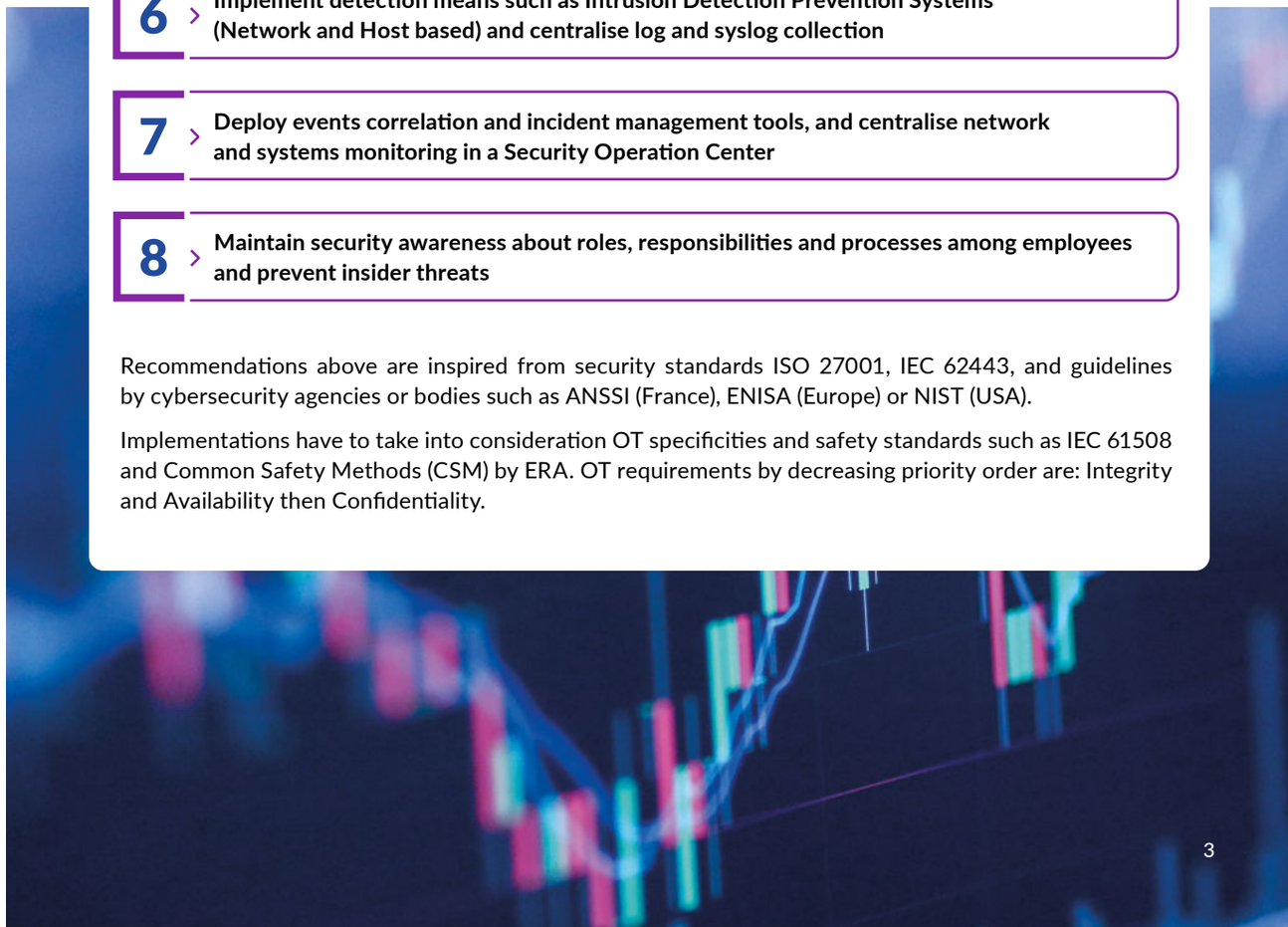
Finally railway infrastructure managers and operators remain vulnerable to Advanced Persistent Threats (APT) which would decide to specifically target Operational Technologies (OT).

RECOMMENDATIONS IN A NUTSHELL

1. Map assets and identify critical targets according to impact assessment
2. Investigate threats, vulnerabilities and evaluate likelihood of threat scenarios
3. Harden and patch systems configuration, enforce zone segmentation and perimeter protection with firewalls, gateways or data diodes
4. Apply resilience mechanisms from IT (such as backup and recovery strategies) to OT and legacy systems, or define organisational countermeasures
5. Strenghten and unify physical and logical access control following a role based approach (RBAC) and the least priviledge principle
6. Implement detection means such as Intrusion Detection Prevention Systems (Network and Host based) and centralise log and syslog collection
7. Deploy events correlation and incident management tools, and centralise network and systems monitoring in a Security Operation Center
8. Maintain security awareness about roles, responsibilities and processes among employees and prevent insider threats

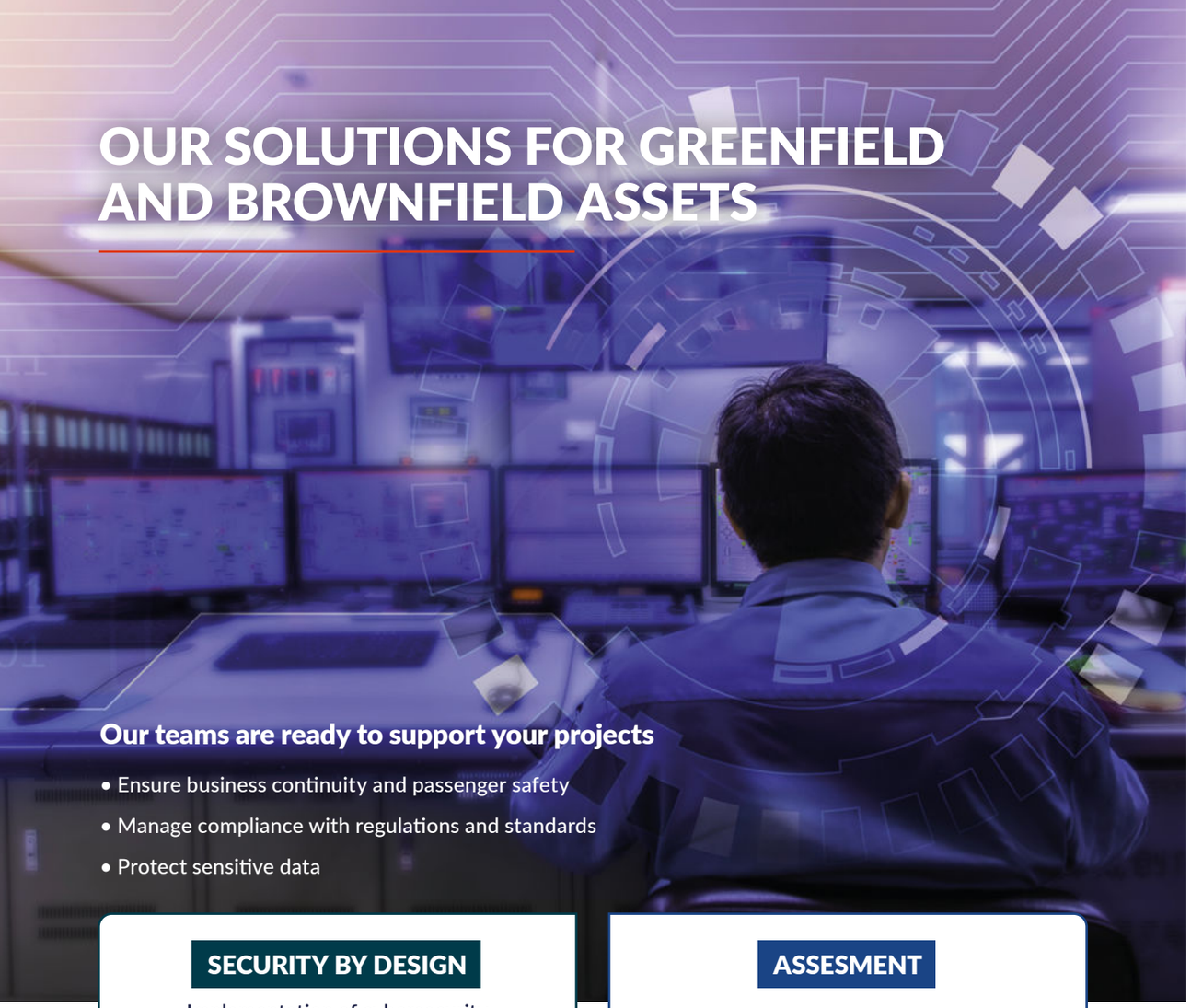
Recommendations above are inspired from security standards ISO 27001, IEC 62443, and guidelines by cybersecurity agencies or bodies such as ANSSI (France), ENISA (Europe) or NIST (USA).

Implementations have to take into consideration OT specificities and safety standards such as IEC 61508 and Common Safety Methods (CSM) by ERA. OT requirements by decreasing priority order are: Integrity and Availability then Confidentiality.



ENSURE BUSINESS CONTINUITY AND SAFETY

OUR SOLUTIONS FOR GREENFIELD AND BROWNFIELD ASSETS



Our teams are ready to support your projects

- Ensure business continuity and passenger safety
- Manage compliance with regulations and standards
- Protect sensitive data

SECURITY BY DESIGN

Implementation of cybersecurity across the project lifecycle and into the supply chain

METHODOLOGICAL FRAMEWORK
REQUIREMENTS
HOMOLOGATION

ASSESMENT

Security assessment and definition of security recommendations

MAPPING
CONFORMITY
VULNERABILITIES

GOVERNANCE

Advisory and support at organisational and strategical level

SECURITY POLICIES
AWARENESS
ROADMAP

SOLUTIONS

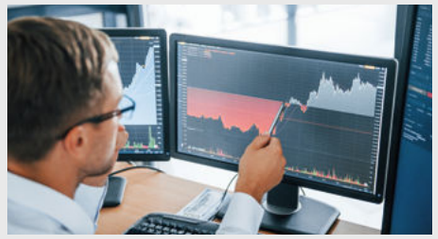
Advisory and support at technical and technological level

STUDIES
TESTS
IMPLEMENTATION

SYSTRA'S ADDED VALUE

- Knowledge of transport systems including telecom, command-control, signalling, auxiliary systems and passenger services
- Expertise in cybersecurity for OT (Operational Technologies)
- Ability to address both security and safety
- Knowledge of standards and guidelines specific to the cybersecurity of railway systems
- Participation in CENELEC and UITP working groups about cybersecurity of rail transport infrastructures

ZOOM: AGILE RISK MANAGEMENT



Decision making requires having a clear overview on priorities being supported by an incremental risk management process.

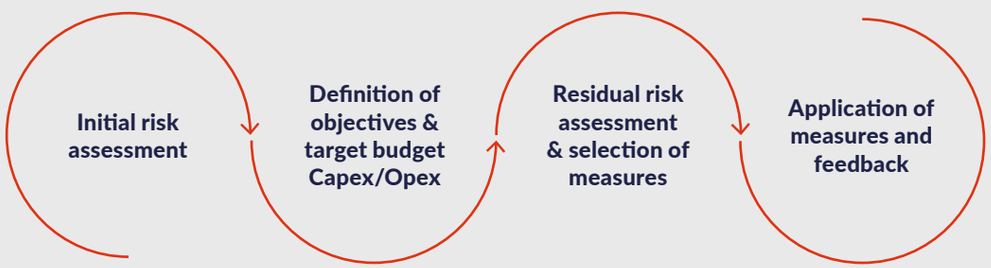
The EBIOS Risk Management methodology by ANSSI (compliant with ISO 27005) promotes a dynamic and threat centric approach, paying attention to the analysis of threat scenarios at strategic and operational levels.

Risk scoring has to take into account impacts (operational, safety, financial) and threat likelihood.

Likelihood of threat scenarios can be computed according to the analysis of past cyberattacks and upcoming threats.

New security exploits are made public every month revealing new weaknesses in transport systems and infrastructures. They can be packaged in order to simplify or industrialise their use.

As technological changes continuously arise (e.g. 5G, FRMCS, Cloud, IoT, etc.) with significant impacts on the vulnerability exposure, security measures shall be adapted as quickly as possible.



OUR ECOSYSTEM

OUR MAIN REFERENCES

STAKEHOLDERS MAPPING AND MINIMUM-SECURITY MEASURES IN THE RAIL SECTOR

CLIENT: **ENISA** (European cybersecurity agency), Europe

Under the framework contract “Supporting cybersecurity for transport sector activities - Lot 2 - cybersecurity for the railway sector", SYSTRA carried out a study, a survey and interviews to assist ENISA to evaluate the NIS Directive implementation in the rail transport sector. SYSTRA has supported ENISA in the following tasks:

- Analysis of standards and existing regulations (e.g. ISO 27001/2, IEC 62443, draft TS 50701, DIN VDE 831-104, NIST CSF, NIST 800-82, APTA, ANSSI ICS guidelines, NIS Directive, LPM)
- Review of predefined security measures applicable to railway systems
- A survey targeting railway infrastructure managers and operators
- Drafting report, summary report and press-release

ENCRYPTION OF GROUND-BOARD RADIO COMMUNICATIONS

CLIENT: **Transport operator**, USA

SYSTRA designs and implements a One Time Password framework for the PTC radio communication. SYSTRA carried out the following tasks:

- Data collection and mapping of information systems
- Data analysis, identification of vulnerabilities and risk analysis
- Definition of recommendations and a roadmap
- Feedback of results to operational and management teams for implementation

SECURITY ASSESSMENT OF METRO SYSTEMS

CLIENT: **Transport operator**, Africa

SYSTRA supported the client in the following tasks:

- Security assessment planning and preparation
- Data collection and IS mapping
- Vulnerability mapping and analysis
- Short risk analysis
- Definition of security recommendations and roadmap
- Reporting to management and operational teams

SECURITY BY DESIGN OF METRO SYSTEMS

CLIENT: **Project owner**, France

SYSTRA carries out the following tasks:

- IS mapping
- Analysis of the architecture and identification of critical systems
- Project management and follow-up of cyber related activities
- Upgrade of cyber requirements according to national regulations
- Participation to risk analysis with systems suppliers
- Conformity control to cybersecurity requirements
- Preparation of homologation files
- Implementation of cybersecurity governance

SECURITY ASSESSMENT OF TRAMWAY SYSTEMS

CLIENT: **Transport operator**, France

SYSTRA provides consultancy services and carries out the following tasks:

- Data collection and interviews
- Security assessment preparation and planning
- IS mapping
- Conformity analysis according to NIST 800-53 (CMMC)
- Analysis of systems architecture
- Analysis of assets configuration (Firewall, VPN, Microsoft, Linux Infrastructure)
- Risk analysis
- Definition of roadmap
- Reporting to management and operational teams

www.systra.com
systems@systra.com

SYSTRA

SYSTRA Australia
Level 15 - Chifley Tower
2 Chifley Square
Sydney NSW 2000
AUSTRALIA

SYSTRA France
72-76, rue Henry Farman
75015 Paris - FRANCE
Tél. : +33 (0)1 40 16 61 00

SYSTRA Singapore
333 North Bridge Road
#05-01 KH KEA
Singapore 188721
SINGAPORE

SYSTRA UAE
Al Masraf Tower
Dubai
UNITED ARAB EMIRATES

SYSTRA UK & Ireland
1 Carey Lane
London EC2V 8AE
UNITED KINGDOM

SYSTRA USA
New York Headquarters
520 Eighth Avenue, Suite 2100
New York, NY 10018 - USA

CONFIDENCE MOVES THE WORLD