INTERNATIONAL RAILWAY SAFETY COUNCIL 2022

IRSC Spain

# IRSC 2022

## INTERNATIONAL RAILWAY SAFETY COUNCIL

**SEVILLA, OCTOBER 16-21, 2022**

adif ALTA VELOCIDAD | adif

EUROPEAN UNION AGENCY FOR RAILWAYS

AESF AGENCIA ESTATAL DE SEGURIDAD FERROVIARIA

adif

# OT/IT Convergence

## Challenges in Cybersecurity

IRSC Spain

**IRSC 2022**

INTERNATIONAL RAILWAY SAFETY COUNCIL

SEVILLA, OCTOBER 16-21, 2022

EUROPEAN UNION AGENCY FOR RAILWAYS

AESF AGENCIA ESTATAL DE SEGURIDAD FERROVIARIA

adif

adif ALTA VELOCIDAD | adif

# INDEX

# CHARACTERISTICS OF THE IT/OT ENVIRONMENT - THE STARTING POINT

# Characteristics of the IT/OT Environment.

RISK MANAGEMENT

From VUCA to BANI

EXTERNAL CONTEXT

DIGITAL TRANSFORMATION

- Agility
- Automation
- Data Driven
- Customer Orientation
- Response to Change
- Digital Culture

## IT

Systems and networks that **manage data** as well as the **information lifecycle**

## OT

Systems and networks that **monitor and control** physical devices under **continuous operation and non-optimal conditions.**

MANAGEMENT MODELS

**IT**

- Common governance.
- Standard systems.
- Decisions are made based on data.
- Arises from the need to generate, process, transmit and store information.

**OT**

- Organization in silos.
- Proprietary systems.
- Isolated systems.
- Arises from the need to control the quality of industrial processes.

BUSINESS CONTEXT

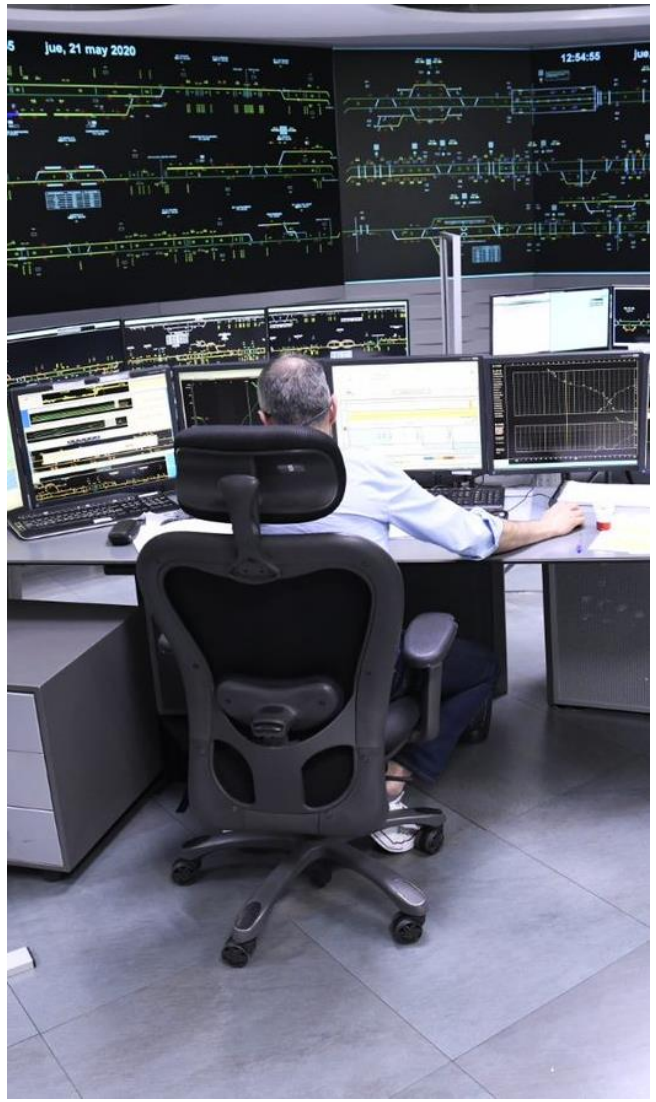
CYBERSECURITY CULTURE

**IT**

- Leadership based on software quality/security.
- Confidentiality.
- Integrity.
- Availability.
- High risk awareness.

**OT**

- Leadership that results in efficient management of incidents that influence operation.
- Availability
- Integrity
- Confidentiality
- Low risk awareness.




# Characteristics of the IT/OT Environment

PHYSICAL

THINGS

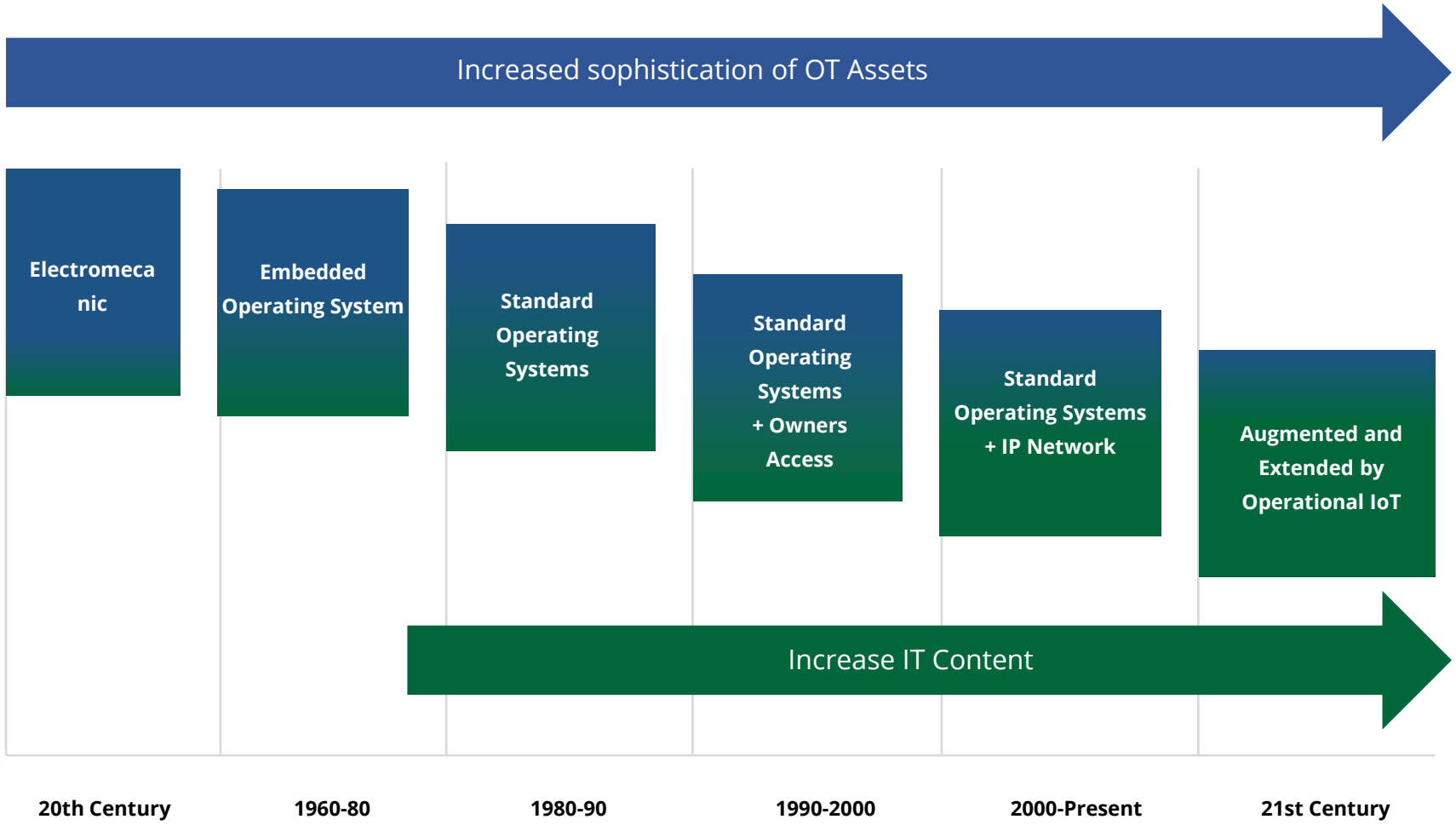
PEOPLE

BUSINESS

DIGITAL

# Characteristics of the IT/OT Environment

## OT Operational Systems

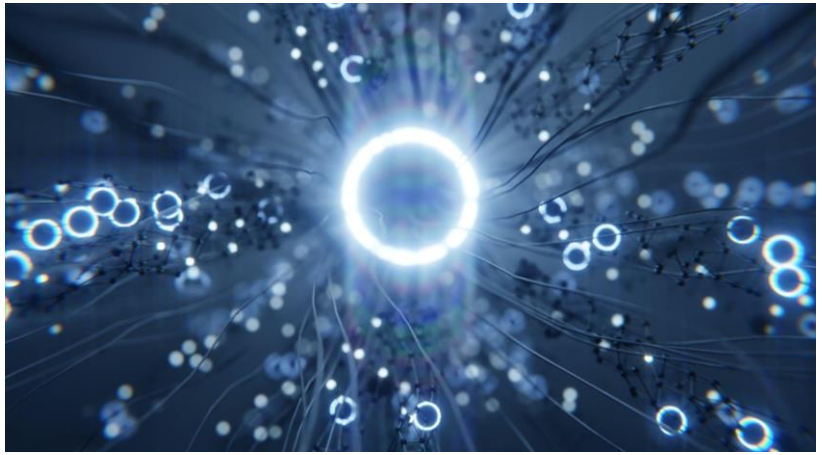


# COMPREHENSIVE IT/OT SECURITY

- A converge security Model is required
- OT must be part of the digital planning of the company
- Digital transformation and IoT increases the value of OT

# Comprehensive IT/OT Security

Must be **documented, secure, managed and recoverable.**



**Internally connected** with corporate IT platforms to support advanced analytics.

**Externally connected** to enable service management and remote support.

# Comprehensive IT/OT Security

- **The industry is experiencing its fourth revolution, known as Industry 4.0.** This is characterized by incorporating the latest advances in Information Technology (IT) into industrial engineering. Added to that, digitizing existing production and distribution models to achieve an intelligent, digitized and connected supply chain.
- Industry 4.0 is developed in a context of constant technological evolution for which a **cyber-resilient attitude must be adopted without hesitation.**
- **Cyber risks in OT are a reality.**

IT CYBERSECURITY + OT CYBERSECURITY = **TOTAL** CYBERSECURITY

The OT/IT convergence process needs to be addressed

# PROPOSED MODEL

Alignment

Integration

Governance

Trust

# Proposed Model

Alignment → Integration

### RISK MANAGEMENT

Aligning security policies, patching, contingency and updating environments

### CONSOLIDATION

Technological optimization that allows cost reduction avoiding duplication of hardware purchases, licenses, support and maintenance.

### AGILITY

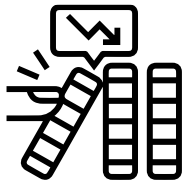
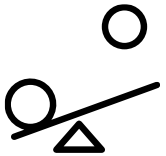
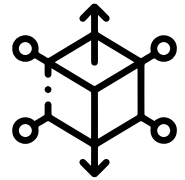
Aligned governance to use common processes, standards, and architectures

### OPTIMISATION

On the basis of integrated and governed OT/IT systems, new digital services adjusted to business requirements emerge.

**OT/IT CONVERGENCE MATURITY**

# Proposed Model

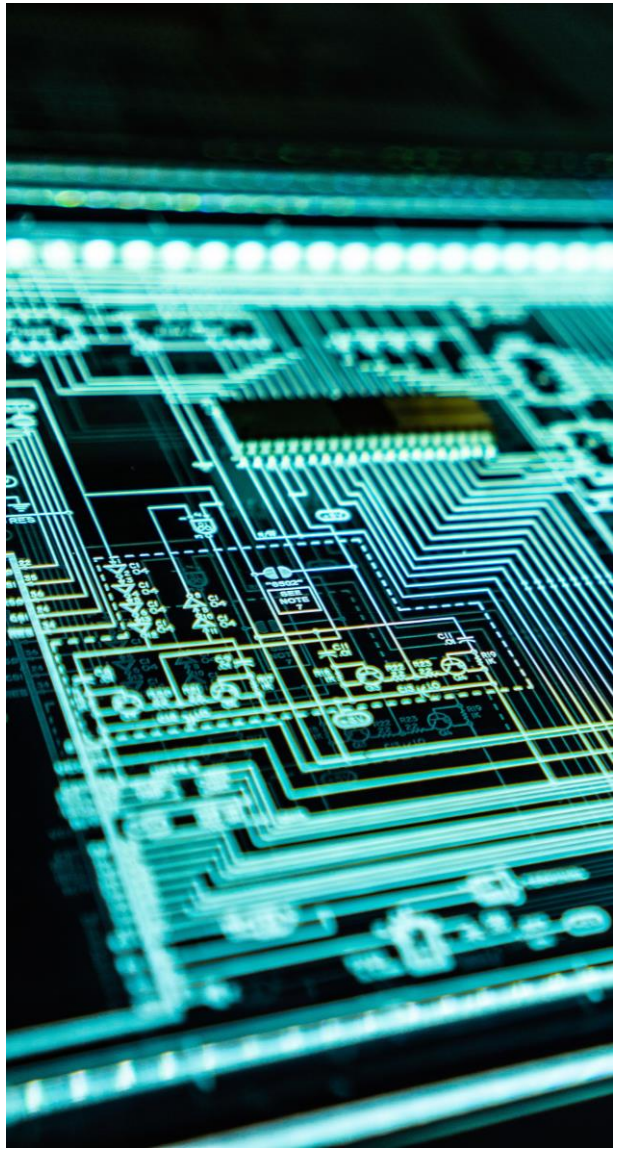
| WHERE | WHY | HOW | WHAT | WHO |
|---|---|---|---|---|
| Identify how convergence (OT that looks like IT) is happening in your business | Reaching a consensus that convergence means change in OT management | Align how you manage OT with how you manage IT | Integrate IT and OT systems and infrastructures | Reaching a consensus that convergence means change in OT management |
|  RESEARCH |  ESTABLISH THE FOUNDATIONS |  REDUCE RISKS |  LEVERAGE DATA |  TRANSFORM |

# CONVERGENCE CHALLENGES

IRSC Spain

**IRSC 2022**
INTERNATIONAL RAILWAY SAFETY COUNCIL
SEVILLA, OCTOBER 16-21, 2022

EUROPEAN UNION AGENCY FOR RAILWAYS
AESF AGENCIA ESTATAL DE SEGURIDAD FERROVIARIA
adif
adif ALTA VELOCIDAD | adif



# Convergence Challenges

Cultural change.
New form of leadership.

Expansion of the current verification processes in OT.

New risk management.

Budget for cybersecurity in OT environments.

Low culture in cybersecurity.

Lack of technical personnel specialized in operational and security environments.

A large influence from contractors in the management of the configuration

Absence of single OT technology governance.

Precise communications protocols and systems.

Outdated information systems (Windows XP, Windows 7, etc.).

Minimal flexibility in the evolution of systems (focused on operation and not on adaptation and evolution).

# Convergence Challenges

## IT culture:

Frequent change, shorter product and system lifespan, usability for the user/customer and importance of "the user experience"

**Solution approach:** Develop standards, evaluate requirements, build/purchase the best solution at the lowest cost, plan upgrades and support.

## OT culture:

Reliability and safety, fault tolerance, determination, consistency and longevity. Engineering culture

**Solution approach:** **O**ptimize repetitively to improve performance, and use. Block product.

# Conclussions

Modern operational environment (OT) systems are based on IT-derived infrastructures and systems, which increases the overlap of skills needed to manage both IT and OT. This justifies greater adoption of IT best practices in OT management.

*Thank you for your attention!*

INTERNATIONAL RAILWAY SAFETY COUNCIL 2022
IRSC Spain

adif ALTA VELOCIDAD | adif

www.irsc2022.com

EUROPEAN UNION AGENCY FOR RAILWAYS

AESF AGENCIA ESTATAL DE SEGURIDAD FERROVIARIA

adif