Open Digital Signalling

Czech Republic – Spain Railways Business Forum

Jose Miguel Rubio

21 May 2024

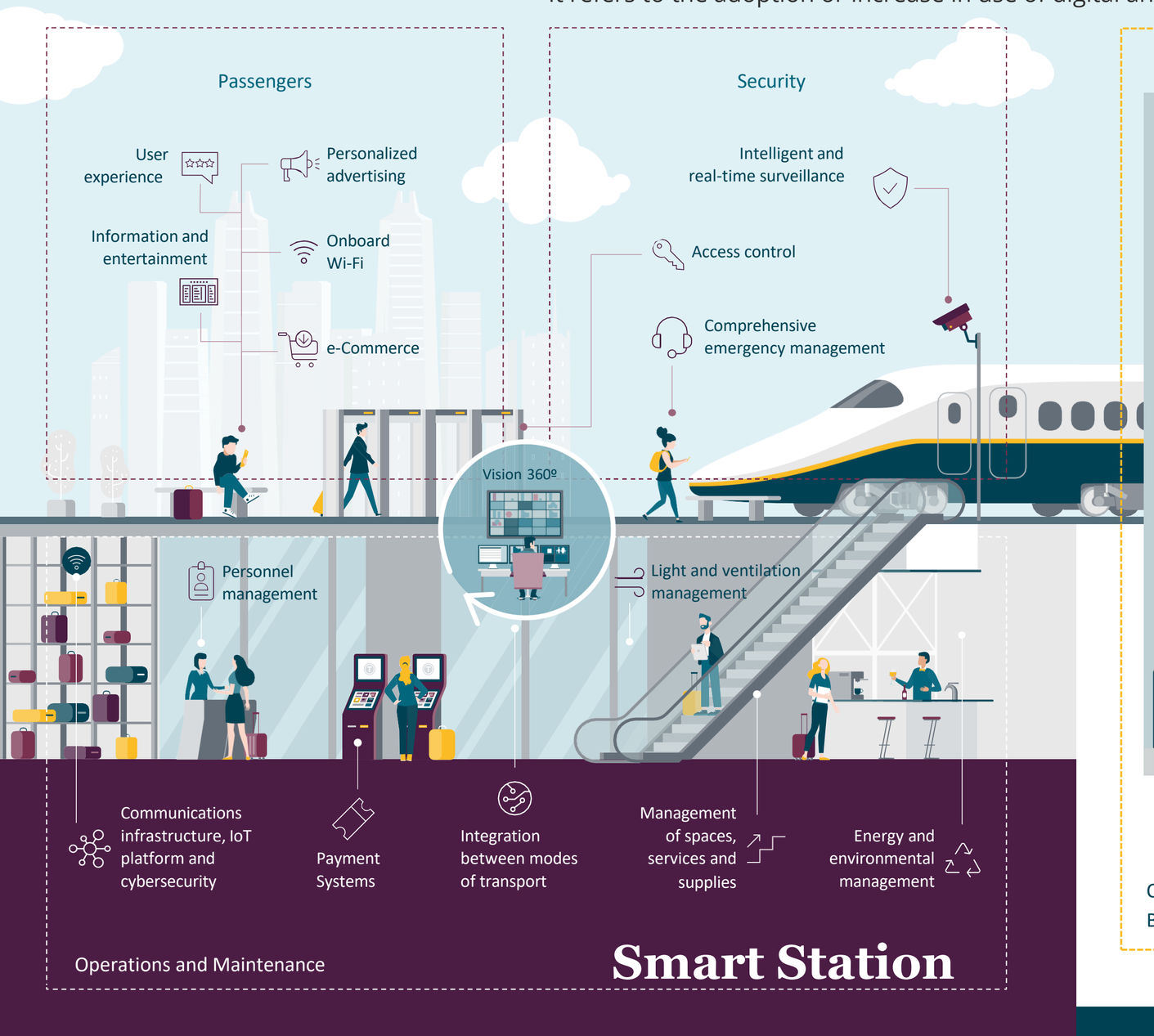
“Digitalisation is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities”

Gartner’s IT Glossary

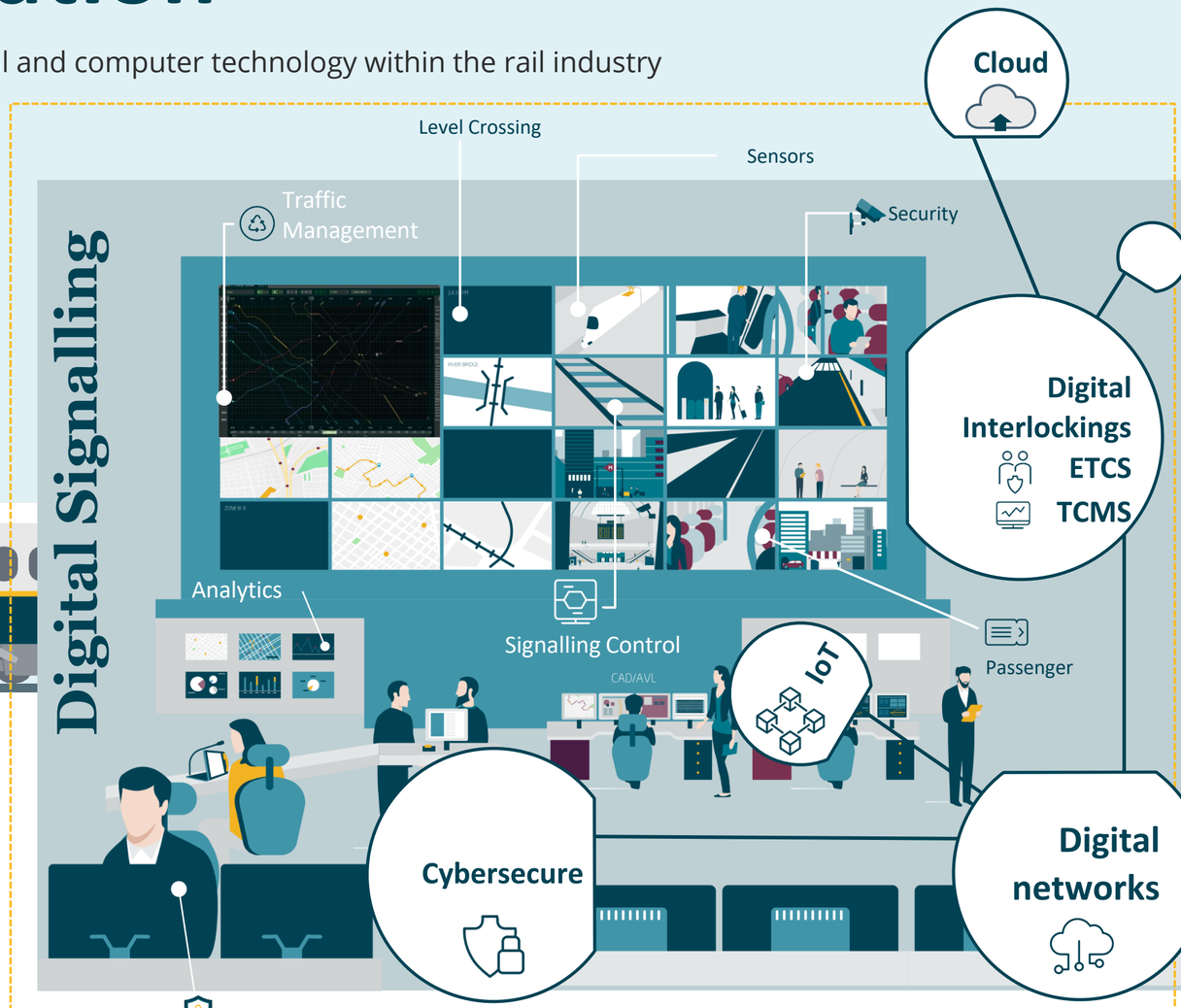
Digitalization

It refers to the adoption or increase in use of digital and computer technology within the rail industry

indra



Smart Station



Digital signalling is a technological disruption and relies on digital networks that enable the digital transmission of information

Cloud | IoT | 5G | IA | Big Data | Edge Computing | Business Intelligence | Business Analytics | Digital Twins | Deep Learning | Artificial Vision

Source: Indra

What do we require from an Open Digital Signalling solution?

1. **Digitalization must be addressed in all system layers**, from the Train Control and Management Systems to the trackside elements. Digitalization until the last mile.

2. **The interface between components must be open**, meaning public and standard, and this is where EULYNX takes its place. But the system of systems architecture must be ready for the real world, it must be ready to interact with non-digital or proprietary trackside elements and must allow us to interface with legacy and/or proprietary interface systems.

3. The architecture must be ready to incorporate non signalling assets, creating an **Internet of Things for railway infrastructure**

4. **ETCS is a must**. In-Cab signalling allowing greater safety, better punctuality and increase in performance.

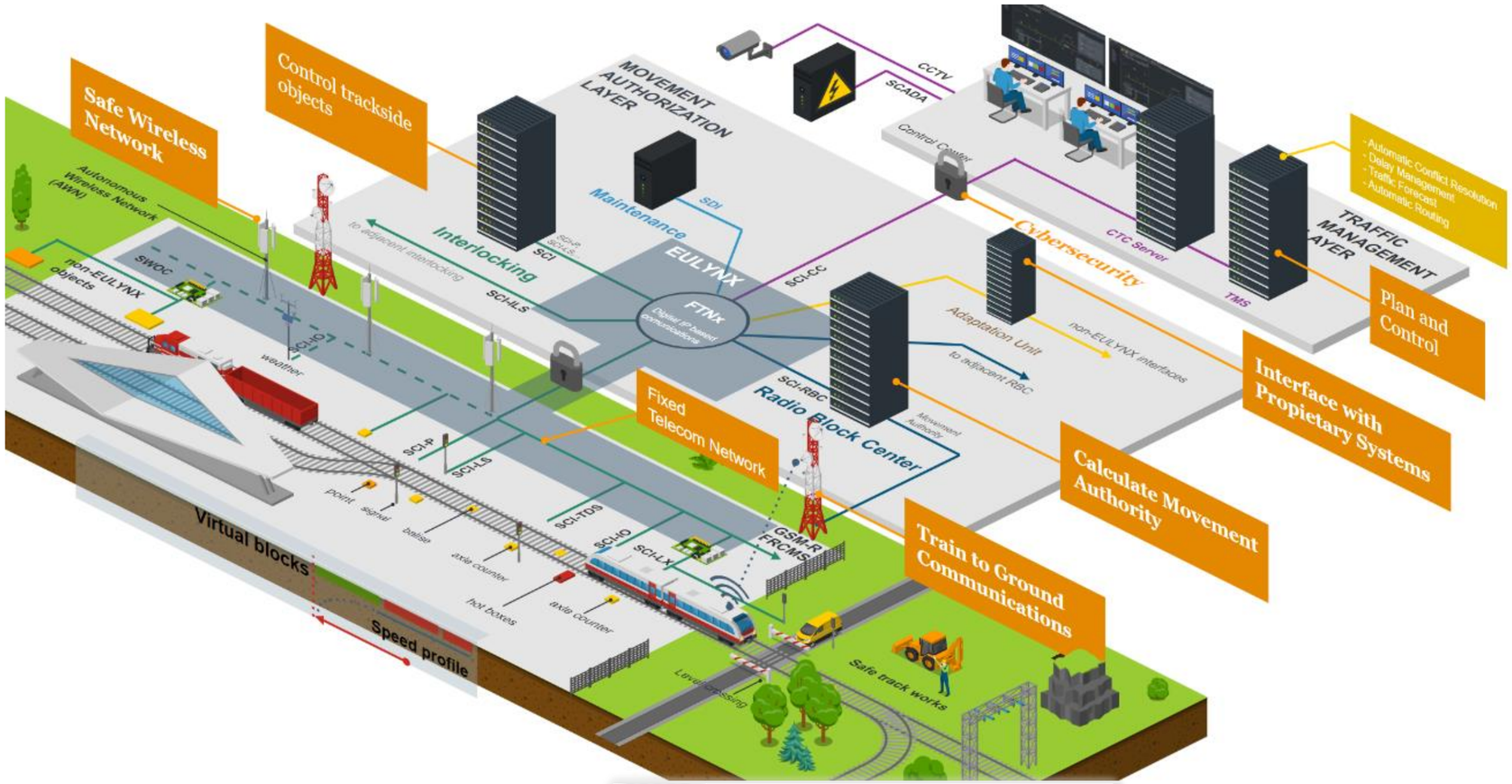
5. **Cybersecurity across the entire architecture.**

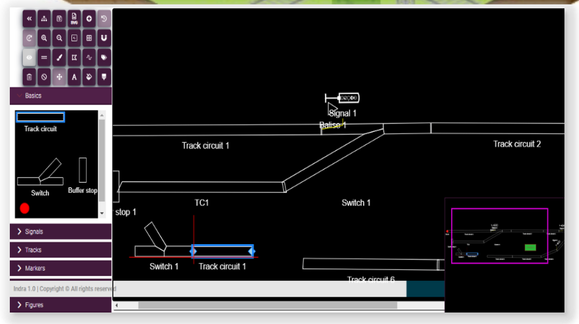
… safety first

Digital Signalling Architecture

1. **Autonomous Wireless Network**, connecting the last mile with safe wireless or wired mesh networks.
2. **Smart Wayside Object Controller**, providing **EULYNX** endpoint for legacy objects.
3. **Internet of Things for railway infrastructure**, using MQTT lightweight protocols
4. Integration with proprietary interface systems (RBC, Interlocking,...) providing **EULYNX** façade for them thanks to the **Adaptation Unit**.
5. Built-in Integration with ETCS and Traffic Management Systems
6. **Cybersecurity** by design.

while keeping safety first





Not only the system, also the design process

Illustration created with Icograms.com

Cybersecurity

1. The **Network Information Security** (NIS) Directive was the first EU-wide legislation to cover cybersecurity in rail

2. **ENISA report on rail cybersecurity** defines different cyber risk scenarios

3. Compliance with NIS includes:

- Securing network and information systems by taking technical and organisational measures appropriate to the risk.
- Ensuring service continuity by taking appropriate measures to prevent and minimise the impact of any cyber security incidents.
- Notifying the regulator of any cyber security incident that has a significant impact/effect on the public.

Some cyber risks for railways

Compromise Signalling systems

1. An attacker gathers information (physical trespassing, malicious employee, phishing).
2. The attacker builds a device or software to command-and-control junctions and trains.
3. The attacker takes control of the junctions and trains.
4. False signaling information is injected and leads to a major disruption or a train accident.

Sabotage of Traffic Management

1. An ICS malware is introduced into the IS (phishing, removable device).
2. The ICS malware propagates itself to the OT systems.
3. The attacker obtains remote access to traffic supervision systems.
4. The attacker disrupts traffic supervision systems which results in an emergency train traffic interruption.

Ransomware attack

1. An attacker infiltrates the IS via credential theft.
2. The attacker identifies vulnerable systems of the IS.
3. The attacker takes control of a large number of the IS components.
4. Ransomware is deployed and executed on the compromised systems.

5. Data of the compromised systems is encrypted which makes them unusable.
6. The attacker demands a ransom in exchange for data recovery.

Destroy datacentre

1. A physical event occurs and affects the datacenter.
2. Permanent physical damage affects the datacenter IT systems and the backups.
3. IT-related activities are disrupted. Recovery requires more time due to the destruction of backups.

Theft of personal data

1. An attacker steals the credentials of one of the booking management system administrators via phishing.
2. The attacker obtains privileged access over the booking management system.
3. The attacker downloads the clients' personal data and proceeds to leak or sell it.

Leak of sensitive data

1. A publicly exposed and unprotected database is found by an attacker.
2. The content of the database is exfiltrated (email addresses, date of birth, etc.).
3. Social engineering attacks targeting the stollen data owners are performed by the attacker.

DDoS Attack

1. An attacker creates a botnet to launch a DDoS attack against the target's internet exposed-devices.
2. The targeted devices are unable to handle incoming requests which results in their shutdown.
3. Passengers are unable to book tickets due the unavailability of the internet-exposed devices.

Source: ENISA. Railway cybersecurity

Cybersecurity is the technology, measure or practice of protecting electronic systems, devices, networks, software and data from malicious attacks.


indra
At the core