# SAFETY4RAILS Final Conference

The SAFETY4RAILS project Stephen Crabbe, Fraunhofer EMI, Coordinator of the project





The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883532.

# **Project overview**





\* Image informed by Department of Communications, Climate Action & Environment, NIS Compliance Guidelines for Operators of Essential Service (OES), August 2019, p.8 and p.22.

- EU H2O2O project, 24 months, start 01/10/2020, 31 partners, incl. 8 end-user organisations
- Increase security and resilience of railway and metro infrastructures to combined cyber physical threats including natural hazards

Objectives: capabilities to support the characteristics of resilient systems



\* SAFETY4RAILS, Grant Agreement, Annex1 Description of Action, Part B, p.32

Consortium



EGO ERARGE TCDD

MTRS

End-users in project:

UREAD UNEW INNO

MdM RMIT ETRA TREE UMH FGC

PRO CEIS EOS

Railways: PRORAIL (NL), RFI (IT), FGC (ES), TCDD (TK) and UIC (worldwide association



# Project inputs / outputs highlighted





#### Inputs: 18 tools (most around TRL 5-6)

\*"SAFETY4RAILS puzzle" SAFETY4RAILS, Grant Agreement, Annex1 Description of Action, Part B, p.31. \* Update in D1.4 Specification of the overall technical architecture, p. 88.

#### **Outputs: Combination and Extension**

- Increase of Technology Readiness Levels (TRLs) of individual input tools
- SAFETY4RAILS Information System (S4RIS) platform
  - Communication between "relevant" tools
  - Increase overall quality of data and insights
  - Decision Support Platform incl. crisis management
  - Scope: "Smart City" concept
- 4 pilots for testing and user validation: MdM Madrid, EGO Ankara, RFI Rome, CdM Milan. (S4RIS at TRL7)
- Identification of further security and resilience research and innovation gaps for addressing in the future

•

### Layered S4RIS Architecture





S4RIS Concept System Architecture Diagram - informed by D2.3 System specifications and concept architecture

## S4RIS platform and contributory tools



\* Resilience cycle image informed by Department of Communications, Climate Action & Environment, NIS Compliance Guidelines for Operators of Essential Service (OES), August 2019, p.8 and p.22.



# **Previous Simulation Exercises (SEs)**



#### Madrid (Metro de Madrid) - February 2022

Combined cyber-physical attack at a metro station close to a stadium after a large sporting event.

#### Ankara (EGO and TCDD ) - May 2022

Series of cyber-attacks and physical attacks targeting sensitives devices and sensors.

#### Rome (RFI) – June 2022

Physical attack – potential terrorist attack via Improvised Explosive Device (IED) carried via baggage and by a terrorist using firearms inside a railway station.

#### Milan (CDM) July 2022

Natural disaster – flooding scenario.

Provided a body of results used as input into today's demo which is <u>not</u> based on a specific location in order to enable a Public event.

# Summary DEMO scenario



#### **PREVENTION (identification and protection)**

Capabilities of 4 tools <u>not directly</u> connected with scenario used for following phases: modelled rail network risk assessment, modelling of crowds, effects of blasts, open source intelligence on CCTV vulnerability.

#### DETECTION

Capabilities of 7 tools based on terrorist attack: entering important room, denial of service attack to monitoring systems, planting of bomb, explosion, overcrowding on platform, panic on social media

#### RESPONSE

Capabilities of 3 tools: impact propagation in rail infrastructure and alternative mitigation measures, prediction of free capacity and time to surrounding stations.

#### RECOVERY

Capabilities of 1 tool: Budget and priorities for repairing/replacing damaged assets.

# **Demo today** - **Prevention** (Identification + Protection)



SAFETY4RAILS

## **DEMO today – Detection**



PRIGM SENSTATION	Point-to-point secure channel between IoT gateway (e.g. from sensors) and central system security, anomaly detection (TRL 6 at project start)
	Contribution: Breach of entry into an important room + sensor data anomaly detection, alerts to RAM2
GANIMEDE	Analysis of live and recorded data streams based on deep learning (TRL6 at project start)
	Contribution: Detection of unattended baggage, alerts to RAM <sup>2</sup>
CuriX	Time series data analysis anomaly detection for technical devices CuriX (IT, OT) (TRL4 at project start)
	Contribution: Detected signs of Denial of Service (DoS) attack on CCTV + explosion noise, alerts to RAM <sup>2</sup>
INGSPARK	Time series data analysis anomaly detection for train speed + overcrowding detection from CCTV images (TRL 3-4 at project start)
	Contribution: Detection of overcrowding on platforms, alerts to RAM <sup>2</sup>
OSINT	Open source intelligence platform (New module)
	Contribution: Social media alerts, alerts to RAM <sup>2</sup>
RAM <sup>2</sup>	Decision support tool, asset inventory visibility, collecting + correlating events, providing clear mitigation steps (TRL6 at project start)
	Contribution: Correlation of events providing users with insight into the overall attack and its progression and mitigation plans for each alert. Messages links to tools supporting Response.

"Postman tool" intended to be used to publish messages to S4RIS platform Distributed Messaging System (DMS) prepared in advance of the demo for PRIGM/Senstation, Ganimede, CuriX, OSINT. WINGSPARK publishing directly in real-time. Structure and content of the JSON messages matches those that the individual tools provide.

## **DEMO today – Response**



DATAFAN	Time series data analysis with machine learning algorithms (TRL 2 at project start)
	Contribution: Predicts the free capacity of surrounding stations to support re-direction of passengers
CAESAR	Tool: Evaluates disruptions on single, or coupled, critical infrastructures; critical components and mitigation strategy performance (TRL 5 at project start)
RAM <sup>2</sup>	<ul> <li>Decision support tool, asset inventory visibility, collecting + correlating events, providing clear mitigation steps (<i>TRL6 at project start</i>)</li> <li>Contribution: Correlation of events providing users with insight into the overall attack and its progression and mitigation plans for each alert. Messages links to tools supporting Response.</li> </ul>

"Postman tool" intended to be used to publish messages to S4RIS platform Distributed Messaging System (DMS) prepared in advance of the demo for DATA FAN. CaESAR publishing directly in real-time. Structure and content of the JSON messages matches those that the individual tools provide.



# DEMO today – Recovery

C A M S

Asset management (TRL6 at project start)

Contribution: Assessment of cost to restore the service after extreme event considering assets damaged

# Bibliography / References



Department of Communications, Climate Action & Environment, NIS Compliance Guidelines for Operators of Essential Service (OES). 2019. "NIS Compliance Guidelines for Operators of Essential Service (OES)." European Commission, *HORIZON 2020 – WORK PROGRAMME 2014-2015 General Annexes, G. Technology readiness levels (TRL).* European Commission, *SAFETY4RAILS Grant Agreement*, version 3.0, dated 20 July 2022. Inc., Postman. 2022. What is Postman. <u>https://www.postman.com/product/what-is-postman/</u>.

SAFETY4RAILS, D2.3 System specifications and concept architecture, September 2021.

# Thank you for your attention!

SAFETY4RAILS Consortium:

Stephen Crabbe

Fraunhofer EMI

Stephen.Crabbe@emi.fraunhofer.de

# https://safety4rails.eu/

