7SHIELD

KR01 – Risk Assessment Tools

Modules

- Critical Infrastructure Resilience Platform (CIRP-RAT)
- Digital Vulnerability Assessment (DiVA)

Prevention

High-level Analytics

Scope

The risk assessment tools are designed to support the risk assessment of cyber (DiVA) and physical (CIRP-RAT) threats. They are equipped with a set of components that host and analyze information with regards to assets, vulnerabilities, measures, etc., being able to calculate the **risk of cyber attacks**, **natural hazards** (i.e., earthquakes) or **man-made events** (i.e., intrusion) **on the infrastructure**.

Regarding the integration in the 7SHIELD framework, they leverage:

i. the 7SHIELD Secure Authentication Mechanism, to avoid multiple logins by the CI operators

ii. the input regarding the infrastructure assets is provided by the MBDA component

iii. the Graphical User Interfaces showing the output of the risk assessment are embedded in the CPTM dashboard.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 883284

Partners

ENGINEERING
Italy

Engineering Group (ENG) is a global player in the digital transformation sector, with relevant expertise in business integration and Critical infrastructure protection against cyber and physical (c/p) attacks, for example providing resources to c/p situational awareness and threat intelligence.

SATWAYS
Greece

Satways LTD (STWS) develops solutions for Security and Public Safety applications, with the aim to provide effective decision support, simplify operations, provide a Common Operational Picture (COP) and collaboration tools across organizations, collect and disseminate data in the field, and coordinate response units and system users.

Purpose

7SHIELD is proposing **two Risk assessment tools** for cyber and physical threats accordingly, identifying hidden vulnerabilities that could be exploited by such threat-agents: Digital Vulnerability Assessment (DiVA) tool and Critical Infrastructure Resilience Platform Risk Assessment Tool (CIRP-RAT).

Such modules provide a **friendly Graphical User Interface** in which the Critical Infrastructure operators can conduct several what-if scenario based assessments, in order to calculate the risk, identify exploitable vulnerabilities and highlight the possible attack-paths for a threat-agent.

It is a question-driven approach, based mainly on threat characteristics, the assets' vulnerability, security measures in place and and potential impacts leading to the risk identification and measurement.

All the modules developed in the frame of 7SHIELD have been designed with the consultancy of identified external stakeholders, first responders and following the **requirements** provided by the partners working in the space sector acting as Pilots, who provided the Critical Infrastructures for **testing and demonstration**.

Contribution

ENG designed and developed the **DiVA tool** staring from its previous version used in different projects such as **HERMENEUT** (H2020-740322), **COMPACT** (H2020- 762128) and **INFRASTRESS** (H2020-833088). This tool was initially designed to assess the cyber risk associated with intangible assets; then it was adapted for specific type of Critical Infrastructures (CI), used in the public administration and, during 7SHIELD, it has been enhanced in order to cope with the cyber risk analysis in the Ground Segment (GS) context.

STWS developed **CIRP-RAT**, based on the Critical Infrastructure Resilience Platform (CIRP), also developed by STWS in the frame of the EU Research project entitled EU-CIRCLE (H2020- 653824). The model and interface have been adjusted and enhanced in order to be **suitable for Space Ground Segments protection** from different types of physical threats (natural, man-made, technical).

Future Improvements

The asset management process from third-party tools could be improved by eliminating the constraints related to a pre-configured mapping and, thus, processing the unknown assets through a dynamic system whereby, with heuristic methods, it is possible to derive the risk assessment data.

The platform could be further enhanced by adding **further threats** in the process, integrating **digital twins** visualizing the calculated data, and adding the ability to **automatically gather information** and data from various sources and devices integrated.

Contacts

- info@eng.it
- info@satways.net

Technology

Several risk assessment methodologies (e.g. ISO31000, RAMCAP, EBIOS, ESA's) have been used in order to analyse what-if scenarios, using parameters related to threats, assets, vulnerabilities, security measures and impacts, to acquire a detailed risk assessment report.

Both DiVA and CIRP-RAT are managing **several repositories** that host information related to the CI parameters. This information is available to third-party applications/users either through a **REST Web API** or through its integration with any message broker (e.g. **KAFKA**).

Besides other technologies used, there are **JAVA** language with **SPRING** framework, **Angular, Thymeleaf , Jenkins pipeline, Hazelcast, Groovy, Zipkin, PostgreSQL, ORM Spring Data / JPA and Sonarqube**.

Stakeholders

The goal of the risk assessment tools is to protect and preserve the CI and its data. For this reason, the data provided by these tools are useful for **CI operators, security managers/officers and decision-makers**. The tools allow enhancement of the resilience of the CIs by offering a deep understanding of emerging risks, existing vulnerabilities, lack of measures in place, and potential impacts on the facilities or the services. The targeted users for this solution originate from both the public and private sector, and include **space agencies, space ground-segment operators and governmental authorities (e.g. Ministries)**.

The modules are versatile, customizable and flexible for all companies due to their high configurability and therefore to the extension of the system at runtime.

www.7shield.eu