7SHIELD

KR17 – Potential impacts from physical/cyber attacks and countermeasures knowledge base

Modules

- Service Continuity Module (SCM)
- Emergency Response Plans (ERP)

Mitigation

Crisis Management

Scope

ERP and SCM were designed to **offer Ground Segment operators** tools to:

- identify organizational specific best practices, methodologies, and standard operating procedures for the creation of the Threat/Emergency specific functional playbooks, indicating specific emergency response actions (**ERP**);
- assess the operability of their infrastructure when impacted by a combination of **physical and cyber threats**, performing several hypothetical scenarios to understand which are the most critical assets and take precautional actions to reduce their vulnerability (**SCM**).

All the above are amalgamated and visualised via the ENGAGE CSIM platform in a hierarchical and user-friendly manner helping navigate the platform operators successfully in order to facilitate the management of an **emergency response**.

Partners

KEMEA
Greece

The **Centre for Security Studies (KEMEA)** is a think tank on homeland security policies and an established research center since 2005 within the Hellenic Ministry of Citizen Protection, aiming to support security policy implementations in Greece, at a strategic level. KEMEA also constitutes the National Greek Authority regarding Critical Infrastructure Protection (CIP) as well as the contact point with the European Commission relevant authorities and the EU Member-States.

Resilience Guard
Switzerland

Resilience Guard Gmbh (RG) is a Business Continuity, Risk Management, and Crisis Management consultancy company based in Zurich, Switzerland. RG's core team has vast international experience with more than 25 years' hands on experience on multinational Business Continuity Management, Risk Management, and Crisis Management implementations in challenging environments and complex organizations.

Contribution

KEMEA produced the ERPs based on the previous experience in general **emergency management policy** and offers general guidance by establishing the **long-term policy priorities and responsibilities** of the operations during response. KEMEA has the main responsibility of the identification and characterization as well as monitoring the Security Operators Plan (SOP) of the Critical Infrastructures within the Greek borders.

RG developed the SCM using a generic operational model to **simulate the critical operations** of a GS and the cascading effects of failures due to physical and/or cyber attacks. The RG's expertise contributed to the correct understanding of the p/c infrastructure layout of a modern GS and subsequently to the development of the **operational model** used for the **impact analysis**.

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

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**.

Purpose

7SHIELD framework is proposing an Emergency Response Plan (ERP) and Service Continuity Module (SCM) in other to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from a **combination of cyber and/or physical attacks** to EU Ground Segments (GSs) of Space Systems.

- The **ERP** module provides a navigation through a set of specific, **self-standing operational playbook** in a form of on-screen instructions tailored to the local GSs particular exposures and not generic and one-size-fits-all procedure. The playbooks also include referenced staff roles during the emergency response to ensure proper coordination. This enables the efficient and successful management of an incident in a structured and comprehensive way by guiding the operators performing specific tasks and actions during an emergency.
- The **SCM** allows to perform a **failure propagation analysis and rapid assessment of a real or hypothetical disaster scenarios**, selecting several physical/cyber (p/c) attacks per component or downtimes. The output of the analysis are a set of images, GIFs and CSV files showing the effect of the disruptions of the GS operations.

Future Improvements

The modules are **adaptable** to each of the situation which is considered critical.

Moreover, Critical Infrastructures are constituted by technologies and governed by operational roles that might change in time, so further adaptation can be done in order to let the predefined procedures/models for threat response and mitigation fit with those changes.

Contacts

- e.georgiou@kemea-research.gr
- n.lalazisis@kemea-research.gr
- dimitris.tsarpalis@resilienceguard.ch

Methodology

Both the ERP and SCM received **feedback from the Satellite Ground Segment operators** and let them highlight the existing practices, organizational structures, infrastructure assets, established procedural mechanism of roles/responsibilities and to identify organizational specific best practices for the creation of output of the modules.

In addition:

- for the creation of ERPs several **standards and regulations** have been taken into consideration (e.g. EU 2016/1148 NIS Directive; ISO 22320:2018; etc.) to ensure that a specific and sufficiently documented process is always in place for implementation;
- further standard techniques in BC practices were adopted in the development of the SCM, such as Input-Output models, failure propagation procedures, and Vendor Dependence Tables. The SCM is encoded using Python environment.

Stakeholders

All sectors of society (i.e., **public/private sector**) should consider emergency preparedness.

Critical Infrastructure stakeholders, as well as **First Respondents** (FRs) could benefit from the ERPs and SCM usage, as an existing gap in the functional integration of response plans and procedures into Integrated Command Control and Coordination System (IC3S) platforms is met. In this line, important social benefits are expected from the adoption of such modules such as the possibility to:

- **minimize reaction time** during an emergency, and response lag due to lack of effective communication, coordination, and uniformity of responses (ERP);
- perform **risk and loss assessment analyses** in order to enhance Business Continuity and minimize economic/service losses (SCM).

www.7shield.eu