D3.1 Transitioning risk management

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 101021274

Protection of Critical Infrastructures from advanced combined cyber and physical threats

Deliverable nº:	D3.1
Deliverable name:	Transitioning risk management from design-time to runtime
Version:	1.0
Release date:	30/11/2021
Type - Dissemination level	Report - Public
Status:	Final
Editors	KONČAR
Contributing WP	WP3 Cyber Situation Awareness

Abstract

This report addresses the transfer of the static risk management results to the dynamic risk management to maintain the system or organisation in secure conditions during its complete lifecycle. Current risk management practices already implemented by PRAETORIAN Critical Infrastructures (Cis) and First Responders (FRs) are investigated with a series of interviews, with a special focus on transitioning practices. Results of the interviews are used to generate a synthesis of the transitioning practices at interviewed CIs and FRs. A short-list of the best practices is presented. As a conclusion, an analysis of the lessons learnt and a proposition on how to continue this survey is given.

Disclaimer

This document contains material, which is the copyright of certain PRAETORIAN beneficiaries, and may not be reproduced or copied without permission.

The information appearing in this document has been prepared in good faith and represents the views of the authors. Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authors accept no statutory, contractual or other legal liability for any error or omission to the fullest extent that liability can be limited in law.

This document reflects only the view of its authors. Neither the authors nor the Research Executive Agency nor European Commission are responsible for any use that may be made of the information it contains. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

No part of this document may be copied, reproduced, disclosed, or distributed by any means whatsoever, including electronic without the express permission of the PRAETORIAN project partners. The same applies for translation, adaptation or transformation, arrangement or reproduction by any method or procedure whatsoever.

PRAETORIAN

PRAETORIAN's strategic goal is to increase the security and resilience of European Critical Infrastructures CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. To that end, the project provides a multidimensional (economical, technological, policy, societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system; (iii) a Hybrid Situation Awareness system, which includes digital twins of the infrastructure under protection; and (iv) a Coordinated Response system. The PRAETORIAN toolset supports the security managers of CIs in their decision making to anticipate and withstand potential cyber, physical, or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

The project specifically tackles (i.e., prevents, detects, responses and, in case of a declared attack, mitigates) human-made cyber and physical attacks or natural disasters affecting CIs. It also addresses how an attack or incident in a specific CI can jeopardise the normal operation of other neighbouring/interrelated CIs, and how to make all of them more resilient, by predicting cascading effects and proposing a unified response among CIs and assisting First Responder teams.

PRAETORIAN is a CI-led, user-driven project, which demonstrates its results in three international pilot clusters – Spain, France and Croatia –, some of them cross border, involving 9 outstanding critical infrastructures: 2 international airports, 2 ports, 3 hospitals and 2 power plants.

Document history:

Version	Date of issue	Content and changes	Partner
0.1	10/9/2021	Table of Contents	KONČAR, THALES
0.2	7/10/2021	Chapter 3 - Methodology	KONČAR, THALES
0.3	26/10/2021	Executive summary, Introduction, Chapter 2, Annex A	KONČAR, THALES
0.4	5/11/2021	AENA, HEP, SDMIS, ZAG interviews added as ANNEX, Chapter 3 updated	EDF, ETRA, KONČAR, THALES
0.5	19/11/2021	CMRS, GPMB, FVP, EDF, KABEG interviews added, Chapter 4 updated, Chapter 5	EDF, ETRA, KONČAR, THALES, UPVLC
0.6	29/11/2021	Post peer review	EDF, ETRA, KONČAR, THALES, UPVLC
1.0	30/11/2021	Final version after review	KONCAR

Lists of Authors, Contributors & Reviewers:

Partner	Authors
EDF	Elsa Helies, Frederic Guyomard
ETRA	Eva Muñoz, Juan José Hernandez
KONČAR	Tamara Hadjina, Hrvoje Keko
THALES	Stéphane Paul
UPVLC	Israel Pérez Llopis

Partner	Interviewees or middlemen
AENA	Luis Uia, Joaquin Rodriguez, Jordi Peral
CMRS	Zdenko Lovrić
EDF	Nicolas Thomeret, Ramzi Zarrouga, Christophe Martin
FVP	Ángel Laguna Argente, Pablo Giménez Salazar
GPMB (incl. GIE)	Stéphanie Sicot, Fabrice Klein

Partner	Interviewees or middlemen
HEP	Krešimir Kristić, Luka Bitunjac, Nikola Slišković
KABEG	Albert Kutej, Mirko Friedrich Ogris
SDMIS	Benoit Sapet, Bruno Perrier, Laurent Herry
ZAG	Gabrijela Abramović, Melita Damjanović, Miroslav Jerković, Ivo Jurič, Nikolina Lovrić, Marin Tica

Peer reviewed by:

Partner	Reviewer
AIT	Stefan Schauer
ICCS	Lazaros Papadopoulos

Table of Contents

Index of Tables

Index of Figures

Abbreviations and Acronyms

AENA	Aeropuertos Españoles y Navegación Aérea
AENOR	Asociación Española de Normalización y Certificación
AESA	Agencia Estatal Seguridad Aerea (National Agency for Aerial Security)
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CAPEC	Common Attack Pattern Enumeration and Classification
CCAA	Croatian Civil Aviation Agency
CERT	Computer Emergency Response Team
CGCT	Code Général de la Collectivité Territorial (General Code of the Territorial Community)
CI	Critical infrastructure
CISO	Chief information security officer
CMRS	Croatian Mountain Rescue Service
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CoTRRiM	Contrat Territorial de Réponse face aux Risques et effets des Menaces (Territorial Response Contract to Risks and impacts of Threats)
CSIRT	CyberSecurity Incident Response Team
CNMV	Comisión Nacional del Mercado de Valores
CNPC	Comisión Nacional de Protección Civil (Civil Protection National Committee)
CNPIC	Centro Nacional de Protección de Infraestructuras y Ciberseguridad
CVE	Common Vulnerabilities and Exposures
DCS	Departure Control System
DCS	Distributed Control System
DREAL	Direction Régional de l'Environnement de l'Aménagement et du Logement (Environment, Planning and Housing Regional Directorate)
DoA	Description of Action
EDF	Electricité de France
ENS^2	Esquema Nacional de Seguridad, Security National Schema
FMECA	Failure Modes, Effects and Criticality Analysis
FR	First Responder
FVP	Foundation Valencia Port
GACR	Groupement Analyse et Couverture des Risques (Risk Analysis and Coverage Group)
GCMA	Groupement Réponse aux crises Majeures et Attentats (major crisis and terror attacks group)
GO	Groupement Opération (Operations Group)

GPrev	Groupement Prévention (fire safety)
GPMB	Grand Port Maritime de Bordeaux
GRC	Governance, Risk and Compliance
GSI	Groupement Support Informatique
HAZOP	HAZard and Operability
HEP	Hrvatska elektroprivreda
ICAO	International Civil Aviation Organisation
IMS	Integrated Management System
ITAM	IT Asset Management
KABEG	Klagenfurt Landeskrankenanstalten
MAGERIT	Methodology for Information Systems Risk Analysis and Management
MOPE	MZLZ – Zagreb Airport Operator Ltd.
MUG	Med. Universität Graz
MZLZ	Međunarodna zračna luka Zagreb d.d. (International Zagreb Airport Jsc.)
NRBCe	Nuclear, Radiological, Biological, Chemical or explosives
ORSEC	Organisation de la Réponse de Sécurité Civile (Organization of the Civil Security Response)
OSTIC	ICT Security Office
PDCA	Plan-Do-Check-Act
RETEX	RETurn on EXperience
SDACR	Schéma Départemental d'Analyse et Couverture des Risques (Departmental Scheme for Risk Analysis and Coverage)
SCADA	Supervisory Control and Data Acquisition
SDMIS	Service Départemental - Métropolitain d'Incendie et de Secours
SIS	Services Incendie et Secours (First Responders)
SOC	Security Operations Centre
SOP	Standard Operating Procedure
ZAG	Zagreb Franjo Tuđman Airport
ZSIS	Institute for Security of Information Systems

Executive Summary

This report addresses the transfer of the static risk management results (at design-time) to the dynamic risk management (at runtime) to maintain the system or organisation in secure conditions during its complete lifecycle. Current risk management practices already implemented by PRAETORIAN Critical Infrastructures (CIs) and First Responders (FRs) are investigated with a series of interviews, with both static risk modelling teams and the dynamic risk modelling teams. Results of the interviews are used to generate a synthesis of the transitioning practices at interviewed CIs and FRs. Finally, a short-list of the best practices is presented and analysed. This report also provides general conclusions about the methodology used and the lessons learnt while conducting the research.

1. Introduction

1.1 Purpose of the document

The main goals of this document are to:

- Report on current risk management practices deployed at different European Critical Infrastructures (CIs) and First Responders (FRs), with a focus on the transition between the so-called *static* risk management activities and the *dynamic* risk management activities;
- Identify best practices and provide recommendations to improve the transition between static risk management and dynamic risk management.

1.2 Scope of the document and caveat

This document relates to methodology, i.e., the study of methods. As a public document, it does not address the content of individual risk management performed by the PRAETORIAN CIs and FRs. The deliverable is as precise and complete as possible, considering that some CIs and FRs requested that some of their practices (i.e., methods and tools) should not be published in a public document and three partners did not respond to the interview invitation.

The results of the interviews were all reviewed by the CIs and FRs before their insertion in the annexes. All results, discussions and the synthesis were approved for publication by the CIs and FRs.

Even though this work was performed as part of work-package 3 - Cyber Situational Awareness, all types of risks are considered in the risk management transitioning process. Risks are not limited to cybersecurity risks.

1.3 Relevance of this study for PRAETORIAN

Risk management is one of the central elements of the PRAETORIAN project:

- Deliverable D2.2 deals with the project's risk assessment methodology;
- In D2.3, the use-cases and pilot scenarios are risk-driven; these scenarios will drive all the research and demonstrations in the project, e.g., drone neutralisation in task T6.5;
- Task T2.5 aims at developing a framework that could be used to propose measures to lower the level of risk;
- In work package (WP) 3, the Cyber Forecaster Engine (D3.2) requires risk assessment as input and aims at bridging the gap between the actual deployment of systems and their risk and threat analysis;
- Deliverable D4.1 deals with physical risks and vulnerabilities, and is an important input for the entire WP 4 to detect vulnerabilities and risks of the selected CIs, and to increase their protection and resilience;
- Task T6.1 proposes a risk-based approach that can prioritize the impacts of emergency situations, so as to guide decision-making;
- In task T10.3, the project is committed in making proposals to expand European security standards and certification by linking the main norms on risk assessment (i.e. ISO 31000 and ISO 27005), and the national best practices of France, Spain and Croatia aiming at identifying the certification scheme promoted by ENISA;

Risk management requires significant efforts within CIs and FRs. Hence, a seamless process should improve the efficiency of risk management throughout the lifecycle of the deployed systems. This deliverable focuses on the transition from static risk management to dynamic risk management. It is our conviction that the identification of best transitioning practices should help optimise the overall risk management process.

1.4 Structure of the document

This document is structured as follows:

- Section 2 gives an overview of scientific and technological challenges related to risk management with special focus put on the issue of transitioning static risk assessment results to dynamic risk management.
- Section 3 presents the method that was used to conduct research in this task.
- Section 4 provides a synthesis of the current risk management transitioning practices at PRAETORIAN's CIs and FRs as detected in the interviews and provides a short-listing of identified best practices.
- Section 5 concludes this deliverable.
- Section 6 provides the list of all references.
- Annex A is a list of questions, which served as interviewer guidelines.
- Annexes B to J present extensive results of the interviews with CI operators and FRs.

2. Scientific and technological challenges related to risk management: a focus on transitioning issues

The ISO 31000 standard [1] opens with these words: "Managing risk is dynamic and assists organizations in making informed decisions about setting strategy and achieving objectives". This is undoubtedly true, but it is also true that the lifecycle of systems and organisations subject to risk management are very complex, with different tempos in terms of change. This has led to the so-called:

- Static risk management activities, which are performed under the hypothesis of an unchanging (at best) or a slowly changing (at worst) world;
- Dynamic risk management activities, which are performed under the hypothesis of frequent, severe or short-notice changes in the system or its environment.

Static risk management typically applies during the development phase of a system for a CI (cf. Figure 2-1). This phase is generally quite long, somewhere between a few months to a few years, depending on the complexity of the system. During development time, it is assumed that the system requirements are quite constant, being subject to contractual amendments. Some new software or hardware vulnerabilities may appear during the development, but these will generally be marginal. Even though agile approaches have increased the pace of development [2], risk management activities and decisions during development are rarely constrained by time: it is possible to write extensive security reports, organise meetings to discuss the best options to treat the risks, and formalise the action plans.

After a successful development, integration and deployment, the system becomes operational (cf. Figure 2-1). This phase may also be very long, typically up to 40 years for long-lived systems, with long periods during which nothing much will happen. Static risk management practices may continue to apply, typically for yearly updates. However, during operations, there is often the assumption that things may change radically or suddenly. Consequently, in such cases dynamic risk management practices are employed. Sudden changes may be due to business or operational reasons, or due to environmental changes, including:

- Natural events, e.g., an earthquake, volcano eruption, wildfire, flood…
- Human accidental events, e.g., new software vulnerability, inappropriate operator interaction…
- Human intentional and malevolent events, e.g., a cyber-attack, social or activist protest events, fire…

In most of those cases, risk-based decisions must be taken quickly. The dynamic risk management procedures must be fine-tuned to allow for speed, otherwise the consequences can be dramatic.

We can see from the examples above that the methods, the data and the metrics used during static risk management are bound to be significantly different from those used during dynamic risk management, while having the same goal. This sets the ground for the core question of this report: how do we best transition from static risk management to dynamic risk management activities?

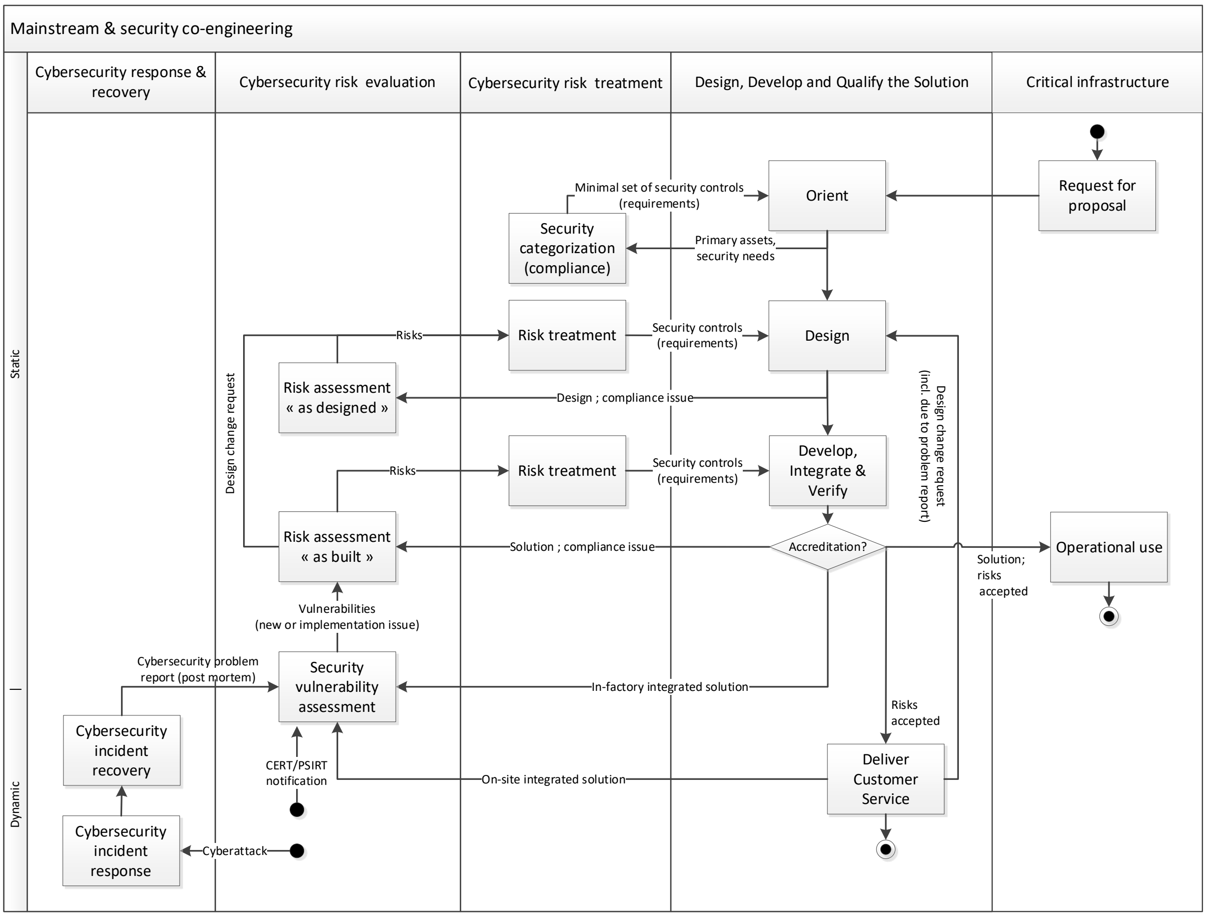

Mainstream & security co-engineering
Static
Dynamic
Cybersecurity response & recovery
Cybersecurity risk evaluation
Cybersecurity risk treatment
Design, Develop and Qualify the Solution
Critical infrastructure
Request for proposal
Orient
Minimal set of security controls (requirements)
Security categorization (compliance)
Primary assets, security needs
Risk treatment
Risks
Security controls (requirements)
Design
Risk assessment « as designed »
Design ; compliance issue
Design change request
Design change request (incl. due to problem report)
Risk treatment
Risks
Security controls (requirements)
Develop, Integrate & Verify
Risk assessment « as built »
Solution ; compliance issue
Accreditation?
Solution; risks accepted
Operational use
Vulnerabilities (new or implementation issue)
Cybersecurity problem report (post mortem)
Security vulnerability assessment
In-factory integrated solution
Risks accepted
Cybersecurity incident recovery
CERT/PSIRT notification
On-site integrated solution
Deliver Customer Service
Cybersecurity incident response
Cyberattack

Figure 2-1 Typical system lifecycle highlighting static and dynamic risk management activities (based on Thales internal practices)

It is not uncommon to see the people performing dynamic risk management start their analysis from scratch. There may be various reasons for that:

- Unawareness of the existence of static risk management material available at some internal or external source;
- Intellectual Property (IP) issues on the available risk management material between the teams belonging to different legal organisations, or different entities within a given organisation;
- Confidentiality issues on the available risk management material, with need-to-know requirements that are not easy to bypass, especially if they are contractual or imposed by regulation;
- Tensions / quarrels between teams, disallowing collaboration on this subject;
- Assumptions that the existing static risk management material will be too difficult or too costly to reuse or adapt for its use at runtime, also known as "actionability".

Likewise, it is common to see the people performing static risk management having no idea that their results may be useful down the line for dynamic risk management. Thus, they will make no specific effort to make the existence of the material known to others, and even less make it easily reusable.

On the other hand, some factors may ease the transition between static risk management and dynamic risk management:

- Organisation’s governance policy mandating systematic risk management during the whole systems’ lifecycle;
- Integrated risk management teams, i.e., the same set of people performing both static and dynamic risk management;
- Contractual requirement to initialise dynamic risk management with the results of the static risk management;

- The physical and organizational proximity of the teams. If the teams are in the same building and meet regularly (e.g. for lunch) the transition may be easier.

This deliverable analyses the risk management practices at all the PRAETORIAN critical infrastructures and first responders in order to assess:

- Their (implicit or explicit) need for transitioning;
- The reality of the transitioning practice;
- The efficiency of this transitioning;
- The criteria that determine this efficiency.

Based on this assessment, some transitioning recommendations are made.

3. Methodology

The description of task T3.1 in the PRAETORIAN Description of Action (DoA) states: "*In this task, we will first study the typology of data required/useful to pass from the risk management teams at design-time, to the risk management teams at runtime by organising 3+ workshops with both static and dynamic cybersecurity risk assessment experts from the technical and end user consortium partners. Then the data-related topics, such as the update rate, need for round trips (e.g., information transferred from the runtime teams to the development teams for a major maintenance / upgrade of the system), or more practical data format considerations will be addressed. Finally, this task will provide suggestions on the best way of signalling the estimated risk situation to the run-time risk management teams at runtime*". Considering the twelve CIs and FRs involved in the project, the workshop approach under COVID-19 conditions did not seem feasible anymore. To investigate current risk management practices already implemented by the project's CIs and FRs, we decided to start a series of interviews, with both the static risk and the dynamic risk modelling teams.

The PRAETORIAN project is organized around three demonstration pilot sites, as shown on Figure 3-1. Each demonstration site is coordinated by one or two technical partners. Those technical partners have the best overview of their local cluster. Therefore, each coordinating partner conducted the interviews with the members of their local demonstration site.

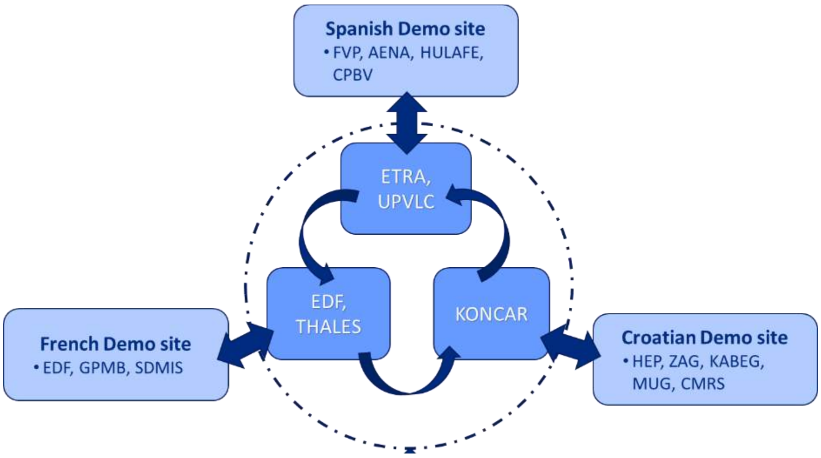


Figure 3-1 Demo sites management structure

Mis en f
Code de
Mis en f
Code de
Mis en f

To retrieve a homogeneous outcome across all demonstration sites, the coordinating partners agreed on interview guidelines prior to the interviews; these guidelines are documented in ANNEX A – Interview guidelines. The interviews consisted of two parts:

- one dedicated to static risk management and the transition to dynamic risk management;
- one dedicated to runtime risk management and the transition from static risk management.

When building the questionnaires, the hypothesis was made that the static and dynamic risk management interviewees could, and probably would, be different. Thus, some questions may seem redundant.

The questions were carefully formulated in order to get unbiased information about the current risk management practices. The same guidelines were used for interviews with CI operators and FR personnel, even though they have a quite different role and a somewhat different approach to risk management. For some stakeholders, questions were translated to the stakeholders' native language to facilitate the communication and avoid misinterpretation. After the interview, the resulting answers were translated back to English. The translation was done by the interviewers.

Each interview was expected to last approximately 1½ hours, theoretically resulting in 3 hours of interview for each CI or FR. Practice proved quite different. Some risk managers at CIs and FRs expressed strong unavailability constraints, which forced the coordinating partners to bypass the questionnaire guidelines and adopt a more direct approach; these constraints usually yielded short interviews, mixing static and dynamic risk management concerns with the same interviewees. By contrast, other

CIs and FRs were prolix on their practices, with interview durations reaching up to 9 hours, organised in a series of short slots when their agenda allowed.

Table 1 provides an overview of the interviewees' roles involved in the interviews. Interviewers were all technical experts and/or researchers, who have a broad understanding of risk management in general and different aspects of critical infrastructure security in particular.

Table 1: People and roles involved in the interviews

Critical infrastructure	People conducting the interview	Interviewed personnel	
		Static risk management team	Dynamic risk management team
Zagreb Airport	**KONČAR** Tamara Hadjina Hrvoje Keko	• Quality Control Expert • Document Control Expert • IT Director • Technical Coordinator in Development Department • Airport Security Manager • Airport Safety Manager	• Quality Control Expert • Document Control Expert • IT Director • Technical Coordinator in Development Department • Airport Security Manager • Airport Safety Manager
HEP (Croatian national energy company)		• Chief Information Security Officer • Hydropower plant director	• Hydropower plant director • Hydropower plant technical director
CMRS (Croatian Mountain Rescue Service)		• Experienced volunteer rescuer	• Experienced volunteer rescuer
SDMIS (French firefighters)	**THALES** Stéphane Paul **EDF** Elsa Hélies	• Firefighter Officer • Chief Information Security Officer	• Firefighter Officer (different from static risk management) • Chief Information Security Officer (same as for static risk management)
AENA	**ETRA** Eva Muñoz	• Head of the Oficina Seguridad TIC (OSTIC) • Two project managers - Innovation Division	• Physical Security Technician • Director of Valencia Airport • IT Area Manager
EDF	**EDF** Frédéric Guyomard Elsa Héliès **THALES** Stéphane Paul	• Technical coordinator in the safety and security of the power plants team • Cyber security referent	• Head of IT Security Mission
FVP	**FVP** Ángel Laguna Argente, Pablo Giménez Salazar	• Chief Information Security Officer	• Chief Information Security Officer
GPMB (incl. GIE)	**EDF** Elsa Hélies Frédéric Guyomard **THALES** Stéphane Paul	• Director of Operations • Administrator	• Director of Operations • Administrator

Critical infrastructure	People conducting the interview	Interviewed personnel	
		Static risk management team	Dynamic risk management team
KABEG	**KONČAR** Tamara Hadjina	• Head of the medical technology department • Technical safety officer for the medical technology sector	• Head of the medical technology department • Technical safety officer for the medical technology sector

4. Transitioning from static to dynamic risk management

This section provides a synthesis of the transitioning practices at PRAETORIAN's CIs and FRs as captured in the interviews (cf. §4.1) and short-lists some of the best practices (cf. §4.2).

4.1 Current practices at PRAETORIAN's CIs and FRs

The full interviews of AENA, CMRS, EDF, FVP, GPMB, HEP, KABEG, SDMIS and ZAG are provided in annexes B to J. This section provides summaries of the interviews with focus on transitioning practices.

4.1.1 Current transitioning practices at AENA

At AENA, operational, financial, technological, legal, compliance and information risks are managed jointly and centrally at a high-level of abstraction (e.g., 18 risks in 2020) by an Audit Committee, supported by an Internal Audit Department. The Audit Committee supervises the risk management system, ensuring that the main risks are identified, managed, communicated and maintained at planned levels.

Each of the high-level risks managed by the Audit Committee is allocated to Operational Areas, where they are decomposed into several area-specific risks. The Operational Areas identify and evaluate the risks that are under their area of responsibility. They propose and report the indicators for proper monitoring. They establish action plans to mitigate the risks, and report on their effectiveness.

For the specific case of the Cybersecurity Operational Area, there is the ICT Security Office (OSTIC), which is supported by external technical staff that works on AENA's premises, together with AENA's personnel. In addition, a Detection and Response Centre (i.e., internal CSIRT) monitors vulnerabilities, detects and notifies technical-related risks. The OSTIC has implemented a risk management and assessment standard based on the MAGERIT methodology [3]. Patches and improvements to be implemented arrive monthly. If a specific incident is detected in that period, the notification is generated and resolved immediately.

When a new product is to be released, an *informal* risk analysis is carried out by a security architect and validated by the Demand Management committee, which typically involves around 25 persons of different trades and airports. A series of controls are put in place. The new product then enters the normal risk management process as described above.

Practically, the risk monitoring and reporting process is implemented in the SAP GRC application [4]. The Operational Areas report in the tool the indicators according to their area-specific periodicity. The indicators are monitored by the Audit Committee. The Governance, Risk and Compliance (GRC) tool supports a large part of the risk management communication between the teams and throughout the systems' lifecycles. The transition between static and dynamic risk management is seamlessly handled through the GRC tool.

4.1.2 Current transitioning practices at CMRS

The interpretation of static vs. dynamic risk assessment has been understood by CMRS as follows:

- Static risk assessment relates to risk assessment performed in preparation of an event, before CMRS is called to act on the field;
- Dynamic risk assessment relates to risk assessment performed during operations, starting as soon as CMRS receives a call to act on the field; it therefore always relates to an incident, accident and / or crisis situation.

CMRS has a representative in national and county Civil Protection Directorate (CPD) headquarters and in that way takes part in performing static risk assessment for specific territories. Static risk management results are key to procurement and training. Results of static risk assessment are used by CMRS to generate Standard Operating Procedures (SOPs). SOPs are generated by senior officers, leaders of specific rescue divisions (speleological, alpine, underwater, etc.). There is no formal transition of static risk assessment results or SOPs to operatives on the field. CMRS is an organisation consisting mainly of volunteers (1000 volunteers and only 20 professionals) and having formal transition is considered ineffective. To overcome this lack of formal transition, CMRS organises exercises (more than ten a year) and trainings (every weekend) for volunteers. Exercises and trainings are led by experienced and certified instructors. Instructors hold certifications from international organisations depending on their field of expertise (cave rescue, rescue dogs, underwater rescue, etc.).

Dynamic risk management is performed *informally* on the field by CMRS. An action plan is established by senior officers (usually also rescue action commanders) and shared with the team orally. Each mission starts with the briefing where each member of the team receives his role and orders. In addition, each action ends with a debriefing and, if necessary, the rescue action commander provides feedback to higher instances. This feedback may, in some cases, trigger changes in SOPs or static risk assessment.

4.1.3 Current transitioning practices at EDF

In EDF, the transition between the static and the dynamic risk assessment are done as follows:

- In the EDF landscape, the risk management is a unified approach. Even if it is realised in two different phases (i.e., design and exploitation), it is shared between the power plant design team (who does the static risk management) and the exploitation team (who is in charge of the dynamic risk management). There is only one risk analysis, shared and updated regularly.
- After the modelling of the level of acceptability of risks by the design team, a snapshot is made of the static risk assessment and given to the exploitation team. The security part of the static risk management of accredited systems is performed using the EBIOS-2010 method [5][1]. For other systems, the analysis are built considering the sectorial requirements for the area of energy facilities. The granularity is quite fine-grained, with typically 2000 supporting assets within a project. To follow the vulnerabilities, the static risk management team is supported by an internal Computer Emergency Response Team (CERT) and the CERT-FR [6].
- In case of sub-contract, the sub-contracted companies must provide a Security Assurance Plan (PAS). This plan describes, amongst other elements, the organisation, the security of the product, and the methods to transfer the security between the sub-contracted company and EDF. A report is made when the transfer of the security is done. The sub-contracted companies use their own methods for risk assessment, traditionally also EBIOS-2010 [5]. Risk assessments of the sub-contracted companies are used as input for the internal static risk assessment.
- On every digital maintenance action, a risk assessment is made to identify the impacts of the intervention on a system. The design team updates the risk analysis every 3 years for accredited systems, or more often when a major vulnerability arises. The exploitation team regularly audits the systems; the results of these audits help to define some new vulnerabilities and to define some acceptable solution to reduce the risk. Based on that, some corrective actions can be established, and validated by an internal committee, and put in the planning to be applied as soon as possible. With this information, the designer team can update the risk management. Overall, the two teams (i.e., design and exploitation teams) work together to identify the risks and threats.
- Besides the risk management, the exploitation team has a close relationship with ANSSI (National Cybersecurity Agency of France) within a dedicated process called "Cybersecurity shared status". It is not an audit. It is an exchange between experts to improve cybersecurity in particular sensitive industries. It lasts a few weeks each

[1] In French only.

year, on several subjects (they change every year) and on varying perimeters such as Site Protection, Telecommunication, Monitoring and Industrial Control Systems.

- The connexion between the design time and the runtime is managed in two committees, one in charge of the technical aspects and the other mainly in charge of the political and strategic needs.
- All the issues due to any modification or changes in the different architecture, process or procedures are reviewed with the digital security point of view. Representatives from both sides are members of these committees. The IT responsible is also present.
- In the EDF organisation, an Operational Technology (OT) CISO is nominated, who follows the different industrial processes and systems. He is aware of the regulatory needs and sectorial obligations.

Overall, the organisation appears as highly segmented, with a solid process to bind them all together and deliver a unified risk analysis.

4.1.4 Current transitioning practices at FVP

The FVP interpretation of static and dynamic risk assessment is understood as:

- Static risk assessment is carried out only once and the result of which is considered constant.
- Dynamic risk assessment is reviewed periodically to consider possible changes in the likelihood of threat occurrence, its impact or the number of assets affected.

The Port Authority of Valencia's cybersecurity team manages both the cybersecurity design-time risk modelling and the run-time risk management.

Static risk assessment is performed once year considering the operational security incidents occurred in the previous year. During this risk assessment, the current assets, risks, threats, and controls are analysed, re-evaluated, and modified if required and new ones are included and assessed. After the execution of the risk assessment, a confidential report is elaborated. The report is not shared inside or outside the organization.

The critical operational IT systems are continuously monitored by the Security Operations Centre (SOC). The SOC service is subcontracted to an experienced cybersecurity company. The companies that work directly with the Port Authority of Valencia or perform subcontracting IT services and works must be certified and comply with the Spanish National Security Framework.

The SOC only handles operational security aspects. Governance, risk and compliance are the responsibility of the Chief Information Security Officer CISO.

A crisis management plan is defined for operations and management. In case of an incident, involved people can react as soon as possible following the predefined procedure.

4.1.5 Current transitioning practices at GPMB

The scope of the GPMB interview is limited to an Economic Interest Group, which manages a single system called VIGIE SIP.

Dynamic risk management is run every year to keep the internal accreditation of VIGIE SIP.

The first risk management of VIGIE SIP was done after its production and deployment, so there has never been any static risk management performed at design-time on VIGIE SIP. Based on the limited scope of our interview, it is therefore impossible to conclude on any transitioning practices at GPMB.

4.1.6 Current transitioning practices at HEP

In HEP, the interpretation of static vs. dynamic risk assessment has been understood as follows:

- Static risk assessment relates to risk assessment performed under hypothesis of slowly changing circumstances.
- Dynamic risk assessment relates to risk assessment performed under the hypothesis of frequent, severe or short notice changes in the system or its environment. Dynamic risk assessment is considered from the perspective of operators at a hydro power plant.

HEP Group is currently in the process of establishing a formalised risk assessment on all levels. At this stage, the project resulted with the procurement of a GRC tool, the establishment of an IT assets repository and an initial risk assessment. HEP is in the process of recruiting human capacity such that with the existing organisational and technical prerequisites they can update and manage risks in virtually real time.

The results of the static risk management are shared between different systems or teams within the organization. Unlike the risk management results, the separation and control of access to data on vulnerabilities of Industrial Control Systems is carried out rigidly respecting the security principle of Least Privilege and extremely restrictive. Only a small number of authorized workers of a power plant have access to the relevant data of their power plant.

Owners of IT assets, business processes and, consequently, owners of related risks participated in the activities of establishing information repositories, risk assessment and business impact analysis, and in the activities of drafting the policy on notifications of incidents with significant effect. According to the applied methodology, the owners provide the relevant information in interviews, which is then competently and critically evaluated, approved and accepted. The next step are periodic exercises and checks, after which, according to the lessons learnt, the procedures are spirally improved in accordance with the changed conditions and circumstances.

A central Security Operations Centre (SOC) detects real time anomalies that are a consequence of realised risks that are identified and processed in the framework of static risk analysis. Real time anomalies detected by the SOC, which are categorised as incidents, are transferred together with the instructions for necessary activities to IT support operators and if necessary (depending on the type of incident) to cybersecurity managers of power plants and their deputies. Static risk management results are not sent directly to run time teams (operators).

Currently, HEP does not have an established systematic procedure of performing the operational risk management at the level of the hydro plant. During a crisis, operators rely on SOPs that are a result of static risk analysis and on operator experience.

Overall, at HEP, the method and processes to transfer static risk management results to dynamic risk management are still under development and a GRC tool is under deployment. Some good risk management practices are already in place, coordinated by a Corporate Security Office. Noteworthy are: (a) the transfer of a Business Impact Assessment (BIA) from the operational teams (power generation and distribution) to the static risk management team; (b) the use of the static risk assessment results by the SOC to raise relevant incidents; (c) the use of the static risk assessment results related to real-time operations by the operational teams to protect the regular hydropower operation.

4.1.7 Current transitioning practices at KABEG

Risk management is organized on a decentralized basis according to special guidelines and manuals issued by KABEG. The departments manage the risks and report to the central risk management.

In this context, static risk management is performed internally, occasionally supported by consultants. Dynamic risk management is also carried out internally, by the same set of people, and updated annually, every six months or quarterly, depending on the division.

At KABEG, static risk management and dynamic risk management are not formally separated. It is a unified risk management process performed by the same set of people, i.e., operators and risk managers. Thus, there is no transitioning at KABEG. KABEG has 13 risk managers, 58 risk officers and 7 IT security experts employed. Those employees are analytical, with excellent communication skills and have undergone special training.

The risk management delivers SOPs that are used during operation time. The effectiveness of the SOPs is continuously monitored, and changes are initiated via the Plan-Do-Check-Act (PDCA) cycle. The basic assumption is that certain security barriers are insurmountable and that the employees are adequately trained. Severe crises are escalated through official channels and additional resources can be engaged.

4.1.8 Current transitioning practices at SDMIS

For SDMIS, the interpretation of static vs. dynamic risk assessment is understood as follows:

- Static risk assessment relates to risk assessment performed in preparation of an event, before SDMIS is called to act on the field;
- Dynamic risk assessment relates to risk assessment performed during operations, starting as soon as SDMIS receives a call to act on the field; therefore, it always relates to an incident, accident and / or crisis situation.

SDMIS uses a rich set of methods for static risk management, depending on the type of risk and including HAZOP, FMECA and CoTRRIM. The transfer of the static risk assessment results for reuse during runtime is part of a regular process. The complete information is transferred, except for CBRNE (chemical, biological, radiological, nuclear or explosives), and conventional attacks, due to -dissemination-restricted intelligence data. For each case study, digests are written (the so-called “fiche reflexes” in French), typically 4-15 pages, but possibly up to 60 pages for major sectors, due to domino effects. The writing of the digest follows a method called Source (e.g., radioactive element) + Flows (e.g., impact distance) + Target (e.g., nearby school). This method is key for the “actionability” of the digest. Indeed, actions during a crisis can be performed on any of these three elements. The digests are reviewed by officers and possibly adapted to increase their effectiveness in the field. This may include adding missing elements, highlighting key elements, or removing noise (i.e., non-relevant data). The transfer is instituted, but also driven by human motivation. There is no transfer support meeting: each one must take the action of reading the reports by himself.

After each rescue operation, minutes are written (in electronic form) with statements of what worked and what did not, and improvement recommendations are made. There is a specific mailbox for comments by the dynamic risk management teams. A triage is performed by the static risk management team, and feedback is provided to the dynamic risk management contributors. This feedback is a time-consuming process, but it is essential to keep the comments coming in, and to continuously improve the process.

4.1.9 Current transitioning practices at ZAG

In ZAG, risk management is performed centrally, coordinated by the Quality Department. There is one risk management process, hence there is no distinction between static and dynamic risk management. Risk management strategy is unique for all different contexts inside the company.

The risk management is structured into four risk management process stages:

- Identify,
- Analyse, assess and prioritize,
- Mitigate,
- Check and track assess.

This covers the complete process lifecycle, and therefore there is a seamless transition between static risk management and dynamic risk management.

There are 15 process owners divided by their processes: System Management, Improvement, Commercial and Marketing, Security, Safety, Compliance and Certification, Airport Operations, Maintenance, Airport Operator, IT, Finance, Procurement, Human Resources, Legal, and Development.

The risk owner, by virtue of their level of responsibility and expertise in that field, is best suited to identify and analyse the risks and subsequently decide on measures to reduce a given risk to an acceptable level. After the initial risk management, risk and opportunity management is part of day-to-day operations of process owners, while global company risk mapping is done once a year.

Risk management delivers SOPs. Revisions are made by SOP authors, approved by process owners or the president of the management board, published on the company portal. All involved stakeholders are automatically notified about the change.

4.2 Short-listing of best practices

This section short-lists some of the best practices amongst those listed above. For these best practices, the positive and negative aspects, as well as constraints in implementing them, are identified and shortly commented.

Best practice n°1: the static risk management team prepares a specific output for the dynamic risk management team, within a continuous improvement scheme

This practice is exercised by SDMIS.

In this practice, the static risk management team prepares a specific output for the dynamic risk management team; the transfer is institutionalised and continuously improved.

Within the organisation under study, the static and dynamic risk management teams are different, but the static risk management team is well aware of the work and objectives of the dynamic risk management team. The static risk management team prepares documents for the exclusive use of the dynamic risk management team. The format and content of the transfer is optimised for maximised efficiency by the dynamic risk management team. A feedback collection and analysis process are in place to ensure a continuous improvement of the transferred information between the static and dynamic risk management teams.

Pros	Globally optimised process at corporate level.
Cons	Additional work for the static risk management team.
Constraints	There must be a very good cooperation spirit between the static and dynamic risk management teams for this process to work in the long run.

Best practice n°2: use of a GRC tool throughout the enterprise, which formalises an overall risk management process

This practice is exercised by AENA, and currently under deployment at HEP.

A GRC tool is used centrally and covers all critical parts of the company.

Pros	The risk management process is formalised throughout the entire lifecycle, and optimised for the organisation, with an optimal coverage (i.e., no parts forgotten).

Cons	- The tool deployment cost is significant, typically above 100K€. It is thus only deployable in large companies. - Since the process is centralised at corporate level, with a least privilege principle hard coded in the tool, it may lead to a loss of overall purpose by some of the stakeholders, especially those who are simply requested to provide inputs with no significant feedback.
Constraints	The GRC tool must be robust and flexible to allow implementing the same principle at all company levels.

Best practice n°3: seamless risk management while continuously improving the SOPs

This practice is exercised by KABEG and ZAG.

Process owners manage the risks and report to the central risk management. There is no special distinction between static and dynamic risk management, i.e. the same people perform both. The risk management delivers SOPs, which are continuously monitored and changed.

Pros	No need for transition since the same people do static and dynamic risk management. Thus, no information is lost in the transition
Cons	May require quality management to ensure the process continuity
Constraints	Organisation dependent, requires an integrated team

Best practice n°4: dynamic risk management based on intensely trained operatives

This practice is exercised by CMRS and KABEG.

Even though CMRS is a first responder and KABEG is a hospital, these two interviewed organisations have a quite similar approach to dealing with dynamic risk management. Both organisations heavily rely on training personnel involved in dynamic risk management. Trainings are highly specialised and continuous. Through this approach, the involved personnel reacts almost instinctively and correctly in highly dynamic and stressful situations.

Pros	- Reduction of paperwork for the transfer of static risk management results to the dynamic risk management teams. - Highly trained personnel, who can ensure quick reaction to unanticipated events.
Cons	The lack of formalised documentation may lead to difficulties for legal investigations in case of an incorrectly managed incident.
Constraints	Training is time-consuming.

5. Conclusion: lessons learnt and way forward

5.1 Key results

In this study, we interviewed nine different organisations, including seven critical infrastructures and two first responders, to understand their risk management practices, and in particular, the way they transition from static to dynamic risk management. The interviews were started with preconceived ideas about the differences between static risk management and dynamic risk management, based on the authors' experience. The interviews showed that the reality of risk management within the different critical infrastructures and first responders was very different from one organisation to the other. The definition of static and dynamic risk management also differed significantly from one organisation to the other. However, it was possible to group the organisations according to their risk management approaches, as follows:

1. Organisations that make a clear distinction between static risk management and dynamic risk management, and perform both activities, in sequence, with dedicated processes and dedicated teams;
2. Organisations that perform risk management as a continuous process, covering all activities from static risk management and dynamic risk management, in a holistic and seamless manner;
3. Organisations that perform only dynamic risk management, without any inputs from some external static risk management processes, even if some relevant static risk management results are known; it is to be noted that for some of these organisations, dynamic risk management is sometimes reduced to security vulnerability management;
4. Organisations that perform only static risk management; for these organisations, main goal of static risk management is the dimensioning and allocation of resources, whilst dynamic risk management is not systematic, i.e., it is only an informal process.

Based on this categorisation, it can be argued that the transition from static risk management to dynamic risk management is only an issue for the organisations belonging to the first group. However, we analysed in detail the processes of all organisations and we were able to extract best practices that optimise or annihilate the transitioning issue:

1. The static risk management team prepares a specific output for the dynamic risk management team, within a continuous improvement scheme
2. Use of a GRC tool throughout the enterprise, which formalises an overall risk management process
3. Seamless risk management while continuously improving the SOPs
4. Dynamic risk management based on intensely trained operatives

We believe that these practices are general enough to be used beyond the companies that currently implement them. However, they are highly dependent on the organisational structure of the companies, and some of them are mutually exclusive. Thus, it is impossible to recommend this set of four best practices as THE solution. It is also unknown, whether this set of practices is representative of all critical infrastructures and first responders. The survey should probably be extended to a wider set of companies to assess the coverage of current transitioning practices. This activity should be covered as a follow-up of the PRAETORIAN project.

5.2 Other lessons learnt

From a methodological viewpoint, some lessons should also be learnt from this research.

When we created the questionnaires, we assumed that the static and dynamic risk management teams would be different. To this end, some questions were common in both static and dynamic risk management questionnaires (cf. Annex A).

However, in some cases, the interviewer faced the same team. The way the questionnaire was built made, it was difficult to identify the common questions and avoid repetitive questions. As a lesson learnt, the questionnaire should be organised in at least three parts: (i) generic context and risk management questions; (ii) static risk management specific questions, including transitioning to dynamic risk management; (iii) dynamic risk management specific questions, including transitioning from static risk management.

We also assumed that the definitions of static risk management and dynamic risk management were shared in the risk management community. As already discussed above, this was not the case. The contours of static risk management and dynamic risk management are fuzzy. Most critical infrastructures and first responders have different interpretations of those terms. It would have been useful to systematically ask each organisation to provide its own definitions, and then build the rest of the interviews using these definitions as basis.

The length of the interviews was quite often an issue, due to the low availability of the interviewees. To cope with this availability issue, it would have been useful to have a first short interview to understand if there is indeed a transitioning process between static and dynamic risk management within the targeted organisation. Then, if such a process is identified, a second more detailed interview could have been run to understand the details of this transitioning process. This could have saved us significant interview time.

Last but not least, it is important to note that these interviews were a moment of “intimacy” between the interviewers and the interviewees. Even if the questionnaires only addressed methodology and not the content of the risk assessments, some companies were very careful on what they revealed and censored some organisational details before publication. Indeed, describing how a company manages risks sometimes reveals a lot of information on which parts are left out, possibly indicating vulnerabilities. The interviews were also a time during which the interviewees took a step back on their own processes, sharing opinions with their interviewers. Some interviewees declared having a better understanding of the strengths and weaknesses of their own processes after the interviews, which was an unexpected side effect.

6. References

[1] ISO 31000, “Risk management – Guidelines,” International Organization for Standardization, 2018.

[2] A. Shimel and M. Miller, “A Brief History of DevSecOps and Where We Go From Here,” RSA Conference, Webcasts, Jul 30, 2019.

[3] M. A. Amutio, J. Candau and José Antonio Mañas, MAGERIT – Methodology for Information Systems Risk Analysis and Management, Madrid, Spain: Ministry of Finance and Public Administration, July, 2014.

[4] SAP, “Governance, Risk, Compliance (GRC) and Cybersecurity,” [Online]. Available: https://www.sap.com/uk/products/erp-financial-management/grc.html. [Accessed 25 11 2021].

[5] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), “Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) - Méthode de gestion des risques,” 2010.

[6] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), «Centre gouvernemental de veille, d’alerte et de réponse aux attaques informatiques (CERT-FR),» [En ligne]. Available: https://www.cert.ssi.gouv.fr/. [Accès le 25 11 2021].

[7] “Spanish National Security Framework (Esquema Nacional De Seguridad),” Gobierno de España. Ministerio de la Presidencia. Secretaría General Técnica, April 2010.

Annexes

I. ANNEX A – Interview guidelines

General observations - confidentiality

Given that the deliverable is public, it is reasonable to expect a certain degree of reluctance. However, we are *not* interested in particular risk assessment results and exact vulnerabilities of the critical infrastructure operated by project partner, which are surely confidential. The focus in this task is on generalized methods and practices instead.

Design-time Risk Management Interview Guidelines

Introduction: Explain the conceptual difference between static risk management during design-time, and dynamic risk management during operational time (run-time). Explain the inevitable trade-off and removal of information to make risk actionable.

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

2. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

3. What types of risk / threats do you manage?

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

5. In your field, is static risk management mandatory by regulation? Which regulation?

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?
   7.1. Do you perform the risk management yourself or is it sub-contracted?
   7.2. How many people are involved?
   7.3. What are their required skills?
   7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?
8. Are there provisions to infer from other risk management teams?

9. Who has the last word on the risk treatment options?
   9.1. Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive, and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

10. How much time / budget is dedicated to this initial risk assessment?
    10.1. Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we'll get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.

11. What is the risk study time frame being considered?
    11.1. For how long your risk assessment is valid?
    11.2. When do you schedule minor updates or complete reviews of your studies?

<u>*Methodology*</u>

12. What are the utilized risk management methods / techniques?

13. What input data is required?

14. At what level of abstraction are you working?
    14.1. Typically, how many business assets? Supporting assets?
    14.2. Do you list all vulnerabilities, e.g. using CVEs?
    14.3. Is there maybe an official (mandatory) list of vulnerabilities?
    14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK?
    14.5. Do you assess compliance to all security measures?
    14.6. Are there particular flaws or vulnerabilities that require special focus?

15. What are the general assumptions (hypotheses)?
    15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?
    15.2. Is there already provision for dynamic updates of these hypotheses?

16. How often is the risk management activity conducted?
    16.1. Are there provisions for risk model (i.e. security file) updates?
    16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)?
    16.3. Are those triggers OK or should there be others?

16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

18. How are the standard operating procedures designed?
    18.1. What is the process of amending the procedures?
    18.2. Does the risk management team participate in the design of SOPs for the operational teams?
    18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?
    19.1. What specific risk management standards must you comply with?
    19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports)*.
    19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure*.

20. Do you collaborate with national security entities or other national and international bodies?

21. How do you model acceptable levels of risk?
    21.1. What risk treatment strategy do you use?
    21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?
    21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)?
    21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?
    21.5. An example: in some contexts in transmission system operators the N-1 criterion (ability of system to cover the failure of largest system unit), a.k.a. no single point of failure, is often used, contrasted to more elaborate probabilistic models that are used in other contexts. This criterion is only an illustrative example, other types of CI may utilize different assumptions, the idea is to try to catch what these criteria are.

22. Are cascading effects a specific issue for you? How are they currently managed?
    22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

<u>Use of static risk management results</u>

23. Who in your organisation reads the risk management report after completion?

24. How are the risk management results used during design-time?

25. Are the risk management results of one system / programme shared with other systems / programmes / teams within your organisation?
    25.1. If there is risk management performed at specific project level versus the programme, team, or organizational level, is there sharing between different levels?

26. Is the risk management report sent outside of your organisation? To whom?

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

27. Is there a process to transfer the results from design time to run time?

28. Have you already transferred some static risk assessment results for reuse during runtime?
    28.1. Do you communicate your results to the run time teams (directly?)?

29. Who took this initiative?
    29.1. Has this been called for by runtime operators or someone else?

30. To whom were the results transferred?

31. What was the main goal of this transfer? Was this a shared goal with the recipients?

32. Do you have an established procedure of reporting the risk management results to stakeholders outside your company?

33. Were the complete results transferred or only some parts? Which parts?

34. With what level of abstraction were the results transferred?

35. How much effort was dedicated to the transfer operation?

36. How efficient was this transfer?

37. Did you receive some feedback from the runtime teams after the transfer? How much time after? And what type of feedback?

Real-time / Run-time Risk Management Guidelines

Introduction: Explain (briefly) the conceptual difference between static risk management at design time and dynamic risk management during operational time (run-time). to support attack detection & response. Explain the inevitable trade-off and removal of information to make risk actionable.

Expected results of the interview:

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of operational risk management at run-time?

2. What is the business or technical context of this operational risk management? Describe the context and area where the end user is working (e.g. hydro power plant, control centre etc.)

3. What types of operational risk / threats do you face in your normal operation? What principal threats affect your operation?
   3.1. What are the primary threats that affect your normal operation?

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (technical risk, procedural risks) and flowing of these risks to relevant stakeholders.

5. In your field, is dynamic risk management mandated by regulation? Which regulation?

6. Do you have an accreditation / certification to maintain?
   6.1. Who is the accreditation / certification body?
   6.2. At what rate must the accreditation / certification be renewed?

Logistics

7. Who performs the operational risk management?
   7.1. Do you perform the risk management yourself or is it sub-contracted?
   7.2. How many people of involved?
   7.3. What are their required skills?

8. How often are the risk management results updated?
   8.1. Are there events that trigger (should trigger) an update?
   8.2. Outside of those events, who can decide to launch an update?

9. How much time / budget is dedicated to risk management updates?

10. Are the updates usually performed by the same people who did the initial analysis? If no, are their skills / competencies different or similar?

11. Outside of a crisis situation, who has the last word on the risk treatment options whilst the system is operational?

12. During a crisis, what is the decision chain? Who has the last word on the response to apply?

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

13. Is there a process to transfer the results from design time to run time?

14. Do you usually start the risk assessment from scratch or to you have the static risk assessment results as input?

15. Who took the transfer initiative?

16. From where / which team do the results originate?

17. What was the main goal of this transfer? Was this a shared goal with the static risk analysis providers?

18. Do you reuse the complete static risk analysis or only parts thereof?

19. How useful are these inputs? (Estimate)

20. What are the areas where the inputs where the most useful, e.g. business / operational impact analysis?

21. Did you have to rework the inputs, typically the level of abstraction?

22. Is some form of traceability organised between the static and dynamic risk management results?

23. Have you already provided feedback to the static risk management teams?

24. Is this feedback manual or automated?

Risk Management Methodology

25. What are the (operational) tasks involved in risk management during runtime?

26. What input data are required for dynamic risk management and how do you collect the data?

27. At what level of abstraction are you working?
    - 27.1. Typically, how many business assets? Supporting assets?
    - 27.2. Is it different to the abstraction level in static risk management? (Note: see also the answer to question 21 above).
    - 27.3. How do you handle the detected vulnerabilities? Is there a procedure for doing so?
    - 27.4. Do you assess compliance to all security measures?
    - 27.5. Are there particular flaws or vulnerabilities that require special focus?
    - 27.6. Are there applicable international standards? (List only the most important ones).

28. What are the general assumptions (hypotheses)?
    - 28.1. How often are these hypotheses updated?
    - 28.2. Is there a provision for dynamic updating of these hypotheses?

29. How often is the risk management activity conducted?
    - 29.1. What triggers the risk management related actions? (Set intervals, actions, etc)
    - 29.2. Are there provisions for the risk model updates?
    - 29.3. What specific triggers are there to update the risk model? Is it triggered periodically, on a specific action or triggered by an external factor?
    - 29.4. Are the existing triggers OK or do you think there should be other ones?
    - 29.5. What is the typical lifecycle of the risk model?

30. Are there different hierarchical levels in the company that perform the risk management? For example, are the risk management results at lower organizational levels in the company prepared on their own and then fed higher in the organization?

31. Do you have a standard operating procedure guidebook?
    - 31.1. What standards is this book compliant with?
    - 31.2. Are there applicable international standards considering the SOPs? (List only the most important ones).

32. How are the standard operating procedures designed?

32.1. What is the process of amending the procedures?
32.2. What triggers the SOP updates?
32.3. Is there participation / collaboration with static risk management team in the design of SOPs?
32.4. Who are the specialists involved in design, mandating and eventual invalidation of SOPs and the corresponding operational documentation?

33. Is there a specific standard family (e.g. similar to ISO 27000 family of standards) that governs the risk management?
33.1. What specific risk management standards must you comply with?

34. How do you model acceptable levels of risk?
34.1. What risk treatment strategy do you use?
34.2. Do you define different strategies in different operational contexts?
34.3. Is there a risk aversion matrix (aka risk appetite matrix)?
34.4. Is that matrix unique within the organization or are there multiple ones?

(In some operational contexts of e.g. transmission system operation different risk models and acceptable risk levels are modelled in different fashion. The idea is to capture what the assumed criteria are).

35. Are cascading effects a specific issue for you? How are they currently managed?
35.1. Note: this is an important question for T2.2. Please give enough focus here.

<u>*Use of risk management results for detection and response*</u>

36. How are the risks / threats presented (e.g. semaphore, numerical presentation, alerts…)?

37. How many of these security events are real attacks? Are there often false positives? (Estimate).

38. Have you already experienced a false negative (i.e. undetected attack until too late)?

39. How often do you trigger corrective actions?

40. Are there automatic notification systems when the corrective actions are triggered?
40.1. Is there a system for automatic notification when corrective actions are taken manually or automatically?
40.2. Note: The idea is to get the situation "from the field".
40.3. Is there an identified lifecycle for an alarm / notification – is it automatically dismissed after some time even with no action on behalf of the operator?

41. Are there automatic risk mitigation actions in the systems you monitor?

41.1. If so, how are you informed on automatic results (think primary and secondary reserve activation, automatic generation control in terms of power system, closing of perimeter in the critical infrastructures primarily dealing with physical risks such as airports)

42. Crisis management: How do you perform escalation when the resources at your disposal are not enough to handle the current level of risks?
    42.1. Note: this is an important question for T2.2. Please give enough focus here.

Other uses of risk management results

43. Are the dynamic risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

*Operational context questions (**optional**)*

44. How many different risk sources do you handle in a typical hour/day of operation?
    44.1. Is that number consistent with what was handled during static risk management?

45. How many observables / events do you manage in a typical hour of operation? Is there a seasonality (e.g. flood season?)

46. How many of these alerts are classified as security events? Estimate a percentage.

II. ANNEX B – AENA extensive interview

Design-time Risk Management Interview

Participants: they are from AENA Central Services (Madrid)

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

Board of Directors: defines, updates and approves the Policy, as well as setting the acceptable risk in each situation, being ultimately responsible for the existence and operation of an adequate and effective risk management system

The Audit Committee supervises the risk management system, ensuring that the main risks are identified, managed, communicated and maintained at planned levels.

Internal Audit Department: assists the Audit Committee; supervising the correct operation of the system; homogenizing and consolidating reports related to the identification and evaluation of risks and their corresponding indicators, mitigating activities and action plans; and reporting to the Management Committee and the Audit Committee.

Corporate and operational areas: they identify and evaluate the risks that are under their area of responsibility, as well as the mitigating activities, proposing and reporting the indicators for proper monitoring, establishing action plans to mitigate the risks and reporting on their effectiveness.

In relation to the cybersecurity operational area, there is the ICT Security Office (OSTIC) that is supported by different technical assistances that work on site (on premises) with AENA's personnel.

Risk analysis is done when they do audits. The compliance auditor is the one who does it. It is a **service for security review**, and the auditor goes through the different AENA centres according to an annual planning. A different service also focuses on hacking on IT and OT infrastructures.

There is a Demand Management committee. When a new product is to be released, an “informal” risk analysis is carried out and a series of controls are put in place.

They also have a Detection and Response Centre - internal CSIRT. When it detects a technical-related risk, a notification is generated. They monitor vulnerabilities.

They also have the GRC office that reviews new files, feasibility of new solutions. They have consultants, people in the office, that review the plans and check fulfilment with 27001 (frame of reference).

2. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

AENA is the world's leading airport operator with more than 293 million passengers in 2019 (Spanish airports + Luton). Risk management covers all of AENA's activity as an airport infrastructure operator.

It should be mentioned that the air control centre (ATC) is the responsibility of the ENAIRE company and not of AENA: the control towers are owned by AENA but the systems are owned by ENAIRE and are not supervised by AENA.

3. What types of risk / threats do you manage?

The 2020 (reviewed in 2021) risk map shows the main risks to which AENA has been exposed. The System review, carried out in the context of the health emergency to adapt it to the new reality, has identified in the Map a total of 18 risks. They are all classified into operational, financial, technological, legal and compliance and information.

Each of these risks can be disaggregated into the operating units into several more specific risks, but their reporting and monitoring in the high-level risk analysis are carried out jointly.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?

AENA classifies risks into strategic, operational, financial, technological, legal and compliance, and information. Type of risks:

STRATEGIC: Risks that can arise from a chosen business strategy, and those from external and internal sources that could have a significant direct or indirect impact on the Group achieving its long-term vision and objectives. This category includes risks arising from changes in the environment in which the Group operates (political, economic and social), in the competitive environment (aeronautical and non-aeronautical market), and changes that affect fees and operations, among others. All risks related to the governance model are included in this type.

OPERATIONAL AND TECHNOLOGICAL: These are the risks of suffering losses or lower activity due to weaknesses or failures in internal systems, controls or processes. Operational risks include those, among others, resulting from failures in the security of infrastructure and systems, investments, coordination of operations and air control; in addition to those related to employment and human resources.

FINANCIAL AND NON-FINANCIAL: Events that may have negative impacts and significantly affect the results of financial operations, usually due to market, credit and liquidity risks.

LEGAL AND COMPLIANCE: Risks related to the mandatory nature of legal provisions established by national and international bodies and institutions in relation to compliance with general legislation (environmental, commercial, criminal, tax, labour, etc.), and sector and internal regulations.

INFORMATION: These are risks related to the reliability of the sourcing, and preparation of financial and non-financial information, both internal and external, that are significant for the Group, or which affect the reputation of the Company.

4.1. Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

Once the risks have been identified at AENA (currently 18 risks identified), responsibilities are designated for each risk. Each risk is associated with an operating unit, which is responsible for identifying and evaluating said risks and their different components, as well as action plans and mitigating activities.

The ICT Security Office (OSTIC) is responsible for cybersecurity operational risk, which uses a specific methodology to manage each risk at a specific level. This methodology is MAGERIT[2] and the tool used is PILAR.

They are implementing ISO 27001 in the OSTIC. The Central Services are certified, most of the IT infrastructures are already centralized. They already have Madrid and Barcelona certified. They are in process with Palma de Mallorca. Valencia is not in the plan. They will continue the process after consulting AENOR, the Spanish certification authority. What they have done so far was due to the commitment with CNPIC as the regulator entity. Nevertheless, AENA will apply the same procedures even if the infrastructure is not yet certified, since the services that are provided about ICT security are global.

In Valencia they do an audit every two years to check if everything is well implemented, and they propose corrective actions. They have very broad action plans, there are 14 domains according to 27001 for all ICT security.

5. In your field, is static risk management mandatory by regulation? Which regulation?

In general, you must comply with a regulatory framework:

CAPITAL CORPORATIONS LAW

- Article 540: obligation to publish an annual corporate governance report that includes, among other aspects, information on the risk management and control system.

- Article 529 ter: the Board of Directors has the non-delegable power to determine the risk control and management policy and to supervise the internal information and control systems.

- Article 529 quaterdecies: the Audit Committee's function is to supervise the effectiveness of the risk management system.

CNMV RECOMMENDATIONS

- Technical Guide 3/2017 on EIP's Audit Committees, recommends the annual reassessment of the list of risks.

- Code of good governance of listed companies, revised in June 2020.

LAW 11/2018 ON NON-FINANCIAL INFORMATION

In relation to physical and operational security, there is the National Security Program for Civil Aviation. On the other hand, ICAO Annex 17 Security incorporates standards and recommendations for the Protection of international civil aviation against acts of unlawful interference.

[2] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

ISO 27001 is applied for ICT security (Cyber risks) by AENA. ENAIRE applies the ENS[3] (Esquema Nacional de Seguridad, Security National Schema) but AENA does not.

At CNPC level (Comisión Nacional de Protección Civil, Civil Protection National Committee) a global risk analysis is made at the company level, and it includes everything -not only cyber-.

There is going to be a regulatory change, from the state aviation safety agency, they will draw up a mandatory regulation for airport managers. It will be focused on very specific physical security systems.

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

ISO 27001, AENOR

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?

7.1. Do you perform the risk management yourself or is it sub-contracted?

7.2. How many people are involved?

7.3. What are their required skills?

7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?

This was answered in question 1, where the responsibilities of the board of directors, the audit committee, the Internal Audit Department and AENA's operational areas are defined.

For the Cybersecurity part:

For example, in the case of a new product, this is done by the Demand Management committee. First, there is a person with a security architect profile, to know the systems and networks at a high level. Very technical profile, but with a very general vision. He/she makes recommendations at a general level. Example: innovation projects all have a cyber component. The project with the approval goes to the Demand Management committee, and here it is analysed from all aspects, it can be 25 people, and different airports are involved.

8. Are there provisions to infer from other risk management teams?

The Internal audit management reports directly to the AENA’s Management Committee. They review, ask questions, the methodology they use is not known.

The financial management also does risk analysis. They also do their audits and reviews

To sum-up, there are three levels:

1. Risk management policy -> Board of Directors. Approval of 18 high-level risks.

[3] https://ens.ccn.cni.es/es/esquema-nacional-de-seguridad-ens

2. Audit committee. Internal audit department. Management of the internal risk management system. GRC SAP Tool.

3. Corporate and operational areas. Specific risks with the application of different methodologies and tools are reported to the internal audit department.

9. Who has the last word on the risk treatment options?
   9.1. Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive, and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

At a high level: the Management Committee. From there, each one has their responsibilities at their levels.

For the cybersecurity part: The OSTIC has its representative, who analyses and makes recommendations. Above the OSTIC we have the Director of Cybersecurity. He makes the final decision. The risk is intended to be minimal, and someone has to accept it.

10. How much time / budget is dedicated to this initial risk assessment?
    10.1. Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we'll get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.

Complicated, it depends on parameters. It is a minimum percentage of the cost of security with respect to IT. This year it will be about 7.5% with respect to IT (Budget for the OSTIC). Other elements such as firewalls, and IT systems run by the communications department, or antivirus, are counted as well. So, in case there is obsolete equipment to replace, this might vary. We have to give clear criteria.

11. What is the risk study time frame being considered?
    11.1. For how long your risk assessment is valid?
    11.2. When do you schedule minor updates or complete reviews of your studies?

Formal analysis, signed by Management: The most critical parts have reviews every year.

Detection of new vulnerabilities is done daily.

There are agreement with other entities that report threats, so that measures can be taken.

<u>Methodology</u>

12. What are the utilized risk management methods / techniques?

Risk Management methodology: COSO III Framework & GRC SAP Tool

Cybersecurity: MAGERIT (Methodology for Information Systems Risk Analysis and Management) & PILAR Tool

13. What input data is required?

GRC SAP TOOL: general information about each high level risk (risk name, definition, responsibilities, categorization) key risk indicators (A number of indicators which shows to what extent does the risk start to materialise), Key risk indicators record, impact and probability for each risk, actions (ongoing activities, contingency plans, and actions plans)

Cybersecurity (PILAR): definition and classification of assets, asset value in terms of the different dimensions of the security (confidentiality, trustworthiness, availability, authenticity and traceability), threat frequency, threat deterioration, potential impact, potential risk (potential impact X frequency x 10), level of effectiveness of safeguards.

14. At what level of abstraction are you working?

14.1. Typically, how many business assets? Supporting assets?

REMEDY tool, with asset management module.

14.2. Do you list all vulnerabilities, e.g. using CVEs?

They are proposing a Vulnerability Management Project, it is very complex. They need a specific tool and an implementation process of years to know the minimum level of detail. This is now under defining a tendering process.

14.3. Is there maybe an official (mandatory) list of vulnerabilities?

There is a patch management committee, vulnerabilities are defined at the generic level.

14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK?

Yes, through a corporate REMEDY tool in the case of cybersecurity

14.5. Do you assess compliance to all security measures?

Yes, through the different internal and external audit systems according to the process to which it refers

14.6. Are there particular flaws or vulnerabilities that require special focus?

Yes. Especially those of cybersecurity and on the other hand those applied in the legislation of illicit acts in air transport.

15. What are the general assumptions (hypotheses)?

15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?

Every 6 months for the System as a whole, each specific risk may have updates with other frequencies

15.2. Is there already provision for dynamic updates of these hypotheses?

Not automatically, but through periodic reviews and committees at different levels

16. How often is the risk management activity conducted?

16.1. Are there provisions for risk model updates?

16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)? Periodically, triggered by an external factor (as Brexit or COVID – 19 Situation), or on an specific action when the level of tolerance of some risk is exceeded

16.3. Are those triggers OK or should there be others?

16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

Revision of the risk management system annually, monitoring risk management system activity daily according to the Key risk indicators and measures associated to each risk.

Existing triggers are OK.

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

Yes, this is explained the levels of responsibilities in question 1. AENA's operational and corporate areas report the indicators and execute the action plans, feeding AENA's risk management system managed by the Internal Audit Department and the Audit Committee.

18. How are the standard operating procedures designed?

Depending on the area to which it corresponds with operating instruction systems (e.g. EXAS in operations and security).

18.1. What is the process of amending the procedures?

Drafting by the corresponding centralized unit, approval by the Management Committee of the unit involved and depending on the range of the Operating procedure, in this case is the AENA Management Committee

External approval (AESA, Agencia Estatal Seguridad Aerea- National Agency for Aerial Security) for security procedures that affect the security of air transport and modify the certificates currently in force.

And the same for the safety of air operations (also AESA).

18.2. Does the risk management team participate in the design of SOPs for the operational teams?

No, but they do review them if they are included in the risk management programme.

18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?

It depends on each SOP, centralized operating units and even field units for local procedures.

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?

19.1. What specific risk management standards must you comply with?

Regulations generated by EASA (EU Agency) and applied in Spain by AESA (National Agency) regarding operational safety and physical security of airports.

Regarding other areas (financial, cybersecurity, industrial facilities), those that are common to any other facility and company.

19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports).*

19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure.*

ISO 27001 ICT Security.

20. Do you collaborate with national security entities or other national and international bodies?

Yes, both through government agencies and organizations or through local security committees at each airport.

21. How do you model acceptable levels of risk?

For each generic risk, tolerance levels are defined based on indicators. If these levels are exceeded or are close to being exceeded, alarms are created to activate contingency / mitigation actions. These indicators are monitored by the corresponding operational areas. For each high-level risk, a probability and an impact are assigned by creating a criticality index and placing it on the risk map.

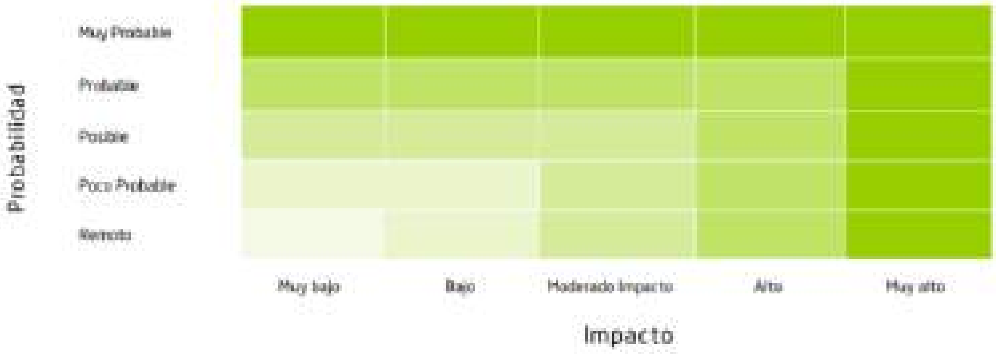
21.1. What risk treatment strategy do you use?

COSO III Framework

21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?

Yes, for the global risk management system, AENA uses the COSO III methodology, but in a specific way each of the operational risks can be applied a specific methodology, as is the case of the cybersecurity MAGERIT methodology.

21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)? YES



21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?

For the 18 high level risk is unique.

22. Are cascading effects a specific issue for you? How are they currently managed?

22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

n/a

Use of static risk management results

23. Who in your organisation reads the risk *management* report after completion?

The entire Management Committee where all the organization and operation units are represented.

In addition, it is the task of each Management to designate the people in their area of responsibility who will analyse the report or parts of it.

24. How are the risk *management* results used during design-time?

Both "active" risks and residual risks are always a starting point.

25. Are the risk *management* results of one system / programme shared with other systems / programmes / teams within your organisation?

Yes, at the level of each of the 18 risks. In general, there is no direct relationship between each of the 18 risks, but there is between the management of a risk and other program systems in the organization related to it.

25.1. Sometimes risk management is done at project level, and sometimes at the programme or organizational level – is there sharing between different levels?

Yes, at the level of each operational department.

26. Is the risk management report sent outside of your organisation? To whom?

Not entirely.

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

27. Is there a process to transfer the results from design time to run time?

Yes, there is a risk monitoring and reporting step in the methodology used. This process is implemented in the SAP GRC application where the operational areas, which are those that are in the execution of risks (run time), report on the indicators according to the estimated periodicity in each one of them. These indicators are monitored by Audit Committee, which is the one that manages the system at a high level and designs it, in addition, the system reviews are centralized from there.

28. Have you already transferred some static risk assessment results for reuse during runtime?

28.1. Do you communicate your results to the run time teams (directly?)?

The 18 risks identified in the risk map establish a general framework. For each risk, a series of threats / events that can occur are established and managed by each corresponding operating unit. It could be said that from the static risk analysis, the results are transferred to the dynamic analysis.

29. Who took this initiative?

    29.1. Has this been called for by runtime operators or someone else?

    The Audit Committee and the Internal audit department are responsible for transferring static risk assessment to dynamic and the correct runtime when a risk appears or is near tolerance threshold.

30. To whom were the results transferred?

    From Internal audit department to operative department (as IT, airports, security…)

31. What was the main goal of this transfer? Was this a shared goal with the recipients?

    The proper performance of the risk monitoring and evaluation. And the proper development of actions plan and contingency plans that are carried out.

32. Do you have an established procedure of reporting the risk management results to stakeholders outside your company?

    Yes, in the annual report on public non-financial information on AENA's website there is a section on operational and financial risks, where interested parties are informed of the risk management system.

33. Were the complete results transferred or only some parts? Which parts?

    The parts related to each responsible operative area. These parts include indicators, actions of the management of risk, assessment of the risks

34. With what level of abstraction were the results transferred?

n/a

35. How much effort was dedicated to the transfer operation?

n/a

36. How efficient was this transfer?

n/a

37. Did you receive some feedback from the runtime teams after the transfer? How much time after? And what type of feedback?

Yes, the operative areas have the responsibility to report the monitoring of the risk that are responsible for.

Real-time / Run-time Risk Management Interview

Interviewees: Luis Uia (physical security technician), Joaquin Rodriguez (Director of Valencia Airport), Jordi Peral (IT Area Manager)

Interviewer: Eva Muñoz (ETRA)
Dates & times of interviews:

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of operational risk management at run-time?

Cybersecurity: Nothing locally, everything is centralized, either CSIRT or OSTIC. There are reviews that everything is well connected and updated, physically it is control of leaked communications sockets to just a mac, antivirus, everything updated.

2. What is the business or technical context of this operational risk management? Describe the context and area where the end user is working (e.g. hydro power plant, control centre etc.)

Counter and boarding system, passenger info systems, AENA computers and AENA companies connected to a multi-service server. There is a macro LAN, the national police has its internal network but it goes out through AENA's router, it is integrated into AENA's.

Also about the emergency teams, health, etc., everything is within the macro LAN. There is a specific rack for emergency communications.

3. What types of operational risk / threats do you face in your normal operation? What principal threats affect your operation?
   3.1. What are the primary threats that affect your normal operation?

1. The most important thing is malicious email. It affects many workers. From the OSTIC there are awareness campaigns.

2. Someone might use the wi-fi network to break into the network. AENA thinks that it is not so easy.

3. About denial of service attacks or communications interference? They haven't found anything.

There are two types of communications. Ground communication, and ground-air equipment, which is more critical and protected, carried by ENAIRE.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (technical risk, procedural risks) and flowing of these risks to relevant stakeholders.

Critical, medium or low vulnerabilities arrive from the OSTIC reports. They are related to software patches.

5. In your field, is dynamic risk management mandated by regulation? Which regulation?

Not at the regulatory level, it is company policy. Organized monthly.

6. Do you have an accreditation / certification to maintain?
    6.1. Who is the accreditation / certification body?
    6.2. At what rate must the accreditation / certification be renewed?

Everything related to OSTIC, this is explained previously in this interview.

Logistics

7. Who performs the operational risk management?
    7.1. Do you perform the risk management yourself or is it sub-contracted? All airport systems management (communications and public address system) is outsourced with a file. The part of IT systems is another file, it applies to the systems and security patches. Subcontracted and supervised by AENA.
    7.2. How many people of involved? For IT systems there is a technician with the file, but there is support from central services.
    7.3. What are their required skills? Training or certifications are requested depending on the systems. For example at the Linux level, but not Cisco.

n/a

8. How often are the risk management results updated?
    8.1. Are there events that trigger (should trigger) an update?
    8.2. Outside of those events, who can decide to launch an update?

Everything comes from Madrid. See static risks management part.

Recurring incidents can be reported to OSTIC to trigger a review.

Everything is constantly monitored and everything is reported... it will depend on the criticality of the affected system. They do not know if this can make that risk management is reviewed or simply that the issue is solved.

Patches and improvements arrive monthly to be implemented. If a specific incident is detected in that period, the notification is generated and resolved immediately. It is fast if there is a critical incident.

9. How much time / budget is dedicated to risk management updates?

Risk management is at Audit Management. It would be necessary to find out how much staff they have, what time they invest, etc.

10. Are the updates usually performed by the same people who did the initial analysis? If no, are their skills / competencies different or similar?

n/a

11. Outside of a crisis situation, who has the last word on the risk treatment options whilst the system is operational?

It is decided from Central Offices (Madrid). The tools to be used come from central services, the action plans involve airport managers, IT areas, the steps to be taken are reported, but the strategy comes from central. No airport takes action unilaterally. They verify that everything is implemented correctly. The premise is to work globally.

12. During a crisis, what is the decision chain? Who has the last word on the response to apply?

A crisis committee is created involving OSTIC and airport directors.

There is a group for ICT incidents where there are Central Services and airports, with the objective to know everything in real time and manage it as quickly as possible.

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

13. Is there a process to transfer the results from design time to run time?

Yes, there is a risk monitoring and reporting step in the methodology used. This process is implemented in the SAP GRC application where the operational areas, which are those that are in the execution of risks (run time), report on the indicators according to the estimated periodicity in each one of them. These indicators are monitored by the audit committee, which is the one that manages the system at a high level and designs it, in addition, the system reviews are centralized from there.

14. Do you usually start the risk assessment from scratch or to you have the static risk assessment results as input?

We use static risk assessment results as input

15. Who took the transfer initiative?

n/a

16. From where / which team do the results originate?

From each operative department

17. What was the main goal of this transfer? Was this a shared goal with the static risk analysis providers?

n/a

18. Do you reuse the complete static risk analysis or only parts thereof?

n/a

19. How useful are these inputs? (Estimate)

n/a

20. What are the areas where the inputs where the most useful, e.g. business / operational impact analysis?

Both of them, in the annual non-financial information report, where AENA informs about his results

21. Did you have to rework the inputs, typically the level of abstraction?

n/a

22. Is some form of traceability organised between the static and dynamic risk management results?

Yes, the Audit Committee and the Audit Management are in charge. At the operational area level, you have some working groups in place, which are in charge of reporting

23. Have you already provided feedback to the static risk management teams?

Yes, one of the steps of the RISK methodology (COSO III Framework) is reporting and monitoring, where the operational departments report to the auditee committee and provide feedback about the running time of the risks (risks identified on the map)

24. Is this feedback manual or automated?

Manual, except for the indicators which it is through the tool (GRC SAP tool)

Risk Management Methodology

25. What are the tasks involved in risk management during runtime?

Having established indicators for each risk and those responsible for each operating unit of AENA, they have to monitor the indicators at the frequency that has been estimated. And if the tolerance is reduced, apply or execute the measures of the action plans. If a risk occurs, the established contingency plans and procedures must be executed.

26. What are the utilized risk management methods / techniques?

Cyber: MAGERIT methodology

27. Do you have a standard operating procedure guidebook?
    27.1. What standards is this book compliant with?
    27.2. Are there applicable international standards? (List only the most important ones).

The OSTIC has implemented a risk management and assessment standard based on the MAGERIT methodology.

ISO 27001

28. Are cascading effects a specific issue for you? How are they currently managed?
    28.1. *Note: this is an important question for T2.2. Please give enough focus here.*

No, as a general rule. Being a critical infrastructure, there are very strict procedures and the cascading effects are limited.

__Use of risk management results for detection and response__

29. How are the risks / threats presented (e.g. semaphore, numerical presentation, alerts…)?

A tolerance is defined and this is given by the registry of indicators identified in each risk. If the tolerance is exceeded, an alarm is activated. Every risk and its tolerance well displayed at a semaphore.

30. How many of these security events are real attacks? Are there often false positives? (Estimate).

n/a

31. Have you already experienced a false negative (i.e. undetected attack until too late)?

Yes

32. How often do you trigger corrective actions?

When the tolerance of some risk is compromised, this is valued and corrective actions are taken.

33. Are there automatic notification systems when the corrective actions are triggered?
    33.1. Is there a system for automatic notification when corrective actions are taken manually or automatically?
    33.2. Note: The idea is to get the situation "from the field".
    33.3. Is there an identified lifecycle for an alarm / notification – is it automatically dismissed after some time even with no action on behalf of the operator?

Yes, through the tool. On the other hand, the Audit Management and the team are in charge of monitoring the action plans, contingency actions and the actions or measures implemented. The actions taken on the platform must be included and the values of the indicators must be updated so that the tolerance value is updated.

34. Are there automatic risk mitigation actions in the systems you monitor?
    34.1. If so, how are you informed on automatic results (think primary and secondary reserve activation, automatic generation control in terms of power system, closing of perimeter in the critical infrastructures primarily dealing with physical risks such as airports)

Yes, there are contingency plans for each of the risks. In addition, AENA has a business continuity plan that, if at any time there is an attack or failure of the electricity grid, the plan becomes operational and AENA's activity would continue.

35. Crisis management: How do you perform escalation when the resources at your disposal are not enough to handle the current level of risks?
    35.1. Note: this is an important question for T2.2. Please give enough focus here.

AENA considers that it has all the resources at its disposal to manage the risks that are identified on the map. We have a business continuity plan that will be run when a crisis has been triggered. In an extreme situation the operation would stop.

Other uses of risk management results

36. Are the dynamic risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

Audit committee and the internal Audit committee, yes and when relevant for the proper risk management system.

*Operational context questions (**optional**)*

37. How many different risk sources do you handle in a typical hour/day of operation?
    37.1. Is that number consistent with what was handled during static risk management?

n/a

38. How many observables / events do you manage in a typical hour of operation? Is there a seasonality (e.g. flood season?)

n/a

39. How many of these alerts are classified as security events? Estimate a percentage.

n/a

III. ANNEX C – CMRS extensive interview

Important notice: The interpretation of static vs. dynamic risk assessment has been understood as follows:

- Static risk assessment relates to risk assessment performed in preparation of an event, before CMRS is called to act on the field;
- Dynamic risk assessment relates to risk assessment performed during operations, starting as soon as CMRS receives a call to act on the field; it therefore always relates to an incident, accident and / or crisis situation.

Design-time Risk Management Interview

Interviewee: Zdenko Lovrić (volunteer rescue operative, CMRS)
Interviewer: Tamara Hadjina (researcher, KONČAR)
Dates & times of interviews:

- 29/10/2021, 9:00-11:00

Can you briefly describe your organisation?

CMRS: 1000 volunteer rescuers, 20 professionals (heads of commission/sector, project management, administration).

The Croatian Mountain Rescue Service (CMRS) is a national, voluntary, professional, humanitarian and non-partisan association working in the public interest. It is dedicated to preventing accidents and providing rescue and first aid services in mountains and other hardly accessible or inaccessible areas as well as in extraordinary circumstances which require special know-how and equipment for preserving human, material and environmental resources.

The CMRS is a non-profit association that performs services of national interest. There are 25 mountain rescue bases (stations) across the entire territory of the Republic of Croatia.

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

CMRS has a representative in Civil Protection Directorate (CPD) under the Ministry of Interior. County CPD headquarters makes risk assessment for their territory once a year and the results are provided to CMRS.

2. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

Response to natural disasters (earthquake, floods), rescuing lost or injured people primarily in non-urban and inaccessible areas.

3. What types of risk / threats do you manage?

Natural risks, industrial risks, societal risks.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
    4.1. Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

Risk assessment received from CPD categorizes risk, but CMRS is not concerned with those. Results of risk assessment are used to prepare the logistics.

5. In your field, is static risk management mandatory by regulation? Which regulation?

Risk assessment performed by CPD is regulated by national law.

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

CPD issues certificate to legal experts who perform periodical yearly risk assessment in collaboration with CMRS county representative.

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?
    7.1. Do you perform the risk management yourself or is it sub-contracted?
    7.2. How many people are involved?
    7.3. What are their required skills?
    7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?

See above answers.

8. Are there provisions to infer from other risk management teams?

See above answers.

9. Who has the last word on the risk treatment options?
    9.1. Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive, and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

CMRS representative in CDP county headquarters.

10. How much time / budget is dedicated to this initial risk assessment?
    - *10.1. Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we'll get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.*

n/a

11. What is the risk study time frame being considered?
    - 11.1. For how long your risk assessment is valid?
    - 11.2. When do you schedule minor updates or complete reviews of your studies?

Static risk assessment is done once a year.

Smaller updates are event triggered and based on reports from the terrain.

Methodology

12. What are the utilized risk management methods / techniques?

The government issued RULES ON METHODOLOGY FOR PREPARATION OF CRITICAL INFRASTRUCTURE RISK ANALYSIS (mainly based on ISO 31000:2009).

13. What input data is required?

n/a

14. At what level of abstraction are you working?
    - 14.1. Typically, how many business assets? Supporting assets?
    - 14.2. Do you list all vulnerabilities, e.g. using CVEs?
    - 14.3. Is there maybe an official (mandatory) list of vulnerabilities?
    - 14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK?
    - 14.5. Do you assess compliance to all security measures?
    - 14.6. Are there particular flaws or vulnerabilities that require special focus?

n/a

15. What are the general assumptions (hypotheses)?
    - 15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?
    - 15.2. Is there already provision for dynamic updates of these hypotheses?

If something can go wrong than it will go wrong.

16. How often is the risk management activity conducted?
    - 16.1. Are there provisions for risk model updates?

16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)?

16.3. Are those triggers OK or should there be others?

16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

See previous answers.

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

See previous questions.

18. How are the standard operating procedures designed?

18.1. What is the process of amending the procedures?

18.2. Does the risk management team participate in the design of SOPs for the operational teams?

18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?

The leading rescuers in their fields (division leaders) write SOPs and use risk management results in the process. In SOP development they collaborate with all other services, mainly instructors.

There are different levels of SOPs, for national use, county use, for local use etc. Local SOPs are more detailed while national are on a more general level. SOPs are used only on the level of commanding officers, rescue operatives are not that much concerned with the SOPs.

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?

19.1. What specific risk management standards must you comply with?

19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports).*

19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure*.

n/a

20. Do you collaborate with national security entities or other national and international bodies?

Yes, with both national security entities (Civil Protection Directorate (CPD) under the Ministry of Interior) and international bodies (see the list in question 6 answer).

21. How do you model acceptable levels of risk?

21.1. What risk treatment strategy do you use?

21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?

21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)?

21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?

21.5. *An example: acceptable risk modelling in the transmission system operators, in some contexts the N-1 criterion (ability of system to cover the failure of largest system unit), a.k.a. no single point of failure, is often used, contrasted to more elaborate probabilistic models that are used in other contexts). This criterion is only an example, an illustration. Other types of CI utilize different assumptions, the idea is to try to catch what these are here.*

The list of priorities is:

1. Save human lives
2. Save national critical infrastructure
3. Save people's property (including animals, cattle etc.)

Zero rule is: rescuer must not endanger his own life.

22. Are cascading effects a specific issue for you? How are they currently managed?

22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

Yes, but no specific static risk assessment approach for cascading effects is performed.

Use of static risk management results

23. Who in your organisation reads the risk *management* report after completion?

The leading rescuers in their fields (division leaders).

24. How are the risk *management* results used during design-time?

CMRS is comprised of volunteers so we cannot plan our human capacities in design-time. However, equipment is procured according to risk management results.

25. Are the risk *management* results of one system / programme shared with other systems / programmes / teams within your organisation?

25.1. Sometimes risk management is done at project level, and sometimes at the programme or organizational level – is there sharing between different levels?

n/a

26. Is the risk management report sent outside of your organisation? To whom?

CPD is in charge of risk management report, usually that information is classified as national security document.

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

27. Is there a process to transfer the results from design time to run time?

Yes. The risk assessment report is shared with lead division rescuers. SOPs are written.

SOP are then used to organise trainings and exercises on various levels. Operative rescuers do not receive written SOPs, but through extensive training they bring their level of expertise to automatism.

Once a year exercise of county CPD members.

Twice a year exercise of city CPD members.

10 exercises a year of municipality CPD members.

Rescue instructors organise trainings for rescue operatives every weekend (note: members of CMRS are volunteers with other daily jobs). Every training is dedicated to some of the specific fields of expertise that rescuers are trained to achieve (speleological, underwater, alpine, etc…)

NOTE: all trainings and exercises are done with real people, not puppets.

28. Have you already transferred some static risk assessment results for reuse during runtime?
    28.1. Do you communicate your results to the run time teams (directly?)?

There is no formal or direct communication of results to run time operatives, usually only rescue mission commander is familiar with SOPs. Rescue instructors also organize trainings in accordance with SOPs. See above answer.

29. Who took this initiative?
    29.1. Has this been called for by runtime operators or someone else?

CMRS headquarters.

30. To whom were the results transferred?

See previous answers.

31. What was the main goal of this transfer? Was this a shared goal with the recipients?

To be efficient on the field, with appropriate equipment (personal and teams) and trained staff.

32. Do you have an established procedure of reporting the risk management results to stakeholders outside your company?

CPD is in charge of risk management results.

33. Were the complete results transferred or only some parts? Which parts?

CPD is in charge of risk management results, some parts are classified data of national interest.

34. With what level of abstraction were the results transferred?

n/a

35. How much effort was dedicated to the transfer operation?

Significant effort is dedicated to trainings.

36. How efficient was this transfer?

Very efficient.

37. Did you receive some feedback from the runtime teams after the transfer? How much time after? And what type of feedback?

Each rescue mission ends with debriefing where operatives give information to mission commander on the success of the mission. Mission commander then judges if that feedback is something that should be taken into account regarding the possible change in SOP.

Real-time / Run-time Risk Management Interview

Interviewee: Zdenko Lovrić (volunteer rescue operative, CMRS)
Interviewer: Tamara Hadjina (researcher, KONČAR)
Dates & times of interviews:

- 29/10/2021, 9:00-11:00

Scope / General purpose

1. What is the business or technical context of this operational risk management? Describe the context and area where the end user is working (e.g. hydro power plant, control centre etc.)

See static risk assessment part of the interview.

2. Do you perform yourself or require from your system providers some form of operational risk management at run-time?

There is no formal risk management at run-time. The operatives are guided by rules described in question 21 of the static management part of the interview.

Each volunteer has his equipment at home, in accordance with his/her capabilities obtained through trainings, and takes that equipment to the rescue mission. In case of a longer action a camp is established and additional equipment is brought to the place of the mission.

3. What types of operational risk / threats do you face in your normal operation? What principal threats affect your operation?
   3.1. What are the primary threats that affect your normal operation?

For usual risks, not addressed during static risk assessment, a very fast risk assessment is performed before going to the field. The risk assessment is usually a purely mental operation.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
    4.1. Describe if there is a categorization of risks (technical risk, procedural risks) and flowing of these risks to relevant stakeholders.

See static risk assessment part of the questionnaire.

The dynamic risk assessments are made on-site. An action plan is established and shared with the team orally. Each mission starts with the briefing where each member of the team receives his orders.

5. In your field, is dynamic risk management mandated by regulation? Which regulation?

No.

6. Do you have an accreditation / certification to maintain?
    6.1. Who is the accreditation / certification body?
    6.2. At what rate must the accreditation / certification be renewed?

CMRS rescue **instructors** have certifications from organisation depending on their field of expertise:

- **International Trauma Life Support** (ITLS) – for education in managing out-of-hospital trauma situations
- Rescue3Europe
- International Rescue Dog Organisation (IRO)
- European Cave Rescue Association
- International Commission for Alpine Rescue (ICAR)

Max validity of a certificate is 3 years, after that, instructors have to renew the certificate.

Logistics

7. Who performs the operational risk management?
    7.1. Do you perform the risk management yourself or is it sub-contracted?
    7.2. How many people of involved?
    7.3. What are their required skills?

n/a

8. How often are the risk management results updated?
    8.1. Are there events that trigger (should trigger) an update?
    8.2. Outside of those events, who can decide to launch an update?

n/a

9. How much time / budget is dedicated to risk management updates?

It is done regularly by all the staff (volunteers), it is an integral part of the operations on the field. Debriefing after each operation might result with updates.

10. What is the risk study time frame being considered?
    46.1. For how long your risk assessment is valid?
    46.2. When do you schedule minor updates or complete reviews of your studies?

See previous answer.

11. Are the updates usually performed by the same people who did the initial analysis? If no, are their skills / competencies different or similar?

No, depends on the situation, there are no fixed rules.

12. Outside of a crisis situation, who has the last word on the risk treatment options whilst the system is operational?

For static risk assessment, director of CPD headquarters.

In case of dynamic risk assessment, the commander in charge of the rescue operation.

13. During a crisis, what is the decision chain? Who has the last word on the response to apply?

The commander of rescue operations. Duties for each action are assigned during the briefing that takes place before every action.

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

14. Is there a process to transfer the results from design time to run time?

See previous answers.

15. Do you usually start the risk assessment from scratch or to you have the static risk assessment results as input?

Static risk assessment is an input.

16. Who took the transfer initiative?

CMRS headquarters.

17. From where / which team do the results originate?

n/a

18. What was the main goal of this transfer? Was this a shared goal with the static risk analysis providers?

The staff performing the static and dynamic risk assessments shared the same goal, prepare logistics and train rescuers in order to save human lives, national CI and human property.

19. Do you reuse the complete static risk analysis or only parts thereof?

Depending on the type of action, there are different levels of static risk analysis, national, regional, municipal….

20. How useful are these inputs? (Estimate)

Very useful.

21. What are the areas where the inputs were the most useful, e.g. business / operational impact analysis?

Procuring the right equipment and organise trainings according to inputs.

22. Did you have to rework the inputs, typically the level of abstraction?

During a crisis, there is usually no time to go through plans, so rescuers act instinctively.

23. Is some form of traceability organised between the static and dynamic risk management results?

Not really.

24. Have you already provided feedback to the static risk management teams?

Each action ends with debriefing and if necessary, rescue action commander provides feedback to CPD.

25. Is this feedback manual or automated?

Manual.

Risk Management Methodology

26. What are the utilized risk management methods / techniques?

Depends on the field of expertise of each rescuer and the trainings each rescuer underwent to become the member of CMRS.

27. What are the tasks involved in risk management during runtime?

Steps:

1. Briefing (organizing rescue team for the specific mission, agree on the methods of communication in the mission)
2. Action
3. Debriefing

Actions are mostly urgent and during an operation there is no additional formality.

28. What input data are required for dynamic risk management and how do you collect the data?

Through collaboration with other FR teams on the field.

29. At what level of abstraction are you working?

29.1. Typically, how many business assets? Supporting assets?

29.2. Is it different to the abstraction level in static risk management? (Note: see also the answer to question 21 above).

29.3. How do you handle the detected vulnerabilities? Is there a procedure for doing so?

29.4. Do you assess compliance to all security measures?

29.5. Are there particular flaws or vulnerabilities that require special focus?

29.6. Are there applicable international standards? (List only the most important ones).

See static risk assessment part of the interview.

30. What are the general assumptions (hypotheses)?

30.1. How often are these hypotheses updated?

30.2. Is there a provision for dynamic updating of these hypotheses?

n/a

31. How often is the risk management activity conducted?

31.1. What triggers the risk management related actions? (Set intervals, actions, etc)

31.2. Are there provisions for the risk model updates?

31.3. What specific triggers are there to update the risk model? Is it triggered periodically, on a specific action or triggered by an external factor?

31.4. Are the existing triggers OK or do you think there should be other ones?

31.5. What is the typical lifecycle of the risk model?

n/a

32. Are there different hierarchical levels in the company that perform the risk management? For example, are the risk management results at lower organizational levels in the company prepared on their own and then fed higher in the organization?

Dynamic risk assessments are performed at all hierarchical levels and results are shared on the field.

33. Do you have a standard operating procedure guidebook?
    33.1. What standards is this book compliant with?
    33.2. Are there applicable international standards? (List only the most important ones).

SOPs are in accordance with certificates issued to our rescuers (see question no. 6).

34. How are the standard operating procedures designed?
    34.1. What is the process of amending the procedures?
    34.2. What triggers the SOP updates?
    34.3. Is there participation / collaboration with static risk management team in the design of SOPs?
    34.4. Who are the specialists involved in design, mandating and eventual invalidation of SOPs and the corresponding operational documentation?

There are no updates of the SOPs during operations.

35. Is there a specific standard family (e.g. similar to ISO 27000 family of standards) that governs the risk management?
    35.1. What specific risk management standards must you comply with?

No.

36. How do you model acceptable levels of risk?
    36.1. What risk treatment strategy do you use?
    36.2. Do you define different strategies in different operational contexts?
    36.3. Is there a risk aversion matrix (aka risk appetite matrix)?
    36.4. Is that matrix unique within the organization or are there multiple ones?

    (In some operational contexts of e.g. transmission system operation different risk models and acceptable risk levels are modelled in different fashion. The idea is to capture what the assumed criteria are).

See question 21 of the static part.

37. Are cascading effects a specific issue for you? How are they currently managed?
    37.1. Note: this is an important question for T2.2. Please give enough focus here.

Yes. We are aware of cascading effects as they are part of the results of static risk assessment.

Use of dynamic risk management results

38. Who in your organisation reads the risk management report after completion?

See previous answers

39. How are the risk management results used during run time?

See previous answers.

40. Are the risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

See previous answers.

41. Is the risk management report sent outside of your organisation? To whom?

See previous answers.

Use of cybersecurity risk management results for detection and response (SOC)

42. How are the risks / threats presented (e.g. semaphore, numerical presentation, alerts…)?

n/a

43. How many of these security events are real attacks? Are there often false positives? (Estimate).

n/a

44. Have you already experienced a false negative (i.e. undetected attack until too late)?

n/a

45. How often do you trigger corrective actions?

n/a

46. Are there automatic notification systems when the corrective actions are triggered?
    46.1. Is there a system for automatic notification when corrective actions are taken manually or automatically?
    46.2. Note: The idea is to get the situation "from the field".
    46.3. Is there an identified lifecycle for an alarm / notification – is it automatically dismissed after some time even with no action on behalf of the operator?

n/a

47. Are there automatic risk mitigation actions in the systems you monitor?
    47.1. If so, how are you informed on automatic results (think primary and secondary reserve activation, automatic generation control in terms of power system, closing of perimeter in the critical infrastructures primarily dealing with physical risks such as airports)

n/a

48. Crisis management: How do you perform escalation when the resources at your disposal are not enough to handle the current level of risks?
    48.1. Note: this is an important question for T2.2. Please give enough focus here.

We call for our reinforcement or ask for engagement of other FR teams that are part of national civil protection. In some major crisis national army was also called on, but it can not be the initiative of CMRS as there is a national law and procedure how the army is mobilized.

Other uses of risk management results

49. Are the dynamic risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

CMRS is part of national civil protection programme together with red cross and firemen.

*Operational context questions (**optional**)*

50. How many different risk sources do you handle in a typical hour/day of operation?
    50.1. Is that number consistent with what was handled during static risk management?

Close to 500 operations a year.

51. How many observables / events do you manage in a typical hour of operation? Is there a seasonality (e.g. flood season?)

Yes, there is a seasonality mainly due to summer season where some parts of the country double the number of temporary residents and tourists are more likely to go on adventures that result with rescue mission.

52. How many of these alerts are classified as security events? Estimate a percentage.

There are almost no unjustified calls (≈ 0%).

IV. ANNEX D – EDF extensive interviews

Design-time Risk Management Interview

Interviewees:

- Nicolas T., technical coordinator in the safety and security of the power plants team
- Ramzi Z., cyber security referent in the same team

Interviewers:

- Frederic Guyomard (EDF)

Introduction:

EDF (Electricité De France/ Electricity of France) is a French electric utility company, which dealing with generation, distribution and supply electricity in France and some other countries. They used various types of power plants: nuclear, hydro, wind, solar, etc.

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

During the proposal phase, a risk management are made by another team. During system design phase, we perform ourselves the risk assessment.

2. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

Business context of the risk assessment:

- The control-command of the different power plants
- The evolution of the facilities

3. What types of risk / threats do you manage?

We used a threat referential which is internal to the company.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

There is a categorization defined by experts.

5. In your field, is static risk management mandatory by regulation? Which regulation?

The static risk management is mandatory for the critical systems in the power plants.

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

N/A

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?
   - 7.1. Do you perform the risk management yourself or is it sub-contracted?
   - 7.2. How many people are involved?
   - 7.3. What are their required skills?
   - 7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?

The initial risk assessment is made internally by the team.

Two people are involved in this risk assessment for the cyber part.

The team is specialised in risk assessment, but no certification is required for the people.

8. Are there provisions to infer from other risk management teams?

N/A

9. Who has the last word on the risk treatment options?
   - 9.1. Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

N/A

10. How much time / budget is dedicated to this initial risk assessment?
    - *10.1. Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we'll get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.*

The budget and the time dedicated for the risk assessment depends on the system. For approved systems the budget is more consequent than for other systems.

In average, 2 to 3 days are dedicated for one system. But it depends on the available collaborators and the available skills.

11. What is the risk study time frame being considered?
    - 11.1. For how long your risk assessment is valid?
    - 11.2. When do you schedule minor updates or complete reviews of your studies?

The risk assessment is strictly valid for 3 years for the approved system. For the other the time frame can be a little longer, but 3 years is the average.

Methodology

12. What are the utilized risk management methods / techniques?

They use the EBIOS 2010 method.

13. What input data is required?

They need the next inputs to do the risk assessment:

- Attack scenarios and perimeter
- System description and technical specification

The sub-contracted companies must provide a PAS (Plan Assurance Securité/Security insurance plan). This plan describes the organisation, the security of the product, the methods to transfer the security between the sub-contracted company and us, etc. A report is made when the transfer of the security is done. The sub-contracted companies use its own methods for risk assessment. Traditionally, it is EBIOS 2010. Risk assessments of the sub-contracted companies are inputs for the static risk assessment.

14. At what level of abstraction are you working?
    14.1. Typically, how many business assets? Supporting assets?
    14.2. Do you list all vulnerabilities, e.g. using CVEs?
    14.3. Is there maybe an official (mandatory) list of vulnerabilities?
    14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK?
    14.5. Do you assess compliance to all security measures?
    14.6. Are there particular flaws or vulnerabilities that require special focus?

14.1 Approx. 2.000 assets for the current project

14.2/3 They use the internal CERT and the CERT FR to follow the vulnerabilities

15. What are the general assumptions (hypotheses)?
    15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?

The success rate of the attacks is taken into consideration in the purpose of calculate the level of acceptability of a threat

    15.2. Is there already provision for dynamic updates of these hypotheses?

No, there is no dynamic updates

16. How often is the risk management activity conducted?
    16.1. Are there provisions for risk model (i.e. security file) updates?

16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)?

16.3. Are those triggers OK or should there be others?

16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

With the ANSSI (French National Agency for the Security of Information Systems), reviews are made regularly.

16.2 The risk assessment is made every 3 years or when there is a high alert from the CERT

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

Risk management is centralized.

18. How are the standard operating procedures designed?

18.1. What is the process of amending the procedures?

18.2. Does the risk management team participate in the design of SOPs for the operational teams?

18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?

N/A

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?

19.1. .What specific risk management standards must you comply with?

19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports).*

19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure.*

There is an internal standard: an internal referential with principle sheet

and an external standard: ISO 27005

20. Do you collaborate with national security entities or other national and international bodies?

Yes always.

21. How do you model acceptable levels of risk?

21.1. What risk treatment strategy do you use?

21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?

21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)?

21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?

21.5. *An example: in some contexts in transmission system operators the N-1 criterion (ability of system to cover the failure of largest system unit), a.k.a. no single point of failure, is often used, contrasted to more elaborate probabilistic models that are used in other contexts. This criterion is only an illustrative example, other types of CI may utilize different assumptions, the idea is to try to catch what these criteria are.*

To model the level of acceptability of risks, we made a weighting of the risks based on the principle internal sheet for 200 requirements. From that a snapshot is made of the risk assessment and given to the run team.

22. Are cascading effects a specific issue for you? How are they currently managed?

22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

N/A

Use of static risk management results

23. Who in your organisation reads the risk management report after completion?

The risk assessment is transferred to the exploit teams.

24. How are the risk management_results used during design-time?

N/A

25. Are the risk management_results of one system / programme shared with other systems / programmes / teams within your organisation?

25.1. If there is risk management performed at specific project level versus the programme, team, or organizational level, is there sharing between different levels?

The results of risk management are shared only with the exploit team of the system.

26. Is the risk management report sent outside of your organisation? To whom?

Only with some specific sub-contracted companies if it is necessary. If not, it is only shared internally.

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

27. Is there a process to transfer the results from design time to run time?

N/A

28. Have you already transferred some static risk assessment results for reuse during runtime?
    28.1. Do you communicate your results to the run time teams (directly?)?

The results are transferred to the “CISO for industrial system” and this person is part of the run team.

29. Who took this initiative?
    29.1. Has this been called for by runtime operators or someone else?

N/A

30. To whom were the results transferred?

The results are transferred to the “CISO for industrial system” (RSS2I).

31. What was the main goal of this transfer? Was this a shared goal with the recipients?

N/A

32. Do you have an established procedure of reporting the risk management results to stakeholders outside your company?

N/A

33. Were the complete results transferred or only some parts? Which parts?

N/A

34. With what level of abstraction were the results transferred?

N/A

35. How much effort was dedicated to the transfer operation?

N/A

36. How efficient was this transfer?

N/A

37. Did you receive some feedback from the runtime teams after the transfer? How much time after? And what type of feedback?

N/A

Real-time / Run-time Risk Management Interview

Interviewee:

- Christophe Martin, Head of IT Security Mission

Interviewers:

- Elsa HELIES (EDF)
- Frederic Guyomard (EDF)

Date: 10/11/2021 11h00 – 12h30

Introduction:

EDF (Electricité De France/ Electricity of France) is a French electric utility company, which dealing with generation, distribution and supply electricity in France and some other countries. They used various types of power plants: nuclear, hydro, wind, solar, etc.

Christophe is the head of IT security mission. He is part of the team who are in charge of the exploitation of power plants. They are not the designer of this plants. The risk management is made by the designer team (see design risk management interview) and they update it regularly with the information of the exploitation team.

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of operational risk management at run-time?

The risk management is made internally by the designer team of the power plants (see design risk management interview).

2. What is the business or technical context of this operational risk management? Describe the context and area where the end user is working (e.g. hydro power plant, control centre etc.)

The risk management is made for every system of the power plants.
These systems are divided in several categories:

- Some systems are critical (for security or safety reason), so they must be homologated. For the homologation, the risk management is mandatory and made with the EBIOS method.
- For the other systems, they are divided in 5 categories based on the criticality of the system, inspired on the NSS 17 of IAEA. Some internal committee defined which is the category of each system. A risk management is made for each category, so there is one risk management shared for all the systems in one category.

Also, on every intervention, a risk assessment is made on what is the impacts of the intervention on a system.

3. What types of operational risk / threats do you face in your normal operation? What principal threats affect your operation?
   3.1. What are the primary threats that affect your normal operation?

The exploitation team have an internal referential of risk and threats.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
    4.1. Describe if there is a categorization of risks (technical risk, procedural risks) and flowing of these risks to relevant stakeholders.

There are many categories of risk like fire threats, environment threats, cyber threats, etc.

The cyber threats are in the risk management from recently only, but it exists some rules from long time ago to protect the system (like some rules about password, USB protection, etc.)

5. In your field, is dynamic risk management mandated by regulation? Which regulation?

The risk assessment is mandatory by French regulation but so far, only for the most critical systems.

6. Do you have an accreditation / certification to maintain?
    6.1. Who is the accreditation / certification body?
    6.2. At what rate must the accreditation / certification be renewed?

Some of the system (the critical ones) must be internally homologate.
For the homologation, a risk assessment is mandatory.
The homologation must be renewed every 3 years.

Logistics

7. Who performs the operational risk management?
    7.1. Do you perform the risk management yourself or is it sub-contracted?
    7.2. How many people of involved?
    7.3. What are their required skills?

The risk management is made internally at EDF by the designer team of the power plants.
The two teams (designer and exploitation teams) works together to identify the risks and the threats.

8. How often are the risk management results updated?
    8.1. Are there events that trigger (should trigger) an update?
    8.2. Outside of those events, who can decide to launch an update?

The designer team update every 3 years the risk management for the homologation of the system or more often when a trigger occurs like a major vulnerability or after an audit if it is necessary.

9. How much time / budget is dedicated to risk management updates?

The time and the budget depend of the system.
On average, we can talk about few weeks in a year for the first risk management of a system. It is a little faster for the next risk management because it is updates.
The resources are internal at EDF.

10. Are the updates usually performed by the same people who did the initial analysis? If no, are their skills / competencies different or similar?

The updates are made by the same team who performed the initial analysis.

Transfer methodology (if applicable)

The designer team and the exploitation team work together on one risk management, updated only by the designer team. So, they are not transferring the risk management, they use the same risk management.

The exploitation team regularly made some audits to check the technic and the organisation. The results of this audits help to define some new threats or modify existing ones. Based on that, some corrective actions can be established and validate by an internal committee and put in the planning to be applicate as soon as possible. With this information, the designer team can update the risk management.

The corrective actions can be cyber or physical measures, they can be multiple barriers.

To complete, the exploitation team have a share inventory with ANSSI (National Cybersecurity Agency of France). During several weeks, each year, the ANSSI and the exploitation team work together on several systems to improve the cybersecurity. Every year, systems change. It is not an audit, it is more like a expertise which give advices on some subjects. Some other cybersecurity teams in EDF can be involved too.

Risk Management Methodology

11. What are the utilized risk management methods / techniques?

For the homologated system, the EBIOS method is use.

For the other systems, the IAEA method is use.

12. Are cascading effects a specific issue for you? How are they currently managed?
    12.1. Note: this is an important question for T2.2. Please give enough focus here.

The cascading effects are not an issue on the risk assessment, but it is study in the shared inventory made with ANSSI.

Other uses of risk management results

13. Are the dynamic risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

The risk management of the different systems are shared with the ANSSI as part of the shared inventory program.

V. ANNEX E – FVP extensive interviews

Interview with the Port Authority of Valencia resulted with a compilation of answers presented as a singular text. After this fist iteration an additional interview was carried out where a short questionnaire was presented to the FVP personnel and subsequently they provided answers to those three sets of questions.

First iteration

Interviewee: Pablo Giménez (FVP)
Interviewer: Israel Perez Llopis (UPVLC)

Risk assessment methodology

The Port authority of Valencia cybersecurity team manages both the cybersecurity design-time risk modelling and the run-time risk management.

The methodology in use for that purpose is MAGERIT, which is a Risk Analysis and Management Methodology for Information Systems that was developed and promoted by the former Spanish high council of e-government (currently Commission ICT strategies), in response to the perception that the administration, and, in general, the whole of society, increasingly dependent on information to fulfil its mission.

The analysis and risk management is a key aspect of the Royal Decree 3/2010, of 8 January, which regulates the national security in the area of e-government.

Moreover, MAGERIT is contained in the inventory of methods of analysis and risk management of ENISA (The European Union Agency for Cybersecurity).

Effort dedicated to risk assessment

The estimated effort devoted to the risk assessment exercise is 2 weeks per year and the exercise is repeated every year taking into account the operational security incidents occurred in the previous year.

During the risk assessment the current assets, risks, threats and controls are analysed, re-evaluated and modified if required and new ones are included and assessed. There are several input sources for the assessment process, for example the SIEM tool.

The risk level in order to accept a risk is established by the port authority managers.

After the execution of the risk assessment, a confidential report is elaborated. The report is not shared inside or outside the organization.

Accreditation / certification

The Port authority of Valencia is currently working in the implementation and achievement of the certification compliance of the Spanish national security system.

The Spanish National Security Framework is a law that generates the conditions necessary for trust in the use of electronic media. To this end, it establishes a series of measures that guarantee the security of the systems, data, communications and electronic services, allowing the exercise of rights and the fulfilment of duties via these media.

The framework establishes the security policy for the use of electronic media and consists of basic principles and minimum requirements that allow an adequate protection of information systems, services and their information.

The National Security Framework is inspired by the family of ISO 27000 standards and, more specifically, by ISO 27001. This is why its structure and application correspond to the PDCA Cycle model - Ongoing improvement, considering risk analysis and implementation of measures/controls.

The main benefits of this certification are to have a managed and controlled system with measures/controls that ensure the correct protection of information systems in the face of internal and external threats and incidents.

The framework is based in the NIS (Network and Information Security) EU Directive 2016/1148 that provides legal measures to boost the overall level of cybersecurity in the EU and the European Programme for Critical Infrastructure Protection (EPCIP).

The Valencia Port Authority also complies with the good practices defined by ENISA and IAPH.

Operations

The critical operational IT systems are continuously monitored by the SOC (Security Operations Centre). The SOC service is subcontracted to an experienced cybersecurity company.

A crisis management plan is defined for operations and management. In case of an incident, involved people can react as soon as possible following the predefined procedure.

The Spanish National Cryptologic is continuously monitoring the network traffic and could provide support in case of an emergency.

The companies that work directly with the Port Authority of Valencia or perform subcontracting IT services and works must be certified and comply with the National Security Framework. This is a requirement to be awarded with the contract.

The most common attack detected is the reception of SPAM emails, blocked by the anti-SPAM tools. There is a big amount of incidents.

Awareness cybersecurity training has been provided to all the Valencia Port Authority employees and they will soon be able to access to an online platform that offers various types of awareness courses.

Cascading effects & cyber/physical security convergence

Cascading effects involving other CIs or companies are not currently included in the risk assessment.

Regarding the collaboration and integration between cyber and physical security, some conversations between the different departments have started but they are in a very early stage.

Future Plans

The need of a Business Continuity Plan has been identified and there is currently a public bid to hire a company to develop it.

Second iteration

Interviewee: Chief Information Security Officer (CISO) of the Port Authority of Valencia
Interviewer: Stéphane PAUL (researcher, Thales)

Q0: Could you provide your own definitions of static & dynamic risk assessment?

Static risk assessment is one that is carried out only once and the result of which is considered constant.

Dynamic risk assessment is one that is reviewed periodically to consider possible changes in the likelihood of threat occurrence, its impact or the number of assets affected.

Q1: Can you explain what risk assessment activities were performed on your last IT system procurement:

- Did you perform a risk assessment before the bid?
  We perform a periodic risk assessment of our systems, but not specifically before a procurement.

- Did you include cybersecurity requirements in the bid?
  Yes, always are included functional, operational and cybersecurity requirements in the bid.

- Does the provider need to be certified? If yes against which standard?
  The provider needs to be certified if it is going to provide a business service outsourced by our organization. In Spanish public companies is mandatory to apply the National Security

Framework: https://administracionelectronica.gob.es/dam/jcr:db9fc934-0fd5-425e-8584-bacd4bb464b3/National-Security-Framework-Spain-consoliated-EN-final.pdf

- Did the provider perform their own risk assessment? If yes did you have access to it? Did you reuse it for internal purposes?
  Having a cybersecurity certification is considered by us as sufficient evidence of compliance with cybersecurity good practices, including a risk analysis performed using a recognized methodology, so that we do not require the supplier to communicate us its own risk analysis. Our organization consider the participation of suppliers in those outsourced services in its own risk analysis, assigning specific threats and controls.

- Did you perform a risk assessment during the integration (i.e., just before exploitation)? No, only operational cybersecurity controls are performed before exploitation (hardening procedures and vulnerability scan of the system).

- Who wrote the cybersecurity SOPs for this new procurement?
  The CISO developed a procedure to include all necessary controls in every project, based in the cybersecurity framework we use.

- Do those SOPs include procedures related to risk assessment updates?
  No, in case we are outsourcing business services, the provider must be certified in the National Security Framework. That warranties its risk assessment is updated.

Q2: Can you explain your usual interactions with the SOC:

- Did you provide the SOC with a risk assessment?
  No, our SOC only handles operational security aspects. Governance, risk and compliance are the responsibility of the CISO.

- Did you provide the SOC with the SOPs?
  No, they don't need to know the specific cybersecurity requirements of a system to perform their job.

- Did the SOC perform their own risk assessment? If yes did you have access to it? Did you reuse it for internal purposes?
  No (see the first question in this paragraph).

- What kind of information does the SOC provide you?
  Monitoring and correlation of cybersecurity events, traffic analysis, log collection, incident response, activity reports, periodic vulnerability assessments…

VI. ANNEX F – GPMB extensive interviews

Interviewees: Stéphanie SICOT (GIE), Fabrice KLEIN (GPMB)
Interviewers: Elsa HELIES (EDF), Frédéric GUYOMARD (EDF), Stéphane PAUL (THALES)
Date & time of interview: 30/08/2021, 15:30-17:30

We interviewed Stephanie SICOT and Fabrice KLEIN. Stephanie is an administrator of a "GIE" - EIG (Economic Interest Grouping) and she performs the risk analysis for the EIG main application: **VIGIE SIP**. This critical application is used in the Bordeaux port and many other ports by port community, for the ship monitoring in the port and in the approach zone.

Design-time Risk Management Interview

Scope / General purpose

1. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

GPMB (Grand Port Maritime de Bordeaux) is the port of Bordeaux. GPMB is one of seven large French ports. There are 320 persons in the organisation. It is responsible of the development and maintenance of maritime accesses, the safety and security of the maritime and fluvial domain. It is also responsible for the port infrastructure and the industrial and logistics zones linked to the port activity. It is in the estuary of Gironde, which is the vastest estuary of Europe.

The EIG (Economic Interest Group) is initially a group of 15 French ports, including Bordeaux and some French other regions. It represents 13 organisations. It has a permanent staff of 4 persons. Its aims to develop digital port services to help the growth of ports and maritime trade. All software developers are part of the EIG.

VIGIE SIP is an EIG application used in GPMB and 18 other ports. It is used for dematerializing all administrative formalities during stopover of ships. The service has been deployed since the early 90s, initially on the French Minitel. The current version was built in 2014/2015, based on WEB technologies. It is implemented as SaaS and on-premise. The SaaS version is hosted by DRI, a French Cloud provider.

2. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

The original version of VIGIE SIP suffered many attacks, in particular usurpation attacks. The decision to change to new WEB technologies, with Code Fusion, was considered at the time as a safe and secure pathway. The development work was sub-contracted with strong time delivery constraints. Thus, no risk assessment was performed at the time. Hypotheses were that externalisation and new technologies would solve the issues.

Note: There are other information systems at GPMB that are managed by IS/IT, but not by IEG. Thus, this interview is focused only on Vigie SIP. The main functions provided by the other ISs include (but are not limited to):

- Surveillance/piloting with radar support (VTS),
- Surveillance of water level (i.e. tidal range),
- Electricity support,
- Messaging,
- Accounting…

Some safety / reliability risk assessments are done by GPMB on these systems during design, but no cybersecurity risk assessment. Typically, the redesign of VTS was recently made by the port, to move from 1 to 2 radars. The results were captured in the architecture, and the related requirements were included in the Call for Tender. This process is not detailed further in this questionnaire because: (a) it does not relate to cybersecurity; (b) it is not managed by IEG.

3. What types of risk / threats do you manage?

N/A

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?

4.1. Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

N/A

5. In your field, is static risk management mandatory by regulation? Which regulation?

There are many regulations for ships and ports.

The major is the International Ship and Port facility Security code (ISPS). The ISPS defines security arrangements for ships, ports, and government agencies. It prescribes responsibilities to the port to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade

The DGITM (Directorate General of Infrastructure, Transports and Sea) is an authority that provides “Trafic 2000”, which coordinates port information at European level.

The SOLAS convention (Safety Of Life At Sea) is an international convention which sets minimum safety standards in the construction, equipment and operation of merchant ships.

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

GPMB needs to accredit the VIGIE application to use it on ports. Risk assessment is mandatory for the accreditation. There are no recommendations for the accreditation. It is an internal accreditation.

The Cloud Provider hosting the Vigie SIP needs to be certified ISO 27001.

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?
    7.1. Do you perform the risk management yourself or is it sub-contracted?
    7.2. How many people are involved?
    7.3. What are their required skills?
    7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?

As mentioned above, there is no initial risk assessment made for VIGIE SIP. However, if the case were to occur:

- The risk assessment could be led internally or sub-contracted.
- 1 person of GIE would be involved.
- A combination of operational and cybersecurity skills is required.
- No certifications are required.

8. Are there provisions to infer from other risk management teams?

They are no other risk management teams interacting with EIG.

9. Who has the last word on the risk treatment options?
    9.1. Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive, and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

N/A

10. How much time / budget is dedicated to this initial risk assessment?
    10.1. Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we'll get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.

N/A.

11. What is the risk study time frame being considered?
    11.1. For how long your risk assessment is valid?
    11.2. When do you schedule minor updates or complete reviews of your studies?

N/A.

Methodology

12. What are the utilized risk management methods / techniques?

N/A

13. What input data is required?

N/A

14. At what level of abstraction are you working?
    14.1. Typically, how many business assets? Supporting assets?
    14.2. Do you list all vulnerabilities, e.g. using CVEs?
    14.3. Is there maybe an official (mandatory) list of vulnerabilities?
    14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK?
    14.5. Do you assess compliance to all security measures?
    14.6. Are there particular flaws or vulnerabilities that require special focus?

N/A

15. What are the general assumptions (hypotheses)?
    15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?
    15.2. Is there already provision for dynamic updates of these hypotheses?

N/A

16. How often is the risk management activity conducted?
    16.1. Are there provisions for risk model updates?
    16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)?
    16.3. Are those triggers OK or should there be others?
    16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

N/A

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

N/A

18. How are the standard operating procedures designed?
    18.1. What is the process of amending the procedures?
    18.2. Does the risk management team participate in the design of SOPs for the operational teams?
    18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?

N/A.

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?
    19.1. What specific risk management standards must you comply with?
    19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports).*
    19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure.*

The ISO/IEC 27001 standard is asked for the sub-contracted company (datacentre host).

20. Do you collaborate with national security entities or other national and international bodies?

The EIG collaborate with ANSSI (French National Agency for the Security of Information Systems). ANSSI can perform audit or check some documentation to help the GIE with their analysis, because of critical functions.

ANSSI made a control of the application in 2018.

21. How do you model acceptable levels of risk?
    21.1. What risk treatment strategy do you use?
    21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?
    21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)?
    21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?
    21.5. An example: acceptable risk modelling in the transmission system operators, in some contexts the N-1 criterion (ability of system to cover the failure of largest system unit), a.k.a. no single point of failure, is often used, contrasted to more elaborate probabilistic models that are used in other contexts). This criterion is only an example, an illustration. Other types of CI utilize different assumptions, the idea is to try to catch what these are here.

N/A.

22. Are cascading effects a specific issue for you? How are they currently managed?
    22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

N/A.

Real-time / Run-time Risk Management

Scope / General purpose

1. What is the business or technical context of this operational risk management? Describe the context and area where the end user is working (e.g. hydro power plant, control centre etc.)

See design time interview.

2. Do you perform yourself or require from your system providers some form of operational risk management at run-time?

GPMB performs itself its own dynamic risk management.

3. What types of operational risk / threats do you face in your normal operation? What principal threats affect your operation?
   3.1. What are the primary threats that affect your normal operation?

Two major threats are considered:

- Automated attacks, like Denial of Service attacks. GPMB suffered a DOS attack once during the last 3 years. GPMB suffered of 2 hours loss of service, because of the unavailability of the DRI (i.e. the external cloud provider). This implied an unavailability of the connection with the national system (GDMF) and the European system. In case of some events (ship in distress for example), this cut-off could be critical for GPMB in regard of the law.
- Lost or destruction of the datacentre: to reduce this risk, the EIG have duplicated their data on many servers located in different datacentre.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (technical risk, procedural risks) and flowing of these risks to relevant stakeholders.

Yes, 3 categories are defined:

- infrastructure,
- equipment,
- user (human factor)

but these categories are not used to flow the risks to stakeholders.

5. In your field, is dynamic risk management mandated by regulation? Which regulation?

See design time interview.

6. Do you have an accreditation / certification to maintain?
   6.1. Who is the accreditation / certification body?
   6.2. At what rate must the accreditation / certification be renewed?

See design time interview.

Logistics

7. Who performs the operational risk management?
   - 7.1. Do you perform the risk management yourself or is it sub-contracted?
   - 7.2. How many people of involved?
   - 7.3. What are their required skills?

Three risk assessments have been performed on the WEB version of VIGIE SIP:

- In 2015, run by a 3rd party, following the initial deployment
- In 2018, security audit by ANSSI, which highlighted some major issues.
- In Aug. 2021, run internally, following another audit. This risk assessment is run by 1 person (Stéphanie), with an effort estimate of 5 days.

8. How often are the risk management results updated?
   - 8.1. Are there events that trigger (should trigger) an update?
   - 8.2. Outside of those events, who can decide to launch an update?

Every year, the committee of EIG makes a revision of the risk assessment. If it is necessary, the IEG commission can ask an audit and/or a new version of the risk assessment. This can also be triggered by some events, e.g. attack, new major vulnerability or reliability loss.

There is no other levels of risk management and evaluation at GPMB, so there are no external triggers beyond the IEG.

Note: the IEG accreditation commission is composed of GIE volunteers of very different profiles, including CISO, operational, etc

9. How much time / budget is dedicated to risk management updates?

The risk assessment team had 5 days to run the Aug. 2021 risk assessment. This effort is representative of the risk assessments led at GIE.

GPMB has a regular budget for risk assessment studies, accreditation, security audits and the application of the risk treatment plans. Priorities are set to keep within the yearly budget. New critical vulnerabilities may force a rescheduling of the treatment actions.

10. What is the risk study time frame being considered?
    - 10.1. For how long your risk assessment is valid?
    - 10.2. When do you schedule minor updates or complete reviews of your studies?

Every year, the committee of EIG assesses the need for a revision of the risk assessment. The EIG governance (dedicated committee) can ask an audit and/or a new version of the risk assessment. Renewal of the risk assessment can be also triggered by some events: for instance, attacks or reliability loss.

11. Are the updates usually performed by the same people who did the initial analysis? If no, are their skills / competencies different or similar?

In the specific case of VIGIE SIP, the updates were not made by the same people who did the first analysis, but it is not a rule per say. The two first analyses were sub-contracted. The third and current analysis is run by the EIG team. They have access to the past analyses to do the new one.

When audits are sub-contracted by GPMB, a PASSI accreditation (from the French Regulator) is requested.

12. Outside of a crisis situation, who has the last word on the risk treatment options whilst the system is operational?

The IEG committee has the last word.

13. During a crisis, what is the decision chain? Who has the last word on the response to apply?

Same as usual

Risk Management Methodology

14. What are the tasks involved in risk management during runtime?

IEG uses the EBIOS 2010 method, supported by Excel spreadsheets. There is no intention to shift to the EBIOS-Risk Manager method on the short-term.

15. What input data are required for dynamic risk management and how do you collect the data?

IEG needs as input the following data:

- The previous analysis
- All the documentation of the application
- Responses to ANSSI's questionnaire on maturity level in security of information system and minimal requirements in Information Security

Note: ANSSI is the French National Agency for the Information Systems Security.

16. At what level of abstraction are you working?
    16.1. Typically, how many business assets? Supporting assets?
    16.2. Is it different to the abstraction level in static risk management? (Note: see also the answer to question 21 above).
    16.3. How do you handle the detected vulnerabilities? Is there a procedure for doing so?
    16.4. Do you assess compliance to all security measures?
    16.5. Are there particular flaws or vulnerabilities that require special focus?
    16.6. Are there applicable international standards? (List only the most important ones).

The current risk assessment comprehends 8 essentials functions, 30 feared events and 15 supporting assets (the environment dedicated for each member of VIGIESIP). This level of abstraction is globally stable through time since the 1st risk assessment.

The vulnerabilities are not listed. The IEG uses a CERT and some other information to follow the vulnerabilities of their assets / frameworks / etc. If it is necessary, after a new vulnerability is reported, they migrate version of the software.

17. What are the general assumptions (hypotheses)?
    17.1. How often are these hypotheses updated?
    17.2. Is there a provision for dynamic updating of these hypotheses?

N/A

18. How often is the risk management activity conducted?
    18.1. What triggers the risk management related actions? (Set intervals, actions, etc)
    18.2. Are there provisions for the risk model updates?
    18.3. What specific triggers are there to update the risk model? Is it triggered periodically, on a specific action or triggered by an external factor?
    18.4. Are the existing triggers OK or do you think there should be other ones?
    18.5. What is the typical lifecycle of the risk model?

Obsolescence or major events trigger the risk management updates. There are no provisions for risk management updates. There is no defined lifecycle for the risk model. There are no plans to update the current risk management update process.

19. Are there different hierarchical levels in the company that perform the risk management? For example, are the risk management results at lower organizational levels in the company prepared on their own and then fed higher in the organization?

No.

20. Do you have a standard operating procedure guidebook?
    20.1. What standards is this book compliant with?
    20.2. Are there applicable international standards considering the SOPs? (List only the most important ones).

IEG have a PES (Procédure d'exploitation de sécurité / security operating procedure) based on the ANSSI model

21. How are the standard operating procedures designed?
    21.1. What is the process of amending the procedures?
    21.2. What triggers the SOP updates?
    21.3. Is there participation / collaboration with static risk management team in the design of SOPs?
    21.4. Who are the specialists involved in design, mandating and eventual invalidation of SOPs and the corresponding operational documentation?

The team is quite small, so the standard cybersecurity operating procedures are defined within the team in accordance with the technical manager, the risk analyser and the CISO. There is no specialist, but the job is handled by the whole team.

They have 16 SOP. The updates are triggered by a change, a migration or an audit, or every 6 months.

22. Is there a specific standard family (e.g. similar to ISO 27000 family of standards) that governs the risk management?
    22.1. What specific risk management standards must you comply with?

N/A

23. How do you model acceptable levels of risk?
    23.1. What risk treatment strategy do you use?
    23.2. Do you define different strategies in different operational contexts?
    23.3. Is there a risk aversion matrix (aka risk appetite matrix)?
    23.4. Is that matrix unique within the organization or are there multiple ones?

    (In some operational contexts of e.g. transmission system operation different risk models and acceptable risk levels are modelled in different fashion. The idea is to capture what the assumed criteria are).

GPMB has 4 risk degrees:

- The 1 and 2 degree are acceptable, and if the correctives actions are easy, they plan to do it.
- The 3 and 4 are not acceptable. Some correctives actions must be done in short terms. Treatment is usually enacted through technical or organizational actions. If the risk is about a sub-contracted company, the contract will be amended, and measures will be adapted to reduce or eliminate this risk.

Most treatment actions are internal actions. Sometimes treatment relates to contractual actions with DRI.

24. Are cascading effects a specific issue for you? How are they currently managed?
    24.1. Note: this is an important question for T2.2. Please give enough focus here.

Not for VIGIE SIP.

<u>Use of dynamic risk management results</u>

23. Who in your organisation reads the risk management report after completion?

The risk management report is read by the EIG committee after completion. The committee reads it to accredit the application.

24. How are the risk management results used during run time?

The risk management results are used for the accreditation renewal, and to plan some correctives actions, if some risks are unacceptable.

25. Are the risk management results of one system / programme shared with other systems / programmes / teams within your organisation?
    25.1. Sometimes risk management is done at project level, and sometimes at the programme or organizational level – is there sharing between different levels?

The risk management report it shared between the members of the IEG accreditation commission. Optionally, it may be shared with other IEG members.

It is not shared with other systems/programmes/teams: IEG manages only one application.

26. Is the risk management report sent outside of your organisation? To whom?

It is not.

Use of risk management results for detection and response

27. How are the risks / threats presented (e.g. semaphore, numerical presentation, alerts…)?

An incident analyse report is send to IEG team when a risk is presented.

28. How many of these security events are real attacks? Are there often false positives? (Estimate).

There has been one real attack in the past 3 years (i.e. 2h service interruption). The other alerts, detected by DRI, are not reported to the IEG team. Thus, it is impossible to know how many attempts are unsuccessful. The typology of the attack was on the risk assessment.

29. Have you already experienced a false negative (i.e. undetected attack until too late)?

No.

30. How often do you trigger corrective actions?

During normal operations (i.e. not in a crisis situation), the following triggers are used:

- Every time a risk is unacceptable (risk 3 or 4). For each risk assessment, about 15% of the risks are in this category.
- If a vulnerability is detected on an asset, a framework used, etc. This analyse is done once a year.

A secure development framework is now in place (close to DevOps), which is compliant to OWASP rules. All developers are part of the GIE. Junior developers are coached by the CISO. Code is peer-reviewed by CISO and senior developers.

Monthly progress meetings are organised to discuss the DRI contract.

The other systems, not managed directly by IEG, are mostly not connected to internet (e.g. VTS, tides). Thus, for these systems, there is no specific secure development framework.

31. Are there automatic notification systems when the corrective actions are triggered?
    31.1. Is there a system for automatic notification when corrective actions are taken manually or automatically?
    31.2. Note: The idea is to get the situation "from the field".
    31.3. Is there an identified lifecycle for an alarm / notification – is it automatically dismissed after some time even with no action on behalf of the operator?

There is no automatic notification. They have a documentation in common to follow the corrective actions.

32. Are there automatic risk mitigation actions in the systems you monitor?
    32.1. If so, how are you informed on automatic results (think primary and secondary reserve activation, automatic generation control in terms of power system, closing of perimeter in the critical infrastructures primarily dealing with physical risks such as airports)

No

33. Crisis management: How do you perform escalation when the resources at your disposal are not enough to handle the current level of risks?
    33.1. Note: this is an important question for T2.2. Please give enough focus here.

They never have this case.

Other uses of risk management results

34. Are the dynamic risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

No, the IEG manages only one application.

*Operational context questions (**optional**)*

35. How many different risk sources do you handle in a typical hour/day of operation?
    35.1. Is that number consistent with what was handled during static risk management?

One in the last 3 years.

36. How many observables / events do you manage in a typical hour of operation? Is there a seasonality (e.g. flood season?)

N/A: the IEG does not monitor the application directly. It only receives notifications from DRI in case of a successful attack.

37. How many of these alerts are classified as security events? Estimate a percentage.

N/A

VII. ANNEX G – HEP extensive interviews

Design-time Risk Management Interview

Interviewees: Krešimir Kristić (CISO, HEP Group), Luka Bitunjac, (hydro power plant director, HEP-Production Ltd.)

Interviewers: Hrvoje Keko and Tamara Hadjina (KONČAR)

HEP Group is the Croatian national energy company, which has been dealing with generation, distribution and supply of electricity for more than a century.

HEP is organized as a concern, a group of connected companies (daughter companies).
The parent company (parent body) of HEP Group carries out the function of corporate governance of HEP Group and guarantees conditions for safe and reliable electricity supply to customers.

Within the HEP Group, subsidiary companies (managing, accounting, legal), which conduct regulated activities (transmission and distribution), are clearly separated from companies that conduct non-regulated activities (generation and supply).

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

We do it ourselves during system design phase. That is the first risk assessment that is done.

2. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

Since October 2019, according to national Law which adopts EU 2016/1148 directive and EU 2018/151 implementing regulation, technical context includes all important systems that effect the supply of electrical power which is the key to functional society and economy of Republic of Croatia.

Business context consists of:

1. Communication network and IT security management
2. Risk management
3. Critical systems protection
4. Incident reporting
5. Major incident reporting (incidents with major effect on business continuity)

3. What types of risk / threats do you manage?

Primarily cyberthreats and the connected risks. We are becoming more aware of the need to also incorporate risks associated with business continuity and industrial processes (for example supply chain security). We have completed a business impact analysis (BIA) which covers all key critical industrial processes and critical resources for those processes.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
    4.1. Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

Yes, such categorization exists. Currently not all categories are used to direct the appropriate teams. The GRC system incorporates such categories and there are no technical obstacles to use all risk categories in everyday operation.

5. In your field, is static risk management mandatory by regulation? Which regulation?

Yes. A national law, which aims towards critical infrastructure operators and digital services providers cybersecurity (based on EU 2016/1148 directive).

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

ISO 2700 family (not obligatory, but preferable). IEC 62443 standards family would be a next appropriate security framework important for HEP Group.

Accreditation bodies with appropriate certificates.

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?
    7.1. Do you perform the risk management yourself or is it sub-contracted?
    7.2. How many people are involved?
    7.3. What are their required skills?
    7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?

Initial risk assessment is carried out by special contracted companies.

7.1 Sub-contracted

7.2 Minimum of 4 people, 2 from HEP and 2 from sub-contractor. Additionally relevant expert workers are interviewed.

7.3 ISO 2700x Certified Auditor, Lead Auditor and similar.

7.4 We are not acquainted with such requirements.

8. Are there provisions to infer from other risk management teams?

HEP Academy is established. Other platforms and methods are also used, but those are not defined through internal company procedures and policies.

9. Who has the last word on the risk treatment options?
   9.1. Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive, and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

Formally company management receives the identified risk and approves further risk processing. In general, the influence of risk owners (assets, processes) is crucial and based on the subsidiarity principle, but the management has the last word.

10. How much time / budget is dedicated to this initial risk assessment?
   10.1. Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we'll get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.

It took one year to finish a project of procurement of the **GRC (governance, risk management and compliance), IT assets repository, risk assessment, BIA** with the budget of 100 000 EUR. The project resulted with the procurement of GRC tool, the establishment of IT assets repository and an initial risk assessment.

11. What is the risk study time frame being considered?
   11.1. For how long your risk assessment is valid?
   11.2. When do you schedule minor updates or complete reviews of your studies?

The goal is to have GRC and ITAM installed in 2022 and then have a quasi-real time risk assessment.

11.1 Risk assessment is valid for the moment when it is made and with time the relevance of this assessment decays.

11.2 A revision of complete risk assessment is planned to be performed once a year, while minor updates are planned at least every 6 months. SOC detects IS anomalies in real time.

Methodology

12. What are the utilized risk management methods / techniques?

In the established repository of information assets of the company, GRC tools assign to each entity: (i) vulnerabilities, for each identified relevant asset, are identified (ii) threats that can exploit those vulnerabilities. For each identified relevant threat determine the impact, that is the consequence of the realized threat (on an elaborated scale from 0 to 100) and the probability that the threat will be realized. Risk is determined (calculated) by multiplying the consequences and probabilities. Depending on the level of risk appetite of the Company, the determined risk is treated with appropriate functional, organizational and / or technical measures or the risk is accepted. Based on such grouped risks, the Director of the Company accepts the Risk Treatment Plan, the execution of which is cyclically monitored and the Plan is periodically revised in accordance with the updated risk status.

13. What input data is required?

The required data are: IT assets - entity in the repository, vulnerabilities of the entity, threats that can exploit vulnerabilities, impact for each identified relevant threat, or consequence of the realized threat (on an elaborated scale from 0 to 100), probability that the threat will materialize (risk is calculated by multiplying the consequences and probabilities), the level of risk appetite, and information on the selected risk treatment by appropriate functional, organizational and / or technical measures or simply by accepting the risk.

14. At what level of abstraction are you working?

14.1. Typically, how many business assets? Supporting assets?
14.2. Do you list all vulnerabilities, e.g. using CVEs?
14.3. Is there maybe an official (mandatory) list of vulnerabilities?
14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK?
14.5. Do you assess compliance to all security measures?
14.6. Are there particular flaws or vulnerabilities that require special focus?

Identical IT entities are grouped (identical also according to the vulnerability criterion).

14.1 approx. 25,000+

14.2 A list of vulnerabilities such as the CVE - Common Vulnerabilities and Exposures list is one of the functions of the applied GRC tool.

14.3. There is no official prescribed list of vulnerabilities.

14.4. Yes, within the Threat Intelligence part of the established Security Operations Centre (SOC) of the Croatian Electric Power Industry, we use systems such as CAPEC or MITRE ATT&CK to list vulnerabilities.

14.5. Currently not, but the GRC system enables the assessment of compliance with security measures, legal and regulatory framework, and we plan to establish an assessment of compliance with security measures during year 2022.

14.6. The risk assessment stored only in an Excel spreadsheet, i.e. in any stored document that is periodically updated manually post mortem, is a "dead fish".

15. What are the general assumptions (hypotheses)?

15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?
15.2. Is there already provision for dynamic updates of these hypotheses?

The basic preconditions for risk management are the existing organizational framework, required capacities and skills.

15.1 We have an organizational framework - we know and have standardized what, how and with what should be achieved; we have technical capacities - ITAM and GRC tools, etc., we currently do not have the necessary human resources, and we will train them when we acquire them.

15.2. In part, we have the capacity and procedures to enable automatic updates.

16. How often is the risk management activity conducted?
    - 16.1. Are there provisions for risk model (i.e. security file) updates?
    - 16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)?
    - 16.3. Are those triggers OK or should there be others?
    - 16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

We have performed an initial static risk assessment, we have largely ensured organizational and technical assumptions, it remains for us to establish risk management in almost real time during 2022, as already written in previous responses.

16.1. Yes, procedures and underpinnings for updating risk models exist.

16.2. At the moment, these model updates are not triggered at all, but they will almost certainly be periodic (eg due to a legislative obligation), linked to a specific operator action, or triggered due to some external influence.

16.3. The ultimate goal is to carry out business in accordance with business plans without obstructions and damages. Risk management and model triggering are in that function and should enable this in real time.

16.4. At the moment, our risk model is "dead fish", but we hope that in the coming months we will be able to ensure human capacity so that with the existing organizational and technical prerequisites we can update and manage risks in virtually real time. We note again that the established Security Operations Center SOC detects anomalies in HEP's IS in real time.

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

Risk management is centralized at the level of the group member company and at the company level.

18. How are the standard operating procedures designed?
    - 18.1. What is the process of amending the procedures?
    - 18.2. Does the risk management team participate in the design of SOPs for the operational teams?
    - 18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?

Standard procedures and procedures (SOPs) are regulated by internal acts and organizational mechanisms for monitoring and controlling the implementation of procedures.

18.1. The owner of the business process or other relevant business stakeholder in accordance with the internal acts of the corporation proposes to the management and initiates changes and refinements. By the decision of the management, the responsible organizational units, and / or structures (teams) and employees carry out the procedure: the organizationally competent organizational unit provides a revised sketch of the relevant changes and revisions of the SOP, revised by the competent legal (eg Legal Affairs Sector), control (Sector for Strategy and Development,…) and financial (Sector for Finance…) organizational units. The syndicate organization of the corporation is consulted, but their opinion is not binding. The agreed SOP is submitted for approval to the Management Board of the corporation or the director of the company.

18.2. Currently, the risk management team is not involved in the design of SOPs for operational teams.

18.3. Primarily, the experts involved in the preparation of SOPs and related operational documentation are employees of the directly competent organizational units, followed by lawyers and economists.

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?
    19.1. What specific risk management standards must you comply with?
    19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports).*
    19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure.*

There are two relevant families of standards: ISO / IEC 27000 and IEC 62443.

20. Do you collaborate with national security entities or other national and international bodies?

Yes, with the Institute for Security of Information Systems of the Republic of Croatia (ZSIS) and with the sectoral competent CERT (Computer Emergency Response Team) of ZSIS within the obligations of key service operators prescribed by Law.

21. How do you model acceptable levels of risk?
    21.1. What risk treatment strategy do you use?
    21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?
    21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)?
    21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?
    21.5. An example: in some contexts in transmission system operators the N-1 criterion (ability of system to cover the failure of largest system unit), a.k.a. no single point of failure, is often used, contrasted to more elaborate probabilistic models that are used in other contexts. This criterion is only an illustrative example, other types of CI may utilize different assumptions, the idea is to try to catch what these criteria are.

An acceptable financial amount of realized damage per risk event is a criterion for an acceptable level of risk. It is determined by the owner of the business process (IT assets), approved and ultimately accepted by the director of the company.

21.1. As a rule, the strategy is to minimize the impact of risk on the realization of primarily strategic goals, but also on the realization of tactical and operational business goals.

21.2. In different contexts of the organization's work, we use context-appropriate implementation of the strategy.

21.3. We have and use a risk aversion matrix or a risk appetite matrix.

21.4. The matrix is not unified and is context dependent.

22. Are cascading effects a specific issue for you? How are they currently managed?
    22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

A significant number of possible cascading effects actually have the beginning of their realization in our company, with an initially undesirable and negative impact on our systems, almost identical to all other identified risks. But because of their nature and consequences, cascading risks are especially significant to us. We are currently considering and managing them as any other ("non-cascading") risks.

Use of static risk management results

23. Who in your organisation reads the risk management report after completion?

CISO at the level of the Group and employees delegated by the director of an individual company, usually risk owners in coordination with CISO.

24. How are the risk management_results used during design-time?

Yes, but not enough.

25. Are the risk management_results of one system / programme shared with other systems / programmes / teams within your organisation?
    25.1. If there is risk management performed at specific project level versus the programme, team, or organizational level, is there sharing between different levels?

The results of the risk management of one system or department within our company are shared between different systems or teams within our organization. Unlike the risk management results that are shared, the separation and control of access to data on vulnerabilities of industrial control systems is carried out rigidly respecting the security principle of Least Privilege and extremely restrictive. For example, a small number of authorized workers of a power plant have access to the relevant data only of their power plant.

25.1. There is an exchange of data between projects, equally respecting the security principle of Least Privilege with rigid separation and protection of vulnerability data.

26. Is the risk management report sent outside of your organisation? To whom?

Pursuant to the Law: (i) the competent sectoral CSIRT, more precisely the CERT of the ZSIS, receives reports on the delivery of incident notifications with a significant effect on the delivery of a key service, (ii) the competent sectoral body (Ministry of Economy and Sustainable Development) reports are submitted on request, (iii) reports are submitted to the competent technical body (ZSIS) as part of the implementation of the supervision of the provisions of the Law. Relevant bodies of the National security council, the Ministry of Defence and the Ministry of the Interior of the Republic of Croatia and judicial bodies upon a legally grounded request.

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

27. Is there a process to transfer the results from design time to run time?

SOC detects real time anomalies that are a consequence of realized risks that are identified and processed in the framework of static risk analysis.

28. Have you already transferred some static risk assessment results for reuse during runtime?

    28.1. Do you communicate your results to the run time teams (directly?)?

Real time SOC detected anomalies, that are categorized as an incident, are transferred together with instructions for necessary activities to IT support operators and if necessary (depending on the type of incident) to cybersecurity managers of power plants and their deputies.

28.1 Results are not sent directly to run time teams (operators).

29. Who took this initiative?

    29.1. Has this been called for by runtime operators or someone else?

Corporate Security Office.

30. To whom were the results transferred?

Currently, the data owners, HEP-Proizvodnja d.o.o. (production) and HEP ODS d.o.o. (distribution) in cooperation, under instructions and under the supervision of the Corporate Security Office of the Croatian Electric Power Industry, they ensure the conditions for lifelong management of static risk analysis data and vulnerabilities of industrial plants. The data is currently in the safe, on encrypted media, because by their nature and sensitivity they represent the "soft belly" not only of Croatian Electric Power Industry, but also of the Republic of Croatia! This data will be made available for permanent inspection in a safe and supervised manner to the persons appointed by the owner of this data according to the principle of Least Privilege.

31. What was the main goal of this transfer? Was this a shared goal with the recipients?

As already written in the previous answers, the basic goal is defined by the Information Security Strategy - the realization of business and business results in accordance with business plans without obstructions and damages. The developer of the static risk analysis is the Office for Corporate Security, and users easily agree with this goal, so the cooperation is smooth.

32. Do you have an established procedure of reporting the risk management results to stakeholders outside your company?

    Yes.

Until the last detail, the procedures for reporting to stakeholders outside our company have been defined in accordance with the provisions of the Law. The procedures were verified by simulation exercises involving relevant external stakeholders in all power plants. According to the lessons learnt, the procedures have been improved, and further periodic simulation exercises are being prepared according to the plan.

33. Were the complete results transferred or only some parts? Which parts?

Only minimal necessary data connected to a specific event. There was no real need for such transfer so this procedure was evaluated through simulation with power plants.

34. With what level of abstraction were the results transferred?

Risk assessment data is transferred on highest possible abstraction level and in minimal volume (necessary minimum).

35. How much effort was dedicated to the transfer operation?

Our position is that HEP data can be transferred out of the company in extremely restrictive and secure way and only in case of legitimate legal requirement or in case of national emergency threatening homeland security.

In case of such conditions focus is on determining the level of abstraction and data transfer. 5-6 people from top management and expert level.

36. How efficient was this transfer?

50-60%

37. Did you receive some feedback from the runtime teams after the transfer? How much time after? And what type of feedback?

We receive regular feedback. Depending on the situation, circumstances and the nature of the information, it takes from ten minutes to two to three days. Owners of IT assets, business processes and, consequently, owners of related risks participated in the activities of establishing information repositories, risk assessment and business impact analysis, and in the activities of drafting the Policy on notifications of incidents with significant effect. Dispatchers / operators were also directly and indirectly involved in these activities. According to the applied methodology, the owners provide the relevant information in interviews, which is then competently evaluated, critically evaluated, approved and accepted. The next step is periodic exercises and checks, after which, according to the lessons learnt, the procedures and procedures are spirally improved in accordance with the changed conditions and circumstances.

Real-time / Run-time Risk Management Guidelines

Interviewees: Luka Bitunjac, (hydro power plant director, HEP-Production Ltd.), Nikola Slišković (hydro power plant technical director, HEP Production Ltd.)

Interviewers: Hrvoje Keko and Tamara Hadjina (KONČAR)

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of operational risk management at run-time?

We perform risk management ourselves firstly during the design of the system, that is, the development of project tasks for project development. The first risk assessment procedure for a specific system is related to design.

2. What is the business or technical context of this operational risk management? Describe the context and area where the end user is working (e.g. hydro power plant, control centre etc.)

I work in a hydro power plant, of the barrage type, with an associated accumulation lake, upstream from the settlement, which poses a threat to the population, as well as to the infrastructure and agricultural areas downstream, in the event of a threat. In addition to electricity production, the task of the hydro power plant is to protect against floods during high waters.

3. What types of operational risk / threats do you face in your normal operation? What principal threats affect your operation?
   3.1. What are the primary threats that affect your normal operation?

The main threats to the operation of the system are, first of all, weather troubles as well as conditions in the transmission network (load / frequency disturbances, technical problems in the transmission of energy to the system). Deliberate attacks on the system are a threat that we can and to some extent control now, but do not underestimate (technical protection system, physical protection in the form of a guard, protection against cyber threats in the form of an isolated process system, physically separated from the rest of the network).

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (technical risk, procedural risks) and flowing of these risks to relevant stakeholders.

At the level of the hydropower plant, we do not currently categorize risks, but we adhere to the existing instructions and regulations of the HEP Group.

5. In your field, is dynamic risk management mandated by regulation? Which regulation?

At the level of the hydropower plant, dynamic risk management is not mandatory at the moment and we rely on the central bodies of the company and the legislator for that.

6. Do you have an accreditation / certification to maintain?
    6.1. Who is the accreditation / certification body?
    6.2. At what rate must the accreditation / certification be renewed?

No.

Logistics

7. Who performs the operational risk management?
    7.1. Do you perform the risk management yourself or is it sub-contracted?
    7.2. How many people of involved?
    7.3. What are their required skills?

Operational risk management is carried out ad hoc, during the implementation of new systems and / or replacement / revitalization of existing ones.

8. How often are the risk management results updated?
    8.1. Are there events that trigger (should trigger) an update?
    8.2. Outside of those events, who can decide to launch an update?

The results of the operational risk analysis are transferred to the instructions on actions (similar to SOP) in case of any incident on the observed system, they are updated with each new knowledge.

9. How much time / budget is dedicated to risk management updates?

At the moment it is impossible to determine how much time and budget is invested in the above, given that there is no systematic approach to risk management at this level.

10. Are the updates usually performed by the same people who did the initial analysis? If no, are their skills / competencies different or similar?

As a rule, there are several people, but one person is responsible for the implementation of the project, and thus risk management from the beginning (development of project assignment) to the implementation of the system and the development of instructions for action in all situations.

11. Outside of a crisis situation, who has the last word on the risk treatment options whilst the system is operational?

The director of the hydropower plant has the last word and decides on all aspects of risk management at the plant.

12. During a crisis, what is the decision chain? Who has the last word on the response to apply?

The crisis management mechanism is prescribed by internal instructions and classified depending on the severity and duration of the incident. The first responder is usually the shift leader of the hydropower plant, while the last word regarding the response to the crisis has either the plant manager (in case of a minor incident) or the plant director (in case of a more serious incident).

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

13. Is there a process to transfer the results from design time to run time?

There is currently no such procedure, and it is done based on experience, at the level of the operator and the project / event.

14. Do you usually start the risk assessment from scratch or to you have the static risk assessment results as input?

There is currently no such procedure, and it is done experientially, at the level of the operator and the project / event.

15. Who took the transfer initiative?

The Corporate Security Office has initiated the above processes, and the methodology is expected to be completed and adopted.

16. From where / which team do the results originate?

The Corporate Security Office delivers the results to the persons in charge of the information security at the facilities (in this case hydro power plant).

17. What was the main goal of this transfer? Was this a shared goal with the static risk analysis providers?

The transmission of the results of the analysis will provide a framework in which to implement security protocols and in this sense, the Corporate Security Office is the main coordinator of activities on this (BIA analyses were performed).

18. Do you reuse the complete static risk analysis or only parts thereof?

We use parts of static analysis related to real-time operation (power generation management - distributed control systems (DCS)) and technical protection.

19. How useful are these inputs? (Estimate)

They are extremely useful.

20. What are the areas where the inputs where the most useful, e.g. business / operational impact analysis?

As stated in the answer to question 18, static analysis has the greatest impact on regular operation in terms of hydropower operation (DCS) and technical protection.

21. Did you have to rework the inputs, typically the level of abstraction?

Of course, the results of the analysis are sometimes generalized and need to be "grounded" for a realistic scenario on the plant itself.

22. Is some form of traceability organised between the static and dynamic risk management results?

For the time being, there is no such system at the hydropower plant, but the implementation of the same by Corporate Security Office is expected.

23. Have you already provided feedback to the static risk management teams?

So far, only BIA analysis has been done.

24. Is this feedback manual or automated?

Manual.

Risk Management Methodology

25. What are the (operational) tasks involved in risk management during runtime?

Electricity generation, plant maintenance, production management (DCS), technical protection.

26. What input data are required for dynamic risk management and how do you collect the data?

We do not use such methods, results are received from Corporate Security Office.

27. At what level of abstraction are you working?
    - 27.1. Typically, how many business assets? Supporting assets?
    - 27.2. Is it different to the abstraction level in static risk management? (Note: see also the answer to question 21 above).
    - 27.3. How do you handle the detected vulnerabilities? Is there a procedure for doing so?
    - 27.4. Do you assess compliance to all security measures?
    - 27.5. Are there particular flaws or vulnerabilities that require special focus?
    - 27.6. Are there applicable international standards? (List only the most important ones).

For now, we do not use such procedures on our own.

28. What are the general assumptions (hypotheses)?
    - 28.1. How often are these hypotheses updated?

28.2. Is there a provision for dynamic updating of these hypotheses?

For now, we do not use such procedures on our own.

29. How often is the risk management activity conducted?

29.1. What triggers the risk management related actions? (Set intervals, actions, etc)

29.2. Are there provisions for the risk model updates?

29.3. What specific triggers are there to update the risk model? Is it triggered periodically, on a specific action or triggered by an external factor?

29.4. Are the existing triggers OK or do you think there should be other ones?

29.5. What is the typical lifecycle of the risk model?

For now, we do not use such procedures on our own.

30. Are there different hierarchical levels in the company that perform the risk management? For example, are the risk management results at lower organizational levels in the company prepared on their own and then fed higher in the organization?

For now, we do not use such procedures on our own.

31. Do you have a standard operating procedure guidebook?

31.1. What standards is this book compliant with?

31.2. Are there applicable international standards considering the SOPs? (List only the most important ones).

For now, we do not use such procedures on our own.

32. How are the standard operating procedures designed?

32.1. What is the process of amending the procedures?

32.2. What triggers the SOP updates?

32.3. Is there participation / collaboration with static risk management team in the design of SOPs?

32.4. Who are the specialists involved in design, mandating and eventual invalidation of SOPs and the corresponding operational documentation?

For now, we do not use such procedures on our own.

33. Is there a specific standard family (e.g. similar to ISO 27000 family of standards) that governs the risk management?

33.1. What specific risk management standards must you comply with?

For now, we do not use such procedures on our own.

34. How do you model acceptable levels of risk?

34.1. What risk treatment strategy do you use?

34.2. Do you define different strategies in different operational contexts?

34.3. Is there a risk aversion matrix (aka risk appetite matrix)?

34.4. Is that matrix unique within the organization or are there multiple ones?
(In some operational contexts of e.g. transmission system operation different risk models and acceptable risk levels are modelled in different fashion. The idea is to capture what the assumed criteria are).

For now, we do not use such procedures on our own.

35. Are cascading effects a specific issue for you? How are they currently managed?
35.1. Note: this is an important question for T2.2. Please give enough focus here.

Cascading phenomena are extremely important in operation, because the threat of one system (transmission network or water turbine, etc.) potentially endangers a whole range of systems (flood protection, distribution network, downstream power plants, downstream inundation belts along the river Cetina, etc.), and thus, these phenomena are the primary focus in risk analysis.

<u>Use of risk management results for detection and response</u>

36. How are the risks / threats presented (e.g. semaphore, numerical presentation, alerts…)?

For now, we do not use such tools on our own, but on power plant DCS we use visual and audible signals for warnings and alarms.

37. How many of these security events are real attacks? Are there often false positives? (Estimate).

These are most often warnings that do not ultimately result in a real threat (signals are grouped into 4 levels, the first two are warnings, the other two are failures / threats where an urgent response is required).

38. Have you already experienced a false negative (i.e. undetected attack until too late)?

No, so far there have been no attacks in this sense because the system is physically separated from the rest of the network.

39. How often do you trigger corrective actions?

Generally, once a year during regular repairs.

40. Are there automatic notification systems when the corrective actions are triggered?
40.1. Is there a system for automatic notification when corrective actions are taken manually or automatically?
40.2. Note: The idea is to get the situation "from the field".
40.3. Is there an identified lifecycle for an alarm / notification – is it automatically dismissed after some time even with no action on behalf of the operator?

As noted, notification systems are embedded in a DCS system (SCADA) in which alarms and warnings are defined. There is also an independent population alert system downstream of the dam and reservoir that also has audible warnings. All alarms / warnings must be accepted manually.

41. Are there automatic risk mitigation actions in the systems you monitor?

41.1. If so, how are you informed on automatic results (think primary and secondary reserve activation, automatic generation control in terms of power system, closing of perimeter in the critical infrastructures primarily dealing with physical risks such as airports)

There are automatic systems for primary frequency regulation, secondary power and frequency regulation as well as voltage regulation implemented in accordance with the Grid Code of the transmission and distribution system. According to the above incident situation, reporting rules have been defined among legal entities, as well as internally (Bulletin 478 of the HEP Group). As for the perimeter of the plant, the implementation of such a system of technical protection is underway, and for now it is working through the human component (power plant shift leader).

42. Crisis management: How do you perform escalation when the resources at your disposal are not enough to handle the current level of risks?

42.1. Note: this is an important question for T2.2. Please give enough focus here.

The escalation is carried out by engaging the resources of the superior Production Area and/or the parent operational management centre depending on the crisis situation. In case the crisis situation cannot be solved with own resources, an external contractor is hired in accordance with the valid system maintenance contracts.

Other uses of risk management results

43. Are the dynamic risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

All experiences are jointly analysed in the technical meetings of the Production Area and recommendations are made for risk reduction as stated.

*Operational context questions (**optional**)*

44. How many different risk sources do you handle in a typical hour/day of operation?

44.1. Is that number consistent with what was handled during static risk management?

During the working day, the most probable occurrence of risks is related to events in the transmission network or on certain drive subsystems (turbine control, generator / transformer protection).

45. How many observables / events do you manage in a typical hour of operation? Is there a seasonality (e.g. flood season?)

We have the most threats in the period of "high waters", and that is in the spring period of the year.

46. How many of these alerts are classified as security events? Estimate a percentage.

Very small percentage, certainly below 5%.

VIII. ANNEX H – KABEG extensive interviews

Design-time Risk Management Interview

Interviewee: Albert Kutej (head of the medical technology department, KABEG), Friedrich Mirko Ogris (technical safety officer for the medical technology sector, KABEG)
Interviewer: Tamara Hadjina (researcher, KONČAR)
Dates & times of interviews:

- 25/10/2021, 10:30-12:00
- 08/11/2021, 11:00-12:30

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

By now: at design-time.

2. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

Hospital: The main focus is on maintaining patient care and patient safety

3. What types of risk / threats do you manage?

Security of supply: Energy, water, medication
External threats: Physical attacks, cyber-attacks
Internal threats: Failures of central facilities, staff failures

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

Risk management is organized on a decentralized basis with a guideline.
The departments manage the risks and report to the central risk management.

5. In your field, is static risk management mandatory by regulation? Which regulation?

Risk management is mandatory: Directive 2008/114 / EC, austrian law StGB § 74

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

ISO 90001, ISO27001, certified by Quality Austria

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?

   7.1. Do you perform the risk management yourself or is it sub-contracted?

   generally we do it ourselves. In certain areas, however, with the initial support of a consulting firm

   7.2. How many people are involved?

   There are 13 risk managers in KABEG and additionally 58 risk officers

   7.3. What are their required skills?

   analytical and communication skills and specialist training

   7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?

   TÜv ISO 31000

8. Are there provisions to infer from other risk management teams?

Yes cert, apcid

9. Who has the last word on the risk treatment options?

   Vorstand

   9.1. Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive, and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

   yes!

10. How much time / budget is dedicated to this initial risk assessment?

    10.1. Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we'll get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.

The risk managers and risk officers spend around 20% on risk management

11. What is the risk study time frame being considered?

    11.1. For how long your risk assessment is valid?

    The risk assessment for the entire KABEG is valid for 1 year

    11.2. When do you schedule minor updates or complete reviews of your studies?

    Depending on the division, updates are made annually, every six months or quarterly
    For IT: every six months

Methodology

12. What are the utilized risk management methods / techniques?

FMEA, CIRS

13. What input data is required?

General information of the subdivisions, records of irregularities already detected ...

14. At what level of abstraction are you working?

14.1. Typically, how many business assets? Supporting assets?

Esp. IT: According to ISO 27001 we manage about 7000 assets.
Additional ~ 500 critical medical and non-medical assets

14.2. Do you list all vulnerabilities, e.g. using CVEs?

no

14.3. Is there maybe an official (mandatory) list of vulnerabilities?

no

14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK?

no

14.5. Do you assess compliance to all security measures?

yes

14.6. Are there particular flaws or vulnerabilities that require special focus?

Yes there are high risk vulnerabilities that require special focus!!

15. What are the general assumptions (hypotheses)?

15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?

For IT: semi annually

15.2. Is there already provision for dynamic updates of these hypotheses?

no

16. How often is the risk management activity conducted?

16.1. Are there provisions for risk model (i.e. security file) updates?

On demand

16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)?

at an interval of 5 years

16.3. Are those triggers OK or should there be others?

The defined trigger is considered sufficient

16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

For central risk management of KABEG: 5 years
For IT: generally 5 years like KABEG. Due to the fast pace of IT, the sub-department may have to react to specific events

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

yes

18. How are the standard operating procedures designed?
    18.1. What is the process of amending the procedures?
    It´s defined in the KABEG Risk management manual
    18.2. Does the risk management team participate in the design of SOPs for the operational teams?
    Yes
    18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?
    Competent risk manager

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?
    19.1. What specific risk management standards must you comply with?
    19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports).*
    19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure.*

ISO 27000, OVE E 8101, IEC 80001,

20. Do you collaborate with national security entities or other national and international bodies?

yes

21. How do you model acceptable levels of risk?
    21.1. What risk treatment strategy do you use?
    Depends on individual risk: combinations of mitigation, avoidance, transfer..
    21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?
    It´s generally unique. The strategy contains a minimum-approach and a total approach.
    21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)?
    yes
    21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?
    It´s unique

22. Are cascading effects a specific issue for you? How are they currently managed?
    22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

Yes

Use of static risk management results

23. Who in your organisation reads the risk management report after completion?

Head of department, central risk management, directors, head of internal audit

24. How are the risk management_results used during design-time?

Required measures can already be determined during the design. These are implemented on the responsibility of the respective head of department before the report is approved

25. Are the risk management_results of one system / programme shared with other systems / programmes / teams within your organisation?

The aggregated results are reported to the central risk management only

25.1. If there is risk management performed at specific project level versus the programme, team, or organizational level, is there sharing between different levels?

There is a separate risk management manual for projects. A specific risk profile must be drawn up, monitored and reported for each project

26. Is the risk management report sent outside of your organisation? To whom?

no

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

27. Is there a process to transfer the results from design time to run time?

Not pronounced

28. Have you already transferred some static risk assessment results for reuse during runtime?

28.1. Do you communicate your results to the run time teams (directly?)?

yes

29. Who took this initiative?

29.1. Has this been called for by runtime operators or someone else?

Operators with risk manager

30. To whom were the results transferred?

It´s mostly the same personnel - Operators and risk officers

31. What was the main goal of this transfer? Was this a shared goal with the recipients?

Events that occur during operation should be able to be assigned to a risk level more reliably

32. Do you have an established procedure of reporting the risk management results to stakeholders outside your company?

Management report to state government of Carinthia

33. Were the complete results transferred or only some parts? Which parts?

Summary with global status only

34. With what level of abstraction were the results transferred?

Overview with top risks.

35. How much effort was dedicated to the transfer operation?

The preparation is complex (~ 200 man hours annually)

36. How efficient was this transfer?

The report is created according to the specifications of the state government

37. Did you receive some feedback from the runtime teams after the transfer? How much time after? And what type of feedback?

No special feedback as the same staff is involved

Run-time Risk Management Interview

Interviewee: Albert Kutej (head of the medical technology department, KABEG), Friedrich Mirko Ogris (technical safety officer for the medical technology sector, KABEG)
Interviewer: Tamara Hadjina (researcher, KONČAR)
Dates & times of interviews:

- 25/10/2021, 10:30-12:00
- 08/11/2021, 11:00-12:30

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of operational risk management at run-time?

ourselves

2. What is the business or technical context of this operational risk management? Describe the context and area where the end user is working (e.g. hydro power plant, control centre etc.)

Hospital business continuity, especially IT infrastructure

3. What types of operational risk / threats do you face in your normal operation? What principal threats affect your operation?
   3.1. What are the primary threats that affect your normal operation?

   Availability of staff, Supply of medication, ensuring the supply in general and specifically with electrical energy

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (technical risk, procedural risks) and flowing of these risks to relevant stakeholders.

yes

5. In your field, is dynamic risk management mandated by regulation? Which regulation?

indirectly through the classification as a critical infrastructure and ISO 9001/27001

6. Do you have an accreditation / certification to maintain?
   6.1. Who is the accreditation / certification body?
   6.2. At what rate must the accreditation / certification be renewed?

Yes,
ISO 9001, ISO27001, certified by Quality Austria
Annually

Logistics

7. Who performs the operational risk management?

    Do you perform the risk management yourself or is it sub-contracted?

    Ourselves

    7.1. How many people of involved?

    There are 13 risk managers in KABEG and additionally 58 risk officers

    especially IT infrastructure: additionally 7 persons

    7.2. What are their required skills?

    analytical and communication skills and specialist training

8. How often are the risk management results updated?

    8.1. Are there events that trigger (should trigger) an update?

    not happened yet, but may be

    8.2. Outside of those events, who can decide to launch an update?

    Sole director via central risk management

9. How much time / budget is dedicated to risk management updates?

For IT: 30 man hours annually, but in KABEG we have many other departments.

Estimation for KABEG: at least 300 man hours annually

10. Are the updates usually performed by the same people who did the initial analysis? If no, are their skills / competencies different or similar?

It´s mostly the same personnel

11. Outside of a crisis situation, who has the last word on the risk treatment options whilst the system is operational?

Sole director and central risk management

12. During a crisis, what is the decision chain? Who has the last word on the response to apply?

The head of the crisis staff for the respective crisis

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

13. Is there a process to transfer the results from design time to run time?

    No, there is no special process defined, as there is no separate run time risk management

Risk Management Methodology

14. What are the (operational) tasks involved in risk management during runtime?

Periodical review of risks (and chances). Aggregation of risks and reporting.

Especially for IT: maintaining the requirements for certification ISO 27001, maintaining awareness of risks

15. What input data are required for dynamic risk management and how do you collect the data?

Regular meetings, information from relevant professional groups using suitable tools.

Especially IT: reports from ticket system, server and network management software

16. At what level of abstraction are you working?

16.1. Typically, how many business assets? Supporting assets?

Esp. IT: According to ISO 27001 we manage about 7000 assets.

Additional ~ 500 critical medical and non-medical assets

16.2. Is it different to the abstraction level in static risk management? (Note: see also the answer to question 21 above).

Runtime risk management groups the individual assets into more detailed classes

16.3. How do you handle the detected vulnerabilities? Is there a procedure for doing so?

Detected vulnerabilities are reported with standardized security tickets.

The security tickets are assessed in regular meetings.

16.4. Do you assess compliance to all security measures?

According to ISO 27001 we periodically assess compliance to defined security measures

16.5. Are there particular flaws or vulnerabilities that require special focus?

Yes there are high risk vulnerabilities that require special focus!!

16.6. Are there applicable international standards? (List only the most important ones).

ISMS: Best practice according to ISO 27001

17. What are the general assumptions (hypotheses)?

The basic assumption is that certain security barriers are insurmountable.

That the employees are adequately trained

17.1. How often are these hypotheses updated?

semi annually

17.2. Is there a provision for dynamic updating of these hypotheses?

no

18. How often is the risk management activity conducted? - semi annually

18.1. What triggers the risk management related actions? (Set intervals, actions, etc)

The risk management related actions are marked with milestones and are monitored

18.2. Are there provisions for the risk model updates?

No

18.3. What specific triggers are there to update the risk model? Is it triggered periodically, on a specific action or triggered by an external factor?

It is triggered periodically.

18.4. Are the existing triggers OK or do you think there should be other ones?

We assume that the periodic review is sufficient

18.5. What is the typical lifecycle of the risk model?

About 5 years

19. Are there different hierarchical levels in the company that perform the risk management? For example, are the risk management results at lower organizational levels in the company prepared on their own and then fed higher in the organization?

It is hierarchic, as described in the question.

20. Do you have a standard operating procedure guidebook?

We have the KABEG "Risk management manual"

20.1. What standards is this book compliant with?

ONR 49000, WHO "International Patient Safety Goals"

20.2. Are there applicable international standards considering the SOPs? (List only the most important ones).

ISO 9001, ISO 27001

21. How are the standard operating procedures designed?

21.1. What is the process of amending the procedures?

The effectiveness of the SOPs must be continuously monitored. Changes are initiated via the PDCA cycle

21.2. What triggers the SOP updates?

The triggers for changes are the semi-annual reports and notes from audits

21.3. Is there participation / collaboration with static risk management team in the design of SOPs?

It´s the same personnel!

21.4. Who are the specialists involved in design, mandating and eventual invalidation of SOPs and the corresponding operational documentation?

The department heads with the local risk officers

22. Is there a specific standard family (e.g. similar to ISO 27000 family of standards) that governs the risk management? –YES!

22.1. What specific risk management standards must you comply with?

ISO 9001, ISO 27001

23. How do you model acceptable levels of risk?

23.1. What risk treatment strategy do you use?

Depends on individual risk: combinations of mitigation, avoidance, transfer..

23.2. Do you define different strategies in different operational contexts?

Yes

23.3. Is there a risk aversion matrix (aka risk appetite matrix)?

Yes!

23.4. Is that matrix unique within the organization or are there multiple ones? It´s unique

24. Are cascading effects a specific issue for you? How are they currently managed?

the risks are managed individually. Cascading effects are taken into account in the “presumed effects”

Use of risk management results for detection and response

25. How are the risks / threats presented (e.g. semaphore, numerical presentation, alerts…)?

Numeric with FMEA Risk priority number.

26. How many of these security events are real attacks? Are there often false positives? (Estimate).

60% false positive. Many of these relate to only a few assets.

27. Have you already experienced a false negative (i.e. undetected attack until too late)?

No

28. How often do you trigger corrective actions?

weekly

29. Are there automatic notification systems when the corrective actions are triggered?

29.1. Is there a system for automatic notification when corrective actions are taken manually or automatically?

manually

29.2. Note: The idea is to get the situation “from the field”.

29.3. Is there an identified lifecycle for an alarm / notification – is it automatically dismissed after some time even with no action on behalf of the operator?

I´s not dismissed automatically. Operators have to notice and act.

30. Are there automatic risk mitigation actions in the systems you monitor?

No

31. Crisis management: How do you perform escalation when the resources at your disposal are not enough to handle the current level of risks?

Crises are to be escalated through official channels. For additional resources, the "compass for disasters" of the state of Carinthia is mandatory to be used.

Other uses of risk management results

32. Are the dynamic risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

No

IX. ANNEX I – SDMIS extensive interviews

Important notice: For SDMIS, the interpretation of static vs. dynamic risk assessment has been understood as follows:

- Static risk assessment relates to risk assessment performed in preparation of an event, before SDMIS is called to act on the field;
- Dynamic risk assessment relates to risk assessment performed during operations, starting as soon as SDMIS receives a call to act on the field; it therefore always relates to an incident, accident and / or crisis situation.

Design-time Risk Management Interview

Interviewee: Benoit SAPET (lieutenant, SDMIS)
Interviewer: Stéphane PAUL (researcher, THALES)
Dates & times of interviews:

- 29/07/2021, 9:00-11:00,
- 05/08/2021, 16:00-17:30
- 15/09/2021, 17:00-18:00

Can you briefly describe your organisation?

SDMIS: 6000 individuals, i.e., 4500 volunteer firefighters, 1200 professional firefighters, 300 administrative persons. Main teams: HR, operational (incl. GACR – see explanations below), territorial.

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

GACR (“Groupement Analyse et Couverture des Risques” i.e. “Risk Analysis and Coverage Group”) makes the overall analysis, at a high-level. Then each service makes its own, at a more detailed level. Some heterogeneity is to be expected.

Static risk assessments are performed with respect to major infrastructure or societal evolutions (e.g. extension of underground line). Static risk assessment are made on a given organisation, to identify risks and check if the appropriate means are available, e.g. can we reach the high points of buildings? Work starts with an operational risk assessment, followed by financial, or design risk assessments.

2. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

Response to societal threats and risks, from minor day-to-day responses, to major incidents.

3. What types of risk / threats do you manage?

Natural risks, industrial risks, societal risks.

The cybersecurity risks are managed by the IS/IT team (i.e. GSI – "Groupement Support Informatique"), with the support of external organisations (e.g. Orange) – see details in specific interview below.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
   4.1. Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

Yes.

Usual risks (95%): road accidents, person health incidents… No or little risk assessment performed for this type of risks. Some fire prevention actions through on-site risk assessments (e.g. bars, restaurants…), at regular intervals (1 to 5 years depending on size of organisation).

Particular risks (5%): natural risks, industrial risks, societal risks. The major focus of risk assessments is on this type of risks. The focus is also on the "response" function, by contrast to "protection" and "prevention".

5. In your field, is static risk management mandatory by regulation? Which regulation?

The SDACR ("Schéma Départemental d'Analyse et Couverture des Risques", i.e. "Departmental Scheme for Risk Analysis and Coverage") is compulsory according to the CGCT ("Code Général de la Collectivité Territorial, article L14-24-7", i.e. "General Code of the Territorial Collectivity"). It must be updated every 5 years. It gives a global picture of the situation of the territory. It leads to an investment plan. It has a regulatory status when the budget is allocated.

The CoTRRiM ("Contrat Territorial de Réponse face aux Risques et effets des Menaces" i.e. "Territorial Response Contract to Risks and impacts of Threats") is like the SDACR, but enlarged to inter-services (i.e. private operators, including telecoms, emergency medics, police…)

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

Yes, but only for fire prevention and not really an accreditation / certification. There is a 3-weeks training, with a diploma for the firefighter. One or two visits per year are required to maintain the "fire preventer" title by the individual firefighters.

For other types of risks, SDMIS is not the main risk manager. SDMIS cooperates with the State, through the DREAL ("Direction Régional de l'Environnement de l'Aménagement et du Logement", i.e. "Environment, Planning and Housing Regional Directorate") and risk management teams of Critical Infrastructures. The response plan, i.e. ORSEC ("Organisation de la Réponse de Sécurité Civile" i.e. "Organization of the Civil Security Response"), signed by the Prefect, is transmitted to the DREAL. The DREAL exchanges with the Critical Infrastructures to build its own risk assessment.

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?
   - 7.1. Do you perform the risk management yourself or is it sub-contracted?
   - 7.2. How many people are involved?
   - 7.3. What are their required skills?
   - 7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?

See above answers.

8. Are there provisions to infer from other risk management teams?

See above answers.

9. Who has the last word on the risk treatment options?
   - 9.1. Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive, and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

The director: he validates the action plan. At lower level, each head of service sets priorities.

10. How much time / budget is dedicated to this initial risk assessment?
   - *10.1. Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we'll get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.*

The GACR represents 20 Full Time Equivalent (FTE).

In other teams, it is difficult to evaluate the investment in risk management. As example, Benoit Sapet, who is lieutenant in the operational team, spends 3 to 5% of his time on this topic. Information is essentially collected and transmitted to the GACR.

11. What is the risk study time frame being considered?
   - 11.1. For how long your risk assessment is valid?
   - 11.2. When do you schedule minor updates or complete reviews of your studies?

Regulation states that ORSEC plans must be revised regularly (e.g. every 5 years).

Smaller updates are triggered by specific events and/or terrain reports.

Methodology

12. What are the utilized risk management methods / techniques?

It depends on the type of risk:

- Natural risks: risks are identified as a combination of hazards and stakes.
- Industrial risks: HAZard and Operability (HAZOP) & Failure Modes, Effects and Criticality Analysis (FMECA) are obtained from industrial organisations, and processed internally.

In addition, CoTRRiM (i.e., inter-office analysis) is requested by the French State, following UEFA Euro in France (2016) and terrorist attacks (2015), to allow for a common response.

13. What input data is required?

It depends on the type of risk:

- For industry risks: gross data about installations (e.g. litres of kerosene) from industry.
- For natural risks: typical events (e.g. height of floods) from State services.
- For societal risk: dynamic data from police (e.g. tension at a given place & time), or static data when large manifestations are organised.

14. At what level of abstraction are you working?

14.1. Typically, how many business assets? Supporting assets?
14.2. Do you list all vulnerabilities, e.g. using CVEs?
14.3. Is there maybe an official (mandatory) list of vulnerabilities?
14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK?
14.5. Do you assess compliance to all security measures?
14.6. Are there particular flaws or vulnerabilities that require special focus?

Difficult to say. There is only one key objective, i.e. the response delay, which can be decomposed in 3 sub-delays:

- call management delay,
- resource mobilisation delay
- intervention delay.

15. What are the general assumptions (hypotheses)?

15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?
15.2. Is there already provision for dynamic updates of these hypotheses?

As seen in previous questions, the context is provided by the DREAL. In case of significant change, the Prefect will require an update of the ORSEC plan, which will trigger a risk assessment.

Some realistic worst-case emergency scenarios are established based on past similar events in the world. These scenarios allow for the long-term planning of the organisation & deployment of the forces (staff & equipment) and location of the fire stations. In this strategic analysis, human and equipment unavailability failure modes are systematically considered.

By contrast, the tactical risk studies are always performed assuming the most favourable conditions for the SDMIS, i.e. staff and equipment is available. This is essentially due to budgetary reasons.

These hypotheses highlight a 2-iteration risk management process. The 1st iteration, at strategic level, allows for a global dimensioning of the forces, and their spread out on the territory based on realistic worst-case scenarios. The 2nd iteration, at local and tactical level, takes the previous allocation as granted, and allows for a fine-grained organisation of the local forces.

16. How often is the risk management activity conducted?
    - 16.1. Are there provisions for risk model updates?
    - 16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)?
    - 16.3. Are those triggers OK or should there be others?
    - 16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

See answers to previous questions.

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

See answers to previous questions.

18. How are the standard operating procedures designed?
    - 18.1. What is the process of amending the procedures?
    - 18.2. Does the risk management team participate in the design of SOPs for the operational teams?
    - 18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?

The GO (“Groupement Opération”, i.e. “Operations Group”) writes the policies & SOPs. To do this, they collaborate with all the other services, including HR, training, operations…

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?
    - 19.1. What specific risk management standards must you comply with?
    - 19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports)*.
    - 19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure*.

After having embarked on the collegial approach of the SDIS for "global performance management", inspired by the European Foundation for Quality and Management (EFQM) method, the SDMIS has competed for a first Committed to Excellence (C2E) label in November 2017. The method is a non-prescriptive quality method (unlike the ISO standards for example), used by more than 50,000 organizations, and based on 8 fundamental concepts: (1) Bring value to its "customers", (2) Create a sustainable future, (3) Develop organizational capacities, (4) Promote creativity and innovation, (5) Lead with vision, inspiration and integrity, (6) Manage with agility, (7) Succeed thanks to the talent of its employees, and (8) Achieve exceptional results.

20. Do you collaborate with national security entities or other national and international bodies?

See answers to previous questions. Would need to interview Maxime for international relations.

21. How do you model acceptable levels of risk?
    - 21.1. What risk treatment strategy do you use?
    - 21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?
    - 21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)?
    - 21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?
    - *21.5. An example: acceptable risk modelling in the transmission system operators, in some contexts the N-1 criterion (ability of system to cover the failure of largest system unit), a.k.a. no single point of failure, is often used, contrasted to more elaborate probabilistic models that are used in other contexts). This criterion is only an example, an illustration. Other types of CI utilize different assumptions, the idea is to try to catch what these are here.*

See risk aversion matrix in SDMIS slides, presented for task T2.2. Caption: Green is acceptable, Orange is tolerable, Red is unacceptable and must be treated.

22. Are cascading effects a specific issue for you? How are they currently managed?
    - 22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

Yes. Cascading effects are considered in the ORSEC plans. No specific static risk assessment approach for cascading effects. See however questions n°14 and 27 in the dynamic risk assessment questionnaire on this subject.

Use of static risk management results

23. Who in your organisation reads the risk *management* report after completion?

Nobody reads the analysis part, but all officers read the operational part.

24. How are the risk *management* results used during design-time?

During operational exercises (training, hands-on case-studies…). One limitation is that the scope is perfectly defined. To trigger interesting effects, some “surprises” are included in the exercises.

25. Are the risk *management* results of one system / programme shared with other systems / programmes / teams within your organisation?
    - 25.1. Sometimes risk management is done at project level, and sometimes at the programme or organizational level – is there sharing between different levels?

About particular risks (see question n°4), the approach is always multi-services.

26. Is the risk management report sent outside of your organisation? To whom?

Yes. See answers to previous questions. As a reminder, internally to GACR, externally to DREAL.

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

27. Is there a process to transfer the results from design time to run time?

Yes. The risk assessment report is validated, then shared with officers. Later, digests are written, for a wider dissemination to all in the field, and possibly also for purchase of new material.

28. Have you already transferred some static risk assessment results for reuse during runtime?
    28.1. Do you communicate your results to the run time teams (directly?)?

Yes. In fact, it is a regular process, because there are many updates in a context of staggered working hours.

29. Who took this initiative?
    29.1. Has this been called for by runtime operators or someone else?

The GACR. The rate of transfer is set according to current priorities.

30. To whom were the results transferred?

See previous questions.

31. What was the main goal of this transfer? Was this a shared goal with the recipients?

To be efficient on the field, with appropriate material and trained staff.

32. Do you have an established procedure of reporting the risk management results to stakeholders outside your company?

Yes, the ORSEC plan is shared with all its contributors.

33. Were the complete results transferred or only some parts? Which parts?

The complete set is transferred… except for NRBCe (nuclear, radiological, biological, chemical or explosives), and conventional attacks, due to restricted-dissemination intelligence data.

34. With what level of abstraction were the results transferred?

Note: the question does not really make sense in the SDMIS context.

35. How much effort was dedicated to the transfer operation?

Significant effort, since it concerns a lot of people, incl. GARC, HR for training, purchase…

However, it is difficult to cost, since the transfer is included in everyone's everyday tasks.

36. How efficient was this transfer?

There is space for improvement. Communication is key, but it is always complex, essentially due to the number of hierarchical levels within the organisation. Some information can get lost. Also, the organisation is hybrid, with administration tasks in the office, and operational tasks in the field, with very different working conditions.

37. Did you receive some feedback from the runtime teams after the transfer? How much time after? And what type of feedback?

Yes. There is a specific mailbox for RETEX. Some other departments in France even have RETEX service. A triage is performed, and feedback is provided to the contributors. This feedback is a time-costly process, but it is essential to keep the feedback coming in.

Once a week, there is a specific time dedicated to RETEX during one's watch.

Real-time / Run-time Risk Management Interview

Interviewee: Bruno PERRIER (SDMIS)
Interviewer: Stéphane PAUL (researcher, Thales)
Dates & times of interviews:

- 21/09/2021, 14:00-15:30
- 06/10/2021, 08:30-10:30
- 07/10/2021, 17:15-18:00

Bruno has a small team, essentially centred on crisis management.

Scope / General purpose

1. What is the business or technical context of this operational risk management? Describe the context and area where the end user is working (e.g. hydro power plant, control centre etc.)

See static risk assessment part of the questionnaire.

2. Do you perform yourself or require from your system providers some form of operational risk management at run-time?

SDMIS has no sub-contractors. Whatever the event, SDMIS always works with the risk management team from the concerned organisation (including State related) or infrastructure. The benefit of the collaboration relates to the specifics of the event (e.g., location of gas conducts, electricity lines, etc.). This allows for greater adaptability. SDMIS makes the synthesis. The level of detail for dynamic risk assessment is much greater than what can be done during static risk assessment, in order to raise all doubts.

For static risk assessment, the opportunity of an external audit was considered, but that was never enacted.

3. What types of operational risk / threats do you face in your normal operation? What principal threats affect your operation?
   3.1. What are the primary threats that affect your normal operation?

For usual risks, not addressed during static risk assessment, a very fast risk assessment is performed before going to the field. Depending on the urgency, the risk assessment can be a purely mental operation, or formalised.

There is also a new decision-making tool (named MAX by Medae), on a portable device, with a decision tree. This relates to non-daily tasks, with high technical expertise requirements, e.g., electric car fire, and high stress situations. This tool is still under evaluation. Improvement work is performed with a start-up, since 2 years. The tool is derived from a similar tool for doctors, for rare medical events. Data fed in the tool comes essentially from SDMIS, based on static risk assessments and return on experience. The static risk assessment results are used as framework for structuring the content of the tool.

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?
    4.1. Describe if there is a categorization of risks (technical risk, procedural risks) and flowing of these risks to relevant stakeholders.

See static risk assessment part of the questionnaire.

The dynamic risk assessments are made on-site. An action plan is established, and shared with the team, orally (essentially) or in written form (rarely). The plan may be shared with the station through radio, or an enciphered messaging application.

5. In your field, is dynamic risk management mandated by regulation? Which regulation?

The law mandates to be able to respond to all types of risk. Therefore, no explicit regulation for risk management, but operational conditions & societal pressure indirectly require it. The action doctrine has changed recently due to terrorist attacks.

6. Do you have an accreditation / certification to maintain?
    6.1. Who is the accreditation / certification body?
    6.2. At what rate must the accreditation / certification be renewed?

There are some forecastist ("prévisionist" in French) diplomas, but they are not mandated.

Logistics

7. Who performs the operational risk management?
    7.1. Do you perform the risk management yourself or is it sub-contracted?
    7.2. How many people of involved?
    7.3. What are their required skills?

SDMIS performs alone. The team includes 6 or 7 persons on terrorist attacks, to acquire data and deploy prevention actions.

There is also a methodology office at SDMIS, which helps establish the methods / operational processes to solve a given problem, particularly where new technologies are involved.

8. How often are the risk management results updated?
    8.1. Are there events that trigger (should trigger) an update?
    8.2. Outside of those events, who can decide to launch an update?

Depending on the types of risks, updates can be triggered by:

- Law (static risk assessment)
- Evolution of the conditions (static & dynamic risk assessment)
- Evolution of the systems themselves (static risk assessment)

For static risk assessment, in average, the updates form a continual process, but the scope of the updates can be very different. Major impact updates are seen every 2 or 3 years.

For dynamic risk assessment, see question 27.

9. How much time / budget is dedicated to risk management updates?

For static risk assessment, it is variable depending on the scope. Moreover, it is difficult to assess because it is done regularly by all the staff, as part of their everyday work. In addition, there are many partners, e.g., DREAL. Coordination time is key.

For dynamic risk assessment, there is no allocated time or budget. It is an integral part of the operations on the field.

10. What is the risk study time frame being considered?
    52.1. For how long your risk assessment is valid?
    52.2. When do you schedule minor updates or complete reviews of your studies?

For static risk assessment, a periodicity is defined for ORSEC plans (see static part of questionnaire). However, obsolescence can trigger new updates.

For dynamic risk assessment, the updates are essentially valid only for the ongoing operation. However, post-mortem is used to improve the static risk assessment.

11. Are the updates usually performed by the same people who did the initial analysis? If no, are their skills / competencies different or similar?

Yes & no. More people are involved in the dynamic risk assessment, but the responsible staff for the static risk assessment are systematically invited to contribute to the dynamic analyses.

12. Outside of a crisis situation, who has the last word on the risk treatment options whilst the system is operational?

For static risk assessment, the director, depending on the stakes. There are strong hierarchical relations between people, within SDMIS, but also in the State-related organisations (mayor, prefect…).

For dynamic risk assessment, the commander in charge of the rescue operation.

13. During a crisis, what is the decision chain? Who has the last word on the response to apply?

The commander of rescue operations. The commander is generally the oldest in the highest grade. It is to be noted that the frontier of the rescue operation is often fuzzy (start, end, responsibility of SDMIS, required financial engagement…). The questions often remains open.

<u>Transfer methodology (if applicable)</u>

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

14. Is there a process to transfer the results from design time to run time?

There are 3 types of plans: interventions + ORSEC + prevention.

There is no specific training to use the risk assessment reports. The officers are supposed to be aware of the risk assessment updates and read them. There are executive summaries ("fiche reflexes" in French, 4-15 pages, up to 60 pages for major sectors, due to domino effects) for each case study. The officer takes the latter before going to the field.

Two main reasons may hinder the transfer:

- The large number of possible sites (≈ 200) where SDMIS may act.
- Gaps between the content of the plan and the reality. The officer is supposed to adapt in real-time.

15. Do you usually start the risk assessment from scratch or to you have the static risk assessment results as input?

Start point: executive summaries ("Fiche réflexes") - see previous questions.

On the long-term, the summaries could be included in MAX by Medae.

16. Who took the transfer initiative?

"Transfer is instituted, but also human motivation-driven. There is no meeting. Each one must take the action of reading the reports.

Note: there are, from time to time, some generic training on specific cases / sites.

Some officers have specialties (e.g., NRBC). They have more frequent trainings. They act as counsellors to the commander & chief of site / industry.

17. From where / which team do the results originate?

From the Prevention & Rescue Organisation Directorate ("Direction de la prevention et de l'organisation des secours"), of which:

- the "Groupement Analyse et Couverture des Risques (GACR)" – risk management;
- the "Groupement prévention (GPrev)" – fire safety;
- the "Groupement Réponse aux crises Majeures et Attentats (GCMA)" – major crisis and terror attacks.

18. What was the main goal of this transfer? Was this a shared goal with the static risk analysis providers?

The staff performing the static and dynamic risk assessments shared the same goal, and it is the same staff anyway.

19. Do you reuse the complete static risk analysis or only parts thereof?

Essentially the summary ("fiches reflexes"). Sometimes an "anticipation team" is organised, and they make a more thorough survey of the literature to support the operational team.

20. How useful are these inputs? (Estimate)

Essential.

21. What are the areas where the inputs were the most useful, e.g. business / operational impact analysis?

Both strategic, e.g., location of C3I centres, and tactical information, e.g., access points, rescue procedures, dangerous products…, are key inputs.

22. Did you have to rework the inputs, typically the level of abstraction?

During static risk assessment, some officers review the plans and may adapt them: missing elements, highlighting of elements, removal of noise (non-relevant data), etc.

During a crisis, reality often overwhelms the plans, so the plans must be reworked.

23. Is some form of traceability organised between the static and dynamic risk management results?

Yes, because of the regular updates (whether by regulation or not).

24. Have you already provided feedback to the static risk management teams?

Yes, based on return on experience on the field, and also due to evolving technology.

25. Is this feedback manual or automated?

Both. After a rescue operation, minutes are written (electronic form) with statements of what worked and what did not, and improvement recommendations are made.

There is also the possibility to write emails.

Risk Management Methodology

26. What are the utilized risk management methods / techniques?

The method is called Source (e.g., radioactive element) + Flows (e.g., impact distance) + Target (e.g., nearby school). Actions can be performed on any of these 3 elements.

Training on this method is done for officers since more than 10-15 years.

The static risk assessment prepares the final report using sources + flows + targets schemas.

27. What are the tasks involved in risk management during runtime?

Steps:

4. Immediate rescue operations
5. Assessment, i.e., information collection

6. Identification of secondary risks – note that “secondary” here does not relate to the level of impact, but to the domino effects
7. Action plan, with priorities
8. Execution plan (resource allocation)
9. Organisation of the control-command centre for long-term operations
10. Logistics organisation for long-term operations

These steps are iterated very often, i.e., every 10mn to every 2-3 days depending on the situations.

28. What input data are required for dynamic risk management and how do you collect the data?

A very wide range of data types, e.g., meteorological data, road traffic, public transport…, are required. Collection is essentially through human contact, with some additional electronic applications.

29. At what level of abstraction are you working?
    - 29.1. Typically, how many business assets? Supporting assets?
    - 29.2. Is it different to the abstraction level in static risk management? (Note: see also the answer to question 21 above).
    - 29.3. How do you handle the detected vulnerabilities? Is there a procedure for doing so?
    - 29.4. Do you assess compliance to all security measures?
    - 29.5. Are there particular flaws or vulnerabilities that require special focus?
    - 29.6. Are there applicable international standards? (List only the most important ones).

For static risk assessment:

- Vulnerabilities are monitored for key rescue elements (e.g., communication means, energy supply).
- Scope is very large to ensure continued operations.

For dynamic risk assessment, vulnerabilities are studied essentially for the protection of people. Some situations may require some significant risks to be taken: “save or perish”.

30. What are the general assumptions (hypotheses)?
    - 30.1. How often are these hypotheses updated?
    - 30.2. Is there a provision for dynamic updating of these hypotheses?

No. Not checking facts is considered as a fault, often due to stress.

31. How often is the risk management activity conducted?
    - 31.1. What triggers the risk management related actions? (Set intervals, actions, etc)
    - 31.2. Are there provisions for the risk model updates?
    - 31.3. What specific triggers are there to update the risk model? Is it triggered periodically, on a specific action or triggered by an external factor?
    - 31.4. Are the existing triggers OK or do you think there should be other ones?
    - 31.5. What is the typical lifecycle of the risk model?

See question 27. The main triggers for an iteration are the treatment effects (i.e., lack of effects or completion of the expected effects), and time (i.e., obsolescence of data).

32. Are there different hierarchical levels in the company that perform the risk management? For example, are the risk management results at lower organizational levels in the company prepared on their own and then fed higher in the organization?

Risk assessments are performed at all hierarchical levels, and results are shared on the field.

In addition, there is the "anticipation team(s)" and other teams in the control-command centre.

33. Do you have a standard operating procedure guidebook?
    33.1. What standards is this book compliant with?
    33.2. Are there applicable international standards? (List only the most important ones).

Yes, e.g., operation plans + doctrines + in the future, MAX (prototype). There is no applicable international standard.

34. How are the standard operating procedures designed?
    34.1. What is the process of amending the procedures?
    34.2. What triggers the SOP updates?
    34.3. Is there participation / collaboration with static risk management team in the design of SOPs?
    34.4. Who are the specialists involved in design, mandating and eventual invalidation of SOPs and the corresponding operational documentation?

See question n°18 in static part of the questionnaire. There are no updates of the SOPs during operations.

35. Is there a specific standard family (e.g. similar to ISO 27000 family of standards) that governs the risk management?
    35.1. What specific risk management standards must you comply with?

No.

36. How do you model acceptable levels of risk?
    36.1. What risk treatment strategy do you use?
    36.2. Do you define different strategies in different operational contexts?
    36.3. Is there a risk aversion matrix (aka risk appetite matrix)?
    36.4. Is that matrix unique within the organization or are there multiple ones?

(In some operational contexts of e.g. transmission system operation different risk models and acceptable risk levels are modelled in different fashion. The idea is to capture what the assumed criteria are).

For static risk assessment, there is a corporate acceptable level of risk.

During dynamic risk assessment, there are 2 levels of decisions: a hierarchical decision to send a team, and then a personal human-based assessment, taken on the spot, by individuals.

37. Are cascading effects a specific issue for you? How are they currently managed?
    37.1. Note: this is an important question for T2.2. Please give enough focus here.

Yes. Priority can sometimes focus on secondary effects (i.e., flows and target) rather than on the source – see "source + flow + target" model in previous questions.

Use of dynamic risk management results

38. Who in your organisation reads the risk management report after completion?

All the command chain has access.

39. How are the risk management results used during run time?

To make hypotheses, and help in decision-making during operations.

40. Are the risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

Some risk assessments are classified "Secret defence". Else, all others are open to the command chain.

41. Is the risk management report sent outside of your organisation? To whom?

Risk management reports are not sent outside of the organisation, except in specific cases. Indeed, SDMIS does not hold the IP on the report contents. Exceptions include the need to share during a crisis (if the data is not confidential).

Use of cybersecurity risk management results for detection and response (SOC)

42. How are the risks / threats presented (e.g. semaphore, numerical presentation, alerts…)?

n/a

43. How many of these security events are real attacks? Are there often false positives? (Estimate).

n/a

44. Have you already experienced a false negative (i.e. undetected attack until too late)?

n/a

45. How often do you trigger corrective actions?

n/a

46. Are there automatic notification systems when the corrective actions are triggered?

    46.1. Is there a system for automatic notification when corrective actions are taken manually or automatically?

    46.2. Note: The idea is to get the situation "from the field".

46.3. Is there an identified lifecycle for an alarm / notification – is it automatically dismissed after some time even with no action on behalf of the operator?

n/a

47. Are there automatic risk mitigation actions in the systems you monitor?

47.1. If so, how are you informed on automatic results (think primary and secondary reserve activation, automatic generation control in terms of power system, closing of perimeter in the critical infrastructures primarily dealing with physical risks such as airports)

n/a

48. Crisis management: How do you perform escalation when the resources at your disposal are not enough to handle the current level of risks?

48.1. Note: this is an important question for T2.2. Please give enough focus here.

Reinforcement can be called. Then priorities are set.

Other uses of risk management results

49. Are the dynamic risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

Note: the question has been changed to sharing beyond the organisation.

Yes:

- weekly, with a few other 1st responders, i.e., SIS ("Services Incendie et Secours"),
- every 2 months or so, with a larger group of SIS;
- every 2 years or so, for major events where all French SIS are invited.

In all these events, key return on experience is exchanged.

*Operational context questions (**optional**)*

50. How many different risk sources do you handle in a typical hour/day of operation?

50.1. Is that number consistent with what was handled during static risk management?

SDMIS handles ≈ 100.000 operations per year, i.e., close to 300 operations per day.

51. How many observables / events do you manage in a typical hour of operation? Is there a seasonality (e.g. flood season?)

Yes, there is a seasonality, e.g., due to climate, social heat, Xmas...

52. How many of these alerts are classified as security events? Estimate a percentage.

There are a few unjustified calls (≈ 10%).

Additional Interview for Cybersecurity Concerns

Interviewees: HERRY Laurent (CISO, SDMIS)
Interviewers: PAUL Stéphane (researcher, Thales), HELIES Elsa (researcher, EDF)
Date & time of interview: 28/09/2021, 15:30-16:30

The SDMIS was created in 1999. The IS/IT was established in a few months. Structuring is still ongoing.

There are 30 persons at the GSI (i.e., IT team), of which 2 are cybersecurity experts. There is no internal software development team.

Before 2016, there was no risk assessment, and no CISO. The cybersecurity policy is vulnerability-driven.

In 2016, a risk assessment was established for the whole organisation, using the EBIOS-2010 method. The risk assessment remains valid to this day. It includes the IT related ecosystem, but not the other parts of the ecosystem (e.g., fluids providers). The risk assessment report remains internal to GSI, i.e., it is not shared with external cybersecurity service providers, but the latter know quite well the IS/IT infrastructure of SDMIS.

There is no risk assessment update when a system evolves. GSI performs vulnerability assessment and treatment. In short, the cybersecurity policy remains essentially vulnerability-driven.

When provisioning new systems, applications, hardware… standard requirements are expressed in the call for tender. No risk assessment is requested from the supply chain.

Once the systems are deployed, there are regular pen tests and / or audits focused on the sensitive systems. During an attack / crisis, internal treatment is 1st performed, but if the attack is too strong, external support is planned (service providers, interior ministry, ANSSI).

A global cybersecurity picture is captured every 3 years through external audits by a PASSI supplier (in French "Prestataires d'Audit de la Sécurité des Systèmes d'Information"). These audits are maturity audits, with respect to ISO 27001.

A 3-years cybersecurity roadmap is established based on the maturity audits. It relates only to major actions (i.e., small day-to-day activities are not part of the roadmap). The GSI proposes the roadmap, and justifies it. The top management validates. The budget is allocated in consequence. Roadmap actions are done in collaboration with the editors, with a mix of internal and externalised actions.

X. ANNEX J – ZAG extensive interviews

International Zagreb Airport Jsc. (Međunarodna zračna luka Zagreb d.d./MZLZ) is a company registered in Croatia which, based on the Concession Agreement concluded with Republic of Croatia, has exclusive right to construct, operate and maintain Zagreb Airport (''Franjo Tuđman Airport''/ ''ZAG'' i.e. which operates the entire airport from 2013 onwards for 30 years, including the runway, passenger terminal, cargo terminal, parking lots and future property developments.

Company MZLZ is established by company Zaic – A Limited as sole shareholder of MZLZ. Zaic is company incorporated by 6 shareholders whereas each of them brings its international expertise in the airport development, operation, construction, project management, and structured finance.

For the purpose of performing all right and obligations from the Concession Agreement concession is organized through the group of the companies having different roles, including through: sister company of MZLZ, MZLZ – Zagreb Airport Operator L.td (MZLZ – Upravitelj zračne luke Zagreb d.o.o./ MOPE) which company manages and maintains ZAG and provides airport services.

Design-time Risk Management Interview

Interviewees:

- Marin Tica, IT director
- Gabrijela Abramović – Quality manager
- Nikolina Lovrić – Senior Associate for Integrated Management System
- Melita Damjanović – Technical coordinator, Development department,
- Ivo Jurič – airport security manager (protection and monitoring from illegal obstruction such as terrorism, kidnaps etc.)
- Miroslav Jerković – airport safety manager (safety of aircraft operations)

Interviewers: Hrvoje Keko, Tamara Hadjina

Dates & times of interviews:

- 28/09/2021, duration 1.5h
- 04/10/2021, duration 1.5h

Scope / General purpose

1. Do you perform yourself or require from your system providers some form of risk management as soon as the proposal phase? Or only at design-time?

All projects that have influence on Safety and Security are required to prepare risk management. MZLZ prepares internal risk assessment. Furthermore, for aerodrome risks related to safety of aircraft operations. Risk assessment of a change is mandatory part of change approval.

A general IT risk assessment exists but not for specific project.

According to national Law, which adopts EU 2016/1148 directive and EU 2018/151 implementing regulation such risk assessment should be done periodically.

2. What is the business or technical context of risk management? Describe the context and area where the end user is working (hydro power plant, control centre etc.)

MZLZ identifies, analyses, monitors and reviews factors that arise from political, economic, social, technological, legal and environment issues that have influence on strategic direction and our Organizational context and may affect our ability to achieve intended objectives and stability of our Integrated Management System. MZLZ monitors and reviews this information to understand our context during management review meetings. The output from this activity is input to consideration of risks and opportunities and the actions that we take to address them. Risk and opportunity management is undertaken as part of MZLZ's day-to-day operations and is followed and reported through dedicated software.

The purpose of risk management is to:

- Evaluate and anticipate the risks the company is likely to face
- Help managers decide how to minimize the level of such risks by
- Allocating human, financial and physical resources
- Setting priorities according to goals and allocated resources
- Improve governance and business oversight

In addition, Risks related to safety of aircraft operations under the scope of aerodrome operator's responsibilities.

3. What types of risk / threats do you manage?

Strategic risks: Risks related to the infectious diseases and instability, International risks, Risks related to customer satisfaction, Risks related to investments in developments and capabilities, Risks related to the competitive environment, Risks related to the customer portfolio structure, Risks related to ethics and compliance, Risk related to fulfilment of Concession agreement, Risks related to legal and regulatory changes, Risks related to environment

Risks related to MZLZ' activities: Risks linked to security (terrorism, other types of illegal actions), Risks linked to asset maintenance, Risks linked to the health and safety of people, Risks linked to airport safety

Management organization risks: Risks related to data protection and cyber security, Human Resources risks

Financial risk: Market risk, Liquidity risk, Credit risk

Risks related to safety of aircraft operations under the scope of aerodrome operator's (MOPE's) responsibility

4. Do you categorize the risks? Are those categories related to the interested stakeholders (i.e. are the categories used to flow down the risks to the relevant stakeholders)?

4.1 Describe if there is a categorization of risks (e.g. technical/procedural risks vs. organisational risks, but there may be other categories) and flowing of these risks to relevant stakeholders (e.g. technical/procedural risk flow down to the design team, whilst organisational risks flow down to the management).

Yes. Methodology is the Owner methodological guide to risk management. Risks are categorized according to acceptable and unacceptable risks. Unacceptable risks are:

- ethics and compliance,

- protection of information,
- cybersecurity,
- safety of persons,
- security,
- airport safety,
- deterioration in the state of physical assets.

For risks related to civil aviation the categorization is done as provided in Regulation (EU) 2020/2034.

If a cyber security event occurs which affects 20% of the business it has to be reported as an incident, even if it is not life threatening in line with Law on cyber security of key service operators and digital service provision OG 64/18.

5. In your field, is static risk management mandatory by regulation? Which regulation?

Static risk management that comes from Integrated Management System is not mandatory by regulation.

For aviation related occurrences European Risk Classification Scheme (ERCS) as per EU 2020/2034.

6. Do you usually aim for an accreditation / certification? Who is the accreditation / certification body?

For the Integrated Management System (IMS) certification is based on: ISO 9001:2015 norm request- Quality Management System, ISO norm request - 14001:2015 Environmental Management System, ISO 10002:2018 Customer complaints guidance.

Aerodrome operators within EU must be certified in accordance with Regulation (EU) 139/2014. Hence, the operator of this airport is certified by the CCAA which performs periodic inspections. MZLZ does not have such certificate since it is not formally in the position of the airport operator, but only as the Concessionaire is obliged to ensure that such certificate is in place either by himself or by some other company (in this case MOPE).

Airport's physical protection devices (such as x-ray, cameras etc.) must be from the ECAC list of certified equipment. Both equipment and the vendor must have a certificate.

Logistics // for Initial Risk Assessment

7. Who performs the initial risk assessment?

7.1. Do you perform the risk management yourself or is it sub-contracted?

Initial risk assessment in IMS is performed by process owners. The risk management is structured into four risk management process stages: Identify, Analyse, assess and prioritize, Mitigate, Check and track assess. The risk owner, by virtue of their level of responsibility and expertise in that field, is best suited to defining and deciding on measures to reduce a given risk to an acceptable level.

For aerodrome risks related to safety of aircraft operations - the aerodrome safety manager. Others may be involved as applicable depending on identified hazards, risks and risk barriers.

7.2. How many people are involved?

There are 15 process owners divided by their processes: System Management, Improvement, Commercial and Marketing, Security, Safety, Compliance and certification, Airport operations, Maintenance, Airport Operator, IT, Finance, Procurement, Human Resources, Legal, Development.

7.3. What are their required skills?

Required skills for process owners is global and covers knowledge of applicable national and international regulations, knowledge and skills of the field they manage, IMS awareness.

7.4. If there are certifications required with respect to the skills of personnel / companies, what are these certifications?

ISO 9001:2015 under 7.1.6. requires that the organization shall determine the knowledge necessary for the operation of its processes and to achieve conformity of products and services. Organizational knowledge can be based on: internal and external sources.

Airport has a training centre where employees are trained and certified to work at the airport specific jobs (maintenance, safety, security, health and safety at work etc.) according to the training program.

8. Are there provisions to infer from other risk management teams?

n/a

9. Who has the last word on the risk treatment options?

Is the company management involved in the risk management and treatment of the risk? *Note: Please do not put this question as too suggestive, and be as open as possible here as there might be risk management personnel that have the last word without being in the company management.*

Final risk arbitration requires decision of management board. Risk owners, in agreement with top management, should determine the expected evolution for each risk (increase/stable/decrease) for next year, based on expected future changes (context/control environment).

For aerodrome risks related to safety of aircraft operations - the aerodrome safety manager. Risk approvals depend on assessed gravity of consequences and involved may be the accountable manager, division director(s) and departmental manager(s) as applicable.

10. How much time / budget is dedicated to this initial risk assessment?

Note this is an informative question: the response in absolute terms (in maybe monetary terms) may not be relevant across different infrastructures, but we will get relevant results given the context above. We're dealing with transition from static to dynamic and investment issues are important – if you invested no resources in static risk management you won't care about transition either.

Global company risk mapping is planned to be once per year. A total of 15 interviews is planned to be carried out: Top management, process owners and subject matter experts will be individually interviewed throughout the risk mapping week (5 days). The planned hours spent in interviews are about 40 hours.

11. What is the risk study time frame being considered?

11.1. For how long your risk assessment is valid?

Global company risk assessment is valid for one year.

11.2. When do you schedule minor updates or complete reviews of your studies?

Within MZLZ, risk mapping is planned to be carried out between April/June each year.

Methodology

12. What are the utilized risk management methods / techniques?

The risk management methodology is structured into four risk management process stages:

Identify

The purpose of this stage is to list the main risks likely to harm the MZLZ's goals and interests. Risks sustained as well as incurred (due to action or inaction) by an MZLZ's activities must be taken into account.

Analyse, Assess and prioritize

Each risk is analysed and assessed in a risk form which summarized the main characteristics of the risk, namely :

- listing and analysing its causes, consequences and management factors for the activity concerned and determining a maximum credible scenario,
- rating,
- actions plan.

Mitigate - Each risk is to be treated

Check and track assess - This stage consists of :

- risk mapping updating
- reporting on the progress of measures

For risks related to civil aviation as provided in Regulation (EU) 2020/2034.

13. What input data is required?

- annual interviews
- conversations with identified experts
- non-conformities, observations and recommendations made during internal and external audits
- feedback on incidents
- Customer complaints
- the risks identified at the process level

For risk related to safety of airport operations input depends on identified hazard(s) and risk(s).

14. At what level of abstraction are you working?

14.1. Typically, how many business assets? Supporting assets?

All business assets that have influence on business stability of company.

14.2. Do you list all vulnerabilities, e.g. using CVEs? Yes.

14.3. Is there maybe an official (mandatory) list of vulnerabilities? No.

14.4. Do you list all attacks, e.g. using CAPEC or MITRE ATT&CK? Yes.

14.5. Do you assess compliance to all security measures? Yes

14.6. Are there particular flaws or vulnerabilities that require special focus? Yes, vulnerabilities related to infrastructure.

15. What are the general assumptions (hypotheses)?

15.1. Some of these hypotheses relate to how the system is used in practice. They can become outdated as the system is operating. How often are these general hypotheses updated?

15.2. Is there already provision for dynamic updates of these hypotheses?

No generalization can be made. Global company Risk assessment is performed at least once per year.

16. How often is the risk management activity conducted?

16.1. Are there provisions for risk model (i.e. security file) updates?

16.2. How are the risk model updates triggered currently (e.g. periodically, on a specific action, triggered by an external factor)?

16.3. Are those triggers OK or should there be others?

16.4. What is the lifecycle of your risk models? (While similar question has been answered before, we may elicit more quality answers here).

Global company risk mapping is planned to be once per year. A total of 15 interviews is planned to be carried out: Top management, process owners and subject matter experts were will be individually interviewed throughout the risk mapping week (5 days). The planned hours spent in interviews are about 40 hours.

17. Are there different hierarchical levels in the company that perform the risk management? For example, are lower levels in the company producing their own and feeding the results higher?

YES. Each process has its owner (director/manager) and they communicate with Quality department that coordinates various processes.

Details are already given in previous answers.

For aerodrome risks related to safety of aircraft operations - the aerodrome safety manager. Only experts may be involved as applicable depending on identified hazards, risks and risk barriers.

18. How are the standard operating procedures designed?

18.1. What is the process of amending the procedures?

Revisions are made by SOP authors, approved by process owners or president of management board, published on company portal and all involved stakeholders are automatically notified about the change.

18.2. Does the risk management team participate in the design of SOPs for the operational teams?

Yes.

18.3. Who are the specialists involved in the design and mandating of SOPs and the operational documentation?

All experts in their relevant field.

19. Is there a standard (e.g. similar to ISO 27000 family of standards) that governs the risk?

19.1. What specific risk management standards must you comply with?

19.2. *Note: Different critical infrastructures use different standards (industrial automation, aviation, ports).*

19.3. *Note: Try to collect the references to principal standards here – it is not an exercise in taxonomy of all standards touched by a particular critical infrastructure.*

Applicable standards are: ISO 9001, 14001 and 10002.

Regulation: EU Commission Regulation 139/2014; for risks related to civil aviation as provided in Regulation (EU) 2020/2034 EUR-Lex - 32020R2034 - EN - EUR-Lex (europa.eu)

20. Do you collaborate with national security entities or other national and international bodies?

For civil aviation matters with competent authority - CCAA – Croatian Civil Aviation Agency

Security events (those not connected to IT!!) are reported to central European event database and automatically transferred to national agencies:

- CCAA
- Croatian agency for investigation of accidents and incidents in air, sea, road and rail transport (according to REGULATION (EU) No 996/2010)
- If a cyber security event occurs which affects 20% of the business it has to be reported as an incident, even if it is not life threatening in line with Law on Law on cyber security of key service operators and digital service provision OG 64/18

21. How do you model acceptable levels of risk?

21.1. What risk treatment strategy do you use?

Each company global risk is assessed according to:

- the impact and probability of its occurrence, used to determine its criticality,
- the effectiveness of the control devices associated with it and considered for the assessment of impact and probability.

Risk Mapping is represented by a matrix in which each risk is positioned according to its impact, on the y-axis, and its probability, on the x-axis.

21.2. Do you defined different strategies in different contexts or is your strategy unique within your organisation?

Strategy is unique.

21.3. Do you defined a risk aversion matrix.(a.k.a. risk appetite matrix)?

Yes

21.4. Do you defined different risk aversion matrixes in different contexts or is your risk aversion matrix unique within your organisation?

An example: in some contexts in transmission system operators the N-1 criterion (ability of system to cover the failure of largest system unit), a.k.a. no single point of failure, is often used, contrasted to more elaborate probabilistic models that are used in other contexts. This criterion is only an illustrative example, other types of CI may utilize different assumptions, the idea is to try to catch what these criteria are.

All processes use IT infrastructure and rely on IT to function properly. Realistically, an event caused by IT should be treated as security event.

Airport shall align with COMMISSION IMPLEMENTING REGULATION (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures.

For civil aviation risks the model in use is as provided in Regulation (EU) 2020/2034.

22. Are cascading effects a specific issue for you? How are they currently managed?

22.1. This is a very important question given that the project is handling the cascading events, so we should give it enough space.

Airport is aware of their interdependence with the power system. They have redundant local systems which are regularly tested and maintained and ready to be activated in case of power system blackout.

Airport is tightly connected to other companies but has no control over them:

- Flight control
- MZLZ Ground Handling Service Ltd
- Airline companies – departure control systems (DCS) - > local DCSs -> manual check in

IT is again critical because risk assessment should take in consideration impacts from other responsible stakeholders. Cyber risk form connected interdependent companies can be transferred to the airport.

Use of static risk management results

23. Who in your organisation reads the risk management report after completion?

Management board, process owners.

For aerodrome risks related to civil aviation, concerned managers and external stakeholders as applicable.

24. How are the risk management_results used during design-time?

If the risk is unacceptable, we use mitigation measures immediately to put the risk on the lowest level.

The owners of defined risk barriers are responsible for their implementation and follow-up.

25. Are the risk management results of one system / programme shared with other systems / programmes / teams within your organisation?

    25.1. If there is risk management performed at specific project level versus the programme, team, or organizational level, is there sharing between different levels?

Yes.

For aerodrome risks related to civil aviation, depending on identifed hazard(s), risk(s) and risk barriers.

26. Is the risk management report sent outside of your organisation? To whom?

Yes, to shareholder if the Company.

For aerodrome risks related to civil aviation, to involved stakeholders as applicable.

Transfer methodology (if applicable)

The questions in this section are directed towards finding out whether there already exists a methodology to transfer the risk management results from design time to run time, as well as the interviewee's estimates on the efficacy of the procedure.

27. Is there a process to transfer the results from design time to run time?

Quality department assures that measures are taken to mitigate the detected risks.

28. Have you already transferred some static risk assessment results for reuse during runtime?

    28.1. Do you communicate your results to the run time teams (directly?)?

Indirectly, via process owner/manager.

29. Who took this initiative?

    29.1. Has this been called for by runtime operators or someone else?

Quality Department and process owner managers.

30. To whom were the results transferred?

Results are transferred to relevant process owner and management board of the company.

31. What was the main goal of this transfer? Was this a shared goal with the recipients?

Main goal is to reduce the risk on the lowest level.

32. Do you have an established procedure of reporting the risk management results to stakeholders outside your company?

Yes, shareholders, relevant authority (CCAA) and auditors.

The interview ended here. Other questions were obsolete since the answers became predictable and circled around same answers.

Operational risk management or dynamic risk management is not considered as a separate topic at the airport. Static risk management results in standard operating procedures, which are then obligatory for everyone.