Risk Observatory Requirements

G. Gigante, D. Pascarella, A. Vozella (CIRA), A. Roelen,
J. Verstraeten (NLR), S. Metge (Airbus), G. Greene (CAA UK)

Short abstract: Future Sky Safety is a Joint Research Programme (JRP) on Safety, initiated by EREA, the association of European Research Establishments in Aeronautics. The Programme contains two streams of activities: 1) coordination of the safety research programmes of the EREA institutes and 2) collaborative research projects on European safety priorities.

This deliverable is produced by the Project P4 "Total System Risk Assessment". The main objective of this study report is the definition of Risk Observatory Requirements (business requirements, user requirements and system requirements).

Programme Manager	M.A. Piers, NLR
Operations Manager	L.J.P. Speijker, NLR
Project Manager (P4)	J.G. Verstraeten, NLR
Grant Agreement No.	640597
Document Identification	D4.1-ES
Status	Approved
Version	2.0
Classification	Public

EXECUTIVE SUMMARY

Problem Area

Safety is a dynamic characteristic of the aviation system, whereby safety risks must be continuously mitigated. Furthermore, the aviation system entails the complex interaction of different organizations. Each organization has to implement a safety management system, which should interact to assure effective system-wide safety management. The ICAO Safety Management Manual (DOC 9859) gives guidelines on safety management fundamentals, but a uniform and complete approach should be envisaged at European level. Stakeholder interviews and a literature survey unveiled some particularly critical aspects and defined the problem context driving the Project P4 "Total system risk assessment" of Future Sky Safety:

- Safety Data Collection and Analysis: there is insufficient safety data available/used (both from the own operation or other operations) to get a full picture of safety risks, this causes uncertainty with regard to current safety performance. Available human resources are mostly used for processing data (often manual processing is needed – therefore, organizations can feel overloaded with data) and reactive analysis based on individual occurrences;
- Safety Indicators and Safety Performance Monitoring: there is a need for a uniform approach to safety indicator definitions and safety performance monitoring;
- Hazard and Risk Management: some difficulties emerged in the identification of new hazards when a change in systems or procedures occurs;
- Safety space: the safety information does not give appropriate means to executive management to make informed decisions on resource allocation for safety management. The allocation of excessive resources to protection or risk controls may result in the product or service becoming unprofitable, thus jeopardizing the viability of the organization. On the other hand, excess allocation of resources for production at the expense of protection can have an impact on the safety performance of the product or service and can ultimately lead to an accident. It is therefore essential to provide an early warning, if an unbalanced allocation of resources exists or is developing. The need to balance production and protection has become a readily understood and accepted requirement from a product and service provider perspective.

Description of Work

The definition of Risk Observatory (RO) requirements has been sequenced through a series of standard steps starting from analyzing business scope to derive business requirements, going on with formalizing user requirements and ending with system requirements. Requirements definition, whatever the class they belong to, needs to accomplish typical activities, which the WP4.1 "Risk observatory requirements" team has carried out in the assigned period, from the start of the project to the last quarter of the first year:

1. Planning and Monitoring
    a. Identification of applicable standards to guide analysis and formalization of requirements
    b. Identification of proper RO stakeholders
    c. Identification of proper inputs for analysis
2. Eliciting and collecting inputs
3. Analyzing collected information
4. Defining requirements

Meetings and teleconferences have been held to discuss and agree to a common approach to the work. During the task execution some intermediates documents have been produced:

- Stakeholder Interview Questionnaire
- Interview Analysis Reports per domain (airports, airlines, aircraft manufacturer, ANSPs)
- Project Analysis reports (for relevant previous research projects)
- Project Analysis summary (synthesis of all projects)
- Business Requirement document (D4.1.1)
- User and System Requirement document (D4.1.2)
- Minutes of meeting

Results & Conclusions

Business requirements and a first version of User and System Requirements have been defined. The business scope of the RO has been outlined with a high level business model proposal representing the basic input to next work packages. User needs have been collected and formalized. In the first interactions users have shown a bit reticence to describe their internal information flow and have provided high level needs. Currently system requirements provide a high-level view of the main functions and of the quality and security requirements. They provide inputs to the development of a look-and-feel prototype. User feedbacks after their evaluation of that prototype will further specify user requirements, allowing the refinement of the system requirements. The requirements will be used in the RO design phase.

Applicability

This report is applicable to Project P4 "Total system risk assessment" of Future Sky Safety. It provides the set of high level requirements (business, user, and system requirements) for the development of a prototype risk observatory.