Final version: v1.0
Version date: April 20, 2017

On the Implementation of a European Space Traffic Management System

II. The Safety and Reliability Strategy

R. Tüllmann[1], C. Arbinger[1], S. Baskcomb[2], J. Berdermann[3], H. Fiedler[4], E. Klock[5], and T. Schildknecht[6]

[1] DLR Gesellschaft für Raumfahrtanwendungen, Oberpfaffenhofen, Germany, e-mail: ralph.tuellmann@dlr-gfr.de
[2] ROSAS Center Fribourg, Switzerland
[3] DLR Institute for Communication and Navigation, Neustrelitz, Germany
[4] DLR Institute for Space Operations and Astronaut Training, Oberpfaffenhofen, Germany
[5] Austro Control, Vienna, Austria
[6] Astronomical Institute of the University of Bern, Switzerland

ABSTRACT

This is the second (Paper II) in a mini series of three papers that summarise the final results from an evaluation study which DLR GfR and its partners conducted on behalf of ESA. The objective of this study was to generate a roadmap for the implementation of a European Space Traffic Management (STM) system within the next two decades under consideration of an evolving Air Traffic Management (ATM) system. In Paper I (Tüllmann et al. 2017a) we demonstrated that collision risks do not prevent suborbital space flights from the very beginning. We provided proof of concept that this kind of travel is generally possible, provided significant advances in heat and collision shielding technologies can be achieved. Potential technical, conceptual and organisational setups in response to Europe's STM needs were discussed, focussing on technology and infrastructure development, Space Debris, Space Surveillance & Tracking, Space Weather Monitoring and ATM and STM integration. The initial roadmap was presented showing that the European STM system could become operational in the 2030 – 2035 time frame. Finally, the Top 10 STM-related issues were identified that need to be solved on EU and UN level. In Paper II, we now cover the relevant Safety & Reliability (S&R) aspects which should be reflected in a STM concept of operations. In this context relevant contributors to unsafe operations and hazardous events as well as the parties at risk are identified. Safety Management Systems in aviation business are investigated in order to check to what extent their S&R concepts and good-practices are applicable to STM operations. An initial Risk Classification Scheme for STM purposes is presented and has been applied to classify the Space Weather risks identified in Paper I. Initial values for the acceptable levels of safety for spaceplane occupants and for third parties at risk are presented and the hazards originating from re-entering objects and airspace sharing are discussed. Paper II finishes with the outline of the envisaged Space Navigation Service Provider (SNSP) certification process. This mini series of papers is concluded by Paper III (Tüllmann et al. 2017c) in which we provide initial system and S&R requirements, constraints and recommendations that should be considered for a European STM setup.

Key words. Space Traffic Management – Air Traffic Management – suborbital point-to-point flights – Space Weather Monitoring – Space Surveillance and Tracking – Space Debris & collision risks – Safety & Reliability – risk classification – certification

1. Introduction

The overall purpose of this paper (Paper II) is to present a high-level strategy for a Safety and Reliability (S&R) concept reflecting all relevant operational aspects of a European Space Traffic Management (STM) system (see Paper I (Tüllmann et al. 2017a) for a general introduction into STM, its definition and discussion of needed infrastructure, concepts and services). In order to do this, the first part of this paper (Chapter 1) describes fundamental terms and definitions, outlines the scope & boundary of such a concept, identifies relevant interfaces, existing organisations & STM-related activities and evaluates to what extent S&R knowledge and good-practices are transferable from the aviation to the STM sector.

Based on the results of this analysis, the second part of this work (Chapter 2) covers recommended S&R objectives (including regulations and standards, the overall S&R approach, a safety Risk Classification Scheme (RCS), critical qualitative S&R requirements, initial quantifications of acceptable levels of safety (ALoS), the identifcation of key hazards and occurrence reporting) and an outline for a proposed Space Navigation Service Provider certification process.

1.1. Terms and Definitions

It is not uncommon to find the same S&R terms with slightly different definitions within the suite of regulations, standards and guidelines related to both the space and aviation industry. Examples include ICAO Annex 19 Safety Management, ECSS system Glossary of terms, EU ANS regulation 1035/2011, EASA CS-Definitions and RCC standard 321-16. However, it is important to agree and publish a single set of terms and definitions related to STM (including S&R) in order to help prevent misunderstandings in future S&R work. Ideally, this would re-use and update existing publications.

In the following, a fundamental set of terms used throughout this work is defined in alphabetical order to help understand the context of the high-level discussions in the remainder of this paper:

- ALARP (As Low As Reasonably Practical): The balance of risk mitigation factors, such as safety, time, cost and difficulty of implementing the means of mitigation
- Consequence: A potential result of a Hazard
- Hazard: Any condition, event or circumstance which could induce an undesired consequence
- Reliability: The probability of successful performance of a system over a period of time
- Risk: The probability of the occurrence of a consequence, together with its severity
- Safety: The state in which risks do not exceed an ALoS
- Severity: The extent of harm or damage that could reasonably occur during a consequence
- System: Any combination of equipment (hardware (HW) and software (SW)), procedures, human resources or organisations that perform a function.

Further definitions are also included in the proposed risk classification scheme presented in Sect. 2.3.

1.2. Scope and Boundary

It should be recognised that safety is not aimed at achieving zero accidents, zero hazards or zero errors. The real target is to provide mitigating actions to prevent undesirable situations escalating. There is a lot of common ground between safety and reliability methods, as well as shared foundations. A safe functional system is more likely, if it is also reliable. There are numerous topics related to the scope of the STM S&R strategy, which can be broken down as below:

- Scenarios and operations
- Parties at risk
- Severity of risk
- Contributors
- Timing of risk management activities.

More details on these topics are given in the following subsections.

1.2.1. Scenarios and Operations

In the context of this study and further to the definition given in Paper I (Tüllmann et al. 2017a), the understanding of STM for S&R risk consideration is mainly related to Traffic Management of Suborbital Space Vehicles (SSVs) or spaceplanes[1] in airspace and space as well as to space objects re-entering airspace in a controlled and uncontrolled way. The S&R scope applies to a system and according to the definition of a system, this includes any combination of equipment (HW & SW), procedures as well as the supporting human resources and organisations. Best practices and experience related to safety indicate that the scope of S&R work cannot be too broad.

1.2.2. Parties at risk

The top-level goal of the safety strategy is to minimise injuries and, worst-case, fatalities to people, to an ALARP-level. It is assumed that, at least initially, SSV/spaceplane passengers will not be considered 'general public', rather they will be well-informed individuals with a status similar to crew members. This is important for S&R, because a relatively high level of risk will need to be accepted until the industry matures and higher levels of reliability become practical.

However, the suborbital flights shall also comply with the acceptable level of risk to third parties, i.e. the general public (e.g. passengers in an Airbus A320 and people on the ground). This additional requirement is stricter due to the perceived level of safety of the general public. The people at risk should therefore be grouped as follows:

- SSV and spaceplane occupants:
  - Passengers
  - Crew
- Third Parties:
  - Fellow airspace users
  - General public on the ground.

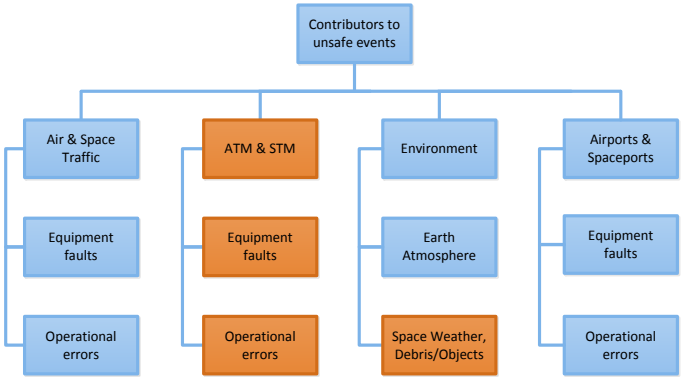

Figure 1: Contributing groups to unsafe events.

1.2.3. Severity of Risk

S&R work extends across the full-scale of severity, from a loss of life to no immediate S&R effect and everything in-between. In this context, S&R can and should be utilised to (i) demonstrate an ALoS so that flights can take place and (ii) systems have been optimised. RCSs are discussed further in Sects. 1.4.3 and 2.3. They incorporate the following severity aspects:

- Catastrophic (e.g. loss of life, loss of space vehicle)
- Hazardous (e.g. loss of significant system, emergency procedure invoked)
- Major (e.g. partial loss of significant system, abnormal procedure invoked)
- Minor (e.g. degraded system performance, increased workload)
- Insignificant (e.g. no immediate effect on safety).

1.2.4. Contributors

When considering risks related to STM, it is important to understand where they fit in the complete safety picture. Figure 1 summarises all the different groups of contributors and highlights the STM part as the boundary of the S&R work for this concept (see orange boxes).

1.2.5. Timing of Risk Management Activities

Risk management activities can be conducted during different time frames, depending on two general risk categories. The first

[1] We assume that the only difference between SSVs and spaceplanes is that the former are used for simple vertical ballistic flights up to altitudes of ~100 km (e.g., for space joyriders) and that the latter are deployed on complex suborbital ballistic point-to-point (p2p) flights (e.g., for passenger or cargo transportation (cf. Paper I, Tüllmann et al. 2017a).

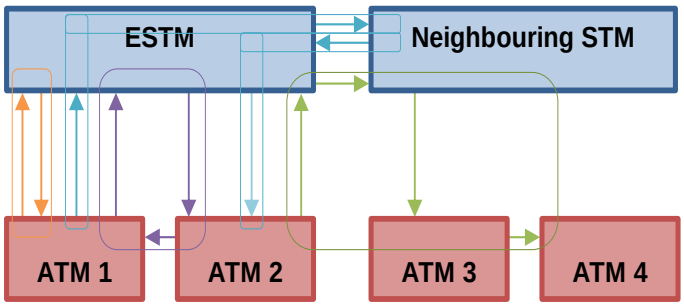

Figure 2: Example flight routes shown for a European STM (ESTM) with different numbers of interfaces. Among them, the turquoise-coloured scenario is the most complex one, requiring multiple handovers between different ATM and STM blocks.

one is related to steady-state risks which are assessed and managed as part of a certification process for equipment types and operators (which is the typical approach in aviation) while the second one is related to mission-specific risks. These risks are assessed and managed prior to each flight in order to achieve the "GO" decision (typical approach for space missions, e.g., when waiting for Space Weather or space debris clearance). As the STM develops and matures, it is anticipated that mission-specific risk activities will migrate to the steady-state phase. However, this can only occur if supported by S&R activities demonstrating that an ALoS is maintained.

1.3. Interfaces

Regarding S&R, interfaces are generally a weak-point in any system. The SES initiative (see the ATM Master Plan 2015) is one example to highlight this importance and which STM can learn from. Interfaces whether internal to the STM or external (see Figure 2) should be identified and minimised.

1.4. Candidate S&R Knowledge-Transfer from Aviation

The current development status of the commercial suborbital space travel industry can be compared to the very early days of aviation. However, one fundamental difference is that we now have lots of experience and proven, good-practices in the art of flying and ATM. Therefore, particularly from a S&R aspect, the commercial space industry as a whole must take advantage of the lessons learned over the decades of aviation and read-across today's best practices. The areas related to S&R in the context of traffic management, a potential STM system could benefit from, have been summarised in the following sub-sections.

1.4.1. Safety Management Systems in Aviation

Safety Management Systems (SMS) are a regulatory requirement for certified aviation operations, like airlines and Air Navigation Service Provider (ANSPs). They were introduced to address the concern that a system is designed to an acceptable level of performance at the start of operations, however, if unchecked, the performance level will gradually reduce and potentially, in the worst-case, lead to an accident. ICAO have published a dedicated annex to the Convention on International Civil Aviation for Safety Management (ICAO 2013a), in which it defines a SMS as: "A systematic approach to managing safety, including the necessary organisational structures, accountabilities, policies and procedures". A Safety Management Manual (ICAO 2013b) has also been produced by ICAO which provides in-depth guidance to the implementation and oversight of safety management.

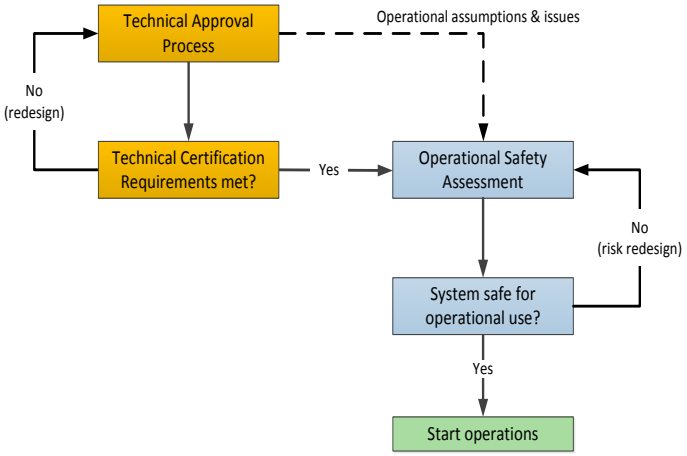

Figure 3: Overview of the safety process for aviation operations.

The framework of a generic SMS is also covering safety policy and objectives (including management commitment and responsibility and safety accountabilities), safety risk management, safety assurance (including safety performance monitoring, change management and continuous improvement of the SMS) and safety promotion (i.e. training and communication).

1.4.2. S&R Assessment Process in Aviation

In Figure 3 the framework of the safety process between equipment (technical) and operational aspects of an aviation functional system is outlined. At this high level, it is possible to apply the process to a STM functional system (see also Sect. 2.8). It is also recommended to integrate as far as possible the S&R effort on the equipment side and the operational side. This is especially relevant if the equipment is being developed concurrently with the operation and in which case iteration loops between the S&R assessments would also make sense.

A key aspect of the S&R assessment is the demonstration that the SW and complex electronic HW have been developed to a sufficient level of robustness. In aviation, there are development standards that are acceptable means of compliance for certification requirements. These include DO-178C (RTCA & EUROCAE 2011a) and DO-254 (RTCA & EUROCAE 2000) for airborne software and electronic hardware, respectively, plus ED-153 (EUROCAE 2009) and DO-278A (RTCA & EUROCAE 2011b) for ANS and CNS/ATM software, respectively

1.4.3. Aviation Safety Risk Classification Schemes

A Risk Classification Scheme forms a fundamental part of any risk management process, and STM and ATM is no exception. Although the details may vary, the basic steps taken to define the required mitigation actions are the same (see Figure4). For ATM a RCS has been produced by Eurocontrol in one of their safety regulatory requirements, ESARR 4 (Eurocontrol 2011), supported by substantial guidance, including a review of other aviation schemes (Eurocontrol 2000). As shown in the next section, the safety RCS also plays a fundamental part in the classification of occurrences during the service life of a functional system.

Figure 4: Generic steps in classifying a risk.

1.4.4. Occurrence Reporting in Aviation

In aviation, regulations exist that specify what occurrence details must be reported to the national supervisory authorities (EU No. 376/2014 and 2015/1018). Collecting data regarding occurrences can play a significant role in improving the S&R of the STM as a whole. This includes all levels of severity because an occurrence could be classified as minor or insignificant on its own, however, as part of a large group of other minor occurrences, it could be a concern – known as an "emerging" property of the system.

If analysed intelligently, occurrence data can allow actions to be taken to mitigate risks before they lead to an accident. However, this is reliant on having sound inputs (i.e. the occurrence details) which are complete and consistent irrespective from which organisation in which country the data originates from. It is also reliant on efficient methods of reporting and communicating and data handling and processing. To help with this in aviation, Eurocontrol has developed a tool called TOKAI (Toolkit for ATM Occurrence Investigation, Eurocontrol 2016a)), which includes a Risk Analysis Tool so a common classification is achieved (Eurocontrol 2015), as well as a process requirement document, ESARR 2 (Eurocontrol 2009).

1.4.5. Top Safety Risks in Aviation

In civil aerospace, accidents can be broken down into the following basic types:

- Collision between moving aircraft (flight or ground)
- Collision between aircraft and ground
- Impact with other avoidable airborne objects (e.g. missiles, drones, birds)
- Impact with other avoidable ground objects (i.e. physical structures)
- Loss of control from avoidable external influence, e.g.:
  - Extreme weather (wind shear, turbulence storms, lightning, etc.)
  - Wake vortex (jet wash, wingtip vortices).

Several aviation organisations have published what they see as the top priorities in safety, which are noteworthy insofar as they can be considered as a checklist to ensure they are taken into account in the S&R assessment of the STM concepts. This should be two-fold: (i) read-across risk to STM and, (ii) preventing unacceptable impacts on these sensitive areas in aviation from spaceplane traffic in shared airspace. For example, Eurocontrol's top five ATM operational safety priorities (Eurocontrol 2016b), based on a review of the two high-risk categories 'runway incursions' and 'loss of separation en-route', are as follows:

- Operations without/with failed transponder
- Landing without clearance
- Detectability of occupied runway
- Detectability of loss of separation (blind spot)
- Loss of separation across adjacent sectors.

1.4.6. Top Level S&R Requirements in Aviation

Aircraft system certification probability requirements for undesirable events which are linked to their severity, based on an accepted probability of 1 catastrophic accident every one million flying hours (1×10^{-6} flight hour^{-1}) due to any and all potential contributors (EASA 2014). With each step down to a lower severity classification, the accepted probability is increased by two orders of magnitude. This is essentially applying to the people on the aircraft. It also protects against the people on the ground inasmuch as a large object falling off an aircraft or the aircraft itself crashing onto the ground is classified as catastrophic. Therefore, it has to be demonstrated by design that this is so unlikely, it is not expected to occur.

Eurocontrol has derived a maximum tolerable probability for an catastrophic accident of 1.55×10^{-8} flight hour^{-1}, due to ATM contributors (Eurocontrol 2011). However, this refers to an overall safety performance of ATM at national level and still needs to be decomposed into the constituent parts of the ATM system (and, if necessary, per phase of flight and/or per accident type) before it can be applied to the classification of individual hazards or consequences. Quantitative requirements for the lower severity classifications have not yet been specified, due to insufficient data regarding the current level of ATM performance.

From the point of view of the STM concept, these figures are linked with the third party risk (see Sect. 2.4.2). They also indicate the difficulty in setting quantitative requirements.

1.5. Existing Organisations and STM-related Roles

Space-related activities in the fields of S&R are being carried out by a number of organisations. The following is a selected summary from Europe and the USA, including their current role in relation to the development of a STM system. It is by no means a comprehensive list and is intended to serve as an indication of the multiple efforts currently ongoing.

- ESA (European Space Agency)
  - Product Assurance and Flight Safety are part of ESA's main activities
  - Strategy and harmonisation of space development activities is led by ESA
    - E.g., European Technology Harmonisation Process
  - Standardisation (see ECSS entry below)
  - Numerous technical papers
    - E.g. assessment of break-up severity on operational satellites (Letizia et al. 2016)
- ECSS (European Cooperation for Space Standardization)
  - The ECSS, steered by ESA and supported by national space agencies, have produced a suite of standards in four branches:
    - Project management – including risk management
    - Product assurance – including safety
    - Engineering – including ground systems and operations

    - Sustainability – including space debris and SSA
- FAA/AST (FAA/Office of Commercial Space Transportation)
  - Regulates US commercial space transportation
  - Issues FAA licenses for commercial launches of orbital and sub-orbital rockets
    - Including safety approval (see FAA-AST 2012)
  - Issues licenses for commercial spaceports
  - Produces and commissions reports and studies, including for example:
    - Flight Safety Analysis Handbook (FAA-AST 2011)
    - Re-entry Hazard Analysis Handbook (Tooley et al. 2005)
    - Space Vehicle Operations Debris Threat Mitigation Study (Johnson et al. 2016)
    - Space Transportation ConOps Annex for NextGen (see FAA-AST 2008)
  - Includes the COMSTAC (Commercial Space Transportation Advisory Committee)
    - Provides information, advice and recommendations to FAA via working groups, e.g. international space policy, legal, operations, standards
    - Members from industry, government, academia and associations
  - Chapter 13 of FAA's System Safety Handbook "The Application of System Safety to the Commercial Launch Industry" (FAA 2000), includes an outline of the licensing, the system safety engineering and software assurance processes
- NASA (National Aeronautics and Space Administration)
  - Research and development agency of the US government
  - NASA's main aims include the development of commercial spaceflight capabilities and research in aeronautics
  - Includes the Aerospace Safety Advisory Panel
    - Evaluates NASA safety performance and provides improvement advice
  - Created the Columbia Accident Investigation Board
    - Instigated a lot of work regarding risk to airspace users and public on the ground from re-entry events
- IAASS (International Association for the Advancement of Space Safety)
  - A non-profit organisation dedicated to furthering international cooperation and scientific advancement in the field of space systems safety
  - Incorporated several technical committees, broken down as follows:
    - Launch and Re-entry Safety
    - Space Hazards
    - Commercial Human Spaceflight Safety
    - Human Factors & Performance for Safety
    - Space Safety Laws & Regulations
  - Conferences are held about every 18 months, proceedings (e.g., Sgobba & Rongier 2014) include topics like:
    - Small debris fragment contribution to collision probability for spacecraft in LEO
    - Demonstrator for Space-Based Space Surveillance
    - Operational Feedback regarding Collision Risk Avoidance at Launch in Europe
    - Lessons learned in Aviation Safety
  - Other topics include Public Risk Criteria and Rationale for Commercial Launch and Re-entry (Wilde 2011)
  - Standards and guidelines are also produced, for example:
    - Space Safety Standard – Commercial Human-Rated System (IAASS ISSB 2010)
    - Safety Design and Operation of Suborbital Vehicles Guidelines (IAASS 2010), including a section on the integration of suborbital space flights into ATM and a list of accident types and significant events based on a similar list from ICAO
  - IAASS is also leading the development of a tool called ADMIRE (Aviation – Debris & Meteorites Integrated Risk Evaluation) to assess risks to aviation due to re-entering space debris and meteorites (Emanuelli 2014)
- ASTM International
  - American-based organisation that enables industry, academia, regulators, etc. around the globe to come together and produce standards and recommended practices
  - At the time of writing, a new committee is being formed to develop and maintain voluntary consensus standards and recommended practices for the commercial spaceflight industry. The scope includes design, manufacturing and operational use of vehicles used for human and unmanned spaceflight.
- RCC (Range Commanders Council)
  - Provides technical and operational support to U.S. test, training and operational ranges. Members are different branches of the US military and NASA.
  - The scope of their work and standards/guidelines produced includes the management of risk related to rocket launches.

2. Recommended S&R Objectives for the STM

This section summarises the proposed objectives related to S&R in order to support certifiable STM operations. Although mainly a qualitative approach, quantitative proposals have been made wherever they can be substantiated with a valid rationale and/or assumption. The different categories covered have been broken down as follows:

1) Regulations and Standards
2) Overall S&R Approach
3) Safety Risk Classification Scheme
4) Acceptable Level of Safety
5) Critical Qualitative S&R Requirements
6) Addressing the Key Hazards.
7) Occurrence Reporting.

2.1. Regulations and Standards

The following aspects originate from the S&R considerations due to the close link with certification and standards. However, they can be applied to the complete regulatory and standards landscape. Regulation should be technology-neutral and enable industry to generate technical solutions and propose any necessary standards. Requirements and standards should be applicable to all space operations in Europe, i.e. not just to products from European manufacturers.

A European organisation should be selected to lead the European effort to select and update existing standards and/or develop new ones, including Minimum Operational Performance Standards (MOPS). This work should be in coordination with a European Standards Organisation (CENELEC, CEN, ETSI), to aid incorporation within legislation and with other industry standard bodies outside of Europe, to ensure a harmonised approach. The ECSS could be a good option for this, supported by experts

and organisations with experience in ATM standards. Compatibility and harmonisation with standards applicable to aviation should be ensured where necessary and where beneficial. This work should also include the selection and publication of a single set of terms and definitions.

ESA should establish and chair a forum to enable regulatory activities to be progressed. This forum should include representatives from the relevant parties, such as national space agencies, national aviation authorities, ECSS, EASA and Eurocontrol, as well as representatives and/or input from industry experts, such as potential Space Navigation Service Providers (SNSPs), ANSPs, ground equipment and vehicle manufacturers, airport and airline operators. A communication and data-sharing link with similar forums outside of Europe should also be established to support the global harmonisation. Similarly, a harmonisation programme should be established with the European aviation equivalent forum.

Finally, because we are at the beginning of this development, a great opportunity currently exists for developing the regulatory framework for the holistic system (STM, SSV/spaceplane and spaceport systems). This is particularly attractive for S&R activities and maximising their benefit for the industry as a whole. With the inclusion of all potential contributors to causing and preventing an accident within the regulatory and standards scope (cf Sect. 1.2.4), the optimum and most efficient solution for the future space transportation industry can be realised. As Sect. 1.5 indicates, there is already no shortage of good information available, indeed consolidation and harmonisation are seen as key steps to be taken regarding regulation and standardisation.

2.2. Overall S&R Approach

2.2.1. S&R Enabling STM Development

From an early stage, the benefits of smart S&R assessments should be promoted. A potential conflict of interest can often be perceived between S&R and efficiency of a functional system. However, besides demonstrating compliance with requirements and minimising risks, joint safety and reliability activities can also benefit the efficiency of a service operation. If started at the right time and conducted intelligently, S&R work can be exploited to justify the presence of all the elements of the functional system, in other words to show that the system is not overcomplex.

In order to support a successful development of the STM and the industry in general, S&R needs to be able to demonstrate that an ALoS is achieved, no matter what the traffic management concept and technology capability. Regarding SSV and spaceplane traffic for example, a move from today's segregation approach of space vehicle and aircraft towards more and more integration (see also Figure 18 in Paper I (Tüllmann et al. 2017a)), until airspace is only closed to other traffic in the event of a space vehicle failure, requires more than technological and operational innovations. It also requires those innovations to have a predicted reliability that enables an ALoS to be demonstrated.

It is assumed that commercial space transportation could become similar to today's air transportation with many flights on a daily basis and considered "normal" by a large portion of the general public. During the development of the STM system, each concept of operations produced should be supported by S&R activities, including a generic safety case and supporting assessments. The S&R techniques should be exploited to assess any options that may arise and aid the decision-making process. This would also include to consider the number and complexity of needed interfaces.

2.2.2. Multi-Directional Approaches

In order to support the STM development, top-level S&R requirements (quantitative and qualitative) need to be defined and accepted (e.g. risk classification, maximum probabilities of occurrence, processes). This is the start of the "top-down" approach. Once the top level requirements have been defined, it will be further required to decompose the requirements for different functional systems and parts within. Then, as part of the development of a functional system including its operations, S&R assessments will be conducted with the overall aim of demonstrating that compliance with the relevant requirements has been achieved. This is the "bottom-up" approach.

The S&R assessments of a functional system should also be split into two broad categories, both of which should contribute to the overall safety case of a functional system:

- Predict the combination of failures/event that could lead to each risk scenario:
  - To be used in the S&R assessment of equipment
  - Recognising that it is impossible to confidently predict all combinations in today's complex systems
  - Lends itself well to the quantitative assessment of random failures
  - To be supported by assurance processes which help demonstrate qualitatively that certain aspects of the system (e.g. software) are as robust as practical
- Implement independent lines of defence against the risk scenarios:
  - To be used in the S&R assessment of operations
  - Lends itself well to a qualitative assessment of the robustness of the complete functional system.

A third S&R area where the activities are broken down into two general classes is related to the timing of the assessments between (i) steady-state and (ii) mission-specific risks (cf. Sect. 1.2.5). Which S&R activities should be carried out when, needs to be agreed and published as part of the overall S&R guidelines for STM activities. It should be periodically reviewed in order to not only maintain its validity, but also to ensure it reflects the most efficient approach.

2.2.3. Safety Management System

Further to Sect. 1.4.1, the requirement for a SMS should be part of the regulations for STM service providers, supported by suitable guidance on acceptable means of compliance. Ideally, this would re-use current publications (perhaps with an update, if necessary). To this end, the existing ICAO documentation related to SMS (Annex 19, see ICAO 2013a) and the Safety Management Manual (ICAO 2013b)) should be reviewed together with the ECSS safety standard (ECSS 2009a) for suitability to STM service providers and supervisory authorities. In addition, the principal ATM EU regulations are in the process of a significant update (EU 2016) and this, together with the associated guidance material from EASA should also be part of the study.

2.2.4. S&R Techniques

There are many well-proven and accepted S&R techniques used today in all safety-critical domains, for example: Goal Structuring Notation, Fault Tree Analysis, Failure Modes, Effects and

Table 1: Safety Risk Probability Index

SRP class	Title	Quantitative Definition	Description
A	Frequent	TBD – see Sects. 1.4.6 and 2.4	Extremely likely to occur (and/or has occurred frequently)
B	Probable		Expected to occur several times (and/or has occurred infrequently)
C	Remote		May occur, but not often (and/or has occurred very infrequently)
D	Extremely Remote		Unlikely to occur, but still could at some time (and/or not known to have occurred)
E	Extremely Improbable		Not expected to occur. May only occur in exceptional cases (and not known to have occurred)

Table 2: Safety Risk Severity Index

SRS class	Title	Description of Potential Effect
1	Catastrophic	Loss of life or loss of a service user's product/object (e.g. spaceplane, aircraft). Extreme widespread environmental damage.
2	Hazardous	Complete loss of a significant system or results in the application of an emergency procedure (to prevent it from being a catastrophic risk) and/or a large reduction in safety margins. Severe environmental damage.
3	Major	Partial loss of a significant system or results in the application of an abnormal procedure (to prevent it from propagating to a hazardous risk) and/or a significant reduction in safety margins. Major environmental damage.
4	Minor	Degraded or affected normal operational procedures or performance, increased workload for operators (to prevent it from propagating to a major risk) and/or a slight reduction in safety margins. Minor environmental damage.
5	Insignificant	No safety effect. No environmental damage

Criticality Analysis, Common Cause Analysis, Human Error Assessment & Reduction Technique and Process Failure Modes and Effects Analysis. There are also many sources of guidance and explanations about the techniques available, for instance, in space and aviation:

- ECSS Space product assurance safety standard (ECSS 2009a), which includes references to more detailed guidance to for example, FTA, CCA, FMECA, Human Error
- Eurocontrol's Safety Assessment Methodology framework and toolbox
  - Including for example, a Safety Case Development Manual (Eurocontrol 2006)
- UK CAA Guidance on Safety Assessments (UK CAA 2010)
- FAA/Eurocontrol ATM Safety Techniques and Toolbox (FAA & Eurocontrol 2007)
- Eurocontrol Experimental Centre review of common techniques (Eurocontrol 2004)
- SAE guidelines & methods for civil aviation (SAE 1996).

As part of the guidance material for system developers in the STM system, recommended S&R techniques should be included. Ideally, this would reference to existing publications which could be used in the generic safety case (see Sect. 2.2.1).

2.3. Safety Risk Classification Scheme

A common Safety Risk Classification Scheme should be agreed and published, together with supporting guidance on its use. This scheme should then be used by service providers for (a) classifying risks, (b) determining probability objectives for their hazards (see last paragraph in this section) and (c) assigning a severity to occurrences (see also Sect. 2.7). A common scheme is important for consistency throughout the different service providers. It should also be harmonised as far as practical with other schemes used in (i) STM outside of Europe, (ii) SSV and spaceplane certification, (iii) ATM and (iv) Operations of spaceports & airports.

Existing schemes used by organisations to demonstrate compliance with the ECSS Risk Management standard (ECSS 2008) and Eurocontrol's safety regulatory requirements, ESARR 4 (Eurocontrol 2011) should be used as the main references. A proposed scheme is contained in the following subsections and should be used as a starting point for discussions and development into a final scheme for publication.

The probability requirements for the undesirable events and hazard consequences identified in the S&R assessments can be determined from the Safety RCS based on their severity classification. If the severity of a hazard consequence is classified as "Catastrophic", the maximum probability requirement would be "Extremely Improbable". The same requirement for the hazard itself can then also be determined by taking account of the likelihood that the hazard leads to the consequence. The quantitative element of requirement will depend, at least initially, on the people at risk (cf. Sect. 1.2.2), however the remainder of the RCS should be suitable for all. In the following section we propose a RCS for STM purposes, reflecting the aforementioned considerations and requirements.

2.3.1. Safety Risk Probability

The Safety Risk Probability (SRP) is the likelihood of the hazard/risk consequences actually occurring. A proposed SRP index is presented in Table 1.

2.3.2. Safety Risk Severity

The Safety Risk Severity (SRS) considers the extent of harm to the functional system that might reasonably occur as a result of the hazard consequence (see also Sect. 1.2.3). In Table 2 the proposed SRS index is shown.

2.3.3. Safety Risk Level

The Safety Risk Level (SRL) is determined from a combination of Tables 1 and 2 regarding probability and severity. In the event that a hazard could lead to multiple potential scenarios with different combinations of SRP and SRS, the worst-case credible SRL should be allocated. An example SRL matrix is presented

Table 3: Example Aviation Safety Risk Level Index

	Safety Risk Severity (SRS)				
Safety Risk Probability (SRP)	5 Insignificant	4 Minor	3 Major	2 Hazardous	1 Catastrophic
A Frequent	Low (5A)	High (4A)	High (3A)	High (2A)	High (1A)
B Probable	Low (5B)	Medium (4B)	High (3B)	High (2B)	High (1B)
C Remote	Low (5C)	Low (4C)	Medium (3C)	High (2C)	High (1C)
D Extremely Remote	Low (5D)	Low (4D)	Low (3D)	Medium (2D)	High (1D)
E Extremely Improbable	Low (5E)	Low (4E)	Low (3E)	Low (2E)	Medium (1E)

Table 4: Safety Risk Tolerability Index

SRL	SRT	Type of Action Required
High	Intolerable	**WARNING** Ensure that risk assessment has been satisfactorily completed and declared mitigation means are in place to prevent propagation to identified hazard. If necessary, do not permit further operation until sufficient control measures have been implemented. As a minimum, SRL must be reduced to Medium.
Medium	Tolerable	**CAUTION** Perform risk mitigation as necessary based on an ALARP principle. Regularly review & monitor risk.
Low	Acceptable	**REVIEW** Risk mitigation is optional, based on an ALARP principle. Regularly review risk.

in Table 3. At least at the beginning more than one SRL matrix will be needed, because of the different risk levels for the different parties at risk (see Sect. 2.4), e.g. SRL 1D might be medium and therefore tolerable for spaceplane occupants, but not for third parties.

2.3.4. Safety Risk Tolerability

The Safety Risk Tolerability (SRT) is defined from the SRL and defines the action to be taken. Table 4 shows the proposed SRT index.

2.3.5. Initial SRL Indices for Space Weather

As an example of use of the previously introduced Risk Classification Scheme, we continue to classify the risks associated with unawareness of Space Weather events for Space Traffic operations as defined in the risk register of Paper I (see Table 4 in Tüllmann et al. 2017a). The results are provided in Table 5 and are based on the frequency of Space Weather events causing hazards and negative impacts on critical infrastructure or services for Space Traffic Control and Operations.

The meaning of the columns and parameters shown in Table 5 is as follows. Columns 1 – 3 list the Risk-ID, Risk title and provide a high-level description of the risks. In column 4, risk classifications are given that characterise the risks in terms of main impact on travel schedule (SC), performance (P), safety (S) and costs (C). The Safety Risk Severity (SRS) given in column 5, the Safety Risk Probability (SRP) in column 6 and the Safety Risk Level (SRL) in column 7 are derived from the Safety RCS discussed throughout Sects. 2.3.1 – 2.3.3. In the case a hazard leads to multiple potential scenarios with different combinations of SRPs and SRSs, the worst-case credible SRL is allocated. In this scheme values highlighted in red represent unacceptable risks for Space Traffic operations on customer and crew level (zone of avoidance) and require immediate mitigation measures.

2.4. Acceptable Level of Safety

Following on from the note in Sect. 2.3 and as part of the "top-down" approach, the following sub-sections propose a way-forward in order to determine the top-level S&R requirements that must be agreed and published. In line with the scope definition in Sect. 1.2.2 for the parties at risk, it is broken down to SSV/spaceplane occupants and third parties.

2.4.1. ALoS – SSV and Spaceplane Occupants

As stated in Sect. 1.2.2, a key assumption here is that the early SSV and spaceplane passengers are not considered to be general public in the same way today's air travellers are. In other words, a higher level of risk will be acceptable to them, which will support the development of the industry. The IAASS guidelines (IAASS 2010) have suggested a quantitative requirement for a catastrophic event as 1×10^{-4} flight^{-1}, assuming a suborbital mission is 1 hour flight in total. Due to the obvious lack of historical data and evidence, this has been derived from the ESA standard crew safety risk (ESA 2012) which states, that the probability of a catastrophic event during the entire mission shall not exceed 1×10^{-4} and pragmatically setting it in the middle of orbital spaceflight (shuttle) and civil aviation (see Sect. 1.4.6). However, this is again a budget for all potential contributors, as identified in Sect. 1.2.4. Therefore, a further study is required to decompose the requirement amongst the contributors.

The S&R assessment should also consider if the undesirable events, under consideration for their impact on SSV and spaceplane occupants, can also pose a risk to third parties. If so, it could mean a more stringent requirement must be applied. For example, if a catastrophic in-flight spaceplane break-up could collide with an aircraft, it would also have to meet the third party requirement (see also Sect. 2.6.4).

Table 5: Risk quantifications associated with unawareness of Space Weather events

Risk-ID	Risk Title	Description	Classification	SRS	SRP	SRL
R-STM-1	Power Outages	STM operation can be affected in case of power outages due to severe space storms	SC,P,C,S	2	D	2D
R-STM-2*)	Imprecise and safety-critical navigation	Due to spatial gradients and temporal variability of the plasma density in the ionosphere	SC,S,P,C	3	B	3B
R-STM-3	Augmentation systems	Performance degradation of space-based and ground based augmentation systems due to ionospheric gradients	SC,P,C,S	3	B	3B
R-STM-4	Radiation damage	Exposition of crew and passengers to harmful radiation (GCR and SCR)	P,C,S	3	B	3B
R-STM-5	Disruption of Communication	HF communications are used in remote regions (ocean, poles)	P,C,S	4	B	4B
R-STM-6	Damage of space infrastructure by radiation belt particles or SEPs	SEPs are highly variable and dangerous during high-intensity, large-fluence events and can affect space vehicles	P,C,S	3	B	3B

Notes. *)Imprecise and safety-critical navigation is not just a risk factor during take-off and landing. In case of space operations, suborbital p2p flights take place at altitudes between 100 km and 500 km, which is in the middle of the ionosphere. Therefore, simple 2D TEC models cannot be used to derive the correct range error information at these heights, as information on ionospheric thickness above and below the space vehicle is needed. In case of aviation performed at altitudes around 10 km, precise positioning during the flight might not be that important, because there is usually a sufficiently-sized safety margin between different airplanes. This is different for space operations carried out at 300 km altitudes, where precise positioning becomes very important due to the high risk of space debris impacts. Hence, not only the position of the space debris has to be known precisely, but also the exact position of the moving space vehicle. In order to mitigate GNSS inaccuracies induced by the ionosphere at these altitudes, the development of near real-time, data-driven and model-assisted 3D TEC reconstruction is required (see Table 4 in Paper I).

2.4.2. ALoS - Third Parties

The current accepted risk levels from aviation should be used as a basis for defining an ALoS to third parties in the air and on the ground. As a minimum requirement, spaceplanes and SSVs should not pose a greater risk to third parties in the air or on the ground than current aviation (see Sect. 1.4.6). Note, however, that there are differences between conventional aviation and space transportation which justify a lower target (Wilde 2011):

- How people respond to accidents
- Much longer return to service for space transportation in event of a third party casualty
- Aviation accidents cause less concern / outrage
- Very different accident rates
- Space transportation risk and complexity is inherently higher than in aviation
- Very different levels of maturity

Based on the above, the FAA has recently issued a final rule on an update to its risk limits for third parties (FAA 2016). The relevant regulatory requirements from the FAA include a detailed breakdown of probability requirements that must be met for launch and re-entry. For example, CFR Part 417 Launch Safety (§ 417.107 Flight Safety) includes the following requirements:

- Total risk to public (excluding ships and aircraft) shall not exceed 1×10^{-4} casualties
- Risk to an individual member of the public shall not exceed 1×10^{-6} per launch per hazard
- Risk of water-borne third-party casualty due to debris impact shall not exceed 1×10^{-5}
- Risk of an airborne third-party casualty due to debris impact shall not exceed 1×10^{-6}.

The process and rationale behind these regulations and requirements should be reviewed for applicability in Europe and read-across accordingly, bearing in mind the anticipated regular suborbital flights. As far as STM itself is concerned, these targets would also need to be broken down and shared accordingly with the potential contributors. These figures should also be considered in the context of re-entering objects in general (see Sect. 2.6.3).

2.5. Critical Qualitative S&R Requirements

In addition to the ALoS discussed in the previous sections, the following S&R qualitative requirements should be applied to the undesirable events classified with the severity stated:

- Any consequence classified as catastrophic shall not be caused by:
  - Any single failure
  - Any single failure combined with a dormant condition
  - Software errors alone
  - Operator errors alone
- Consequences classified as hazardous shall not be caused by:
  - Any single electronic failure
  - Any single electronic failure combined with a dormant condition
  - Software errors alone.

2.6. Addressing the Key Hazards

This section summarises the proposals for addressing the following key hazards in support of the development of a successful STM system:

1) Space Weather
2) Space debris/objects
3) Re-entering objects
4) Shared airspace.

2.6.1. Space Weather

As explained in Sect. 2.3.5 and to further detail in Sect. 3.6 of Paper I (Tüllmann et al. 2017a), Space Weather poses a risk to the STM systems and to human health. For designing a S&R concept for STM, the following general points which are relevant to Space Weather should be considered.

In support of the development of a Space Weather monitoring system, S&R requirements for the SWMC should be (i) defined and validated and (ii) verified. For example, reliability requirements for the detection and reporting of Space Weather events, shall be commensurate with the severity of the potential effects of a failure.

Furthermore, to be in a position to validate the S&R requirements for the Space Weather monitoring system, they should be developed and validated in conjunction with those on the areas listed below. Besides validation, this will also help to find the optimum solution for:

- Spaceplane and SSV radiation shielding (humans and electronics)
- STM equipment that can be impacted by Space Weather
- The Space Surveillance and Tracking system (because of the risk of positional inaccuracies in the ionosphere combined with the risk of collisions with space debris / objects)
- Structural protection of the spacecraft against collisions
- Applying credible avoidance actions in the event of a foreseen collision.

Validation of the S&R requirements will be a key proof-point for the industry development, because the types and frequencies of the Space Weather events cannot be altered plus there will be limitations on the available technology to lessen their impact. It is important to not only determine the risk exposure so the crew and passengers understand, but also to be able to demonstrate that the risk to fellow airspace users and third party people on the ground in the event of a spacecraft incident is acceptable.

2.6.1.1. Human Health Risk from Radiation

One risk from Space Weather that is hard to protect against at suborbital altitudes (but is predictable to some extent), stems from high energy particles and proton events, that can cause radiation damage to crew and passengers aboard the spacecraft. The effects of radiation exposure on human health can be broadly split between two categories, stochastic (random, probability of occurrence in a population is a function of dose, e.g. cancer, leukaemia, genetic changes) and non-stochastic (threshold effects the severity of which increases with dose (at a certain threshold, every individual will see these effects), e.g. radiation "sickness" or nausea, skin reddening, sterility and cataracts).

Radiation levels have been measured, for example a report commissioned by the US DoT “Space Weather Biological and System Effects for Suborbital flights” (Turner et al. 2008) states that the cosmic radiation at sea level is about $0.26\,\mathrm{mSv\,yr^{-1}}$, doubling with each 2 km altitude above sea level. It goes on to say that dose equivalent rates at typical cruising altitudes for commercial flights (8 000 m – 12 000 m) vary from $3-7\,\mu\mathrm{Sv\,h^{-1}}$. Therefore, a five hour flight would result in a total of $25\,\mu$Sv or 0.025 mSv, which is an order of magnitude below the annual exposure at sea level. The annual allowed dose-rate is 20 mSv.

Human health risk from radiation is also linked heavily with the design and technology of the spaceplanes and SSVs themselves. However, the STM should consider the modelling and monitoring of individuals' radiation levels in order to support the pre-flight planning and risk assessment, as well as measuring in support of maintaining exposure data. Flight data comparison with models will also allow for continuous model improvement. Criteria suggested to be monitored include:

- Total exposure duration
- Timing relative to event onset and peak
- Geomagnetic conditions
- Flight profile
- Shielding provided by vehicle
- History of radiation exposure of involved person.

Owing to the expected short duration of flights and the even shorter exposure at altitudes where atmospheric shielding is significantly reduced, the exposure of crew and passengers is minimal, except under extreme circumstances. Under typical conditions, the radiation exposure to crew and passengers on a suborbital flight is less than that for a long duration airline flight. Avoiding exposure to potentially harmful radiation associated with solar or geophysical disturbances can be achieved by locating launch sites at middle latitudes, or lower, or by delaying flights when there are indications that a solar event is in progress or is imminent. For a high-latitude site, a possible launch commit criterion could be based on event probability distributions. Although the radiation risk for crew and passengers is minimal, except as noted, crew and passengers should be monitored for radiation exposure because of the potential for litigation and the possibility, however remote, that the onset of an event such as an unanticipated Solar proton storm could occur during flight. Passengers should also be briefed on the radiation risks in the spirit of informed consent.

2.6.2. Space Debris and Space Objects

The risk from the hazard of objects in space covered in this section is that of a collision with the spaceplane (hazard from object re-entry is covered in the next section). The subject of space debris and space objects is covered in detail in Sect. 3.4 of Paper I. The related salient S&R aspects are captured in this section.

Objects in space are either traceable or non-traceable, with the latter largely outnumbering the former. It is assumed that non-traceable objects will remain in the majority for the foreseeable future. This means, that the S&R approach for evaluating the collision risks must be two-fold. Risk quantifications for traceable objects need to be based on planned flight trajectories and the spacecraft's structural survivability. These risks require a continual assessment throughout the mission, whereas risks for the non-traceable object population need to be based on best statistical information available.

In order to minimise collision risks with traceable objects, the trajectory of both the spaceplane and the objects should be as accurate as practical. Also, since the density of objects varies with both altitude and latitude, the route of each spaceplane mission must be selected based on known risks. Note, that this is also a key input to any assessment on route efficiency when it comes to the implementation of environmental and Clean Space aspects.

To minimise the severity of an impact, the spaceplanes's structural survivability and design should be as robust as practical. In order to determine the hazard severity thresholds for collisions between spaceplanes and space objects, further research into the potential impact effects needs to be carried out. Particular collision-based risk assessments in aviation (e.g. birdstrike, engine/tyre debris impact) should be reviewed to take advantage of transferable experience, methodology and capability. The findings from EASA's “Drone Collision” Task Force

Table 6: Shielding capability versus maximum cross section of the spacecraft)

Shielding capability (debris size in mm)	**Maximum cross-section** (m^2)
1	10
5	100
10	1 000

(EASA 2016) and their future work may also provide opportunity for knowledge-transfer in both directions as the threat potential posed by drones also exists at and in the vicinity of spaceports.

In Sects. 3.4.1 and 3.5 of Paper I, an example p2p flight trajectory has been analysed to see how close the spaceplane would come to traceable objects (approximate size range of 10 cm and above) and a rough order of magnitude estimate on the collision risk with non-traceable objects has been provided. Even if we assume a shielding capability of around 1cm (which is deemed technically very challenging) and that the U.S. will soon expand their Space Surveillance and Tracking Network to detect objects with diameters of >3 cm, there is still a significant gap between the traceable object size and shielding capability. The collision risk has been examined with respect to the spaceplane's cross-sectional area, inclination and latitude of the flight path and the time spent at each attitude (since space object density varies with latitude and orbital altitude). The probability for a non-traceable object greater than 0.1 cm colliding with the space vessel has been estimated to be in the order of 1×10^{-7} per flight per square metre of SSV cross-sectional area. Similarly, for objects greater than 0.5 cm and 1 cm, the order was estimated to be 1×10^{-8} and 1×10^{-9}, respectively (see Table 1 in Paper I (Tüllmann et al. 2017a)).

If we assume an overall catastrophic (loss of life and/or loss of spaceplane, cf. Table 2) ALoS of 1×10^{-4} per flight and that there are 100 potentially catastrophic scenarios for the spacecraft and/or its occupants which have an equal share of the budgeted requirement, then the maximum probability per flight of a catastrophic collision with space debris amounts to $1 \times 10^{-4}/100 = 1 \times 10^{-6}$. In Table 6 the maximum cross-section of a spaceplane is expressed in relation to its needed shielding capability, i.e. to withstand collisions with space debris particle sizes of 1 mm, 5 mm and 10 mm, respectively.

On this basis, suborbital flights with vessels having a cross section of 100 m^2 and 1 mm shielding capability would not be permitted to launch and require further analysis and substantial technology advancements. However, it is important to note, that these figures are provided to give an indication of the feasibility only and that the numerous supporting assumptions must be validated before any further conclusions can be drawn. In addition, the determination of the collision severity must consider the complete mission (e.g. catastrophic effect may not be realised until re-entry) and S&R requirements for more frequent/less severe collisions with debris have to be assessed in order to determine the full set of requirements (including impacts on spacecraft and minimising the creation of more debris).

Furthermore, in order for the spaceplane/SSV industry to develop and become more like aviation today with common use by the general public, it is reasonable to assume that the ALoS for a catastrophic collision would have to be reduced by about three orders of magnitude to $\sim 1 \times 10^{-9}$ flight hour^{-1} (like aviation today). Finally, it is important to note the overriding principle, namely that mitigating against collisions with traceable objects (with known data) is better than mitigating against statistical modelling.

According to Sect. 3.5 in Paper I, the risk resulting from the gap between current shielding capabilities (0.1cm) and the expected traceable object size in the foreseeable future (3cm) is estimated to be in the range of $1 - 8 \times 10^{-3}$ flight^{-1} in terms of collision probability (depending on the assumed cross section of the spacecraft). Therefore, further studies are required to focus on closing the gap between shielding capability and traceable objects as far as practical and advance this risk analysis, as well as propose a recommended practice for operators to manage these risks. Such a study should, at least, take into account the following aspects:

- Technology development on heat and collision shielding to increase reliability of structural survivability of the vessel while simultaneously minimising cost and weight impacts
- Cost, reliability and accuracy of tracking space objects and space vehicles
- Speed of warnings from the Space Surveillance and Tracking network
- Efficiency and environmental impact of spaceplane routes
- Spaceplane controllability, e.g. regarding in-flight detection, collision avoidance performance and trajectory robustness (i.e. the ability to stick to the planned trajectory as closely as possible in normal operations and how it is affected by failure events).

2.6.3. Re-entering Objects

Space objects re-entering the Earth's atmosphere present a risk to airspace users, people on the ground and spaceplane launches. Currently, the risk has to be accepted and up to now, there has been no confirmed report of a casualty as a result of an object falling from space. There are many challenges regarding the tracking of re-entry objects, including the accuracy of any predicted trajectories and how and when the object may break-up. For example, it has been estimated that the probability of an aircraft being hit during the 40 min it took the debris from the Space Shuttle Columbia accident to fall to Earth was somewhere between 0.3 and 0.003 (Emanuelli 2014), i.e. considerably higher than the acceptable risks for third parties stated in Sect. 2.4.2. Another example is the re-entry of the ROSAT X-ray satellite, for which DLR calculated a probability of 1 in 580 that debris would fall on to German territory and 1 in 700 000 that someone could be harmed (DLR 2011).

An increase in the number of re-entering objects, an increase in the density of air traffic and an increase in the general public population could all impact the level of risk. A key S&R assumption is that, at some point in time, it will not be acceptable to accept the risk of a casualty from re-entering objects. This means that the risk must be quantified for today, as well as predicted for the future, to allow states and ATM organisations to know and understand the probability that an object could hit an aircraft in their airspace or a member of public. This will also support decision-making regarding ESA's Clean Space initiatives in the E.Deorbit branch, which are considered to be a qualitative improvement in the risk due to the move from uncontrolled to controlled re-entries. This can then support wider studies (including available technology, financial and environmental impacts, etc.) to investigate, for example, the required tracking accuracy and mitigation actions to be taken. Such studies should obviously involve the relevant representatives from both space and aviation industries.

The risk and mitigation options surrounding re-entering objects are the subject of many studies around the world. In addition to Sect. 3.4.1 of Paper I, for example, IAASS is developing ADMIRE (Aviation Debris & Meteorites Integrated Risk Evaluation), a tool to evaluate risks to aviation from single events, annually and in real-time (Emanuelli 2014) while the FAA has recently published study results on mitigating the debris threat (Johnson et al. 2016).

Currently, the overall risk from re-entering objects has not been quantified with sufficient logic and substantiation. Therefore, a study to produce a global map of the risk from re-entering objects to aviation and the general public should review the current findings and status of conducted and ongoing work.

2.6.4. Shared Airspace

The hazard of spaceplanes sharing airspace with other aircraft poses a risk of collision between spacecraft (or parts of it) and aircraft. Currently, this is mitigated by segregation. However it is assumed that this will not always be acceptable due to the economic and environmental impact, especially considering the predicted growth in both space and aircraft traffic (see also Figure 18 in Paper I). Therefore, S&R investigative work is needed to support this development and allow an equivalent level of safety (ELoS) to be demonstrated for each degree of integration.

It should be assumed that a collision between spaceplane and aircraft would result in an accident with both vehicles lost and multiple fatalities from both. Even if a higher ALoS is agreed for spaceplane/SSV occupants, the ALoS for the aircraft occupants (as third parties) cannot be altered from what it is today and therefore drives the top level S&R requirement. This approach would also satisfy ALoS requirements for third parties on the ground.

Therefore, using the Safety RCS as proposed in Sect. 2.3, a collision between a spaceplane and an aircraft is classified as catastrophic (see Table 2). This means the safety objective shall be extremely improbable (as defined in Table 1) in order to achieve a tolerable level of risk (see Tables 3 and 4). With the classification of catastrophic, the additional requirements stated in Sect. 2.5 shall also apply. This would be in line with the ALoS third party requirements proposed in Sect. 2.4.2 (referring back also to Sect. 1.4.5). If this level of safety cannot be demonstrated, then the degree of integration cannot be increased from the level accepted at that time. Note that this must also take into account contingencies in the event of spaceplane or SSV break-ups.

In support of achieving the above, the spacecraft must essentially interface with ATM in the same way as aircraft, follow the same rules of the air (e.g. ICAO Annex 2) and be equipped with systems and technologies that achieve (at least) the same level of performance within the ATM network as the aircraft. The Air Traffic Control Operator (ATCO) must also be fully aware and understand the minimum, guaranteed performance capabilities of each type of spaceplane and SSV (see Chapter 3.7 in Paper I).

2.7. Occurrence Reporting

Due to the potential gains in system performance and S&R, as summarised in Sect. 1.4.4, the requirement to report occurrences and what data must be provided should be determined and included the relevant STM regulations (see, e.g., EU regulations 376/2014 and the associated implementing regulation 2015/1018).

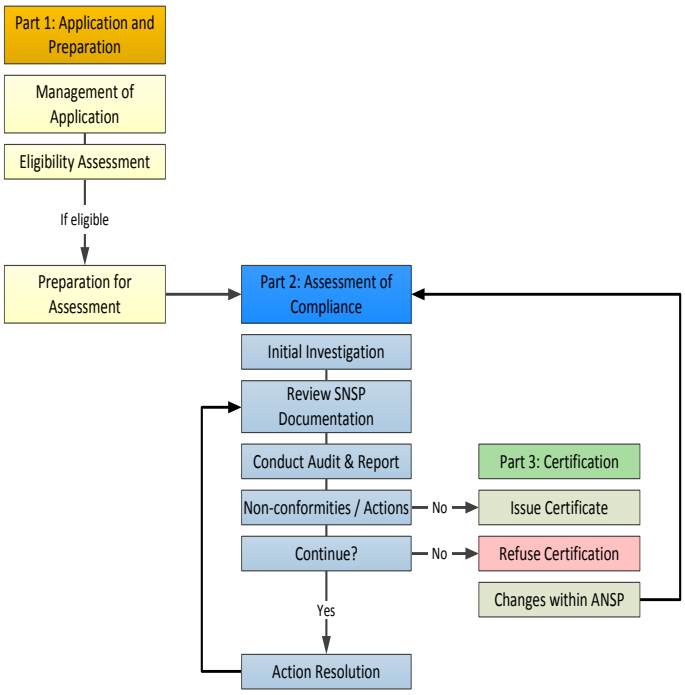

Figure 5: ANSP Certification Process Outline.

In support of this, it is important to promote the value of an open and just culture in organisations. Realising the potential benefits of wide-ranging occurrence data will rely on the people who are providing STM services delivering data that is accurate and complete. As mentioned in Sect. 2.3, occurrences should be classified in accordance with the agreed safety RCS. In this respect, it is fundamental to have a common scheme that all organisations should use in order to ensure a consistent classification. This will support data analysis at a European level, which in turn supports the identification of (i) accident pre-cursors and (ii) emerging S&R concerns, as well as validates the safety risk assessments and quantitative requirements (see Sec 1.4.6). It should also be investigated whether it is practical to set up a shared database with organisations outside of Europe.

An electronic reporting tool that can be accessed by the relevant organisations should be developed to facilitate the reporting, collection and storage of the numerous occurrences. This will ensure the most efficient communication process between organisations and authorities. An investigation on the applicability of Eurocontrol's TOKAI tool (Eurocontrol 2016a) should be conducted.

2.8. Space Navigation Service Provider Certification

Organisations that provide a service within the STM system should be certified as a Space Navigation Service Provider (SNSP). The process for certifying a SNSP should be based on today's aviation approach for an Air Navigation Service Provider (ANSP). Figure 5 outlines a proposal for the SNSP certification process, based on Eurocontrol's guidelines for National Supervisory Authorities (NSAs) for ANSP (Eurocontrol 2012).

This would be one part of the approval process for all actors within the industry which ensures that all the following are certified:

- Spaceports and spaceport operators

- Spaceplane and SSV types and the design and manufacturing organisations
- SNSP and the STM equipment.

Further to some general principles proposed on regulations in Sect. 2.1, regulatory requirements should obviously be defined, as a certification basis, to give the supervisory authority something to audit the SNSP candidate against. For ANSPs, the EU regulation 1035/2011 is currently the main basis. However, this is planned to be replaced in the next two years by a new regulation, together with substantial guidance material (EU 2016).

This suite of certification requirements and guidance, together with the interoperability experience of ATM (e.g. EU regulation 552/2004) and its compliance means, should be reviewed for reading across to STM. The advantages of commonality and harmonisation between the certification of SNSP and ANSP are two-fold, first to exploit the knowledge and experience of service providers and supervisory authorities and second, to maximise the potential for integrating spaceplane traffic into air traffic.

As part of this study is also dedicated to examine a potential SNSP certification process, the following space-related licensing should be considered. For example, the FAA process for licensing commercial launches includes: pre-licensing consultation, policy review, payload review, safety evaluation, financial responsibility determination, and an environmental review (FAA 2000).

The S&R assessment process (outlined in Sect. 1.4.2) should be part of the certification process, including the software and complex electronic hardware assurance. Therefore, as part of the definition of the certification process, the acceptable means of compliance for software and electronic hardware should be specified and based on existing publications where possible. In addition to the aviation guidance stated in Sect. 1.4.2, the ECSS standards and handbooks related to this topic should be considered (e.g. requirements for the development and maintenance of software in spacecraft, launchers, payloads, experiments and ground equipment and facilities (ECSS 2009b)).

3. Technical Requirements

A set of initial high-level requirements has been drafted, covering technical and operational aspects and constraints an integrated European STM system should reflect, such as Safety and Reliability, Space Weather or Space Surveillance and Tracking. In addition, a high-level breakdown of possible operational and organisational interfaces in the global context is also presented. All this information is summarised in Paper III (Tüllmann et al. 2017c). It is explicitly stated that Paper III does not intend to provide a complete set of detailed requirements. Instead the proposed requirements and interfaces presented in that work are meant to provide a first rough guidance and stimulate discussions on how a European STM system could be realised.

Acknowledgements. This work was funded by the European Space Agency through Contract No. 4000117403/16/F/MOS. The view expressed in this publication can in no way be taken to reflect the official opinion of the European Space Agency.

References

EU & Eurocontrol: The Roadmap for Delivering High Performing for Aviation for Europe, European ATM Master Plan, 2015, https://www.atmmasterplan.eu/downloads/202

DLR: ROSAT Mission Reentry, http://www.dlr.de/dlr/desktopdefault.aspx/tabid-10432/620_read-830/#/gallery/1692, 2011

EASA: Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes. CS-25 Amendment 15, 21 July 2014

EASA: "Drone Collision" Task Force Final Report, Oct 2016

ECSS: Space Project Management: Risk Management, ECSS-M-ST-80C, July 2008

ECSS: Space product assurance: Safety, ECSS-Q-ST-40C, March 2009a

ECSS: Space product assurance: Software product assurance, ECSS-Q-ST-80C, March 2009b

Emanuelli, M., Space Debris and Meteorite Forecast for Safer Aviation, in the Space Safety Magazine Special Report: Losing Aircraft in the Space Age, 2014

ESA: System Safety Engineering; Safety Technical Requirements for Human Rated Space Systems, section 5.2.1, ESSB-ST-Q-003-Issue 1, September 2012

EU Reg. 2016/1377: Common requirements for service providers and the oversight in air traffic management/air navigation services and other air traffic management network functions, August 2016

EUROCAE: ED-153: Guidelines for ANS Software Safety Assurance, August 2009

Eurocontrol: Safety Minima Study: Review of existing standards and practices, SRC DOC 1, December 2000

Eurocontrol: Safety Case Development Manual (Part IV, Annex I of Eurocontrol's ANS SAM), DAP/SSH/091, issue 2.2, 13 November 2006

Eurocontrol: Reporting and Assessment of Safety Occurrences in ATM, ESARR 2, edition 3.0, December 2009

Eurocontrol: ESARR 4 - Risk Assessment and Mitigation in ATM, ed. 1.0, 05 April 2011

Eurocontrol: Guidelines for NSAs for the Development of the ANSP Certification Process, Edition 3.0, April 2012

Eurocontrol: Risk Analysis Tool – RAT Guidance Material, edition 2, December 2015

Eurocontrol: TOKAI User Manual, edition 2.4, 2016a

Eurocontrol: Top 5 ATM operational safety studies now available, http://www.eurocontrol.int/news/top-5-atm-operational-safety-studies-now-available, 2016b

Eurocontrol Experimental Centre: Review of Techniques to Support the EATMP SAM, EEC Note No. 01/04 – Volumes I & II, January 2004

FAA: System Safety Handbook, chapter 13: The Application of System Safety to the Commercial Launch Industry, December 2000

FAA: Final Rule Changing the Collective Risk Limits for Launches and Reentries and Clarifying the Risk Limit Used To Establish Hazard Areas for Ships and Aircrafts, 14 CFR Parts 417, 420, 431 and 435, July 2016

FAA-AST: Space Transportation Concept of Operations Annex for NextGen, version 1.0, June 2008

FAA-AST: Flight Safety Analysis Handbook, version 1.0, Sept 2011

FAA-AST: SAFETY APPROVAL Guide for Applicants, version 1.1, July 2012

FAA/Eurocontrol: ATM Safety Techniques and Toolbox, version 2, October 2007

IAASS: Safety Design and Operation of Suborbital Vehicles Guidelines, Suborbital Safety Working Group Manual, October 2010

IAASS ISSB: Space Safety Standard – Commercial Human-Rated System, IAASS-ISSB-S-1700-Rev-B, March 2010

ICAO: Safety Management, Annex 19, 1st. edition, 2013a

ICAO: Safety Management Manual, Doc. 9859, 3rd. edition, 2013b

Johnson, D. R., Sollenberger, R. L., Schulz, K., Yuditsky, T., & Hatton, K., Space Vehicle Operations Debris Threat Mitigation Study, FAA DOT/FAA/TC-16/12, 2016

Letizia, F., Colombo, C. , Lewis, H.G., & Krag, H., Assessment of breakup severity on operational satellites, Advances in Space Research 58, 1255, 2016

RTCA/ EUROCAE: DO-254/ED-80: Design Assurance Guidance for Airborne Electronic Hardware, April 2000

RTCA/EUROCAE: DO-178C/ED-12C: Software Considerations in Airborne Systems and Equipment Certification, December 2011a

RTCA/ EUROCAE: DO-278A/ED-109: Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems, December 2011b

SAE: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, ARP 4761, December 1996

Sgobba, T., & Rongier, I. (Eds.): Space Safety is No Accident – Proceedings from the 7th IAASS Conference, Space Safety is No Accident, Springer, October 2014.

Tooley, J., Habiger, T. M. & Bohman, K. R., Reentry Hazard Analysis Handbook – Space Launch Operations, January 2005

Tüllmann, R. Arbinger, C., Baskcomb, S., Berdermann, J., Fiedler, H., Klock, E., & Schildknecht, T., On the Implementation of a European Space Traffic Management System II. A White Paper, Paper I, 2017a

Tüllmann, R. Arbinger, C., Baskcomb, S., Berdermann, J., Fiedler, H., Klock, E., & Schildknecht, T., On the Implementation of a European Space Traffic Management System III. Technical Requirements, Paper III, 2017c

Turner, R. E., Farrier, T. A., Walterscheid, R. L., Mazur, J. E., & Seibold, R. W.: Space Weather Biological and System Effects for Suborbital Flights, AEROSPACE REPORT NO. ATR-2009(5390)-1, 2008

UK CAA: Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases, CAP 760, December 2010

Wilde, P., D., Public Risk Criteria and Rationale for Commercial Launch and Reentry, October 2011