# Chapter 4
# Structure and Principles of Constructing the SMSs to Provide and Monitor System Safety Based on the RRS Risk Management Doctrine

In terms of the analysis of "risks", features of the design of special systems such as safety management systems (SMSs) are considered that are designed to manage such indicators of the system state as "safety" in the field of civil aviation. The creation of SMSs is conditioned by the need to transit to proactive methods of managing safety in the field of civil aviation, which is possible only on the basis of the methodology for calculating risks. In the flight safety domain, traditional (active–reactive) methods have already run its course, especially in the rare events problem.

This SMS was based on the recommendations of the new Annex 19 (ICAO, 2013) [1], which has a higher status than the SMM (Doc 9859-AN/460-2011) [2]. The NASA [3] and RRS doctrine (SST) recommendations and developments from Chaps. 2 and 3 of this book are also taken into account.

## 4.1 Standard International Requirements to the SMS Structure

### 4.1.1 *Key Definitions and Purpose of the SMS*

This book proposes the following definition:

An "safety management system" (SMS) is a set of interrelated and ordered elements or modules (in the minimum composition, per Annex 19) intended to achieve the management objective of providing the required level of flight safety in accordance with the adopted systematic approach (the alternative "Blue Folder" [4]—see below).

The ICAO systematic approach to flight safety management defines tools for the following: managing the state of systems; creation of a hierarchical structure of the SMS organization, including a module for the manager's responsibility for the flight safety in the business structure.

Kuklev E.A. et al., *Aviation System Risks and Safety*, Springer Aerospace Technology, https://doi.org/10.1007/978-981-13-8122-5_4

This definition is introduced in accordance with standards such as GOST R in the Russian Federation [5]. The content of the definition was discussed at ICAO workshops, as it was not in line with the primary version in Annex 19 (March 2013). However, it does not contradict the essence of the SMS and is more in line with scientific achievements in this field and the recommendations of the international British standard.

Note: The original definition recommended in Annex 19 is "*SMS is a systematic approach…,* etc."; the discrepancy between the meanings of "approach" and "system" has become the subject of discussion.

Types of SMSs by purpose and forms of declaration of functions are the following: SMS—flight safety management, AA SMS—safety management system for aviation activities.

Below (in Sect. 4.3), the possibility of creating an SMS is substantiated that is unified by functions (in the sense of the SST), but different in terms of the professional sphere of application in the form of 2 basic parts:

Part 1—"CORE"—a universal standard core for all SMSs;

Part 2—"DATABASES" (DB)—various, depending on providers.

SMSs (SMS–AA SMS) are designed for proactive and predictive safety management in aviation transport systems. The essence of SMSs in question is the identification and elimination of potential threats in the management of aircraft, finance, and investments in order to achieve such target results as ensuring flight safety by standard indicators, gaining real financial and economic benefits, for example, in the airline's activities in traditional or intermodal transportation. Such SMSs were developed in the "Boeing" corporation [6], in FAA [7, 8], in OJSC "Aeroflot". It is assumed that in highly reliable systems, risk events $R$ are rare (with probabilities below $10^{-6}$ in Prdf) and have the "near-zero" probability), since other values cannot be determined exactly. This justifies the reasonable avoidance of the interpretations of "risk" as "probability", since events of this kind are detected through the values of their parameters only in pdf "tails" and cannot be described reliably. Pdf values for such parameters are very small.

There is no practical meaning in the multiplication of such unreliable quantities with the values of $10^{-7}$, $10^{-8}$, …, $10^{-12}$ used by the researchers in the PSA method, since the results obtained are not useful.

### *4.1.2 Integrated "SMS–QMS" Modules ("Blue Folder")*

An SMS [4] is an active system integrated with other management systems to form a flexible technical and regulatory framework of the organization. At the same time, it identifies hazards and risks that are of importance to the entire organization.

In addition, at the same time, risk control is established in full compliance with reliability standards. Such an SMS focuses on hazards, and at the same time, due to the non-compliance with the strategic goals of the business organization (e.g., the "state/nation"), two mutually dependent QMS and SMS systems can affect safety [4].

10 THINGS YOU SHOULD KNOW ABOUT SAFETY MANAGEMENT SYSTEMS (SMS)

SM ICG Contacts

4. Younossi, SM ICG Chair
al Aviation Administration
Aviation Safety
(202) 267-5164
Amer.M.Younossi@faa.gov

er, Alternate SM ICG Chair
al Aviation Administration
Aviation Safety
(425) 917-6732
Charles.Huber@faa.gov

This publication was prepared by the Safety Management International Collaboration Group (SM ICG). The primary purpose of the SM ICG is to promote a common understanding of SMS principles and requirements, and facilitate their application across the international aviation community.

**Fig. 4.1** The front page of the paper prepared by the FAA ("10 Things You Should Know About Safety Management Systems (SMS)")

Therefore, it is necessary to develop an SMS integrated with the QMS. Generalized recommendations are given in the work ("Blue Folder") by A. Younossi (from the FAA) in Fig. 4.1. These provisions were presented in [9].

### 4.1.3 Main SMS Functions Recommended in Annex 19

Below are the main NASA provisions (page 219 in [3]):

- *identification of accident scenarios;*
- *estimation of the Likelihood of each scenario;*
- *evaluation of the consequences of each scenario;*

However, the term "Likelihood" should be considered (according to OXFORD) [1] as the "Possibility" of "Risk Events" with "near-zero probabilities", i.e., without the use of the term "probability", as accepted in the RRS doctrine (Chap. 2 of this book) and indicated in the SST.

From this, it follows that the key processes for the SMS are the following:

- identification of hazards associated with the activities of the organization;
- risk management based on a standard approach to risk assessment and control;

- predictive compensation of possible consequences in each (proactively) "detected" hazardous scenario of the development of the situation or a possible chain of events.

The NASA recommendation [3] was the basis of methods for proactive system safety management by the criterion "target safety level" using the risk value as an adjustable ATS output parameter.

The management triad known in ICAO (NASA) (Sect. 4.2.1 below) makes it possible to solve these issues.

## 4.2 Prediction of the Safety Level in the SMS for Complex Aviation Systems Using Risk Models for Critical Functional Failures

This section describes theoretical features of the methods used to assess levels and assure the safety of activities and operations in civil aviation on the basis of risk models.

### *4.2.1 Triad of Management Actions in the SMS*

This triad (according to NASA [3]) comprises three types of ATS state management in current situation for $t \in [t_0, T)$ and in predicted or anticipated situations for $t \in [t_x, T)$ [5, 10].

The moment $t_x$ is assigned to monitor the ATS state in the production activity, when it is necessary to ensure a guaranteed result in the planned operations, i.e., "in the future", $t_0$ is the initial moment of time for management and $T$ is the planned period of ATS operation.

The types of safety state management per ICAO are those that were discussed in Chaps. 2 and 3 are listed as:

– active (reactive) (№ 1);
– proactive (№ 2);
– predictive (based on some a priori information (№ 3).

For each type of management, ICAO has developed guidelines recognized by the global aviation community. For each of them, NASA presents a general algorithm for constructing a management procedure, which is recommended for use in SMSs from various providers. The description is given in Sect. 4.2.4 as a scheme for developing scenarios to analyze hazardous situations in ATSs within the SMS.

The risk models adopted by the SST (RRS) on the basis of the *Fuzzy Sets* approach allow solving the tasks of this subsection using the positions of the general theory of managed systems. Here, an analogy with the terminal control can be seen according to [11].

From the glossary of the American Oxford University [1, 9], it follows that "*Risk is a possibility of serious (negative) consequences in the assumed situations under the conditions of determining threats of a given type so as: Threat is a source of hazard*".

This is the rationale for the RRS SST concept (Chap. 2) that risk is a *projected "amount of some hazard in a given state* of the system". Potentially, only *some fuzzy possibility* of occurrence of rare risk events can exist in the ATS, but they are *immeasurable (probabilities are unknown)*. The "probability" as a *clear quantity* can (and must) be *clearly (deterministically) calculated* only from known probability distribution functions (Prdf) and probability densities (pfd).

Management, for example, according to [11] (S. Kabanov), is a deliberate action (in time, space, including terminal control) that affects the selected facility or system, taking into account the measurement of the "discrepancy" (residual) of the objective function and the measured value.

In safety assurance and monitoring systems, it is possible to *reliably measure* (a priori—on the basis of models or a posteriori—on the basis of statistics) only *deviations of the values of control parameters* from standard ones. Otherwise, the concept of *"safety" is a "symbol"*, at most. The use of the concept of risk in the RRS as an "amount of hazard" (hazard measures according to the RAS) makes it possible to "measure risk" and its changes in a convenient physical form (measure), taking into account the variety of various adverse factors.

Indeed, one can take formula (3.2) from Chap. 3 to evaluate the significance of the risk $\tilde{P}$ and its integral value $\hat{P}$ :

$$\tilde{R} = (\mu_1, H_R|\ \Sigma_0) \tag{4.1}$$

$$\hat{R} = f_R(\tilde{R}|\Sigma_0). \tag{4.2}$$

Any of the quantities—elements in (4.1) and (4.2)—can be fixed and included in a set of conditions $\Sigma_0$. Then one can obtain what was proved in the RRS: An indicator of risk (significance) can be any "clearly" or "fuzzily" measurable indicator:

$$\overline{R} \rightarrow \widetilde{R}_1 = \left(\mu_1, H_R| \sum_0 \right) \Rightarrow \widetilde{R}_1 \rightarrow \underset{\sim}{\overset{\frown}{R}}_1 \Rightarrow \text{chances with} \mu_1 \tag{4.3}$$

$$\tilde{R} \rightarrow \hat{R}_2 = f_R(H_R|\ \Sigma_0 \mu_1) \Rightarrow \underset{\sim}{\hat{R}} \equiv \underset{\sim}{H_R} \rightarrow \text{chances with} \mu_1 \tag{4.4}$$

The values of (4.3) and (4.4) depend on the parameters of the systems and their sensitivity functions, which can be expressed through risk factors and parameters of the systems under study. This is almost impossible in the PSA (as "risk is a probability"), even with parametric variances and mathematical expectations in Prdf and pdf:

$$\sigma_x = f_\sigma(\{k_i\}), m_x = f_m(\{k_i\})\ , \tag{4.5}$$

$$P_A(m_x, \sigma_x | \sum_0) \sim 10^{-6} \tag{4.6}$$

Therefore, according to the ICAO principles [1, 6], the state control in classical dynamic systems for civil aviation facilities should be performed using a certain controlled variable [11]. In cases of problems with “risk”, one must consider a priori only predicted values.

In this sense, “risk management” is in line with the formulation of problems with “terminal control” [11] in the theory of optimal systems.

It is assumed that the measured (proactively, predictively) value is the risk $\hat{R}$ (integral characteristic of hazard). This value is compared with an *acceptable level of risk* $\hat{R}_*$, and a residual is determined (a risk defect $\Delta\hat{R} = \hat{R}_* - \hat{R}$ .). This allows for the management of the system state taking into account the significance of the risk. The control (corrective) impact on systems depending on the residual $\Delta\hat{R}$ makes it possible to *“mitigate risks”* or *“accept them”* or *eliminate the possibility* (not the “probability”) of *occurrence* of a predictable (*in advance*) risk event $R$ in the system—before this event can occur. (The management method with the $\Delta\hat{R}$ value is given below in 4.4).

There are known SMSs built on the principles of risk management [1, 6] in “Boeing”, “Airbus” corporations, and other companies, where the key point is the *prediction* of the occurrence of *“accidents and catastrophes designed in the system”* due to the objective existence of conditions for the occurrence of extremely “rare events—with the ‘near-zero’ probability, but causing great damage”.

With this in mind, approaches [1, 6, 7] were proposed for risk assessment from (4.2) to (4.5) based on [7, 12, 13] for flight safety management too. This is also recommended for the management of safe activities of service providers, including the production and industrial manufacture of products such as airplanes, helicopters, engines, propellers [1, 7]: reactive (*i.e., immediate reaction* to the accident); proactive and predictive (predictable–proactive management of the system state by risk factors, as noted above).

Here, the required estimates from (4.3) to (4.5) can be calculated in two forms—through indicators and a matrix of risks with an estimate of the *residual risk* level in the form of “residuals”:

$$\begin{aligned} \Delta I_{\hat{R}12} &= I_{\hat{R}2} - I_{\hat{R}1} \\ \Delta S_{\hat{R}12} &= S_{\hat{R}2} - S_{\hat{R}1} \ . \end{aligned} \tag{4.6}$$

In this *“triad” of management actions*, the key point is to take proactive measures to change the state of the system before the predicted hazardous event $R$ occurs according to the given scenario, as a result of the interrelation of all elements of the preceding events with the initiating event (IE) in the structurally complex system [14]. Such scenarios are classified as functional failures of systems [15], which can be found in the RT by the “event trees” method [3, 15, 16] and—practically—using the FMEA, FMES, FTA, MEL standards and programs [17–19]. But in order to do this, the Prdf and pdf should be exactly specified in the RT, which is practically impossible with low statistics, and therefore, confidence limits are determined for the issues "of the rare events problem". Confidence-based Bayesian estimates do not allow the determination of exact "risk levels" if "risk is a probability". This was proven by NASA [3] and shown in Chap. 3 in paragraph 3.3.

### 4.2.2 Definition of Threats and Risks in SMSs

The provided recommendations on safety assessment and risk models are applicable for civil aviation: in justifying *operational safety requirements for aviation structures and systems* (in assessing the *airworthiness* of aircraft, helicopters, and spacecraft). The basis for identifying functional failures are diagrams of threats and risks and diagnostic models embedded in DBs of SMSs AA № 1, № 2.

It is assumed that the risk database is formed through chains of events based on the risk factor analysis diagram in Fig. 4.2 where phases 1 and 2 (identification and flight safety management) are shown.

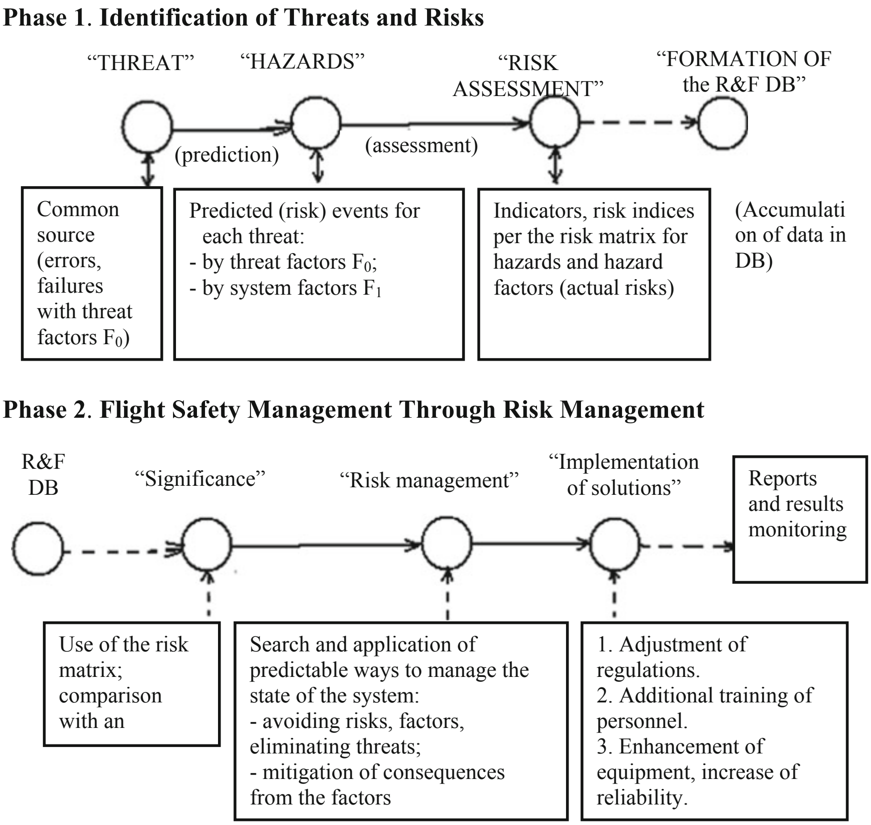
These schemes are intended to be included in the SMS standards, taking into account the requirements of Annex 19 [1].

### 4.2.3 Use of Risk Analysis Matrices in Threats Analysis

*The fuzzy measure $\mu 1$ of the random occurrence of a risk event R will be as follows: "rarely", "very rarely", "frequently", "infrequently", "sometimes"*, which allows the use of known risk assessment matrices by FAA, MES, etc. and avoid the incorrect concept of "predictable" ("guessed") probability of an event, which is accepted in many traditional SMSs—in the Russian Federation and in the USA [3, 6]. The integral assessment of the risk level $\hat{R}$ ("amount of hazard" defined as proposed above) as a function of a two-element set is found by (3.2)–(3.4) taking into account the amount of damage. The general principle of matrix construction and the adjusted ICAO matrix were given earlier in Chap. 2. Here, it is demonstrated by Fig. 4.3 that a row with an incorrect name for the concept "guessed probability" is excluded from the risk assessment matrix (e.g., in the SMM [7]). (In the JSC RR standards [20–22], this row still remains).

The line of fuzzy estimates of the possibility of a random occurrence of a risk event $R$ (with the "near-zero" probability) for the Fuzzy Sets method is given in the form (4.5) (below) or in another, but similar form:

$$\mu_1 : (\text{“very rarely”}, \text{“rarely”}, \text{“infrequently”}, \text{“frequently”}). \tag{4.7}$$



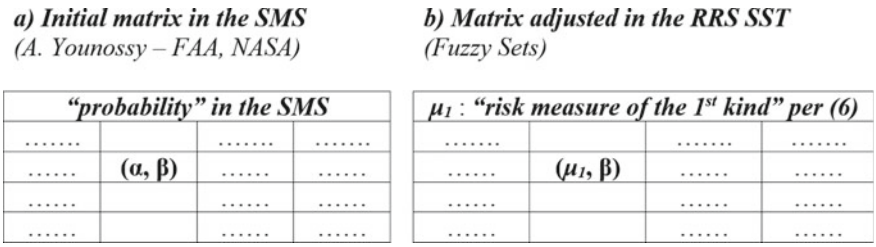
**Phase 1. Identification of Threats and Risks**

“THREAT”
“HAZARDS”
“RISK ASSESSMENT”
“FORMATION OF the R&F DB”
(prediction)
(assessment)
Common source (errors, failures with threat factors F0)
Predicted (risk) events for each threat:
- by threat factors F0;
- by system factors F1
Indicators, risk indices per the risk matrix for hazards and hazard factors (actual risks)
(Accumulati on of data in DB)

**Phase 2. Flight Safety Management Through Risk Management**

R&F DB
“Significance”
“Risk management”
“Implementation of solutions”
Reports and results monitoring
Use of the risk matrix; comparison with an
Search and application of predictable ways to manage the state of the system:
- avoiding risks, factors, eliminating threats;
- mitigation of consequences from the factors
1. Adjustment of regulations.
2. Additional training of personnel.
3. Enhancement of equipment, increase of reliability.

**Fig. 4.2** Risk Factor Analysis Diagram



***a) Initial matrix in the SMS***
*(A. Younossy – FAA, NASA)*

| ***“probability” in the SMS*** | | | |
|---|---|---|---|
| ....... | | ....... | ....... |
| ...... | **(α, β)** | ...... | ...... |
| ...... | | ...... | ...... |
| ...... | | ...... | ...... |

***b) Matrix adjusted in the RRS SST***
*(Fuzzy Sets)*

| ***$\mu_1$ : “risk measure of the 1st kind” per (6)*** | | | |
|---|---|---|---|
| ....... | | ....... | ....... |
| ...... | **($\mu_1$, β)** | ...... | ...... |
| ...... | | ...... | ...... |
| ...... | | ...... | ...... |

**Fig. 4.3** Transformed ICAO risk assessment matrices

The ICAO risk assessment matrices (in “SMS”, “SMM”, “NASA” documents) [3, 7, 23] were transformed and took the form shown in Fig. 4.3, which makes it possible to interpret their physical content.

In matrix cells, pairwise combinations of elements are arranged, as was originally suggested by NASA [3].

In this case, the concept of a scalar, of the *“medium risk”* type that is incorrect for rare events, is completely excluded from consideration. This is difficult to do in the PSA. However, in (4.5), (4.5), and (3.2)–(3.6) (from Chap. 3) are universal relations, where $\mu_1$ may be a PSA probability, if reliable statistics are available, and the “*average number of expected aircraft conflicts per hour*” in the ATC system.

### 4.2.4 Algorithm of the NASA Scenario for the Triad of Proactive and Predictive Safety Management for Aviation Activities by Means of SMSs (FO SMS–AA SMS)

In this subparagraph, the definitions included in the “triad” of Sect. 4.2.1 are explained.

On the basis of the risk concept from ICAO Annex 19, approaches to risk assessment and flight safety or service providers’ activities safety management are proposed, including the industrial production of ATSs. This concept was adopted in this book, and methods for assessing risks (“amount of hazard”) for specified scenarios of hazardous situations were developed.

NASA [3] proposed a universal (unified) algorithm for analyzing hazardous situations in the form of a tuple <…> of fuzzy attributes as follows:

$$\begin{aligned} &< threat - risk\, event - prediction\, of\, events (leading\, to\, a\, catastrophe) \\ &- hazardous\, state - risk\, assessment - control\, impact\ > \end{aligned} \tag{4.8}$$

This algorithm is necessary for developing AA SMS (SMS) standards for risk and threat significance assessment—according to Fig. 4.2.

### 4.2.5 ICAO and ISO Hazard Models in SMSs

The general scheme for constructing hazard models is based on the methodology of Chap. 2 (paragraph 2.5) using the outcome space from the probability space (2.1) with the transition to the *Fuzzy Sets* methodology.

In the SST, the risk is defined as an “amount of hazard” in given critical discrete states with fuzzy subsets of analysis objects in some specially formalized structures of the systems under study.

Following this, it is assumed in the RRS that the primary system safety analysis should be performed using the concept of the system state in a discrete probability space for events with the "near-zero" probability. Then, according to the SST, the measurability of random events by probability is abandoned, and the fuzzy logic of the event algebra is adopted using the *Fuzzy Sets* method. The prediction (proactive and predictive) methods of safety regulation by ICAO are implemented on the methods of calculating the risks of occurrence of negative consequences in technical systems that are detected by SMS-like systems.

The main task in the general system safety theory is to define and interpret the category of "residual risk" arising from the RT concept and to recalculate this "risk" with the help of SST tools into residual "catastrophe risks" that determine "passive" and operational safety in highly reliable systems.

ICAO hazard models can be found as event chains, clear in functions, in the form of scenarios. Then, according to the SST method, it is recommended to *find, without probabilistic indicators, the risks* of negative consequences *from these scenarios*. To this end, Annex 19 recommended to use risk assessment matrices in (Fig. 4.3, in general terms).

## 4.3 Construction of a Generalized Safety Management System (SMS)

The main features of constructing an international SMS are most clearly stated in the document created in the US Federal Aviation Administration (FAA) service under the leadership of Amer Younossi, head of the FAA Flight Safety department. This document ("Blue Folder") presents the main modules of the system recommended by ICAO for inclusion into the new international standards such as Annex 19. The "10 positions" (from "Blue Folder" [4]) are indicated, which should be reflected on the basis of this document (shown in Fig. 4.1).

### *4.3.1 SMS Functions Based on the NASA Principles (for ICAO)*

In the generalized SMS, SMSs should be presented in the form of two modules: AA SMS—Type 1 and Type 2.

*In Type 1 AA SMS (state/national level),* the following tasks are solved:

- Continuous monitoring of the aircraft (all aircrafts in the region);
- Real-time optimization of the flight plan, the use of power plants, taking into account the current meteorological, aerodynamic and statistical data for a specific aircraft;

- Interaction with ground technical services is provided during the flight; thus, reducing the time for maintenance of the aircraft after the flight is completed and for its preparation for the next flight;
- Aircraft systems and units operation are monitored with remote diagnostics provided;
- An automated system for collecting and analyzing the information received is used;
- Fail-safe communication channel on 100% of the surface of the globe;
- Immediate notification of the crew and ground services of failures and deviations in the operation of the onboard systems;
- Analysis, notification, and recommendations on fuel efficiency at any time, at any flight phase;
- Conclusions based on the analysis of accumulated information;
- Database replenishment and administration;
- Current actual level of aviation equipment reliability;
- Automated detection of factors of possible hazard occurrence along the flight route and advance notification of the aircraft crew;
- Optimization of aircraft maintenance;
- Integration of transmitted data;
- Continuous diagnosis of possible aviation equipment failures;
- Timely messages from the crew about the need for unscheduled works to eliminate defects detected in the course of the flight;
- Crew access to ground information systems and resources;
- Consultations with ground services during the flight;
- Transmission and exchange of data between aircrafts; and
- Receipt of information on special flight conditions from the aircraft.

To ensure the effectiveness of these actions, databases are compiled containing common threats, particular threats by hazard factors, risks, a list of risk management functions (chains); the risk values are adjusted; and the impact on the ATS is estimated by means of the SMS in airlines.

### *4.3.2 Principle of Constructing and Determining the Composition of the AA SMS (Type 2) Core*

The main unit of the AA SMS is the "core" in (4.1) consisting of separate modules that make it possible to evaluate and improve the overall level of safety: by identifying characteristics of adverse single and rare events with small statistical samples and to take measures to eliminate and prevent them.

As the main modules of the "core" providing proactive safety management schemes (shown in Fig. 4.2) and the output results from service providers, the following are taken, according to (4.8):

- *identification of threats (list of hazards, events, and factors);*

- *identification of risk events (risk assessment);*
- *determining the consequences (assessment of damage from the knowledge base); and*
- *identification of management actions that effect the system to minimize risks.*

These modules are, in essence, the same as in the SMMs of early editions [2]. But now their number is minimized and stipulated in the new ICAO standard (Annex 19).

The concept of risk in the presented system is interpreted in the original form as it was indicated in Chap. 2 and adopted in the engineering and physical sciences as follows: "*Risk is a possible hazard*". This hazard is caused by threats: management errors, human factors, etc. In the methodology for calculating risks, hazard is always considered *as predictable* if the conditions for the occurrence of a risk event are detected. The *problem is the detection of hidden threats in the system*, depending on the residual risk designed at the stages of development and production of transport equipment in general and aviation equipment (aircraft, helicopters) in particular.

### *4.3.3 SMS Subsystems and Modules*

According to ICAO (Annex 19) [2], SMS should be built as a general system of 2 subsystems global for the country (region). Accordingly, the general system, AA SMS, consists of two subsystems:

SMS-1—State/national level (or sectoral);

SMB-2—Service provider level (airline, airport, maintenance and repair, "Production").

*The first subsystem SMS-1*, operating at the state level of aviation activities (AA), performs the following functions:

- continuous monitoring of flight parameters and system states of all aircraft in the region (this has always been done in civil aviation of the Russian Federation, but on a different technical information basis and for other purposes);
- creation of an interaction "aircraft—ground technical services" system on the basis of the ACARS prototype (A-380) to be used during the flight and during aircraft maintenance; and
- replenishment of databases and administration of all service providers.

*The second subsystem SMS-2*, which is part of the general SMS structure, contains two main standard modules:

***Module 1***—Integration of QMS units with modules that determine the principles of SMS functioning, ensuring the achievement of the main result—providing a target level of safety based on the concept of risks (per ICAO), taking into account all aspects of the provider's activities.

***Module 2—***Tools for measuring and predicting risks, assessing the integral significance of risks, normalizing acceptable risks, formalizing and creating a system for identifying risks and a base of risk factors, managing risks according to scheme (4.8), taking into account (4.7), and preventing occurrence of negative situations in accordance with the recommendations of regulatory documents.

The global AA SMS (and database, DB) created on the basis of SMS-1 and SMS-2 on the NASA prototype, as required by ICAO, performs the following functions:

- Automated collection and analysis of information received onboard the aircraft;
- Analysis of aircraft communications on the entire surface of the globe (FORAS, ACARS and in ground services);
- Processing of the accumulated information from the perspective of analyzing risks and quality of operation of systems and units on the basis of quality standards (reliability of units, hazardous scenarios, etc.);
- Evaluation of the current level of reliability and safety of aviation equipment during the life cycle on the basis of relevant manuals;
- Automated detection of hazard factors along the flight route and advance notification of the aircraft crew of possible threats, activities of the service provider, resources, vehicles, etc.

***Note*** Classification of threats, list of hazards, and hazard models, for example, in the form of scenarios and J. Reason chains, should be defined in another separate standard.

The generalized functional diagram of the SMS-2 "core" is shown in 4.3a. A detailed description of this diagram was given in Fig. 4.3. [5, 10] (above).

### *4.3.4 Functional SMS Diagram and Computer Support of Procedures for Assessing Risks of Occurrence of Adverse Events on the Basis of the ICAO Methodology (SMM)*

The SMS prototypes and their characteristics are described by airline "British Airways" on the example of Bristol airport; USA FAA—"Order", as well as in the IATA "Hand Book" and other documents. Well-known service providers (FAA, Canada, Aeroflot, Transaero, Russia, etc.) also have prototypes of such SMSs.

Here, for the first time, the Fig. 4.3 is showing a generalized SMS diagram, which should be included in a series of standards, developed for presentation to ICAO and for civil aviation in Russia so as the form of national standard.

***The main SMS modules can be as follows.***

- The module of the SMS organizational structure and its subsections should be created in accordance with the ICAO SMM recommendations, primarily on the basis of Annex 19 [1, 6].
- Mandatory proactive flight safety management modules based on risk factors recommended by the SMM [24] and defining the functional composition of the SMS.

- Modules (per ICAO) that implement mandatory procedures for identifying risk factors and a list of hazards and threats [7, 24, 25].
- Information databases (IDB) for proactive risk identification based on statistics (FI decoding) and predicted threats.
- Bases of expert knowledge, which are grouped into the “portfolios” of risk analysis matrices with hypertexts of the predicted consequences.
- Algorithms for developing proactive corrective actions that affect the state of the system.
- Procedures for identifying and classifying simple risks, J. Reason chains, detecting hidden threats (in the form of filters in the protection equipment).
- SMS system of computer support for results of the flight safety monitoring with the formation of integrated flight safety indicators for service providers as follows:

– integral estimation of the flight safety state in real time with the scientific and methodical modules predicting hazards;
– feasibility study of the decisions on factor risk management in the service provision system (airfields, ATC, fuel, etc.).

- A system for displaying information in a generalized form for providing information to the management of the service provider organization and the civil aviation authority of the Russian Federation in the ON-LINE mode and for monitoring the flight safety state in civil aviation of the Russian Federation from the part of ICAO.

In Russian Civil Aviation, there are some examples of SMS, created on basic SMM principles.

## 4.4 Methodological Basis for Solving the Problem of Estimating Residual Risk Taking into Account ILS Chains

### *4.4.1 State Regulation of AA Safety in Civil Aviation of Russia*

The state prioritizes the level of acceptable risk $\hat{\mathrm{R}}_{*\mathrm{i}}$ for occurrence of emergency situations in civil aviation, according to the flight safety program (Order No. 641r of 06.05.2008).

It is assumed here that the concepts of “risks” and their significance mentioned in various documents are set in terms of the RRS included in the SST tools, i.e., as the universal concept of “integral risk” $\hat{\mathrm{R}}$ from Chap. 2. This, in particular, is the convenience of the approach to solving safety issues on the basis of the RRS provisions [26–28].

### 4.4.2 Determination of Acceptable Risk Levels

The concept of “acceptable risk” was originally introduced in the RT—in I. Aronov’s book [16, 29] and in other publications (this book contains this concept cited from [16] in Chap. 1). This term is recommended to be applied both in the state regulation of flight safety and in all aviation activities, including the ATS production (since 2010, also in JSC RR [29]).

Taking into account the results achieved in previous $(i-1)$ periods of operation and production of aviation equipment, an acceptable risk is assigned as:

$$\hat{\mathrm{R}}_{*\mathrm{i}} = \frac{1}{k}\,\hat{\mathrm{R}}_{*\mathrm{i}-1}, \tag{4.9}$$

where $\frac{1}{k}$ is a coefficient of hazard reduction in the adopted measurements in risk units due to the corresponding increase in the level of flight safety at the $i$th stage of the civil aviation industry cycle. In particular, for the period up to 2012 the coefficient (1/2) was introduced, i.e., the acceptable risk should be reduced 2 times:

$$\hat{\mathrm{R}}_{*\mathrm{i}} = \frac{1}{2}\,\hat{\mathrm{R}}_{*\mathrm{i}-1}. \tag{4.10}$$

For example, according to ICAO, in Russia the number of accidents or emergency situations should be reduced by half. This implies the requirement to improve the quality of aviation equipment production and its operation, taking into account the ILS principles. This requirement leads to the need for redistribution and recalculation of risks across the entire ILS production chain, so that in the end, as a whole, an acceptable level of flight safety is ensured in civil aviation of Russia, as established by the state through the level of risk.

The question is, *if the PSA method is used, then which units this “risk” or flight safety level is to be measured in?* In the RRS (SST), this issue is solved with the help of $\hat{\mathrm{R}}_0$.

The “residual predicted risk” is determined by production through a fuzzy measure of the predicted hazard, for example, by applying quality systems that clearly give confidence bounds for the probability of occurrence of functional failure states in a range of the failure event probability up to $10^{-6}$–$10^{-3}$, not worse.

Integral indicators of an acceptable level of risk $\hat{\mathrm{R}}_{*i}$ established by the state, for example, ICAO, in the form of 4–5 or 1–2 catastrophes over 10–15 years of the aircraft operation should be recalculated into residual risk indicators $R_{\mathrm{M}}$ of the equipment transferred to the operator.

However, the problem is that equipment manufacturers ensure the quality of their ATS according to the standard probability indicator only. The manufacturer assumes by default that “*if the AE is reliable, then it is safe*”. But this condition of flight safety does not meet the requirements of international standards. In Chaps. 2 and 3 of the book, it was shown that “catastrophes” (in the RT) with *“non-zero” residual design risk* $\Delta\hat{\mathrm{R}} \neq \Delta\hat{\mathrm{R}}_*$ are not eliminated, but only moved to “infinity” according to the rules of "3" or "6". This is not constructive for civil aircraft, NPPs and HPPs because of small production volumes only the production of high-reliability cars (e.g., TOYOTA) has indicators $\Delta\hat{R}_*$ close to the probability of a possible risk event $R_*$, the occurrence of which is caused by the rule of "6". Here, (3) and (6) rules are indicated: *"Three sigmas" and "Six sigmas".*

At present, manufacturers have not any methods for converting risk factors into reliability indicators, nor are they obliged to modify their production processes in any way.

Thus, the "*Manufacturer-Operator" system* is open (in Russia) in terms of flight safety indicators. While Western systems have been adhering to the well-known ILS principle and supplying equipment to Russia for a long time following the after-sales service method. At the same time, the ILS principle is observed quite fully in accordance with the adopted regulations.

It is assumed that operators' risks $\hat{R}_O$ are functions of the parameters $n_i$ of the flight operations system in airlines,

$$\widehat{R}_O = f_O(n_1, n_2, n_3, \dots n_i, \dots, n_O) \tag{4.11}$$

Manufacturing risks $\hat{R}_M$ are determined by a list of interrelated parameters $k_i$ characterizing the ILS system (ILS parameters), for example, per IATA:

$$\widehat{R}_M = f_M(k_1, k_2, k_3, \dots, k_i, \dots, k_O) \tag{4.12}$$

The difference (discrepancy) $\Delta\hat{R}_{OM}$ of risks $\hat{R}_O$ and $\hat{R}_M$ should not exceed the minimum level $R_{\min}$ determined by an acceptable level $R_{*i}$ as established by the state:

$$\hat{R}_M - \hat{R}_O \le \hat{R}_{*i} = \frac{1}{2}\hat{R}_{*i-1}, \tag{4.13}$$

which is equivalent to the condition indicated above,

$$\Delta\hat{R}_{OM} = \hat{R}_M - \hat{R}_O \le \hat{R}_{*i} = \frac{1}{2}\hat{R}_{*i-1}, \tag{4.14}$$

When using risks in the format of indicators (ICAO, IATA), these ratios determine the principle of proactive management of the system, taking into account the ILS and flight safety indicators in the aircraft operation, as shown above:

$$\Delta I_{\hat{R}12} = I_{\hat{R}2} - I_{\hat{R}1}\ , \quad \Delta S_{\hat{R}12} = S_{\hat{R}2} - S_{\hat{R}1}\ ,$$

where $\Delta I_{\hat{R}12}$ is the discrepancy between the risk indicators, and $\Delta S_{\hat{R}12}$ are additional costs to cover risks in airlines and in the aviation industry, necessary to achieve an acceptable risk level in the form of (4.9).

Thus, it is necessary to substantiate the selection of hazard factors in the two subsystems (“manufacturing”, “operation”) and determine the principles of safety regulation.

In addition, a set of documents of the international level should be established to implement the methodological foundations for the construction of a state system to ensure flight safety in the Russian Federation.

## 4.5 Conclusions

1. The ICAO recommendations (in Annex 19) stated the need for mandatory development of SMSs for various providers’ aviation activities. At the same time, there are some unified requirements for the functions and the minimum composition of SMS modules. The NASA algorithm for providing proactive risk management in ATSs is universal.
2. In order to eliminate contradictions in the interpretation of the functions, composition, and purpose of the SMS, it seems advisable to develop a national standard for civil aviation of the Russian Federation regarding the concept of constructing a unified SMS (AA SMS), in which the “core” and specialized databases should be defined that reflect the specifics of various providers’ aviation activities.

## References

1. Annex 19: C-WP/ 13935—ANC Report (March 2013), based on AN-WP/ 8680 (Find) Review of the Air Navigation Commission, Montreal, Canada
2. SMM: Doc. 9859-A/N460. ICAO, 2009
3. Probabilistic Risk Assessment Procedures for NASA Managers and Practitioners—Office of Safety and Mission Assurance NASA. Washington, DC 20546—August. 2002 (Version 2/2)
4. Amer MY (2012) 10 Things you should know about safety management systems (SMS). SM ICG, Washington
5. Evdokimov VG (2012) Integrated safety management system for aviation activities based on ICAO standards and recommended practices, J TR, 2(45):54–57. (in Russian)
6. SMS & B-RSA (2008): “Boeing”, 2012
7. SMM (Safety Management Manual): Doc 9859_AN474—Doc FAA: 2012
8. Risk management (2009)—Vocabulary—Guidelines for use in standarts. PD ISO/ IEC, Guide 73: 2002.B51
9. Gipich G, Evdokimov V, Kuklev E, Mirzayanov F (2013) Tools: identification of hazard & assessment of risk. report at the ICAO meeting “Face to Face”. “Boeing” Corp., Washington, janv
10. Kuklev EA, Evdokimov VG (1995) Predicting the safety level for aviation systems based on risk models. Journal TR, No. 2 (45), pp. 51–53. (in Russian)
11. Kabanov SA (1997) System management on predictive models. St. Petersburg University, St. Petersburg (in Russian)
12. McCarthy J (1999) U.S. Naval Research Labaratory; Schwartz N, AT & T. Modeling risk with the flight operations risk assessment system (FORAS).—ICAO Conference in Rio de Janeiro, Brasil, Nov

13. Documents of the 37th ICAO Assembly (October 2011, Montreal)
14. Volodin VV (ed) (1993) Reliability in technology. Scientific-technical, economic and legal aspects of reliability.—Blagonravov Mechanical Engineering Research Institute, ISTC “Reliability of Machines”—RAS, Moscow, pp 119–123. (in Russian)
15. Aronov IZ et al (2009) Reliability and safety of technical systems. Moscow (in Russian)
16. Smurov MY, Kuklev EA, Evdokimov VG, Gipich GN (2012) Safety of civil aircraft flights taking into account the risks of negative events. J Trans Russ Fed, 1(38):54–58 St. Petersburg: 2012. (in Russian)
17. Smurov MY, Kuklev EA, Evdokimov VG, Gipich GN (2012) Development of tools for assessing the risks of occurrence of risks of AUI in the AASS of the airport system. J Trans Russ Fed, 2(39), St. Petersburg (in Russian)
18. Evdokimov VG, Kuklev EA, Shapkin VS (2013) Use of flight information to increase the reliability in assessing the levels of possible threats. Scientific bulletin of the MSTU CA. No. 187 (1). Moscow, pp 49–53. (in Russian)
19. Safety provisions (2010) Helicopter European safety group and JSC ALLIED AVIATION CONSULTING—EHEST (ESSI). JSC “AAC”, Moscow, 2010. (in Russian)
20. Guidance on hazard identification. SMS WG (ECAST (ESSI) Working Group on Safety Management System and Safety Culture). Handwritten, 2010. (in Russian)
21. General rules for risk assessment and management (resource management at life cycle stages, risk and reliability analysis management—URRAN). JSC Russian Railways standard STO RR 1.02.034-2010. Moscow, 2010 (in Russian)
22. Documents of the ICAO High-level Conference (SMM). March 2010, Montreal
23. Issues of the system safety and stability theory./Issue 7. Ed. by Severtsev N.A./Moscow: RAS Dorodnitsin CC, 2005. (in Russian)
24. Accident Prevention Manual (1984) Doc. 9422-AN/923. International Civil Aviation Organization
25. Evdokimov VG (2010) Modern approaches to safety management based on the risk theory. International Aviation and Space Magazine “AviaSouz”. NQ 5/6 (33) October–December 2010. (in Russian)
26. Evdokimov VG, Gipich GN (2006) Some issues in the methodology of assessment and prediction of air transport risks. In: The 5th international conference “Aviation and Astronautic Science 2006”, Abstracts, Moscow: 2006. pp 75–76. (in Russian)
27. Evdokimov VG, Grushchanskiy VA, Kavtaradze EA (2008) On the system safety of information support for the development of complex social systems. Fundamental problems of system safety: Coll. of papers/RAS Dorodnitsyn CC, Moscow: University Book, pp 67–77. 14. (in Russian)
28. Aronov IZ (1998) Modern problems of safety of technical systems and risk analysis. Standards and quality, vol. 3. (in Russian)
29. Procedure for determining the acceptable level of risk (URRAN). JSC Russian Railways standard STO RR 1.02.035–2010. Moscow: 2010. (in Russian)