Security Risk Assessment and Risk Treatment for Integrated Modular Communication

Hamid Asgari, *Senior Member IEEE*, Sarah Haines, and Adrian Waller
Thales UK Limited, Research & Technology,
Worton Drive, Worton Grange Business Park, Reading RG2 0SB, United Kingdom
{Hamid.Asgari, Sarah.Haines, Adrian.Waller}@uk.thalesgroup.com

Abstract—Integrated Modular Communication (IMC) is an on-board platform to provide secure and reliable aircraft communications for a diverse set of applications. IMC is viewed as an important part of the future Air Traffic Management (ATM) infrastructure. Integrating communication links and combining diverse applications in a single platform (IMC) do come with some risks to the ATM communications that could potentially increase vulnerabilities and make the system more prone to security attacks. There are several types of attacks on network communications such as disrupting or blocking communication, intercepting, injecting fabricated packets, accessing and modifying the information. In this study, the Security Risk Assessment Methodology (SecRAM) is applied to IMC for identifying runtime threats, assessing the risks involved, and defining measures to mitigate them. The risk assessment is performed to evaluate the impact and likelihood of occurrence of attacks relevant to the identified threats and the resulting risk levels. Consequently, specific mitigation measures as IMC's security controls are proposed to provide cyber resiliency for the IMC. The IMC security controls will be validated in an emulated testbed environment in the GAMMA project.

Keywords – *ATM, Security, Risk Assessment, Threat, IMC.*

I. INTRODUCTION

Commercial aircraft have a communication architecture of diverse radios, routers, switches and associated control equipment with a separate radio generally dedicated to each service. The Integrated Modular Communications (IMC) concept seeks to achieve significant savings in size, weight, power, and cost, for future aeronautical radio fits, by moving away from the existing federated architecture towards an integrated, modular architecture. Combining various systems (i.e., cockpit and cabin) on the same infrastructure as well as integrating the many communication links, could potentially open up the ATM (Air Traffic Management) system to more attacks, thereby increasing vulnerabilities and the overall risk, unless adequate security measures are taken. Therefore, the IMC vision is to achieve secure and reliable communications between the aircraft and the ground over a set of heterogeneous radio links for a diverse set of on-board applications, carried within multiple safety/security domains.

Works has been carried out on the specific functions of IMC under EU FP7 project of SANDRA [1], Innovate UK project of SINCBAC [2], and the UK Aerospace Growth Partnership (AGP) project of HARNet [3]. In the GAMMA (Global ATM Security Management) project [4], we have been looking at the security aspects of IMC. For safety and security of the aircraft and its operations, all possible threats to the aircraft communication systems and its operations must be identified, potential risks must be evaluated, and mitigations must be put in place through efficient implementation of security mechanisms. These security mechanisms must implement and provide different security features to ensure that the IMC system meets the security requirements.

The three main security requirements specified for consideration in information systems are: to prevent unauthorised information disclosure (Confidentiality) and improper malicious modifications of information (Integrity), while ensuring access for authorised entities (Availability). There are several types of attacks on network communications including: disrupting or blocking communication, intercepting, injecting fabricated packets, accessing and modifying the storage, tables or packets.

GAMMA is complimentary to SESAR (Single European SKY ATM Research) project [5] by developing security solutions for current and next generation ATM which is being defined by SESAR. In the GAMMA project, we have been focusing on the methodologies used for: 1) risk assessment and selection of security controls/functions 2) producing operational and system architectures of ATM security systems including IMC. These architectures are described by the enterprise architecture views of the NATO Architecture Framework (NAF) [6]. GAMMA and SESAR both use the NAF and adopt the same modelling tool (MEGA) [7], opening the way for the GAMMA architecture outputs to be reusable in SESAR. GAMMA has also adopted the methodologies developed by SESAR in WP16 including SecRAM (Security Risk Assessment Methodology) [8] and MSSC (Minimum Set of Security Controls) [9].

We have not been focusing on engineering details of IMC functions (security or otherwise), but on research into how an IMC can be protected and would integrate in such an overall ATM security management system. That is, we are not proposing a detailed security architecture or in-depth functions for IMC that we expect to be used in a real development environment; any analysis of security requirements and solutions performed in GAMMA can be used but would need to be revisited.

A significant body of works exists in the literature on risk management. Among these works, there are established security risk assessment standards, frameworks, methodology

and guides (e.g., ISO/IEC 31010 [10], NIST SP800-30 [11], MITRE [12], and ENISA [13]) that are used to aid formal risk analysis procedures in various contexts. The SESAR SWP16.2 defined a methodology, called SecRAM [8]. SecRAM is applied to ATM contexts. An example of its application is given in [14] by building a relevant threat scenario and designing a risk treatment for a cloud-based ATM environment.

In this paper, we report on the use of the SecRAM methodology for identifying threats and assessing the associated risks for IMC. Accordingly, we establish the context and set out the scope for the security analysis of IMC, assessing the risk levels, and set the scene for validating the identified security controls. For validation purposes, the defined security enablers/controls are checked against the stakeholders' security requirements and needs in order to meet them. Embedding security controls in the IMC architecture for combating run-time threats is a step towards the security-by-design concept enabling cyber resiliency and avoiding incremental updates and plug-ins. Cyber resiliency enablement allows the networked systems to be resilient against persistent, stealthy attacks targeted at cyber assets [15].

The remainder of this paper is structured as follows. After this brief introduction in Section I, Section II describes the risk assessment methodology. Section III briefly explains the IMC functional architecture as the context for this security analysis, the scope of the risk assessment study and the assets. Section IV specifies the threat scenarios relevant to the IMC. The security risk assessment process is described in Section V. Section VI proposes the security controls to put in place to mitigate the threats with high risk levels. The validation process is briefly discussed in Section VII. Section VIII concludes the paper and discusses the further work plan.

II. Risk Assessment Methodology

The evaluation of the threats proposed here will follow the SecRAM methodology [8]. SecRAM is the ISO 27005 based Risk Assessment methodology [16] developed by the SESAR program. This methodology requires establishing the context for defining the boundaries of what one wants to analyse; sets out the scope of the security analysis; and specifies the criteria that will be used to assess the risk, in order to provide consistent and defensible results.

The security risk assessment process adheres to the following steps:

1. Establish the context and an accurate scope: description of the system, boundaries, and the dependencies on other systems;
2. Identify the assets that have value for the achievement of stakeholders' objectives;
3. Identify the threats and threat scenarios that an attacker may use to access an asset;
4. Evaluate the impact of attacks, assessing the harm resulting from an attack in terms of Confidentiality, Integrity, and Availability (CIA);
5. Evaluate the likelihood of each threat scenario that could occur;
6. Assess the security risk level associated to the threats based on their likelihood and impact on the assets;
7. Evaluate and verify the evaluated risk level against the defined security objectives. Security objectives correspond to the level of risk that a primary asset is prepared to accept on CIA, before any action is necessary to reduce it;
8. Risk treatment by defining the action to accept, tolerate, reduce, avoid, or transfer the risk; If the action is to reduce the risk, define a set of security controls and the associated requirements to reduce the risk to an acceptable level (i.e. within the risk appetite, see [8]);
9. Risk treatment by defining appropriate action to manage the risk as below:
   - Accept or tolerate, which means the risk level is low enough, no further action is needed.
   - Reduce or treat, which means the risk must be reduced to an acceptable level (i.e. within the risk appetite) by defining a set of security controls and the associated requirements.
   - Avoid or terminate, which means that the risk is too high and treating it is too costly, a decision may be made to withdraw the activity or change its nature so that the risk is not present anymore.
   - Transfer, which means the risk should be transferred to another party who can most effectively manage the particular risk.
10. Implementation of security controls identified above.

We now apply the above process to the IMC architecture.

III. Context, Scope, and Assets

A. The Context – IMC

IMC is viewed as an integrated standalone on-board processing platform offering multi-radio off-board communication to/from different stakeholders/providers and on-board network connectivity for cockpit and on-board passenger applications. The functional architecture of the IMC is shown in Figure 1. The IMC consists of following main sub-systems:

- Router Sub-system (RoS) – Responsible for routing traffic between on-board applications and Processors;
- Radio Sub-system (RaS) – Responsible for converting application data into a link level format, and routing this to one or more transceivers; It comprises a number of Software Defined Radio entities and includes a number of radio baseband processors together with associated RF transceiver hardware which perform the necessary signal processing needed for the supported bearers.
- Control & Management Subsystem (CMS) – Responsible for managing the overall network and security functions, configuring and monitoring of the IMC.

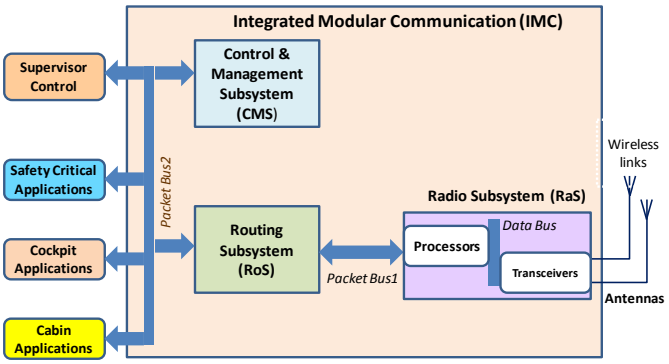

Figure 1: The functional architecture of Integrated Modular Communication and associated applications.

These sub-systems are connected via communication buses. The *Packet Buses* as shown in Figure 1 provide the IP base-band packet interconnect between the IMC subsystems, and between the RoS and the aircraft networks. The IMC off-board communication is via radio links to ground stations. Aircraft on-board applications (i.e., Safety Critical, Cockpit, and Cabin applications) connect to the IMC via the *Packet Bus2*. On-board applications utilising off-board communications services are connected to IMC, via the aircraft networks. The aircraft networks support applications of differing safety criticality levels.

B. Scope

Establishing the context means defining the bounds of what you want to analyse. Design time identification of vulnerabilities in the specification of protocols and functions and mitigation of these are out of the scope of this paper. We only consider run-time attacks in order to make provision for built-in countermeasures.

C. Asset Identification

There are two types of assets: primary and supporting. Primary Assets (PA) are the intangible targets of an attack, which are valuable to an IMC network and its stakeholders. There are two main types of primary assets: information and services. A successful attack would result in damage to the primary assets and have an impact on the network operation.

The main primary assets for IMC in an ATM environment are shown in Table 1.

Table 1: Primary Assets.

Primary Asset	Type	Description
Air Traffic Communication (Com.) Service	Service	The service that allows the transfer of essential data between ATM systems and an IMC for safety-related purposes, requiring high integrity and rapid response; flight control information, alerting, collision avoidance, etc. The service is used by **Safety Critical** applications.
Aeronautical Control & Operational communications	Service	The data service for use by aircraft operators requiring high integrity for handling the operation and efficiency of flights, and support of passengers; The service is used by **Cockpit** applications.
Computing resources	Service	This refers to the IMC system's internal resources, configurations, and operations, e.g. processes, functions, and data-bases.
Control and Management data	Information	Any data that is exchanged concerning the operation and management of the IMC system or its connected networks; Exchanged with the **Supervisor Control** processes and the external GAMMA Security Management Platform.
Airline data	Information	Any data that is exchanged to or from airliner's domain i.e., the operational and airline administrative information to both **Cockpit** and **Cabin** applications.
User data	Information	Any data that is transferred to or from a **Cabin** application process. This is done by a passenger device, accessing the aircraft network (e.g., WiFi or telecom services).

Supporting Assets (SA) are tangible entities that enable and support the existence of primary assets. Entities involved in storing, processing and/or transmitting primary assets are classified as supporting assets. They may have vulnerabilities that can be exploited by threats targeting the primary assets. Table 2 lists, and briefly explains, the supporting assets that may be targeted by a threat scenario and their related primary assets.

Table 2: Supporting Assets.

Supporting Asset	Description	Primary Asset
IMC system	Integrated Modular Communication as a complete system in the ATM environment	Com. Service Computing resources, Airline data, User data, C&M data
IMC's Routing Sub-system (RoS)	Routes data traffic from on-board applications/processes to radio sub-system and vice versa.	Computing resources, Airline data, User data, C&M data
IMC's Radio Sub-system (RaS)	Converting data into a link level format, passing data to one or more transceivers	Computing resources, Airline data, User data, C&M data
IMC's Control & Management Sub-system (CMS)	The entity performing the overall management of IMC functions and security	C&M data
IMC's Internal BUS	IMC internal packet bus as the data link between RoS, RaS, and CMS	Airline data, User data, C&M data,
Satellite link	Satellite link to provide worldwide reliable communication channels	Com. Service, Airline data, User data, C&M data
HF/UHF/VHF links	Different radio Data links	Com. Service, Airline data, User data, C&M data,
Wireless access inks	Broadband wireless access systems for on-the-ground communication.	Airline data, User data, C&M data
Cellular link	Provides cellular connectivity such as 3G.	User data

IV. Threat Scenarios

In this paper, we mainly focus on intentional threats to an IMC network and its assets. Therefore, we do not analyse the complete spectrum of threats (e.g. faults, accidental, natural, terrorist damages, or unintentional misconfiguration of policies). Only the most relevant threats have been selected and applied to the supporting assets. These threats are intended for confidentiality, integrity and availability violation, disruption of services, unauthorised access to data and objects, and unauthorised disclosure of information.

Table 3 shows the identified IMC threats. Threat 1 (T-IMC1) and Threat 2 (T-IMC2) correspond to attacks from on-

board and off-board applications respectively. Threat 3 (T-IMC3) is specified in which an attacker inserts malicious software into the IMC. An example of Threat 3 is related to the configuration of the router that needs to be protected. There are known ways of achieving this protection. Threat 4 (T-IMC4) is related to the abuse of administrator privilege. Threat 5 (T-IMC5) is related to Jamming attacks. For more details please see GAMMA deliverable D2.1 [4].

Table 3: Identified IMC Threats.

IMC Threat	Description
T-IMC1	**On-board application attack:** An application on board the aircraft uses its data connection to the IMC to attack an ATM primary asset (e.g. flight/airline information managed by another application).
T-IMC2	**Off-board application attack:** An off-board application uses its data connection to the IMC to attack an ATM primary asset. This could be a ground segment application, or something external to the ATM system (e.g., Internet traffic destined for the cabin).
T-IMC3	**Subverted software or hardware:** Corrupted software or hardware in the IMC attacks an ATM primary asset (e.g., denying communication to ATC).
T-IMC4	**Abuse of management interface:** An administrator of the IMC (e.g. someone setting configuration parameters) abuses his/her privileges, or someone impersonates the administrator, and uses this to attack an ATM primary asset.
T-IMC5	**Jamming of data links:** A jamming device is used in proximity to ATM channels to perform this attack. These devices prevent IMC from communicating application data.

The impact on targeted supporting assets of the IMC Threats 1 to 4 will be the leakage or unauthorised modification of data within the IMC, and could cause reduced availability or even complete failure of the IMC.

V. Security Risk Assessment

For each threat, the impact on the Confidentiality, Integrity and Availability of the information and services is assessed according to the following scale [8]:

- Scale 1: No impact / Not Applicable
- Scale 2: Minor – limited impact to the IMC operation, but it is still able to function
- Scale 3: Severe – performance of an IMC process is compromised in order to malfunction
- Scale 4: Critical – performance of the IMC functions is compromised that can have major consequences
- Scale 5: Catastrophic – The IMC operation and its network are compromised making the IMC system inoperable/malfunction.

The impact is valued and assessed according to the loss or degradation of Confidentiality (C), Integrity (I), and Availability (A) for every primary asset. The overall impact is then calculated as the highest of the three impact values of C, I, and A.

According to the SecRAM, the likelihood is built from a split into 'exposure' or frequency of occurrence of the threat source and 'potentiality' that, once the threat source occurs, the threat scenario sequence is completed successfully. Once both likelihood layers have been evaluated, the overall likelihood is obtained from the average of both values rounded up to the next integer. Both likelihood layers related to a threat scenario can be estimated and realised according to the scales shown in Table 4.

Table 4: Likelihood scales.

Scale	Exposure	Potentiality
1	Very rare	Very unlikely - practically impossible
2	Rare	Unlikely – very low chance
3	Occasionally	Likely - possible
4	Frequently	Very likely – high chance in medium term
5	Continuous	Certain - high chance in short term

The impact and likelihood scoring shown in the first column of tables (Tables 4 to 8) is subjective and depends on definition of scales above, best practices, intuition, and the security experts' knowledge. Once the likelihood and impact of each threat has been assessed, the risk-level can be calculated using Table 25 given in the SecRAM Guidance document [17].

VI. Security Controls

As stated in [8], treatment actions or security controls are defined to protect supporting assets. They are a collection of measures for managing risks and to ensure the security objectives are met. They include, but are not limited to, procedures, policies, more robust technical solutions, and management actions. The security objective level comes from the definition of the Impact Area such as performance, economic, etc., see [8]. A security need is defined whether a risk needs to be treated or not; when the level of a risk is higher than the security objective of a supporting asset (i.e. the lowest security objective it is targeting), a treatment shall be applied.

The risk treatment option should be selected from the actions defined in step 8 of Section II (i.e. Tolerate, Reduce, Avoid, or Transfer). Normally, the "Tolerate" option for the threats with 'Low' risk level and the "Reduce" option in combating threats with 'Medium' and 'High' risk levels are selected to meet security objective levels.

In defining the security controls, it is important to take into account the three parameters (i.e., likelihood, impact, and risk-level). For example, if the likelihood is high and impact is low, but risk level is high, the security control should be primarily defined to counter the likelihood and it could overlook the impact. Once the type of treatment has been evaluated, the best set of security controls must be chosen.

In this paper, we only show security controls for threats with a risk-level of high. This is to reduce the risk level to the acceptable level that corresponds to the security objective of supporting assets. The most feared and critical threat scenarios are with the risks evaluated as High with low security objectives. These should have high priority in treating them. The security controls are iteratively identified, firstly through the application of MSSCs developed by SESAR [9] and then - in case the level of risk was not reduced enough - through the definition of additional technical, organisational or procedural security controls. The latter come from three sources: newly

identified or devised security controls or through refinement of the MSSCs. Table 4 to Table 8 show the results of security assessment for T-IMC1 to T-IMC5 respectively and the relevant MSSCs that must be put in place to reduce the risk level from High to Low. More details about these specified security controls are given in GAMMA deliverable D2.3 [4]. In these tables, the first column shows the Impact, Likelihood, Risk level, and Security Objective. The second column shows the Supporting Asset (SA), the third column shows the relevant C, I, or/and A as security requirement, and the forth column describes the Security controls to protect the SA.

Table 5: Defined Security Controls for threat T-IMC1.

	SA	CIA	MSSC Description for T-IMC1
Impact = 5, Likelihood = 3, Risk Level = High, Security Objective = Low	IMC	C	Authorise connections to ATM network and to IMC
	CMS	C	Protect ATM system and IMC documentation against unauthorised access
	IMC	CI	Protect messages from unauthorised access and modification
	Internal BUS	CI	Monitor the use of ATM services and IMC
	CMS	CI	Restrict access to the IMC to authorised users only
	IMC	I	Change management process on ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM system and IMC prior to acceptance
	IMC	I	Protect IMC and ATM against malicious code
	CMS	I	Control management process for ATM and IMC to prevent malicious software changes
	IMC	I	Security test ATM and IMC after updates to prevent malicious changes
	IMC	I	Users required to report any observed or suspected security weaknesses or malfunctions in IMC system or services.
	IMC	A	Test back-up copies of IMC software regularly

Table 6: Defined Security Controls for threat T-IMC2.

	SA	CIA	MSSC Description for T-IMC2
Impact = 5, Likelihood = 4, Risk Level = High, Security Objective = Low	IMC	C	Authorise connections to ATM network and to IMC
	CMS	C	Protect ATM system and IMC documentation against unauthorised access.
	Internal BUS	CI	Protect information exchange
	Internal BUS, RoS, RaS	CI	Protect messages from unauthorised access and modification
	Internal BUS	CI	Monitor the use of ATM services and IMC
	IMC	CI	Restrict access to the ATM to authorised users only
	IMC	I	Change management process on ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM system and IMC prior to acceptance
	CMS	I	Protect IMC and ATM against malicious code
	IMC	I	Control management process for ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM and IMC after updates to prevent malicious changes
	IMC	I	Users required to report any observed or suspected security weaknesses or malfunctions in ATM systems or services
	IMC	A	Test back-up copies of ATM and IMC software regularly

Table 7: Defined Security Controls for threat T-IMC3.

	SA	CIA	MSSC Description for T-IMC3
Impact = 5, Likelihood = 3, Risk Level = High, Security Objective = Low	CMS	CI	Secure access controls. ATM and IMC only accessible by authorised personnel
	IMC	I	Change management process on ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM system and IMC prior to acceptance
	CMS	I	Protect IMC and ATM against malicious code
	IMC	I	Control management process for ATM and IMC to prevent malicious changes
	IMC	I	Security test ATM and IMC after updates to prevent malicious changes
	IMC	I	Users required to report any observed or suspected security weaknesses or malfunctions in ATM systems or services
	CMS	CI	Secure access controls. ATM and IMC only accessible by authorised personnel

Table 8: Defined Security Controls for threat T-IMC4.

	SA	CIA	MSSC Description for T-IMC4
Impact = 5, Likelihood = 3, Risk Level = High, Security Objective = Low	CMS	CI	Monitor and record privileged operations
	CMS	C	Users must protect their authentication information or devices.
	CMS	CI	ATM accessible to authorised users only
	CMS	CI	Restrict the use of utility programs that might be capable of overriding system and application controls
	IMC	CI	Users shall ensure that unattended equipment has appropriate protection.
	CMS	I	Protect log files
	IMC	A	Test back-up copies of ATM and IMC software regularly

Table 9: Defined Security Controls for threat T-IMC5.

	SA	CIA	MSSC Description for T-IMC5
See *Note 1*	All IMC's wireless communication links	CIA	Use anti-jamming techniques; it is out of scope of this paper

Note 1: In Table 9, the related parameters are: Impact = 5, Likelihood = 3, Risk Level = High, and the Security Objective = Low.

From the above tables, the threats can be mitigated using existing mechanisms to be considered as built-in security controls/enablers for IMC, to satisfy the stated security requirements (see Figure 2). The GAMMA deliverable D4.3v2 provides more details of functional architecture and interactions of its components for embedding the defined security controls in the fabric of IMC [4].

To summarise, the security controls specified in Tables 4 to 8 can be categorised as below:

- Authenticating users of the IMC.
- Controlling access to the resources via access control mechanisms.
- Using cryptographic protection to protect the confidentiality and integrity of assets. This requires the services of a Key Manager.
- Monitor and control the relevant processes in the IMC.

The risks can be reduced by performing monitoring of activities to identify activities that are not expected and then take actions against them.

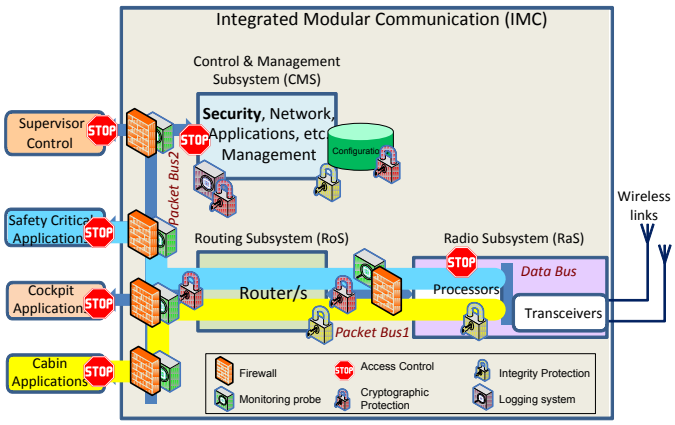

Figure 2: The IMC architecture with security controls.

VII. Validation, Verification, and Evaluation

The general aim of GAMMA is to validate, verify and demonstrate the security related capabilities introduced in the project (including those of the IMC) for future ATM context. Validation is regarded as the process of checking whether the proposed solution satisfies the identified requirements. Verification is the process of checking whether the proposed solution complies with the design specification in order to function correctly as expected. Evaluation is the process of determining that the proposed solution meets the desired quality and performance characteristics. It should be noted that there is always a trade-off between security and performance, as the security mechanisms introduce additional delay in processing and forwarding messages. These three processes are crucial for understanding the implications of applied methods. The overall assessment of the project outcome will be carried out following the European Operational Concept Validation Methodology (E-OCVM) [18] currently used within SESAR.

The plan for validation exercises and the validation platform are given in GAMMA project deliverables D5.1 and D5.3 respectively [4]. In the final stage of the project, the applicability of the project outcome will be demonstrated and experts' knowledge will be used to validate the effectiveness of security controls in reducing the risks and in satisfying the identified security requirements.

VIII. Conclusions

In this paper, we described the use of a security risk assessment methodology (SecRAM) and performed a study to identify and prioritise run-time threats to the IMC. Using this methodology step-by-step, we identified possible threats to IMC, assessed the risk levels related to these threats, and identified the security controls to bring the high risk levels down. We established that some of the threat scenarios require monitoring to reduce the threat risk levels. In order to realise the security state of IMC's network system, monitoring should be carried out for observing and gathering data from different indicators, processing events, identifying adversary activities, and possible damages. Work is being conducted in the GAMMA project to implement a number of security-enabled prototypes including an emulated IMC relevant to the ATM context for validation purposes individually and collectively.

Acknowledgment

Work towards this paper was partially funded by the Commission of the European Union, FP7 Collaborative GAMMA Project, 312382. The authors would like to thank their project partners in the development of work presented in this paper.

References

[1] SANDRA project - Seamless Aeronautical Networking through integration of Data links Radios and Antennas, http://sandra.aero/2013/.

[2] SINCBAC Project - Secure Integrated Broadband and ATM Communications, http://gtr.rcuk.ac.uk/projects?ref=101290.

[3] HARNet project - Harmonised Antennas, Radios, and Networks, Innovate UK, http://gtr.rcuk.ac.uk/projects?ref=113029.

[4] GAMMA (Global ATM Security Management), http://www.gamma-project.eu/; Project Deliverables, D2.1: "Treat Analysis and Evaluation Report", Jan. 2015; "D2.3: Risk Treatment Report", Jan. 2015; D4.3: "ATM Solution Architecture model – Version 2", April 2015; D5.1, "Validation Excersies Plan", D5.3: Validation Platform Architecture Definition".

[5] SESAR (Single European Sky ATM Research) collaborative project, SESAR website: http://www.sesarju.eu/.

[6] NATO Architecture Framework (NAF) Version 3.0, Nov. 2007, https://en.wikipedia.org/wiki/NATO_Architecture_Framework,

[7] MEGA (Model Based System Engineering) tool, http://www.mega.com/en/consulting/model-based-system-engineering.

[8] SESAR Joint Undertaking, "SESAR ATM Security Risk Assessment Methodology" – Project 16.02.03 D02, 2013, SESAR website: HTTP://WWW.SESARJU.EU/.

[9] SESAR ATM Project 16.02.05-D137, SESAR Minimum Set of Security Control, SESAR website: HTTP://WWW.SESARJU.EU/.

[10] ISO/IEC 31010: Risk management - Risk assessment techniques, Geneva, International Organization for Standardization & International Electrotechnical Commission, 2009, preview on line: https://www.iso.org/obp/ui/#iso:std:iec:31010:ed-1:v1:en

[11] National Institute of Standards and Technology (NIST), "Guide for Conductig Risk Assessment", Special Publication 800-30 Rev. 1, Sept. 2012, available on line: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[12] The MITRE Institute, "Risk Management", System Engineering Guide, Sept. 2013, available on line: http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management.

[13] European Network and Information Security Agency (ENISA), "Risk Management: Implementation principles And Inventories for Risk Management/Risk Assessment methods and tools", June 2006.

[14] A. Marotta, et al., "Applying the SecRAM Methodology in a Cloud-based ATM Environment", Eighth International Conference on Availability, Reliability and Security (ARES), Regensburg Germany, pp. 807 – 813, Sept. 2013.

[15] D. J. Bodeau, and R. Graubart, “Cyber Resiliency Assessment: Enabling Architectural Improvement”, MITRE Technical Report, May 2013, available on line: http://www.mitre.org/publications/technical-papers/cyber-resiliency-assessment-enabling-architectural-improvement.

[16] Bristish Sandard, “ISO/IEC 27005”, 1st edition, chapter 7 (guidance for establishing the context), 2008, available on line: www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf.

[17] SESAR Joint Undertaking, “SESAR ATM SecRAM Implementation Guidance Material”, D03, Edition 00.02.06, May 2013, Project 16.02.03, SESAR official website: HTTP://WWW.SESARJU.EU/.

[18] E-OCVM, European Operational Concept Validation Methodology E-OCVM, 3rd Edition, February 2010.