2019 HAWAII UNIVERSITY INTERNATIONAL CONFERENCES
SCIENCE, TECHNOLOGY & ENGINEERING, ARTS, MATHEMATICS & EDUCATION JUNE 5 - 7, 2019
HAWAII PRINCE HOTEL WAIKIKI, HONOLULU, HAWAII

CYBER SECURITY RISK ASSESSMENT FOR THE CONTINUING AIRWORTHINESS

KLIM, ZDZISLAW
SKOREK, ADAM
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
UNIVERSITÉ DU QUÉBEC À TROIS RIVIÈRES
TROIS-RIVIÈRES, QUÉBEC
CANADA

Dr. Zdzislaw H. Klim

Prof. Adam W. Skorek

Department of Electrical and Computer Engineering
Université du Québec à Trois-Rivières
Canada

Cyber Security Risk Assessment for the Continuing Airworthiness

Synopsis

The basic role of the Cyber Security Risk Assessment within the Airworthiness Security Process is to provide an evidence that the security measures implemented into aircraft systems are enough to mitigate the risk to an acceptable level. To establish that the cyber security risk of the aircraft is acceptable, the likelihood and the severity of the threat conditions are considered, and the conclusion based on the risk matrix is driven when the cyber security risk is acceptable or not.

Cyber Security Risk Assessment for the Continuing Airworthiness

Zdzislaw H. Klim & Adam W. Skorek

Université du Québec à Trois-Rivières (Canada)

Keywords: aircraft cyber security, risk matrix, IT risk analysis, IT risk management, threat analysis

ABSTRACT

The cyber security risk assessment process provides a step-by-step approach to determine if an unsafe condition, due to the cyber security issue, exists for aircraft in service. The methodology defines when and how the risk assessment process is to be used to determine if an unsafe condition exists and what risk level is associated with the aircraft fleet. Conducting the cyber security risk assessments for aircraft fleet includes several specific tasks as the threat sources and threat events identification, the vulnerability of the aircraft systems assessment, the description of the threats conditions as well as their likelihood and severity assessment. The last task consists of the cyber security risk level evaluation based on the predefined risk levels matrix.

The threat events are characterized by the threat sources that could initiate the events that have the potential for causing undesirable consequences or impact. These threat events must be defined with enough detail to accomplish the purpose of the risk assessment. To enable effective risk assessment accomplishment, the general and specific descriptions of threat events must identify how each event could potentially harm organizational operations and assets including mission or functions.

A security measure is a feature, function or procedure used to mitigate security risk, even if it was not implemented specifically for that purpose. The vulnerabilities are defined and assessed against the implemented security measure. Therefore, the determination of the vulnerabilities is based on the analysis of the effectiveness of all security measures built into system. The logic of the security architecture access points, assets, security measures, and interdependencies between security measures and their supporting assets can be captured by identifying the protection against cyber security attack.

The threat scenario is a specification of intentional unauthorized electronic interaction, consisting of the contributing threat source (attacker/hacker), vulnerabilities, operational conditions, and resulting threat events by which the target was attacked. The list of all relevant threat scenarios should be completed to obtain a correct risk overview. The impact of an attack on safety or safety margins is due to the changes in the condition of the assets caused by the attack. These changed conditions are the threat conditions. The ultimate impact of the given threat condition may be evaluated by the loss of availability, integrity or confidentiality.

Finally, the level of threat of a threat condition is determined by its likelihood of occurrence and severity of impact magnitude. The risk level matrix combines the likelihood and severity of the threat condition under analysis and provide the cyber security risk level.

1. INTRODUCTION

The purpose of the risk assessment process is to establish a risk management plan to maintain an acceptable safety level of the fleet throughout the aircraft fleet life-cycle. By recording the risk and implementing the mitigation plan, an agreement between the Certification Authority and Aircraft Manufacturer can be reached more quickly, with timely action more likely to be successful. The risk assessment process provides the guidance for estimating the risks associated with identified unsafe conditions; defining, prioritizing, and selecting suitable corrective actions for all identified unsafe conditions; and verifying that the corrective actions were effective.

Aircraft in the twenty-first century are amazingly complex machines built with increasingly many types of electronic subsystems. These systems are often interconnected to external participants through radio frequencies, datalinks, satellite links, or other communication means. While the information sharing between systems provided by the continuous advance of technology allows aircraft new capabilities and efficiencies that were unreachable in the past, these same technologies provide vulnerabilities through which an aircraft can be attacked. Information system assurance is a critically important requirement not only for the typical information systems we use every day, such as banking, finance, industry, entertainment, shopping and social networking, but also for airborne systems [1].

As the 21st century progresses, computer systems have become a target for a new type of criminal who attacks software with malicious intent. Reliability requires that a system "perform adequately under the operating conditions encountered". For modern computer systems the "conditions encountered" increasingly are a hostile operating environment in which criminals attempt to gain unlawful access to, or modify the information stored on the system or to make the system unusable for its intended purpose. The threats include an array of different types of malicious software ("malware") such as: computer viruses, Internet worms, Trojan horses, logic-bombs and spyware, as well as methods of attack such as the creation and use of zombies, denial of service attacks, phishing, and spoofing to name only a few [2].

The risk management allows the detection of actions, which could reduce the risk and mitigate the consequences of an attack. A good risk management approach leans on risk assessment composed by three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment. A threat assessment identifies and evaluates threats based on various factors, including capability and intentions as well as the potential lethality of an attack. A vulnerability assessment is a process that identifies weaknesses that may be exploited by terrorists and suggests options to eliminate or mitigate those weaknesses. A criticality assessment is a process designed to systematically identify and evaluate an organization's assets based on their values, the importance of its mission or function or the significance for a safety [3].

The risk assessment identified the threats, vulnerabilities, inherent risks, and the controls that may be used to mitigate the risks encountered in the system. It provides a basis in which core architectures, standards, and technologies may be evaluated in a consistent manner regarding security. The risk assessment process provided a thorough qualitative and quantitative evaluation of threat-sources, vulnerabilities, risks, and controls associated with the systems [4].

Formal assessment of risk considers the impact of the threat, the likelihood of it occurring and the consequences of it occurring. It is not possible to eliminate every potential threat through detection or mitigation, so it needs to be determined which risks are acceptable, which need management, and which must be eliminated to the greatest extent possible [5].

Risk is the likelihood of threats exploiting vulnerabilities, causing loss of confidentiality, integrity and availability, and possibly resulting in impact on businesses. Risk management in information security has become a strategic issue for organizations, due to demands from the market, the government, regulatory agencies and from clients and, hence, this process must be constantly improved and widely understood [6].

A key problem in the security analysis is the tendency to take a selective approach to risk assessment, focusing almost exclusively on imagining hazard scenarios and then analyzing the prospective consequences. There is relative neglect of several steps that are crucial for risk assessment to have any real credibility: establishing and trying to quantify threat likelihood, evaluating risks, setting risk acceptance criteria and establishing how much risk is likely to be reduced as a result of the security measures [7].

2. CYBER SECURITY RISK ASSESSMENT PROCESS

The procedure to conduct the cyber security risk assessment defines and describes all activities that are necessary to understand the risk issue and to evaluate the risk level. Conducting the cyber security risk assessments for aircraft fleet includes the following specific tasks:

1) Identification of threat sources that are relevant to the aircraft operation;
2) Identification of threat events that could be produced by those sources and can affect the aircraft operation;
3) Identification of security measures;
4) Identification of vulnerabilities within aircraft as well as within the aircraft system operation;
5) Identification of threats scenarios;
6) Identification of threats conditions;
7) Determination of likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
8) Determination of adverse impacts to aircraft systems resulting from the exploitation of vulnerabilities by threat sources and through specific threat events;
9) Determination of security risks at the aircraft level as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation.

2.1. Identification of Threat Sources

From an aircraft cyber security point of view the potential threat sources can be identified mainly at the aircraft system level including the threats related to information systems and components, information technologies and networks. There could be considered also as the threat source an environment of aircraft operation, for instance the common infrastructure, common controls and external dependent networks.

There are two types of threat sources of concern in the security risk assessment: the adversarial and non-adversarial threat sources. An adversarial threat source is an intent or method targeted at the intentional exploitation of vulnerability and the non-adversarial is considered as a situation that can mistakenly trigger vulnerability.

2.1.1. Adversarial Threat Source

The adversarial threat source can be characterized by the adversary capability, adversary intent and adversary targeting. The assessment scales to assess the risk factors of adversarial threat sources regarding capability, intent and targeting are usually defined. These scales are qualitative and might be defined at five levels as very high, high, moderate, low and very low [10].

2.1.2. Non-adversarial Threat Source

The non-adversarial threat source is related to an erroneous action taken by individuals during executing their everyday responsibilities and resulting in an accidental threat source. Another non-adversarial threat source can be triggered by failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters or conditions. The non-adversarial threat source must be assessed by the potential range of effects from the threat sources. The assessment scales to assess the range of effects for non-adversarial threat sources are qualitatively defined similarly to the adversarial threat source.

2.2. Identification of Threat Events

The threat events are characterized by the threat sources that could initiate the events that have the potential for causing undesirable consequences or impact. These threat events must be defined with enough detail to accomplish the purpose of the risk assessment. Multiple threat sources can initiate a single threat event. Conversely, a single threat source can potentially initiate any of multiple threat events. Therefore, there can be a many-to-many relationship among threat events and threat sources that can potentially increase the complexity of the risk assessment.

To enable effective risk assessment accomplishment, the descriptions of threat events must identify how each event could potentially harm organizational operations and assets including mission or functions. To perform the likelihood assessment, it is required to identify each pairing of threat source and threat event separately since the likelihood of threat initiation and success could be different for each pairing. Alternatively, it is possible to identify the set of all possible threat sources that could potentially initiate a threat event.

2.3. Identification of Security Measures

The security measures that will be in place to prevent, detect, or respond to the attack are used to mitigate or control a threat condition. A security measure is a feature, function or procedure used to mitigate security risk, even if it was not implemented specifically for that purpose. In addition to aircraft systems, a security measure may also include operational requirements within the security environment (features, policies, or procedures documented in security guidance).

Types of security measures include, but are not limited to [9]:

a) Deterrent – the aim is to discourage a malicious user from causing an unauthorized event. One example is the policy or law frequently displayed when a user starts a session.
b) Preventive – all measures intended to prevent an occurrence of unauthorized events.
c) Detective – all measures intended to detect and report an unauthorized event. This includes monitoring and auditing of security logs, and file integrity checkers.
d) Corrective – all measures intended to react to an occurrence of unauthorized events or a security policy violation. For example, after incident detection, a new rule on the firewall is setup to block the malicious access.
e) Restorative/recovery – after the occurrence of a security event, all measures intended to put the system back into a normal state. For instance, if the integrity of data is lost, the data could be restored from a trusted backup.

The technical requirements for the security measures define the features and attributes of the security measures. They are validated through an analysis showing that the chosen design will work correctly as required by the threat scenarios for the system.

This includes considerations of whether the strength of mechanism is enough for the threat sources, such as the choice of cryptographic protocols, encryption, key length, and those key management mechanisms used to generate, to transport, to load and to protect keys. Another example is the choice of firewall type and its ability to filter effectively according to the network protocols allowed by the network design.

2.4. Identification and Assessment of Vulnerabilities

The vulnerabilities are defined and assessed against the implemented security measures. Therefore, the determination of the vulnerabilities is based on the analysis of the effectiveness of all security measures built into system. The logic of the security architecture access points, assets, security measures, and interdependencies between security measures can be captured by identifying the implemented protections.

The vulnerability in the context of the aircraft security risk assessment is any flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (unintentionally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. The primary purpose of vulnerability identification and assessment is to understand the nature and degree to which organization, mission and information systems are vulnerable to threat sources identified and the threat events that can be initiated by those threat sources.

The vulnerabilities are commonly found in the hardware, software, and firmware components of information systems or in the environments in which the systems operate. The vulnerabilities associated with architectural design and mission or business processes can have a greater impact on the ability of organization to successfully carry out missions and business functions due to the potential impact across multiple information systems and mission environments.

2.4.1. Vulnerability designation

Inherent vulnerabilities are intended conditions of the system that can be exploited by an attack. They occur because of operational considerations or external events which are part of the standard operation and environment of the airplane and its systems, even if those standard conditions are not probable. Every time there is an interface, or just a logical dataflow, between the system and its external elements, that interface might result in an inherent vulnerability for the system. Processes by which software or application data is loaded or modified might also have inherent vulnerabilities.

To discover the assets vulnerabilities, it is recommended to consider all functions with data flows or interfaces, physical or logical, to entities that are in a different security domain with a lower security assurance. Each such dataflow represents an inherent vulnerability that could be exploited by an attacker, therefore all network layers should be considered in the analysis. The well-known vulnerabilities are those vulnerabilities that have been documented in previous use of items within the system. A baseline of these should be established prior to the final security vulnerability assessment as part of the certification security assessment baseline. Available public databases may be used, along with vendor notifications.

2.4.2. Vulnerability assessment

A vulnerability assessment does not classify vulnerabilities according to risk, severity or likelihood. Instead a set of classification attributes is defined to support risk analysis proceeding at higher levels of the development. A minimum objective is that different people at different times can identify, evaluate and classify vulnerabilities for a specific type design and arrive at similar results. This facilitates the evaluation of the final implementation and provides a basis for ongoing evaluation as service history accumulates.

The identification and classification include a description of the resulting effects on the system if the vulnerability is exploited by attack along with a classification of the attributes of the vulnerability related to exposure, exploitability, and scope. Several industrial standards have been developed that are used the vulnerability databases. An industrial standard that is compatible with well-known vulnerability databases may be used as part of the assessment. One of the classification standards that may be considered include CVSS, the “Common Vulnerability Scoring System”, Version 3.0, May 2015 [11].

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. The CVSS, v3.0 provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three metric groups, Base, Temporal and Environmental, each consisting of a set of metrics.

The purpose of the CVSS Base Metric Group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: Exploitability metrics and Impact metrics, as shown in figure 1.

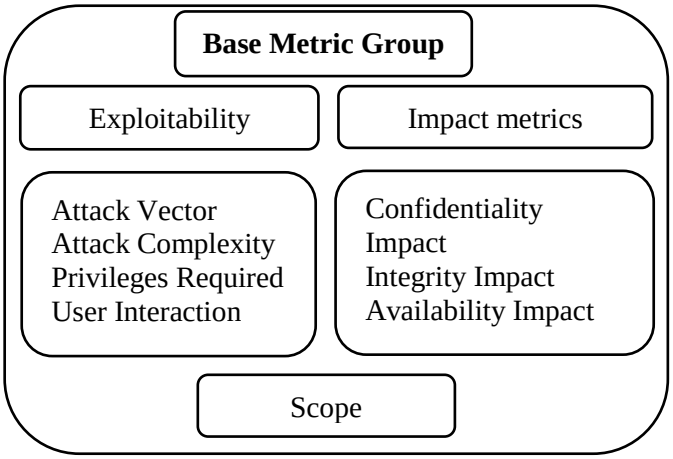

Figure 1. CVSS v.3 Base Metric Group [11]

The Exploitability sub-score from CVSS v.3.0 can be used for the Vulnerability Assessment expressed by the Likelihood of an effort to exploit the vulnerability once the attack is initiated. The exploitability sub-score range values vary from 0.1 up to 3.9. The likelihood categories were defined using these range of values as follows:

Table 1. Likelihood category according to the CVSS exploitability sub-score

Exploitability Sub-score CVSS v.3.0	Likelihood Category
3.15 – 3.90	Frequent
2.39 – 3.14	Probable
1.63 – 2.38	Remote
0.87 – 1.62	Extremely Remote
0.10 – 0.86	Extremely Improbable

The defined above procedure of the likelihood assessment is related to the likelihood of the threat events resulted in adverse impact following the initiation or occurrence of the threat event. Therefore, the overall likelihood of threat events is a combination of the likelihood of initiation/occurrence and the likelihood of impact.

2.5. Identification of Threat Scenarios

The threat scenario is a specification of intentional unauthorized electronic interaction, consisting of the contributing threat source (attacker/hacker), vulnerabilities, operational conditions, and resulting threat events by which the target was attacked. An attack requires attackers/hackers with access to some aspect or interface of the system. Inherent vulnerabilities are intended conditions of the system that can be exploited by an attack. They occur because of operational considerations or external events which are part of the standard operation and environment of the airplane and its systems, even if those standard conditions are not probable.

The Airworthiness Security Risk Assessment is organized according to the threat scenarios, each of which classifies the pertinent information about potential successful attacks. A threat scenario is organized in terms of:

- Threat source of the attack from security environment
- Identification of the attacker and the security perimeter
- Track of the attack path through the security architecture up to the asset
- Characteristics of the security measures on the attack path that would mitigate the attack (considering the vulnerabilities)
- Final threat conditions that are the effects of the successful attack.

The list of all relevant threat scenarios should be completed to obtain a correct risk overview. The analyst should use a structured methodology to identify relevant threat scenarios with the appropriate validation actions to ensure completeness. The logic of the security architecture access points, assets, security measures, and interdependencies between security measures and their supporting assets should be captured by identifying the system protection and the potential vulnerabilities.

In the case of multi-stage attacks on security architectures with layers and defense in depth, the initial attacks will need to compromise supporting assets to obtain the necessary capabilities to launch additional attacks

to reach the target assets, as shown in Figure 2. To focus attention on the security architecture itself, the diagram is simplified to show only the assets and security measures themselves.

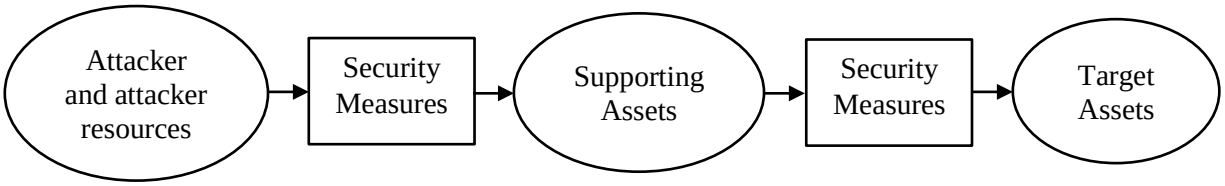

Figure 2. Two stages threat scenario [9]

To perform the security risk assessment, it is important to gather the full set of data necessary to assess each stage of protection (security measures) and to generate the additional data for assessing the next stage of the threat scenario and up to the final target assets threat condition. When evaluating the protections, the presence of a security measure implies an associated failure condition if the measure is defeated. The resulting threat condition is evaluated as to airplane level impact – that is, the severity of the specific resulting threat condition, which maps directly to a failure condition.

2.6. Identification of Threat Conditions

The impact of an attack on safety or safety margins is due to the changes in the condition of the assets caused by the attack. These changed conditions are considered to be the threat conditions. The specific definition of the threat condition can be formulated as follows [9]:

A condition having an effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more acts of intentional unauthorized electronic interaction, involving cyber threats, considering flight phase and relevant adverse operational or environmental conditions.

Therefore, the "threat condition" is analogous to "failure condition" as defined in CFR Title 14 25.1309 [12] and EASA CS-25 25.1309 [13]. However, where "failure conditions" result from natural causes (e.g. a part failure), the "threat conditions" result from intentional unauthorized electronic interaction.

The security risk assessment is based on judging the severity of attacks on the safety of the aircraft. However, the complexity of an aircraft, or even of a common aircraft system or item, is high enough that it is not a simple thing to judge the safety of an aircraft. The standard approach is to classify the final conditions (threat conditions) severity that immediately contribute to the airworthiness of the aircraft, and to classify the severity of the impact of all other events in terms of these top-level conditions. There is a similarity between the aircraft and systems safety assessment and security assessment.

Many of the top-level threat conditions may occur through failures and will be documented as failure conditions as indicated in Table 2, so that any list of threat conditions can start with a list of failure conditions. A safety analysis considers the following main classes of failure conditions:

Table 2 – Failure Conditions Classes

Class of Failure Condition	Definition
Loss of function or loss of continuity in function	Intended function is not performed, intended information is not provided, including intermittent failures in the continuity of data over a required service interval
Malfunction	Intended function is performed incorrectly or not provided when or where needed

An airworthiness security risk analysis, on the top of relevant failure conditions, must consider the following classes of threat conditions as indicated in Table 3 and these might lead to the allowed overlap.

Table 3 – Assets and Threat Conditions Classes [9]

Class of Threat Condition	Definition
Loss of Confidentiality	Exposure of information
Unintended function	Unintended function is performed; this includes the presence of malware.
Tampered information	Intended function appears to be performed correctly but is incorrect but satisfies safety integrity mechanisms. Includes coherent corruption.
Spoofed information	Intended information appears to be correct and correctly sent, but either source or destination is incorrect.
Misuse	An intended function being invoked by an unauthorized entity.
Counterfeiting	Tampering with persistent data. Includes but is not limited to coherent corruption of software part or user modifiable data.

2.7. Determination of Likelihood of Occurrence

The level of threat of a threat condition is determined by its likelihood. The likelihood is measured by the qualitative evaluation of how often a successful attack might occur. The definition of likelihood is based on the definition of qualitative probabilities in the family of standards on airworthiness assessment means that includes CFR Title 14 25.1309 and EASA CS-25 25.1309 as Frequent, Probable, Remote, Extremely Remote, and Extremely Improbable [13], not on the derived probabilities per flight hour.

To determine the level of threat of a successful attack for a threat scenario, it is necessary to know the likelihoods of its parts: the likelihood of attack by the threat source, the likelihood that known vulnerabilities will be exploitable by the attack (based on operational considerations and how the capabilities of the attacker match the difficulties of exploiting the vulnerability), and the effectiveness of the security measures. The combined effect on the likelihood of the threat scenario itself will depend on the joint distribution of these likelihoods and the events of the threat scenario.

Therefore, to determine the likelihood that threat events of concern result in adverse impacts, it is necessary to consider the:

a) Characteristics of the threat sources that could initiate the events
b) Vulnerabilities / security measures that were implemented to impede the adverse impact.

The proposed approach employs a three-step process to determine the overall likelihood of threat events. First, the analysis assesses the likelihood that threat events will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events). Second, it is necessary to assess the likelihood that threat events once initiated or occurring, will result in adverse impacts to organizational operations and assets or individuals. Finally, the assessment of the overall likelihood is a combination of likelihood of initiation or occurrence and the likelihood of resulting in adverse impact [10].

The likelihood of threat event initiation must take into consideration the characteristics of the threat sources of concern including capability, intent and targeting. If threat events require more capability than adversaries possess (and adversaries are cognizant of this fact), then the adversaries are not expected to initiate the events. If adversaries do not expect to achieve intended objectives by executing threat events, then the adversaries are not expected to initiate the events. And finally, if adversaries are not actively targeting specific organizations or their missions or business functions, adversaries are not expected to initiate threat events.

An analyst might use the assessment scale from Table 4 and to provide a rationale as well for the assessment allowing explicit consideration of deterrence and threat shifting. The likelihood of threat event occurrence from non-adversarial sources can be assessed by using the similar table and to provide a similar rationale for the assessment.

Table 4 – Likelihood Assessment of an Adversarial Threat Event Initiation [9]

Qualitative Values	Description
Frequent	Adversary is almost certain to initiate the threat event
Probable	Adversary is highly likely to initiate the threat event
Remote	Adversary is somewhat likely to initiate the treat event
Extremely Remote	Adversary is unlikely to initiate the threat event
Extremely Improbable	Adversary is highly unlikely to initiate the threat event

To evaluate the likelihood that threat events resulting in adverse impacts on an asset an analyst might use the assessment scale indicated in Table 1 and to provide a rationale for the assessment allowing explicit consideration. Threat events for which no vulnerabilities or predisposing conditions are identified, have a very low likelihood of resulting in adverse impacts.

As was stated above, the overall likelihood of a threat event is a combination of: (a) the likelihood that the event will occur (e.g., due to human error) or be initiated by an adversary and (b) the likelihood that the initiation or occurrence will result in adverse impacts. For this methodology of the security risk assessment the dedicated scale for assessing the overall likelihood of threat events was elaborated as a combination of the likelihood of initiation/occurrence and the likelihood of impact. The results are provided in the table 5.

Table 5 – Overall Likelihood Assessment of the Threat Condition

Likelihood of Threat Event Initiation or Occurrence	Likelihood of Threat Events Result in Adverse Impacts				
	Frequent	Probable	Remote	Ext. Remote	Ext. Improbable
Frequent	Frequent	Frequent	Probable	Remote	Remote
Probable	Frequent	Probable	Remote	Remote	Ext. Remote
Remote	Probable	Remote	Remote	Ext. Remote	Ext. Remote
Extremely Remote	Remote	Remote	Ext. Remote	Ext. Remote	Ext. Improbable
Extremely Improbable	Remote	Ext. Remote	Ext. Remote	Ext. Improbable	Ext. Improbable

Please note, that the term likelihood, as discussed in this paper, is not likelihood in the strict sense of the term; rather, it is a likelihood score.

2.8. Determination of Severity Levels

The determination of the impact magnitude is considered as the assessment of the severity of effects caused to assets by the successful attack. In the security risk assessment, the severity is considered as a qualitative indication of the magnitude of the adverse effect of a threat condition.

In fact, the impact of an attack can be evaluated based on the analysis of the well-defined threat condition. The threat condition is changing the initial condition of the assets in terms of safety margins. Generally, a threat condition which reduces the effectiveness of a security measure is effectively causing a reduction in safety margin of the assets operation and may have the corresponding severity level.

The severity of impact is Catastrophic, Hazardous, Major, Minor, or No Effect as defined in AMC 25.1309 extended to include the "No Safety Effect" classification. The detailed definition of the severity levels is provided in Table 6.

Table 6 – Definition of the Severity Levels [13]

Term	Definition
No Safety Effect	Would not affect the operational capability of the airplane, and would not increase crew workload
Minor	Slight reduction in safety margins or functional capabilities, or Slight increase in crew workload, or Some physical discomfort to passengers or cabin crew
Major	Significant reduction in safety margins or functional capabilities, or Significant increase in crew workload, or Discomfort or physical distress to passengers or cabin crew, possibly including injuries.
Hazardous	Large reduction in safety margins or functional capabilities, or Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely, or Serious or fatal injury to an occupant other than the flight crew.
Catastrophic	Occurrence of multiple fatalities, usually with the loss of the airplane.

Each threat condition represents the condition of an asset of the system. The classification of a system, which may be an asset, is supplemented by all threat conditions and their respective severity of effect. The most severe threat condition effect determines its overall severity. In the Cyber Security Risk Assessment, the safety aspect, as defined by the 25.1309, is not a unique potential impact related to the Company business. Other specific impacts might be considered also, as financial, operational or legal and the effects on the customer or reputation.

Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. A dedicated scale of the magnitude of effect impacting the integrity, availability and confidentiality must be developed and the magnitude of impact level need to be defined similarly to the severity levels shown in table 6.

2.9. Determination of Risk Level

The risk of an event with adverse effect is unacceptable when an organization or agency will not tolerate the number of times that effect can be expected to occur over the expected span of operation without further mitigation. Within current aircraft regulations, this level of unacceptability is expressed by classifying the adverse effect according to the severity category and requiring that the occurrence likelihood for each severity category be less than a mandated likelihood.

Therefore, if the minimum requirement is met, the risk level is considered *Acceptable* and if the threat scenario occurs with the frequency higher than minimum required for the given severity, the risk level is defined with using one of the four levels: Low, Medium, High, Extremely High. The risk levels defined above, from Low up to Extremely High are considered *Unacceptable* for the given design and the corrective action must be taken to return to the certification level regarding the security issue. For the higher risk levels the allowed time for the rectification must be shorter, with the greatest attention going to high-risk events, therefore the corrective action must be more elaborated, dynamic and well controlled.

The Risk Matrix for a given severity classification and the related likelihood of the threat occurrence was developed according to the logic defined above and is presented in Table 7.

Table 7 – Definition of the Risk Matrix

SEVERITY LIKELIHOOD	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Frequent	Acceptable	Low	Medium	High	Extremely High
Probable	Acceptable	Acceptable	Low	Medium	High
Remote	Acceptable	Acceptable	Acceptable	Low	Medium
Extremely Remote	Acceptable	Acceptable	Acceptable	Acceptable	Low
Extremely Improbable	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable

If the risk is found to be unacceptable, the risk mitigations may be defined to modify or improve the system. The risk acceptability should then be reviewed after updating the risk assessment to consider the modified system. This may repeat until an acceptable risk is found.

3. CONCLUSION

The entire cyber security process is presented as a sequence of the specific tasks of the risk assessment process for clarity. However, in practice, some iteration among the tasks is both necessary and expected. The risk assessment must start by an identification of the potential threat sources at the aircraft system level including the threats related to information systems and components, information technologies and networks. Usually, two types of threat sources of concern in the cyber security risk assessment need to be considered: the adversarial and non-adversarial threat sources. An adversarial threat source is an intent or method targeted at the intentional exploitation of vulnerability and the non-adversarial is considered as a situation that can mistakenly trigger vulnerability.

The vulnerability in the context of the aircraft cyber security risk assessment is any flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (unintentionally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. Vulnerabilities can be identified at varying degrees of granularity and specificity. The level of detail provided in any vulnerability assessment need to be consistent with the purpose of the risk assessment and the type of inputs needed to support follow-on likelihood of the successful attack determination. The identification and classification of the vulnerability includes a description of an easiness that the specific vulnerability is exploited by attack.

The identified risk levels, from Low up to Extremely High are considered unacceptable for the given design and the corrective action must be taken to return to the certification level regarding the security issue. For the higher risk levels the allowed time for the rectification must be shorter, with the greatest attention going to high-risk events, therefore the corrective action must be more elaborated and well controlled.

The cyber security risk assessment is a part of the aircraft information security incident management process and assures that security events and security issues with aircraft systems recorded in the field are communicated in timely manner allowing corrective action. The cyber security risk assessment tool was developed to ensure the continuing airworthiness process for aircraft cyber security evaluation.

REFERENCES

[1] The Charles J. Middleton, *Risk Assessment Planning for Airborne Systems: An Information Assurance Failure Mode, Effects and Criticality Analysis Methodology*, Department of the Air Force Air University, June 2012.

[2] John B. Bowles, William Hanczaryk, *Threat Effects Analysis: Applying FMEA to Model Computer System Threats*, Reliability and Maintainability Symposium, RAMS 2008.

[3] Galileo Tamasi, Micaela Demichela, *Risk assessment techniques for civil aviation security*, Reliability Engineering and System Safety, 96 (2011), 892-899.

[4] Dennis C. Iannicca, Daniel P. Young, Suresh K. Thadhani and Gilbert A. Winter, *Security Risk Assessment Process for UAS in the NAS CNPC Architecture*, 2013 IEEE Integrated Communications Navigation and Surveillance (ICNS) Conference, April 23-25, 2013

[5] Solomon Wong, Nina Brooks, *Evolving risk-based security: A review of current issues and emerging trends impacting security screening in the aviation industry*, Journal of Air Transport Management, 48 (2015), 60-64.

[6] Janice Mayer, Leonardo Lemes Fagundes, *A Model to Assess the Maturity Level of the Risk Management Process in Information Security*, 2009 IFIP/IEEE Intl. Symposium on Integrated Network Management, 61-70.

[7] Mark G. Stewart, John Mueller, *Aviation Security, Risk Assessment and Risk aversion for Public Decision-making*, Journal of Policy Analysis and Management, Vol. 32, No. 3, 615–633 (2013).

[8] RTCA DO-355 Information Security Guidance for Continuing Airworthiness.

[9] RTCA DO-356 Airworthiness Security Methods and Considerations.

[10] NIST SP 800-30 Guide for Conducting Risk Assessments, Information Security.

[11] Common Vulnerability Scoring System v3.0, User Guide, FIRST.Org, Inc.

[12] 14 CFR Part 25 Airworthiness Standards: Transport Category Aircraft, FAR Regulations.

[13] EASA, AMC 25.1309 System Design and Analysis, Acceptable Means of Compliance.

[14] ICAO Doc 9859 – Safety Management Manual (SMM)

ACKNOWLEDGMENTS

Authors acknowledge financial support from the Research Group on Industrial Electronics of the University of Québec at Trois-Rivières.

Dr. Zdzislaw H. KLIM is an Associate Professor and currently teaches reliability at a graduate level in the Department of Mechanical Engineering at the Polytechnique de Montréal. His research interests are in the fields of systems reliability and maintainability analysis, and safety and risk assessment. He is also an Associate Professor at University of Québec at Trois-Rivières (Canada). He was a Principal Engineering Specialist in the Department of Reliability, Maintainability and Safety at Bombardier Aerospace for the past 22 years. His responsibilities included reliability and safety analysis for in-service aircraft systems, technical support for new programs and development of the new methods for reliability, safety and cyber security assessment. He holds Bachelor and Master degrees in Mechanical Engineering and a Ph.D. in reliability from the Technical University of Wroclaw, Poland. He has more than 35 years of experience in the field of reliability, maintainability and safety analysis. He is the author of more than 50 technical papers and reports. He is a Member of the Society of Automotive Engineers (SAE), Association of Professional Engineers of Quebec (O.I.Q.) and a President of the Montreal Chapter of Society of Reliability Engineers (SRE). zdzislaw.klim@polymtl.ca

Dr. Adam W. SKOREK is a Professor in the Electrical and Computer Engineering Department of the University of Québec at Trois-Rivières (Canada) and Director of the Research Group in Industrial Electronics. He founded the Electro-Thermal Management Laboratory (2012) which succeeded both the NanoHeat Laboratory and the UQTR's Industrial ElectroHeat Laboratory founded and directed by himself since 1989. He gives electrical engineering courses for Bachelor, Master and Ph.D. students. He was a Visiting Professor at the Management Faculty of Technical University of Białystok (Poland) where he conducted research and teaching activities in the area of computer applications in industrial processes (2006-2018). His research was granted by the Natural Sciences and Engineering Research Council of Canada (NSERC), the Canadian Foundation for Innovation (CFI), Fonds de recherche du Québec – Nature et technologies (FRQNT), MITACS (Canadian R&D Organization) and industrial corporations including Bombardier, IBM, ABB, Hydro-Québec, ALCAN and Ontario-Hydro. He has published and co-published over 130 papers including works on High Performance Computing analysis of electro-thermal phenomena and reliability. He completed a Master of Electrical Engineering Program at Białystok University of Technology (Poland) receiving both Master and Bachelor engineering degrees in 1980. He received his Doctor degree of Technical Sciences in Electrical Engineering from the Warsaw University of Technology (Poland) in 1983. He is a Fellow of the IEEE, a Fellow of the Engineering Institute of Canada and a Member of the Academy of Engineering in Poland. Adam.Skorek@uqtr.ca