Towards Dynamic Cyber Security Risk Assessment of Military Aircraft

Theo Verhoogt, René Wiegers, Judith van Bruggen, Piet Hoogeboom, Nikita Noskov
Netherlands Aerospace Centre
Anthony Fokkerweg 2
1059CM Amsterdam
THE NETHERLANDS

Theo.Verhoogt, Rene.Wiegers, Judith.van.Bruggen, Piet.Hoogeboom, Nikita.Noskov@nlr.nl

ABSTRACT

To support their operation, military aircraft are becoming more and more reliant on advanced on-board software and connection to networks, making cyber-security an essential part of flight operations. This paper describes a preliminary high-level security cyber security risk assessment framework for military flight operations, which is a first step in the development of a dynamic security risk assessment methodology. The framework is based on the notion that vulnerabilities in aerial vehicles make them susceptible for cyber threats, which translates into risks regarding their freedom of movement, ultimately impacting mission assurance. Because of the interdependencies that exist, communication between component, aerial platform and mission layers in a structured way is essential. To enable this, the framework consists of two parts, one part describing the common elements per layer and the second part describing the dependencies and interactions between the layers such as structured exchange of goals, assets and risk information

1.0 INTRODUCTION

Cyber-security has become an essential part of flight operations. The on-board software of military aircraft is getting more complex, there is an in-creasing dependence on networks for operation and the use of unmanned aerial systems is increasing. Not only the systems of the aerial platform itself, but also the systems and procedures in its environment can be the target of a cyber-attack in order to obtain information, mislead, disrupt operations or potentially take control of the aerial platform.

Cyber security risk assessment is used to identify risks, caused by potential threats, which can affect the operation of an organisation. By knowing these risks an organisation can determine if, how, and when they want to mitigate these risks to minimize the impact of a potential threat on their operations to accomplish their goals.

The ultimate goal, from a military operations perspective, would be a dynamic cyber security risk assessment methodology that would minimise the cyber security risks during a mission, maximizing the freedom of movement of the aerial platforms. Looking at the current status in the field of Security Risk Assessment (SRA) methodologies, many different SRA methodologies exist, often ‘optimised’ for one specific domain and/or application [1-7]. This makes standardisation on a common security risk assessment method difficult and complex. Furthermore current security risk assessment processes are rather static and cost a lot of time to execute, which may be less than optimal in the dynamic environment of military flight operations.

A multi-layered risk assessment framework is proposed to help address these challenges. The framework enables a multidisciplinary approach, where risk assessment can be performed in parallel by experts such as mission planners, pilots and aircraft system experts. Communication between the layers in a structured way is essential. To facilitate this, the framework consists of two parts, one part describing the common elements per layer and the second part describing the dependencies and interactions between the layers. By defining the interfaces between the layers, the framework allows experts to apply a risk assessment methodology optimised for their specific field of expertise. The presented approach is based on an evolutionary process, starting from the current status in the field of (cyber) SRA methodologies. As user acceptance is essential, each step will be verified and validated in a representative environment before progressing to the next step.

In this paper, the preliminary cyber security risk assessment framework is described as first step in the development of a dynamic cyber security risk assessment methodology for military flight operations.

2.0 (CYBER) RISK ASSESSMENT FRAMEWORK

Looking at different security risk assessment methodologies, common elements can be discerned, which can be structured in a logical way to describe a high-level security risk assessment framework.

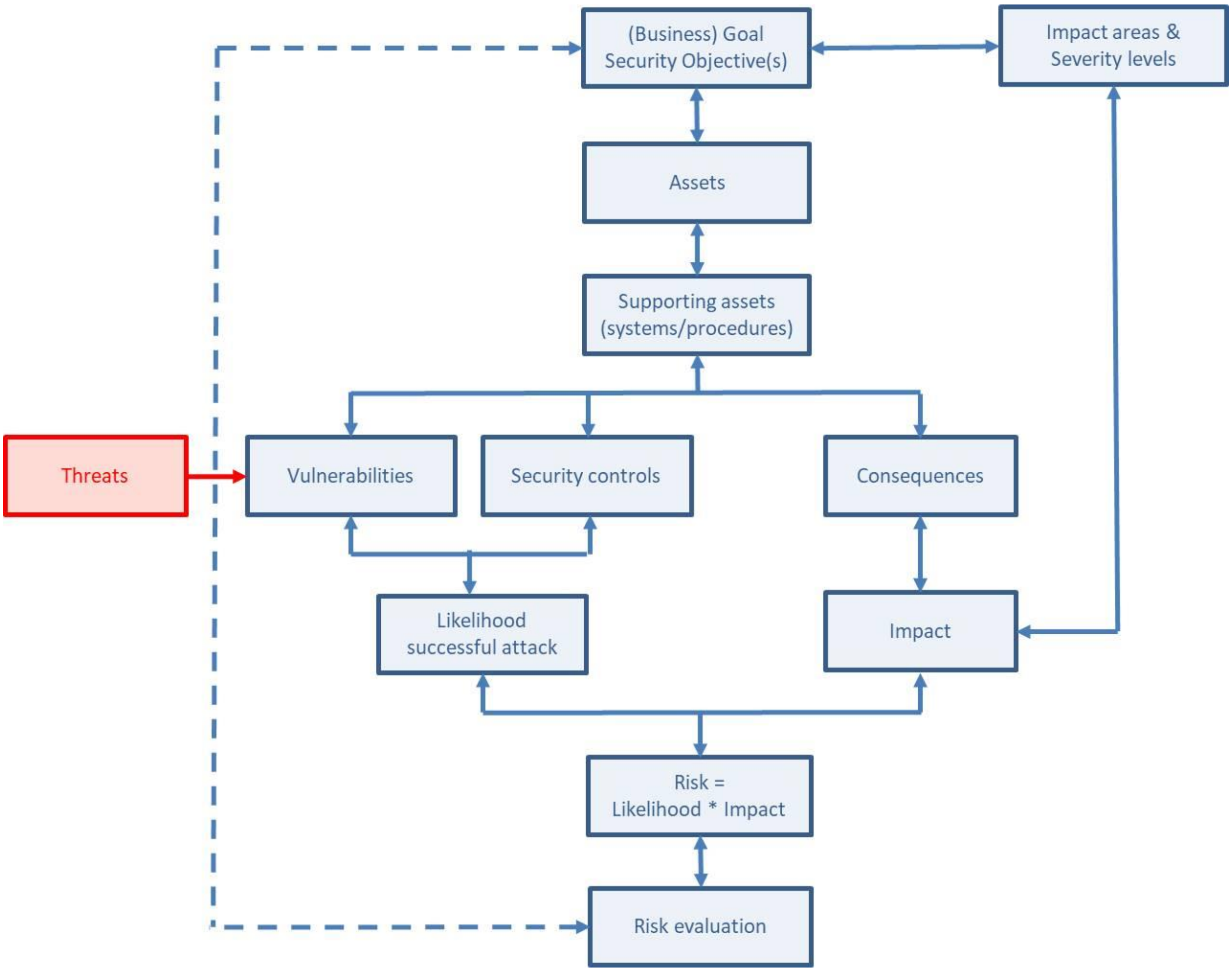

Figure 1: Common Elements.

A problem in describing a high-level framework is often the terminology that is used. A word can have different meanings depending on the domain, experience etc. Very often definitions are used to overcome this problem, but the disadvantage is that it limits the applicability of the high-level description. So in this overview of common elements wording will be used, which in general will be recognisable by all stakeholders, without a clear definition, trying to prevent limiting the scope of each element. Furthermore no descriptions of metrics/units are specified for the common elements. It is up to executive management to define the proper definitions, metrics and units. All common elements should be addressed in one way or another during a security risk assessment.

Starting point is the **Goal**. This can be different for every organisation, management level, person etc. Very often there will be interaction between different levels. For example the high level goal of an organisation can be split into specific goals for different departments etc. Also each lower level will contribute to the overall goal of the organisation. From security perspective the goal is the 'element' that is essential for the 'business', and for this reason should be protected. Because 100% security is impossible it should be determined what the impact is if the protection (partially) failed. Preferably several **Impact Areas** should be defined (such as finance, loss of lives etc.) including **Severity Levels**.

So-called **Primary Assets** are required or are critical to achieve a 'goal'. For example, to perform Close Air Support (the goal) an aircraft is a primary asset. In general each primary asset can be divided into so-called **Supporting Assets**, such as (sub) systems, procedures, but also human actors.

An attack can only be successful if a **Threat** finds a **Vulnerability** in one of the supporting assets and uses this vulnerability to execute the attack. So, in theory, if there are no vulnerabilities in the supporting assets, the primary asset is 100% protected and no threat will impact the goal and no (additional) security means/costs are necessary. For each supporting asset the vulnerabilities shall be identified as well as the **Security Controls** already in place, if any.

Domain knowledge is important to understand the relationships between supporting assets. If a threat exploits a vulnerability of a specific supporting asset, this may affect other/connected supporting assets, and in the end also one or more primary assets. By analysing all the possible combinations an overview can be made of the **Likelihood** per primary asset, that a successful attack will take place, using the vulnerabilities of the supporting assets.

To determine the 'absolute' risk, applied security controls shall be ignored when determining the likelihood. This can be useful for senior management because they have to determine how they will handle the risks (transfer, avoid, reduce or accept). Furthermore it can be used to determine the effect of a security control, by performing a second assessment including the security control.

In parallel to the determination of the likelihood, an assessment should be made what the **Impact** will be if a supporting asset (partially) fails because of a successful attack, expressed in **Consequences**, such as for example confidentiality, integrity and availability for ICT components. By combining these consequences per supporting assets, the impact on the primary asset can be determined, expressed in a severity level of an impact area, as defined at the beginning of the risk assessment process.

The **Risk**, per asset, is defined as the product of likelihood and impact, which will be followed by a **Risk Evaluation** to determine whether, when, and how the risk will be mitigated to accomplish the goal that was set at the beginning.

By combining the risks of each primary asset, the risk that the goal can't be met can be determined. Figure 2 gives a schematic overview of the SRA framework based on the common elements.

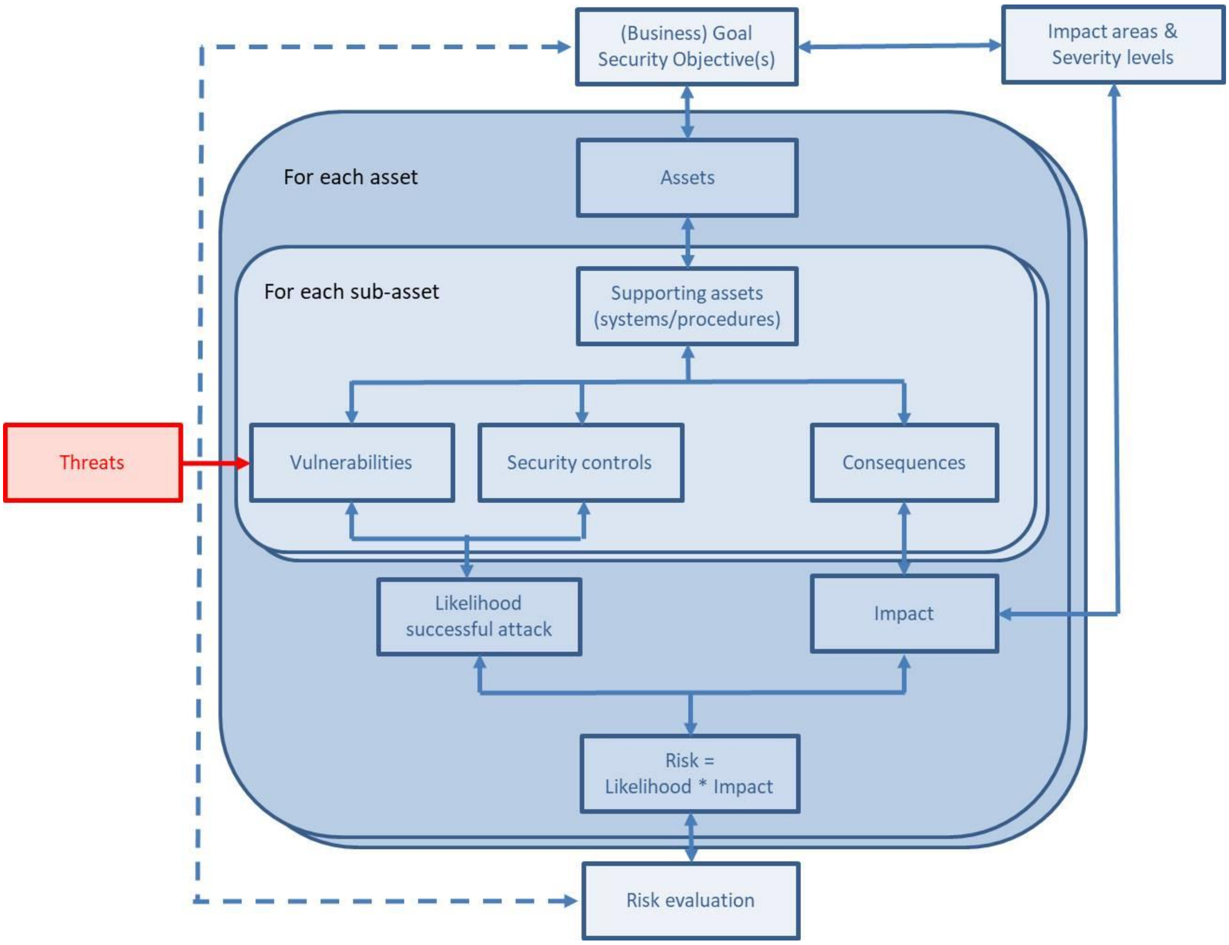

Figure 2: Schematic overview of the SRA framework.

It should be realised that this latest activity, combining risks, is in general not a straightforward process. It is not a simple addition due to the difference in relationships between supporting assets. Of course it is possible to start a SRA from scratch, but very often a lot of information (threat lists, overview of vulnerabilities, overview of security controls etc.) is already available in the organisation.

Security risk assessment should be performed on a regular basis. The first time an assessment is made, considerable time and effort is required, but the following iterations will require less time and effort.
The common elements mentioned above, including the interdependencies between these elements, are the common denominator of all security risk assessment methodologies and are for this reason the building blocks of an SRA Framework.

2.0 INTERACTION BETWEEN LAYERS

Looking at military flight operations, a possible breakdown in (organisational) layers can be:

- Mission
- Aerial platform
- Component

Each layer has its own goal(s). Of course the goal of the lower layer will be derived from the goal of the higher layer, and each lower layer will contribute to the goal of the higher layer. In general this is valid for all SRA common elements. It is possible to start a SRA from the Mission layer and drill down to the lowest layer. This will require a lot of effort and expertise. Each lower layer has its own security requirements and expertise, uses its own vocabulary and can be different for each mission. Therefore it would be easier and more efficient for each layer to perform its own SRA. The advantage is that each layer can use the information already supplied by a higher layer (such as a threat list) and can enrich this information. The multi-layered SRA framework is a framework that will help improve the communication, by a structured exchange of specific information such as goals, assets and risk information between the different layers, but doesn’t exclude the possible use of specific SRA methods.

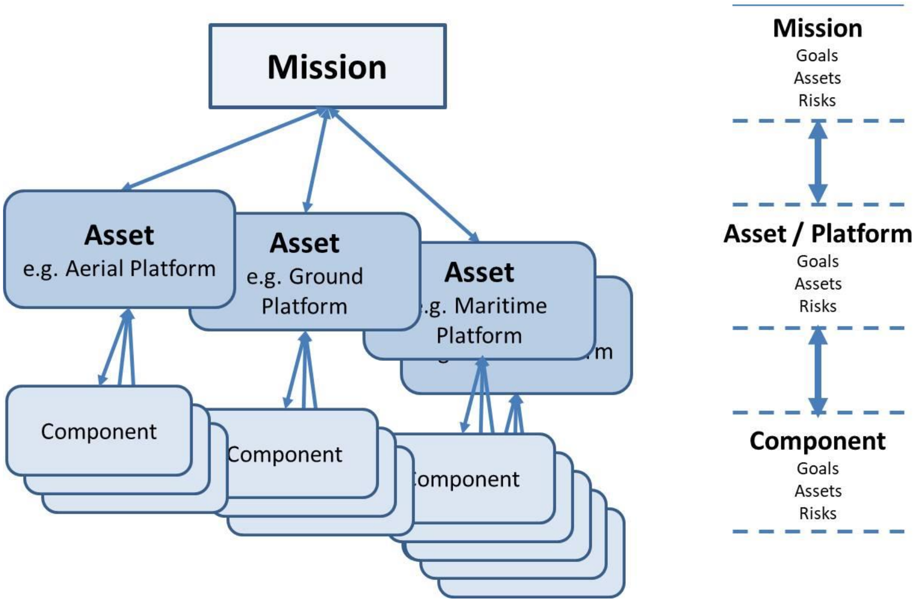

Figure 3: Mission overview and interdependencies.

During the mission preparation and evaluation phase more time is available and it is easier to consult specialist/experts. During the mission execution phase less time and limited specialised expertise are available. For this reason it is wise to make the assessment in the planning phase and determine in this phase what the mitigations will be to overcome the threat during the execution phase, and preferable by predefined threat levels, which makes it easier to react during the mission execution phase.

In general a lower organisational layer can be seen as a supporting asset of the higher level. So the likelihood and impact of this lower layer shall be handled on the higher level in the same way other supporting assets are analysed on that level, with the assumption that the impact of the lower layer is the consequence on the higher level. Also no identification of threat, vulnerabilities and security control has to be performed on the higher level, because it is already done on the lower level. The higher level will, based on the consequences, set the impact areas of the lower level (see Figure 4).

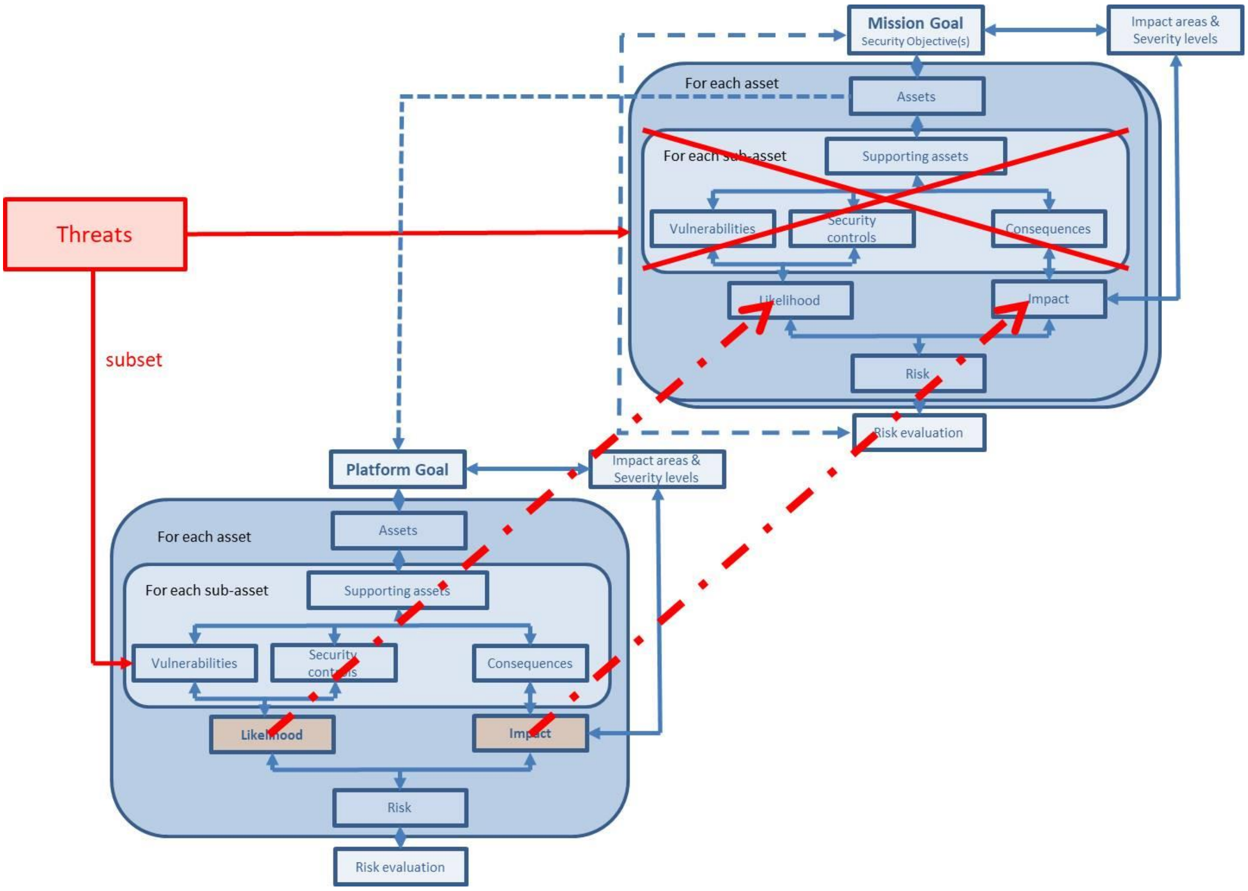

Figure 4: Communication between layers.

4.0 CONCEPT OF OPERATIONS

As the threat environment can change, the ultimate goal is a fully automated response during the execution of a mission. To accomplish this it is necessary that during the preparation phase of a mission all possible threats, risks, mitigation measures etc. are analysed and recorded.

At component layer this environment contains information on existing vulnerabilities, the feasibility to exploit these vulnerabilities and possible impact on the component. The security risk assessment focuses on an in-depth analysis and test of the component. Different attack scenarios are explored to find possible weaknesses, and to verify the effectiveness of implemented counter measures. This is process is repeated regularly.

On the aerial platform layer the experts will define threat scenarios using for example attack trees which provide a systematic way to model possible ways in which a threat can reach its goal. A threat scenario is a functional description of how one or more threats (a person or natural event that can exploit an vulnerability) can influence the aerial platform, resulting in a security event with high impact on the nominal operation of the aerial platform. A threat scenario is the heart of the risk assessment process, because it combines the three components of *impact*, *vulnerabilities* and *threats*. When performed individually, the three components can yield a large set of information. The threat scenario simplifies this process by focusing on high impact security events, significant vulnerabilities and meaningful threats. Processing of the threat scenarios is preferably a fully automated process, using the threats as input to assess and record the consequences of these threats at the component layer. This will determine what the impact and risks will be for an aerial platform. The same mechanism will be also applicable for the mission layer.

It is very important that during the execution phase the risk level can be assessed very quickly if the threat level changes. For this a general key identifying the threat level shall be used as input, a possible candidate can be Information Operations Condition (INFOCON). INFOCON consists of five different levels. For each level the criteria and recommended actions (preventive, mitigation etc.) are described. These criteria and recommended actions shall be made specific for the use of aerial platforms. This means in practice that during the preparation phase the risk assessment should be performed for each threat level as depicted in Figure 5. The idea is that when the threat level changes, the risks and associated mitigating options actions are known, enabling a faster and better informed decision- making process.

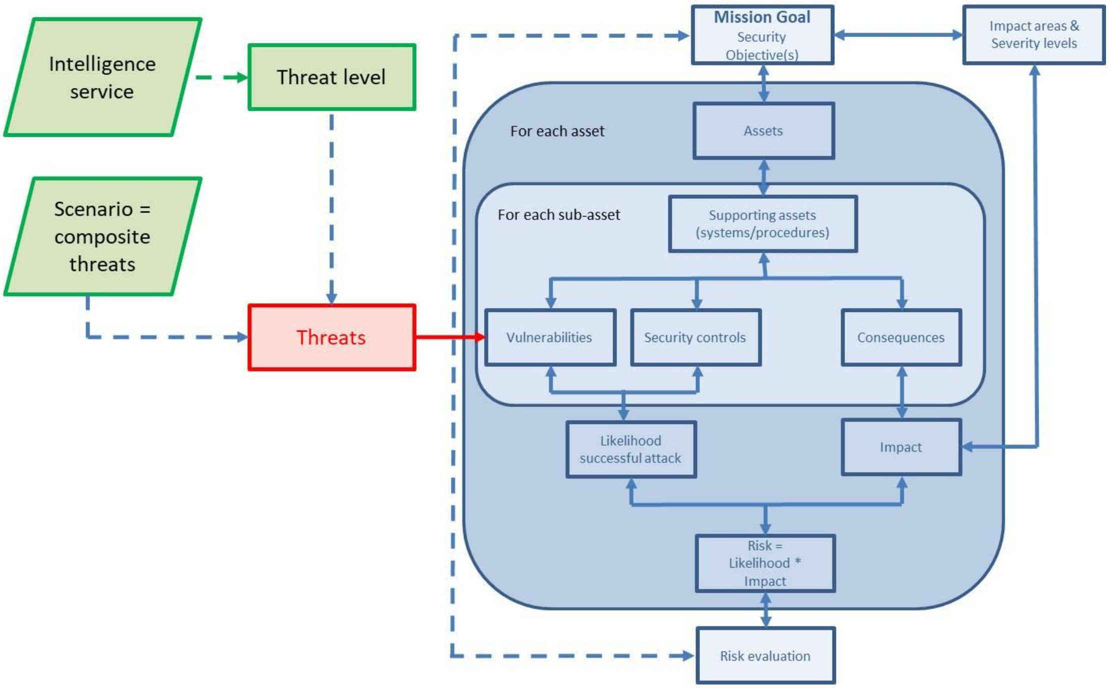

Figure 5: Security Risk Assessment using threat levels.

5.0 VERIFICATION AND VALIDATION

To be able to verify and validate our preliminary cyber security framework, a methodology (describing the risk assessment processes and techniques) implementing this framework is under development in cooperation with the operational experts of the stakeholder. At component level this methodology was verified by assessing two representative aircraft components. The first step consisted of a paper-based assessment, followed by a verification of the results on an actual (physical) system. This enables also the possibility to verify if there are, from security risk assessment point of view, difference in the outcomes of the paper-based and physical-system based assessments. Short-term work includes verification of the interfaces and the interaction between the layers by means of workshops. Workshops involving operational experts of each layer and realistic mission planning scenarios will be used to validate the cyber security framework.

6.0 CONCLUSIONS

In this paper we presented a SRA framework that will be used as starting point for a dynamic (cyber) security risk assessment methodology. Future work includes extension of the risk assessment framework to include the chain of activities in the flight preparation phase and development of tooling and (analysis) methods to support the risk assessment.

7.0 REFERENCES

[1] Dahl, H., M.S. Lund, K. Stølen, V. Meduri, M. Felici, A. Tedeschi, V. Normand, B. Fontan, F. Innerhofer-Oberperfler, F. Massacci, E. Chiarani, D5.1 Evaluation of existing methods and principles, Report for Secure Change, 7th Framework Programme, version 3.0, 31 July 2009.

[2] Elahi, G., Security Requirements Engineering: State of the Art and Practice and Challenges, 2009.

[3] ENISA, Inventory of risk assessment and risk management methods, 2006.

[4] Everdij, M (NLR), Gijsen, B. (TNO), Smulders, A. (TNO), Verhoogt, T.H. (NLR), Wiegers, R. (NLR), Cyber security management of future ATM services, December 2015.

[5] Fabian, B., S. Gürses, M. Heisel, T. Santen, H. Schmidt, A comparison of security requirements engineering methods, Requirements Engineering (2010), 15:7-40.

[6] Mellado, D., C. Blanco, L.E. Sánchez, E. Fernández-Medina, A systematic review of security requirements engineering, Computer Standards and Interfaces, 2010.

[7] Muñante, D., V. Chiprianov, L. Gallon, P. Aniorté, A review of security requirements engineering methods with respect to risk analysis and model-driven engineering, CD-ARES 2014, International Cross Domain Conference and Workshop, University of Fribourg, Switzerland, September 8th – 12th, 2014.