Threat-based Risk Assessment – Safety through Security

PROTECT

Thorsten Wollweber, Team Lead Product Security & GRC
19 June 2024

AIRBUS

:a strong & successful player

+1600
employees

39
years of
experience

50+
current
R&D / R&T projects

300+
clients
aeronautics, space, transport, energy, nuclear, institutions…

210m€
2023
turnover

Our services portfolio

Safety Consulting

- SAFETY COMPLIANCE & CERTIFICATION
- DEFENCE SYSTEMS & INFRASTRUCTURES
- ATM / UTM
- AUTONOMOUS VEHICLES
- SMART MOBILITY
- HYDROGEN MOBILITY

Cybersecurity Consulting

- GOVERNANCE, RISK & COMPLIANCE
- EXPORT CONTROL & DATA PROTECTION
- VULNERABILITY ASSESSMENT & PENETRATION TESTING
- SIMULATION & TRAINING
- ARCHITECTURE DESIGN & INTEGRATION
- CRISIS & SECOPS MANAGEMENT

Managed Services

- MANAGED SECURITY SERVICES
  - SOC SERVICES
  - VULNERABILITY MANAGEMENT
  - DIGITAL RISK PROTECTION
  - ATTACK SURFACE MANAGEMENT
  - INCIDENT RESPONSE & FORENSICS
- INTEGRATED SECURITY SERVICES
  - ACCESS TO THE FULL RANGE OF CYBERSECURITY SERVICES MANAGED THROUGH A SINGLE CONTRACT

SIMULATION OF NETWORKS WITH CYBERRANGE

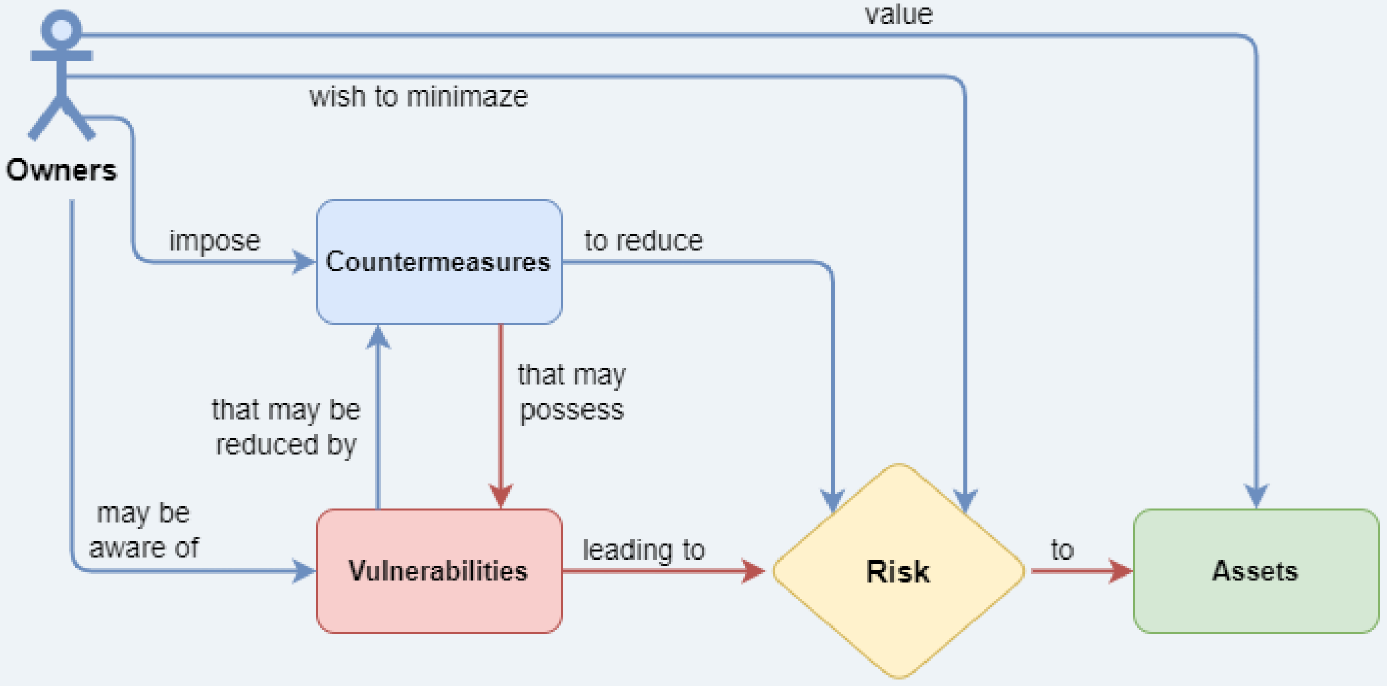
Sustainability Consulting

- ENVIRONMENTAL & REGULATORY STUDIES
- PROCESS SAFETY MGT & SAFETY ENGINEERING
- MODELLING HAZARDOUS PHENOMENA
- DECARBONISATION & CLIMATE CHANGE
- ECO-DESIGN & LIFE CYCLE ASSESSMENT
- SUSTAINABLE SUPPLY CHAIN & DUE-DILIGENCE
- SUBSTANCES & MATERIALS

: Risk Modell

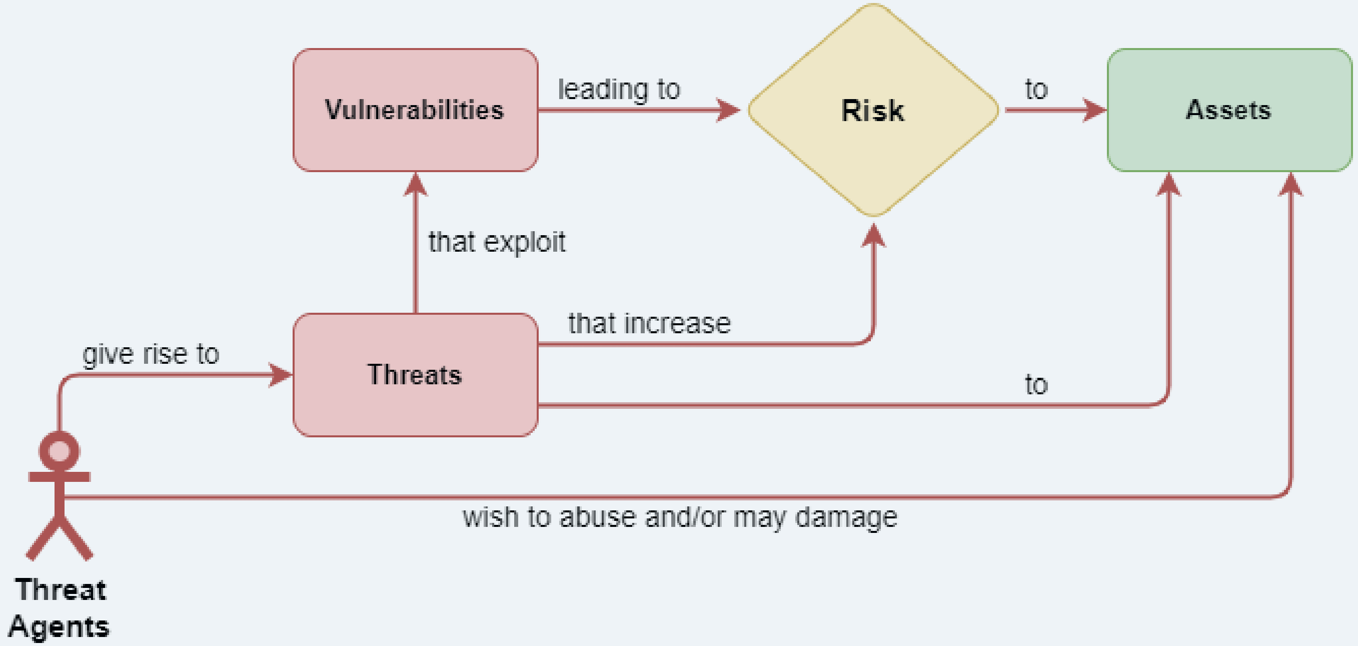
Perspective of the

Asset Owner



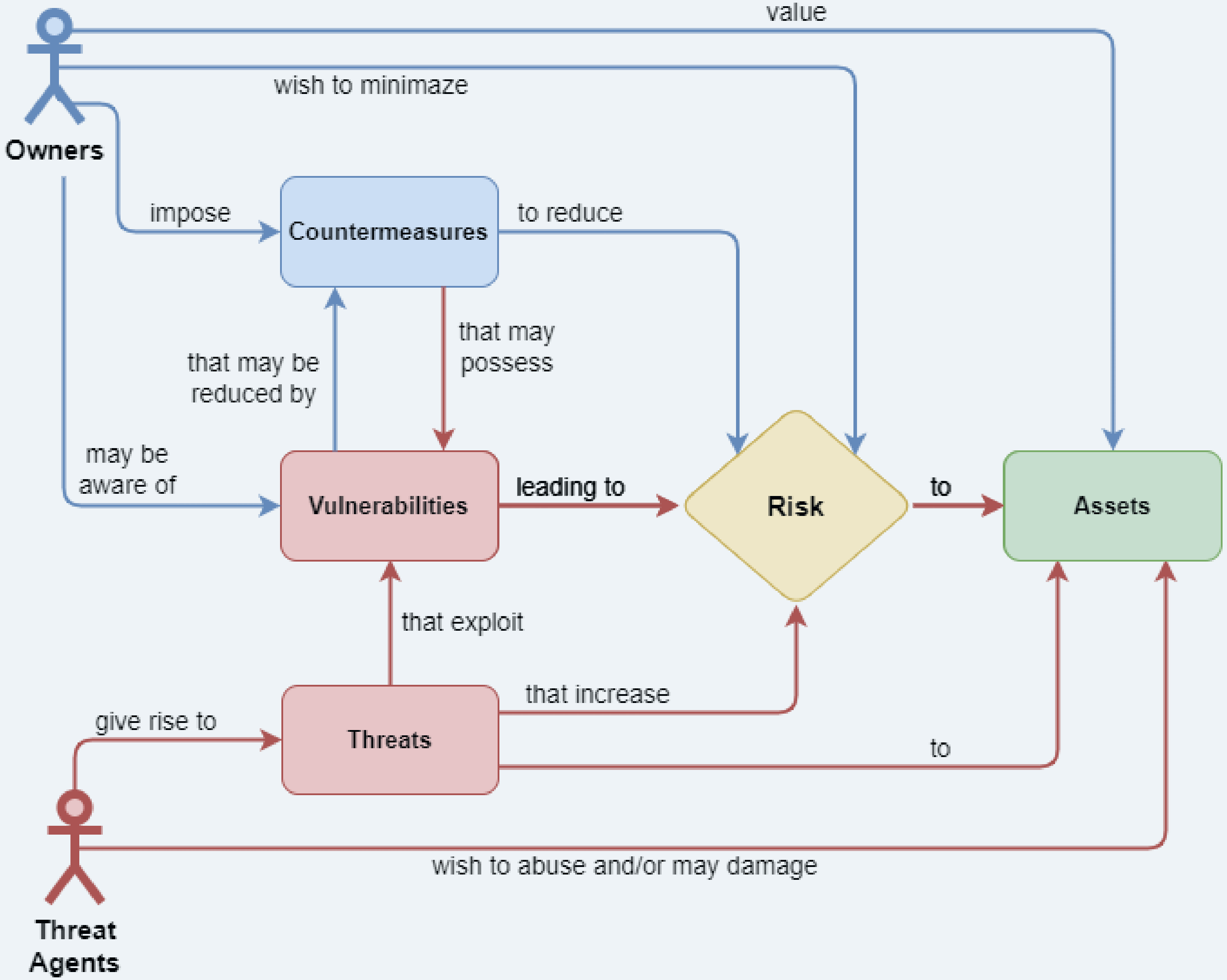
: Risk Modell

Perspective of the **Attacker**



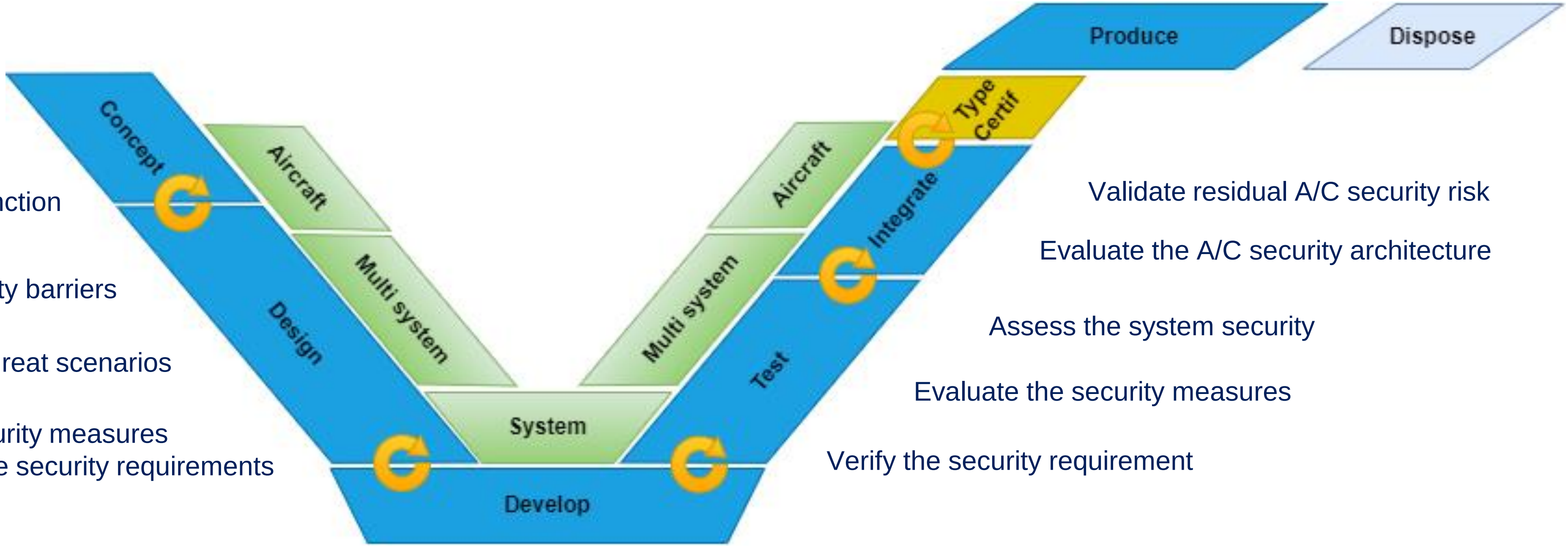
: Risk Modell

The **holistic approach**



AIRBUS

[Aircraft] security process



Vulnerability management

Removal of security measures

Define the context

Define the impact on each function

Identify Path and security barriers

Define the threat scenarios

Define security measures
and validate security requirements

Validate residual A/C security risk

Evaluate the A/C security architecture

Assess the system security

Evaluate the security measures

Verify the security requirement

Supplier activities:
Security measure implementation &
Vulnerability analysis & Penetration test

Requirements Based Engineering builds on >>> functions

Assets?

Functions! (sometimes data)

https://upload.wikimedia.org/wikipedia/commons/5/54/Vue_a%C3%A9rienne_du_domaine_de_Versailles_par_ToucanWings_-_Creative_Commons_By_Sa_3.0_-_073.jpg

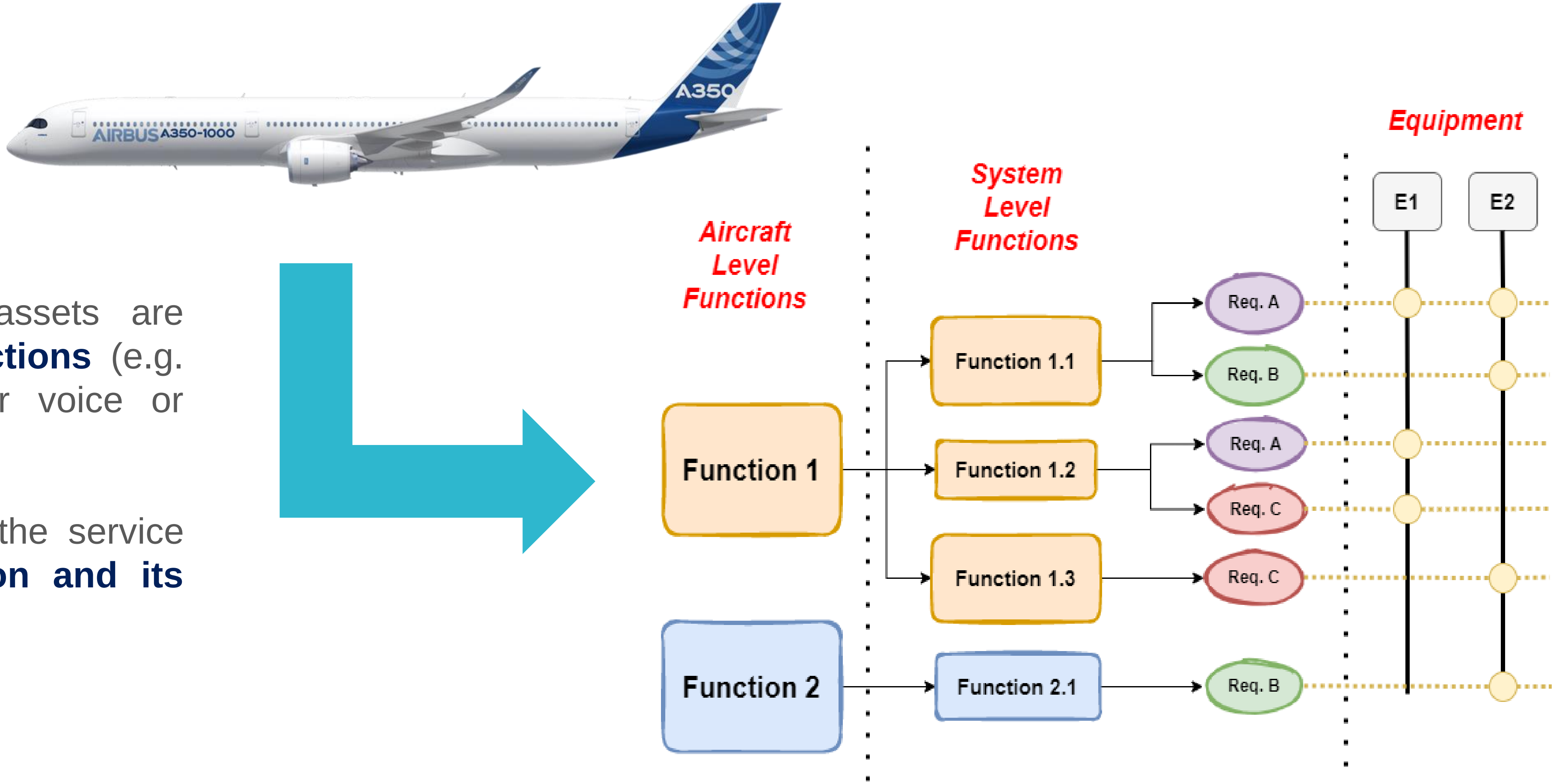
https://upload.wikimedia.org/wikipedia/commons/9/9e/Gold1oz.jpg

https://upload.wikimedia.org/wikipedia/commons/6/69/IBM_PC_5150.jpg

Functional Breakdown

- At Aircraft level, the assets are defined by **Aircraft functions** (e.g. provide internal data or voice or video communication).

- An asset is defined by the service provided by **the function and its functional breakdown**.



: **impacts & consequences** (with examples of categories and impact tables)

Impact on what (category)?

- **Safety**
- **A/C Operations**
- Commercial (use with caution)
- *Other example?*

Consequence depends on your threat model

- **CIA**
- **STRIDE**
- *Other example?*

Elevation of Privileges, Code Execution and (Non-) Functional Attacks

> Functional Attack

Use the intended (“allowed”) communication means for an unintended function.

Examples?

> Non-Functional Attack

Find communication means (“paths”) to create communication which was not intended by the design engineer.

Examples?

> Code Execution

What do you need to communicate from computer A to computer B?

Examples?

> Elevation of Privileges

How can you execute program code on a computer?

Examples?

A/C Level

Security Architecture Concept

- generic attacks
- abstract impacts @ function level
- define barriers respecting existing architecture
- assume *Escalation of Privilege* on every intermediate target
- assign goals to be implemented @ system level

System Level

Threat Assessment

- refine SAC scenarios
- implement barriers and/or goals
- consider OSI Layers
- Interfaces (HW, protocol)
- SW Functions (SQL injection, API, command injection)
- add scenarios for newly discovered Entry Points/Vectors/Targets

Fundamental paradigm: { **Everything is a security measure!** }

Everything which reduces either the likelihood of a successful attack or the severity of an impact is a security measure.

If it reduces the likelihood of an attacker succeeding*, it is a security measure.
No matter whether it is (not exhaustive)…

- a dedicated technical security function,
- a technical function already part of the system baseline,
- a technical function identified through another process (e.g. safety),
- an operational procedure suggested by us or already present,
- prerequisites for the attack…
  - availability of information & equipment,
  - accessibility of interfaces,
  - necessary knowledge.

* There are also security measures which reduce the impact.

White Hat – Black Hat

“Why would you do this anyway?”

In order to evaluate the “strength” of a Security Measure, you need to take the attacker’s perspective.

> **Step 1 (White Hat):** What measure do you need?

> **Step 2 (Black Hat):** What does it need to bypass this measure?

Likelihood – Reduction Factors

Preparation Means

Knowledge Equipment	None / Public Information and no preparation time	Uncontrolled Information and no significant preparation time	Insider Knowledge or Significant preparation time
None / Standard	0	2	6
Special COTS	0	2	6
Special	n/a	4	6
Bespoke	n/a	5	6

Definition of Equipment Categories

- **None/Standard:** No equipment or something commonly already found in the possession of an average person
- **Special COTS:** Something which can be readily bought, but which is usually not yet in the possession of an average person
- **Special:** Something which cannot be readily bought, but which needs to be assembled/built
- **Bespoke:** Special equipment which requires a substantial amount of resources to assemble

Likelihood – Reduction Factors

Execution Means

Expertise Equipment	Layman	Proficient	Expert	Multiple Expert
None / Standard	0	4	6	10
Special COTS	4	4	6	10
Special	n/a	6	8	12
Bespoke	n/a	n/a	10	12

Definition of Expertise Categories

- **Layman:** Someone without specific expertise
- **Proficient:** Someone with basic IT/Aircraft operations expertise (depending on the nature of the threat scenario)
- **Expert:** Someone with security expertise specific to the attack (depending on the nature of the scenario)
- **Multiple Expert:** Specific security expertise in more than one field (e.g. FPGA security expertise and WLAN security expertise or FPGA security expertise and Aircraft security operations expertise).

Likelihood – Reduction Factors

Window of Opportunity

Reduction	Description
0	The attack can be carried out at any time.
1	The attack can be carried out during regular cruise flight.
2	The attack vector is available while the Aircraft is on the ground.
3	Maximum reduction for mandatory operational procedures limiting the window of opportunity.
6	The attack vector is only available in a restricted time phase, e.g. on the ground in maintenance mode.
8	The attack can only be carried out during a very restricted time slot independent from the flight phase (e.g. during system reboot).

Note:

In the case of prepared attacks, the window of opportunity has to be evaluated taking into account how and when the malicious code can be passed onto the target (person or system), not when it is actually executed.

\ Attacker Profile

“Why would you do this anyway?”

This depends on **motivation (only)**!
Security Measures aim to hinder the successful execution.
The attacker profile assesses the precondition.

Motivation is linked to the attacked asset

- Branding impacts
- Considerable financial impacts
- Considerable impacts on airline operations
- Safety impacts without risk for attacker’s personal safety
- Safety impacts including risk for attacker’s personal safety

Attacker profiles

- Untargeted malware attack
- Drive-by attacker
- Commercially motivated attacker
- Terrorist or nation state actor

\ Attacker Profile

“Who would want to try this anyway?”

- Attackers have different **rarity (R)** and feeling of **impunity (I)**

	Branding	Financial	Operations	Safety	Suicide
Malware	R: 0 / I: 0				
Drive-By	R: 0 / I: 0 – 3	Yellow area: not *intended* by attacker (but mind collateral damage potential)			
Commercially Motivated	R: 2 / I: 0 – 3				🟨
Terrorist/Agent	Red area: not *relevant* for assessment		R: 6 / I: 0 – 1		

- Definition of Feeling of Impunity

Reduction	Definition
0	The attacker can believably claim that the attack was not intentional or the attacker is sure that she cannot be identified (full anonymity). For Agent: The agent will aim at not being discovered/uncovered. In addition, an agent will not fear prosecution. For Terrorist: A terrorist will execute the attack disregarding the anonymity. The threat of prosecution will not stop the terrorist.
1	The attacker assumes that she will be identified but because of the insignificant level of impact of the attack, she still believes that she will not be severely prosecuted (high anonymity)
2	Consequence severe but the attacker assumes that she might not be identified (moderate anonymity)
3	The attacker is aware that she will be identified and prosecuted when carrying out the attack, but risks it anyway (low anonymity)

{ Effectiveness Capping

There is a finite limit to effectiveness…

- If the attacker has already spent three months preparing, will another month really mean anything?
- Likewise, if the attacker has already gone through five technical barriers, will the sixth one really be a problem?
- Does it make a difference whether there is five minutes or one minute to carry out the attack?

Sum of security measure effect is capped per factor:

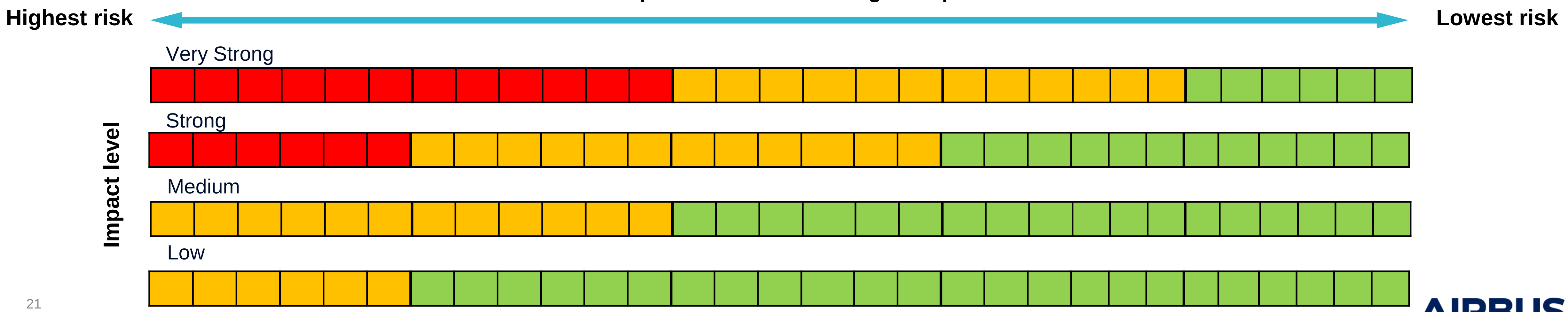
Criterion	Maximum Combined Reduction
Preparation Means	6
Window of Opportunity	8
Execution Means	18

Putting It All Together – Example

The grid represents risk levels and not acceptability criteria which is outside of the scope.

Very Likely	🟩 Low	🟨 Medium	🟨 Medium	🟥 High	🟥 High
Likely	🟩 Low	🟩 Low	🟨 Medium	🟨 Medium	🟥 High
Unlikely	🟩 Low	🟩 Low	🟩 Low	🟨 Medium	🟨 Medium
Very Unlikely	🟩 Low	🟩 Low	🟩 Low	🟩 Low	🟨 Medium
Extremely Unlikely	🟩 Low	🟩 Low	🟩 Low	🟩 Low	🟩 Low
	No Impact	**Low**	**Medium**	**Strong**	**Very Strong**

Color the 30-points-scale according to impact level



Highest risk ↔ **Lowest risk**

Impact level

Very Strong

🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟩🟩🟩🟩🟩🟩

Strong

🟥🟥🟥🟥🟥🟥🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩

Medium

🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩

Low

🟨🟨🟨🟨🟨🟨🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩

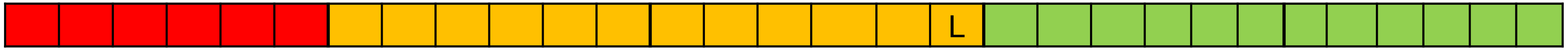
Putting It All Together

	Outside Security Process		Inside Security Process		Effectiveness Capping
	Technical	Operational	Technical	Operational	
Preparation Means	SM1 (v)		SM3 (x)		$C_p = \max(e_r – 6, 0)$
Window of Opportunity		SM2 (w)			$C_w = \max(e_r – 8, 0)$
Execution Means			SM4 (y) SM5 (z)		$C_e = \max(e_r – 18, 0)$
Current Execution Likelihood	$L_{OT} = 30 – e_c$	$L_{OO} = L_{OT} – e_c$	$L_{IT} = L_{OO} – e_c$	$L_{IO} = L_{IT} – e_c$	$L = \max(L_{IO} + c, 1)$

e: sum of row/column

Risk Display

	Outside Security Process		Inside Security Process		Effectiveness Capping
	Technical	Operational	Technical	Operational	
Preparation Means	SM1 (5)		SM3 (1)		0
Window of Opportunity		SM2 (2)			0
Execution Means			SM4 (6) SM5 (3)		0
Current Execution Likelihood	**25**	**23**	**13**	**13**	**13**



Risk Projection

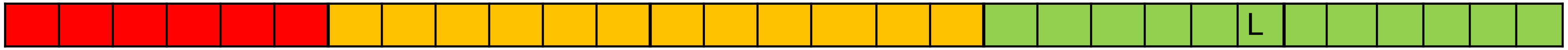
“What about Security Objectives?”

	Outside Security Process		Inside Security Process		Effectiveness Capping
	Technical	Operational	Technical	Operational	
Preparation Means	SM1 (5)		SM3 (1)		0
Window of Opportunity		SM2 (2)		SM6o (2)	0
Execution Means			SM4 (6) SM5 (3)		0
Current Execution Likelihood	**25**	**23**	**13**	**11**	**11**

🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	L	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Likelihood Capping

	Outside Security Process		Inside Security Process		Effectiveness Capping
	Technical	Operational	Technical	Operational	
Preparation Means	SM1 (5)		SM3 (3)		2
Window of Opportunity		SM2 (2)	SM6(6)	SM7(2)	2
Execution Means			SM4 (6) SM5 (3)		0
Current Execution Likelihood	25	23	5	3	7



Attacker Profile

“Who would want to try this anyway?”

	Outside Security Process		Inside Security Process		Effectiveness Capping
	Technical	Operational	Technical	Operational	
Preparation Means	SM1 (5)		SM3 (1)		0
Window of Opportunity		SM2 (2)			0
Execution Means			SM4 (6) SM5 (3)		0
Current Execution Likelihood	25	23	13	13	13
Execution Likelihood incl. Attacker Profile					(-3) 10

🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟩	L	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Security Measures Reassessment & Risk Evolution

“There is a new vulnerability.” & “We need to change the design.”

	Outside Security Process		Inside Security Process		Effectiveness Capping
	Technical	Operational	Technical	Operational	
Preparation Means	SM1 (5)		SM3 (1)		0
Window of Opportunity		SM2 (2)		SM6 (2)	0
Execution Means			~~SM4 (6)~~ **SM4 (2)** SM5 (3)	**SM7 (5)**	0
Current Execution Likelihood	**25**	**23**	**13**	**11**	**11**

Most of the original calculation remains intact!

“thank you”

{contact us}

www.protect.airbus.com

protect@airbus.com