NTT DATA

Cybersecurity engineering in space SW products

SPA workshop September 2023

Patricia Rodríguez Dapena

26/08/2023 NTT_23-018_CYBERENG_PRE-v1.0

FUTURE AT HEART

Why the need?

Space-based services are more and more needed in essential services such as military, utilities, communications, aviation and emergency communications, etc. and therefore makes them particularly attractive for cyberattacks with unpredictable impacts.

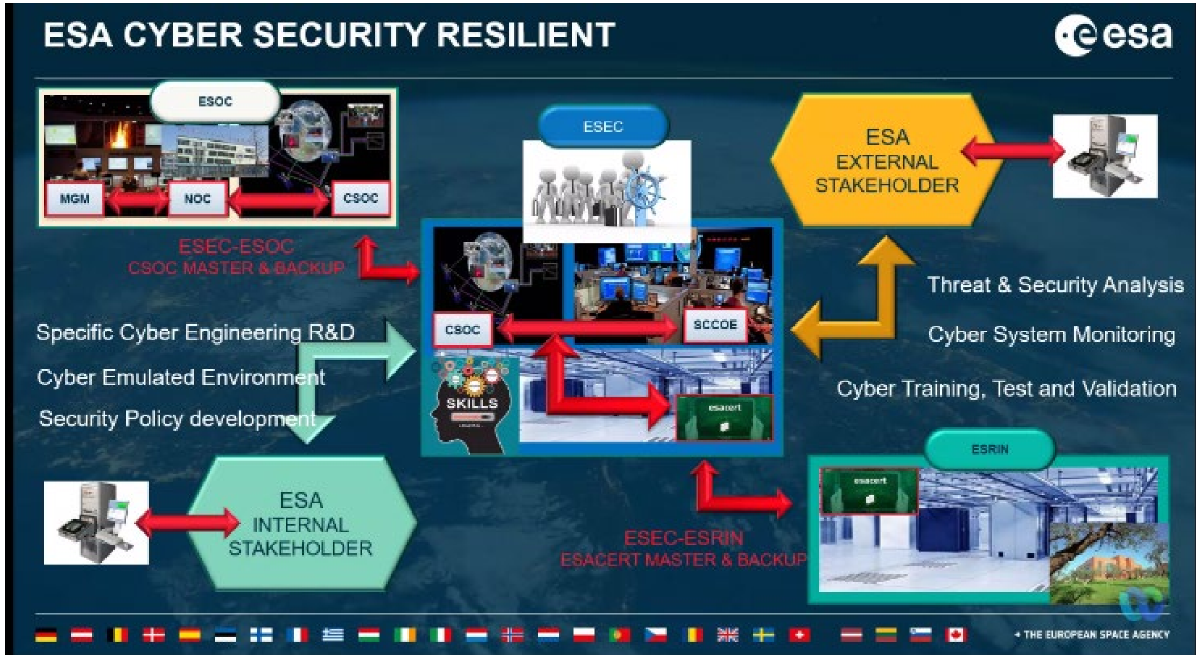
Many examples of cyber-attacks in space systems. One example, in February 2022, a large number of satellite modems in Ukraine and elsewhere in Europe were subject to a cyberattack and disabled.

The proliferation of interconnection of space systems with other daily systems, as well as the role of other small satellites and NewSpace missions make the cybersecurity engineering an important matter.

There is not much guidance about how the cyber vulnerabilities are analysed and how the satellite systems, while being developed, are to be **built secure-by-design**.

Cybersecurity tackles different matters (e.g., **Secure systems**, Secure technology, Secure infrastructure and environment, Secure operations, Secure personnel and organizations…). This project for ESA will only focus on the first aspect of the problem: provision of guidance for the engineering of cybersecurity while space systems and in particular its SW is developed.

Industry days for ESA cybersecurity activities. 23.06.2022.



Organizations involved in the ESA Cybersecurity resilience strategy

- Implementation of individual security mechanisms through standardization and validation of security protocols
- Identification and implementation of reference architectures for space- and ground-based data processing system.
- **Integration of security into the ESA system engineering process**

Cybersecurity definition and space

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Defending against loss of Confidentiality, Integrity, or Availability (C-I-A):

- *Loss of confidentiality results in unauthorized disclosure of information.*
- *Loss of integrity can result in falsification of transactions as well as unauthorized modification or destruction of information.*
- *Loss of availability results in a temporary or permanent loss of access to critical resources or critical functionalities of a system, including safety related ones.*

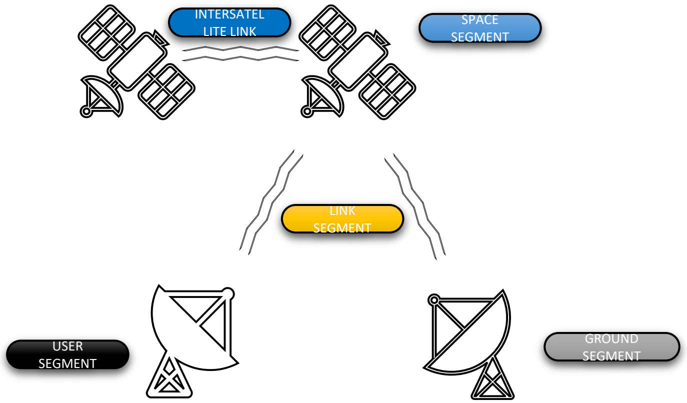
Cybersecurity engineering means the engineering of a cybersecure product. This is intended mainly to inject mechanisms or develop the product to avoid or reduce to the minimum the loss of C-I-A that might result in harm to Space operations and use, assets, or individuals.

Important definitions in Cybersecurity engineering:

Threats
Vulnerabilities

Attack vectors
Cybersecurity risks
Cybersecurity mechanisms

Cyberattacks on satellite systems



The threats can take various forms, for example:

- transmission of false data from an untrusted source,
- Spoofing attack,
- Jamming attack, or
- Malware (e.g., infecting ground-based systems such as satellite control centers)

Example of **potential consequences** of satellite cyberattacks are:

- The loss of satellite control that may force the satellite to re-enter the Earth's atmosphere and burn up or to collide with other space object.
- disruption of all communications and permanently damage the satellite by depleting its propellant supply or causing damage to its electronics and sensors.
- the data on board may be compromised or lost.

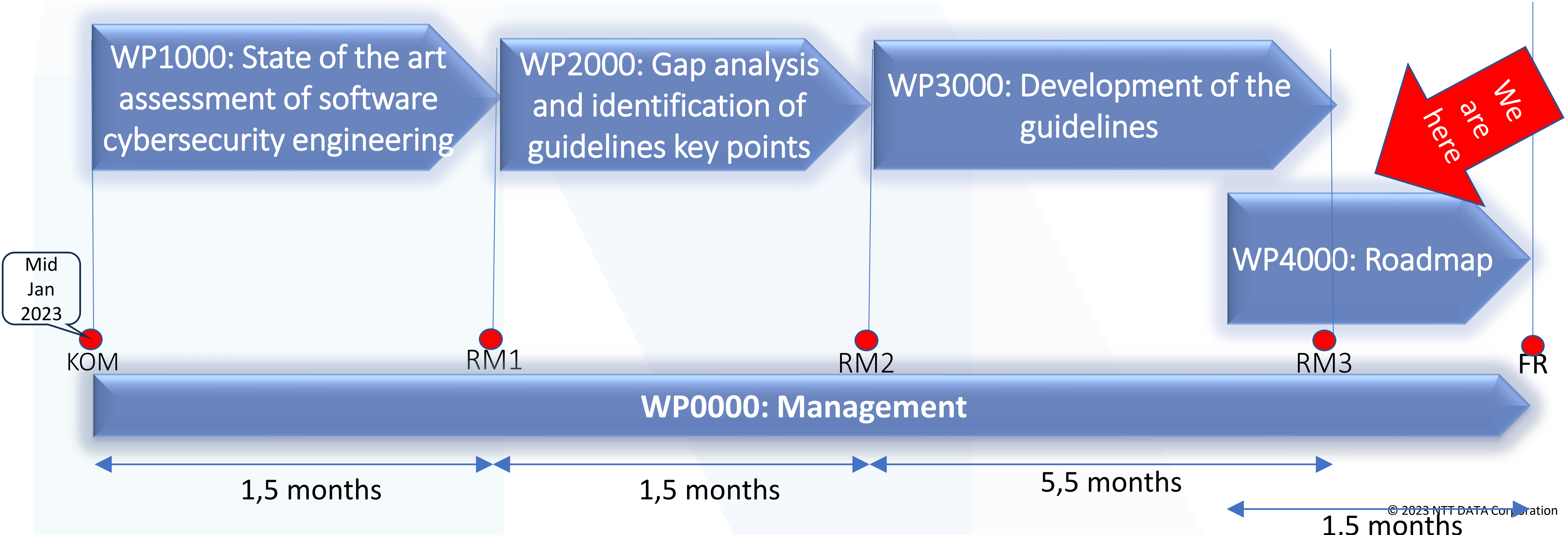
ESA project

No guidance nor clear ECSS requirements for cybersecurity Engineering in space systems

ESA Contract Ref: 4000136516/21/NL/AR/va - ESA ARTES ITT ref: AO/1-10773/21/NL/ND

Title: INNOVATIVE MISSIONS AND TECHNOLOGIES

Budget Line: ARTES 4.0 Core Competitiveness Generic Programme Line Component A: Future Preparation (ARTES FPE 1A.108)



WP1000 and WP2000 objectives

State of the art

Analysis of existing specific standards or development guidelines

- Analysis of references in the automotive domain
- Analysis of different industries' frameworks
- Cybersecurity analyses
- Coding standards
- SPACE standards
- NewSpace standards and literature
- Safety vs. Security

GAP analysis

- ECSS-Q-ST-80Crev1 GAP analysis
- (ECSS-Q-ST-80-10 Draft)
- ECSS-E-ST-40C GAP analysis (draft rev 1)
- Other ECSSs
- ESSB
- CCSDS
- Conclusions from the Gap analysis

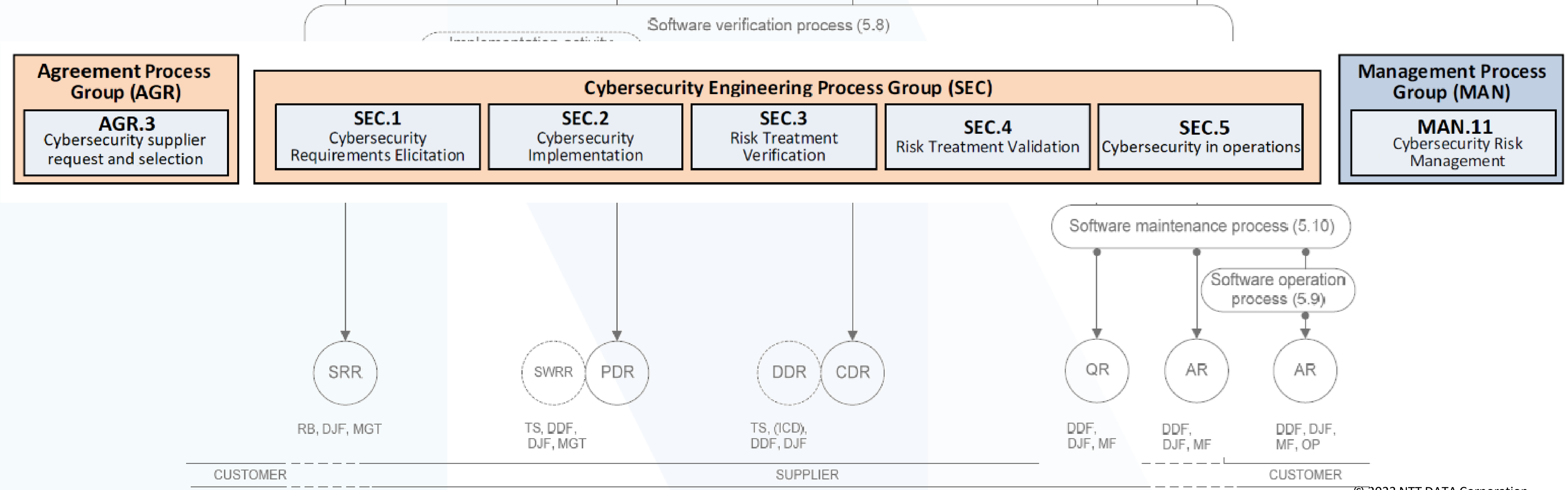
WP3000 objectives

Objectives: **To create a hands-on guideline defining technical steps for cybersecurity engineering.**

- Define the cybersecurity assessment activities and processes guidelines (mission agnostic).
  - background information, objective and scope, forms and report **templates**, reporting recommendations.
  - For each process the following information will be given as a minimum: overview, inputs, outputs, management and task descriptions.
  - A catalogue of vulnerabilities and threads will be defined.
  - A list of mechanisms to be implemented to make the SW more cybersecure will be provided.
- How to integrate safety and cybersecurity analyses and analyse their dependencies
- Include the results of case study

Cybersecurity processes

- Cybersecurity security processes already in the draft proposed updates of ECSS-Q-HB-80-02 SPICE for Space, based on AutomotiveSPICE process reference model for cybersecurity.
- The guidelines introduce how and when to implement them following the activities diagram:



Part of draft TN3: TARA Analysis

The TARA methodology includes three activities:

- Cyber Threat Susceptibility Analysis (CTSA)
  - Step 1. Establish assessment scope
  - Step 2. Identify candidate Threats & Vulnerabilities
  - Step 3. Eliminate implausible Threats
  - Step 4. Apply scoring model
  - Step 5. Construct the threat matrix

NTT DaTa

Step 2

ID	Threat Name	Reference (as per TN3 list)
1	Threat 1	T1
2	Threat 2	T2
3	Threat 3	T3
…		

Step 3

Threat ID TN3	Threat Name	Plausible?
T13	Activate Firmware Update Mode	Yes If firmware update mode is activated some expected response functions from engaging in reaction to an emergency or process malfunction can't be performed.
T40	Monitor Process State	No It is considered in T21
T60	Automated Collection	Yes Attackers could sneak in scripts to extract information about the operation of the satellite itself

Step 4

ID	Name	Severity	Probability	Risk Level
T05	Inter-Process Communication	0,8	0,7	0,56
T63	Network Effects	0,6	0,7	0,42
T06	System Services	0,8	0,5	0,4
T16	Loss of Availability	0,8	0,5	0,4
			0,5	0,3
			0,5	0,3
			0,5	0,3
			0,5	0,3
			0,7	0,28
T22	Process Discovery	0,4	0,7	0,28
T56	Indicator Blocking	0,4	0,7	0,28
T11	Network Device Configuration Dump	0,4	0,5	0,2
T02	Disable Crypto Hardware	0,6	0,3	0,18
T13	Activate Firmware Update Mode	0,6	0,3	0,18

Example of Threat Risk Scoring Spreadsheet

Probability/ severity impact	0,05	0,10	0,20	0,40	0,80
0,10	0,005	0,010	0,020	0,040	0,080
0,30	0,015	0,030	0,060	0,120	0,240
0,50	0,025	0,050	0,100	0,200	0,400
0,70	0,035	0,070	0,140	0,280	0,560
0,90	0,045	0,090	0,180	0,360	0,720

Step 5

Req ID	Requirement	Threat ID TN3	Threat Name	Description
REQ01	Bootloader should check if update software is available. If bootloader	T06	System Services	Adversaries may abuse system serv… execute commands or programs… execute malicious content by int… creating services either locally o… services are set to run at boot, … achieving persistence (Create or Modify System Process), but adversaries can also abuse services f… one-time or temporary execution.
			Activate	Adversaries may activate firmware update mode o… devices to prevent expected response functions fr… engaging in reaction to an emergency or process malfunction. For example, devices such as protecti… relays may have an operation mode designed for

Draft TN3: TARA Analysis

The TARA methodology includes three activities:

- Cyber Risk Remediation Analysis (CRRA)
  - Step 6 Select mechanisms to mitigate.
  - Step 7 Identify plausible Counter Measures.
  - Step 8 Assess countermeasure merit.
  - Step 9 Identify an optimal Counter Measure solution.
  - Step 10 Prepare recommendations

Step 6

REQ01	T06	System Services	M088	Filter Network Traffic
REQ02	T30	Loss of Safety	M027	Safety Instrumented Systems
REQ03	T16	Loss of Availability	M026	Redundancy of Service
	T30	Loss of Safety	M027	Safety Instrumented Systems
REQ04	T24	Block Reporting Message	M019	Out-of-Band Communications Channel
REQ05				

Vulnerability ID tn3	Vulnerability Name	Mitigation ID TN3	Mitigation Name
V01	Buffer Overflow	M088	Stack Canaries
		M089	Address Space Layout Randomization (ASLR)
		M090	Input Validation
V02	Catch NullPointerException	M091	Use Null Object Design Pattern
V03	Heartbleed Bug	M092	Updated and patched version o[illegible] OpenSSL

Step 7

Mitigations	Effectiveness of the mitigation by threat								
Mitigation Name	Cost	T05	T63	T06	T16	T23	T24	T30	T60
Disable or Remove Feature or Program	1			DM, LM					
Execution Prevention	3	LM, NM							

ID	Name
1	Very low cost. Implementation of mitigation is afforda[illegible] financial resources. Can be easily carried out without[illegible] costs.
2	Low cost. Implementation of mitigation has a mode[illegible] manageable in terms of financial resources. It may req[illegible] but not of a large magnitude.
3	Medium cost. The implementation of mitigation invol[illegible] terms of financial resources. It may require some sig[illegible] specific budget allocation.
4	High cost. Implementing mitigation involves consider[illegible] financial resources. It may require significant investm[illegible] budget allocation.
5	Very high cost. Implementing mitigation is very costly[illegible] demanding. It may require major investments, acqu[illegible] technologies and allocation of significant r[illegible]

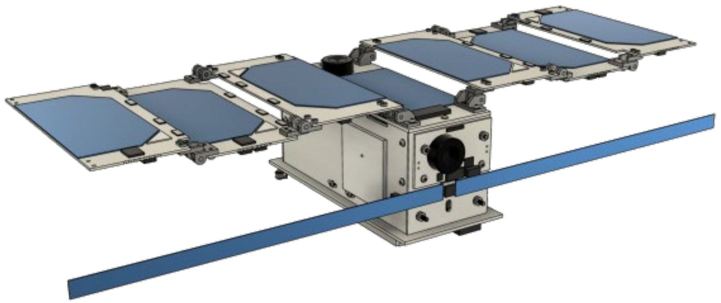
Step 8

CM ID	Neutralize			Limit			Detect			Recover			CM Merit Scoring		
	NH=9	NM=7	NL=5	LH=7	LM=5	LL=3	DH=5	DM=3	DL=1	RV=9	RH=7	RM=5	Utility	Cost	U/C Ratio
M019	T63	T16, T23		T63	T24						T16, T24	T23	54	5	10,8
M011					T06			T06					8	1	8,0
M046		T16		T23		T16		T23					20	3	6,7
M016				[illegible]			[illegible]						12	2	6,0

Effectiveness	Mitigation Category			
	Detect	Neutralize	Limit	Recover
Very high	DV=7	NV=11	LV=9	RV=7
High	DH=5	NH=9	LH=7	RH=5
Medium	DM=3	NM=7	LM=5	RM=3
Low	DL=1	NL=5	LL=3	RL=1

Draft TN3: TARA Analysis main results

Case study and results of TARA use: FOSSASAT OBSW



Recommendations to protect the SW system:

Creation date	Identifier	Recommendation	Originator	Unit/s	Threat or vulnerability mode origin	Status
25/08/2023	REC-001	The system should provide an alternative method for sending critical report messages to operators. This could include using radio/cell communication to obtain messages from field technicians that can locally obtain telemetry and status data. Out-of-band channels include, for example, local (nonnetwork) accesses to information systems, network paths physically separate from network paths used for operational traffic, or nonelectronic paths such as the US Postal Service. Out-of-band channels do not have the same vulnerability/exposure as in-band channels, and hence the confidentiality, integrity, or availability compromises of in-band channels will not compromise the out-of-band channels. Not having these extra	M19	Network	T16, T23, T24. T63	O

Draft TN3: Reference Threads and vulnerability tables and Counter measures details

ID	Vulnerability Name	Mitigation ID TN3	Mitigation ID MITRE	Mitigation Name
V01	Buffer Overflow	M088	N/A	Stack Canaries
		M089	N/A	Address Space Layout Randomization (ASLR)
		M090	N/A	Input Validation
V02	Catch NullPointerExce	M091	N/A	Use Null Object Design
V03	Heartbleed B			
V04	Improper Da Validation			
V05	Least Privile Violation			

Threat ID TN3	MITRE ID	Threat Name	Mitigation ID TN3	Mitigation ID MITRE	Mitigation Name
T01	T1092	Communication Through Removable Media	M011	M0942	Disable or Remove Feature or Program
			M063	M1028	Operating System Configuration
T02	T1600.002	Disable Crypto Hardware	M042	M0941	Encrypt Sensitive Information
T03	T1414	Clipboard Data	M012	M1051	Update Software Maintenance

Draft TN3: Reference description of some Counter measures' techniques

- Prevention mechanisms
- Removal mechanisms
- Protection mechanisms

Coding standards

References	ISO/IEC TS 17961:2013/Cor 1:2016 - Information technology — Programming languages, their environments and system software interfaces — C secure coding rules . ISO/IEC TS 17961:2013/Cor 1:2016 SEI CERT Oracle Coding Standard for Java. https://wiki.sei.cmu.edu/confluence/display/java SEI CERT Coding Standard https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards (for Android, C, C++, Java, Perl) CWE coding standard. MITRE. https://cwe.mitre.org/about/index.html https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
Objectives	The use of coding standards (i.e., CERT, CWE, etc.) focused on the avoidance of cybersecurity vulnerabilities help to prevent known vulnerabilities (buffer overflow, secure passwords, secure function calls, deception, memory corruption bugs, etc.). Two main references can be used: • CERT: a secure coding standard maintained by the Software Engineering Institute at Carnegie Mellon University. It supports commonly used programming languages such as C, C++, and Java. In addition, the CERT Risk Assessment is defined, for each guideline included in the secure coding standard, to help determine the possible consequences of violating that specific rule or recommendation. There are three sections to the risk

Draft TN4: Roadmap

Few example of issues still to be further developed:

- Strengthen the list of threads and vulnerabilities for different space systems and their relationship with defence mechanisms
- Test and validate the effectiveness of the defined defence mechanisms (Counter measures)
- Assess the exiting software analysis tools versus the cybersecurity coding rules
- Expand the requirements of the validation test environments of space systems to include the possibility of, for example, penetration testing
- Test and improve the TARA method on more SW systems (also define reference tables: cost, etc).
- Expand this guide to specialize it a) at the systems level, not just SW and b) for the subsystems ground segment, flight, operations
- Integrate the guide into the ESA Master Plan for security and cybersecurity
- Refine the ECSS standards to add cybersecurity Engineering and the TARA method (threads/mechanisms, etc)
- Define the Software (cybersecurity) criticality classification for space (as in ISO 21434 for automotive) and tailor the ECSS requirements for the projects.

Thank you!