Executive Summary Report

4000137016/21/NL/MGu - Cybersecurity by design for mixed criticality embedded systems

Document ID	Revision	Date
400013701621NLMGu_Exec	1.0	2023-08-28

Author: Damir Bartakovic

SYSGO GmbH

Am Pfaffenstein 8, D-55270 Klein-Winternheim

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose of this Document

This document constitutes the Executive Summary Report for the activity initiated by the European Space Agency with the title "Cybersecurity by design for mixed criticality embedded systems" and under the contract No. 4000137016/21/NL/MGu.

The work was done by SYSGO GmbH, Klein-Winternheim with support of Airbus Defense and Space GmbH and Thales Alenia Space.

1.2 Referenced Documents

Ref.	Document ID - Document Title
[CC]	Common Criteria Sponsoring Organizations, Common Criteria for Information Technology Security Evaluation. Version 3.1, revision 5 (final), April 2017, https://www.commoncriteriaportal.org/ccra/index.cfm
[ECSS]	ECSS-E-ST-40C, Space Engineering Software, March 2009 ECSS-Q-ST-80C Rev.1, Space Product Assurance – Software Product Assurance, 15 Feb. 2017
[DO-356A]	RTCA DO-356, 2018 – Airworthiness Security Methods and Considerations, Revision A, June 21
[ED-203A]	EUROCAE ED-203, - Airworthiness Security Methods and Considerations, Revision A, June 2018
[TRL]	Space engineering – Technology readiness level (TRL) guidelines, ECSS-E-HB-11A, 1 March 2017

1.3 Abbreviations and Acronyms

Abbreviation / Acronym	Description
ADS	Airbus Defense and Space
CPU	Central Processing Unit
FPGA	Field Programmable Gate Array
MPU	Memory Protection Unit
OS	Operating System
RTOS	Real-Time Operating System i.e. PikeOS for MPU in this document
TAS	Thales Alenia Space

Table 1 Abbreviations and Acronyms

2 Background

With the inexorable trend towards more software-driven (defined) system components and system safety and security awareness, the reliance on the on-board SW platform for mission safety and security will become critical.

To support the implementation of secure, dependable and safe applications, the underlying hardware and operating system need to be itself secure, dependable and safe. Also, the development requires support by the provider of the hardware and the operating system to be able to develop applications that have themselves these properties in a demonstrable manner. Possible support might be provided in the form of specific requirements, design patterns and design conventions.

Dependability and safety are properties well established in space and aviation. Aviation safety is the result of all actions taken to prevent accidents, errors or unintentional defects in the design, construction, maintenance and operation of a spacecraft or aircraft.

Security has been historically low priority for the space and aviation industry but getting more attention nowadays. Aviation security is the result of all actions taken to prevent accidents, errors, unintentional defects or intentional attacks in the design, construction, maintenance and operation of a spacecraft or aircraft. In other words, security is highly focused on the deliberate actions that are geared towards inflicting harm to an individual, organization, or even assets.

The hardware to be considered in this activity is the NG-ULTRA FPGA (see https://dahlia-h2020.eu/ and https://nanoxplore-wiki.atlassian.net/). The NG-ULTRA FPGA is the first European FPGA based on 28nm FD-SOI technology, and it is the third of the BRAVE family FPGAs family. It includes in the same component both, the FPGA part (PL, Programmable Logic), and the System-on-Chip part (PS, Processor System). This component offers wide-ranging possibilities for the implementation of dependable, safe and secure space systems. However, to support the development of space applications with these properties, an Operating System (OS) is needed to complement it. The OS to be considered in this activity is PikeOS for MPU of SYSGO GmbH (https://www.sysgo.com/pikeos-for-mpu).

3 Overview of the Activity

The result of this activity was the proof that the RTOS PikeOS for MPU offers properties and features that allow implementing securely applications with different security sensitivity levels (mixed criticality and sensitivity) while maintaining safety and dependability for the spacecraft microprocessor platform NG-ULTRA.

A new development to enhance the security of low-cost software platform solutions is considered essential. Requirements like dependability, scalability, obsolescence and reusability have been taken into account as well.

This new development will build on microprocessor platforms (System-on-Chip or SoC) as developed by the EU DAHLIA (Deep sub-micron microprocessor for space rad-Hard application ASIC) program that will be integrated in the NG-ULTRA SoC FPGA (Field Programmable Gate Array).

Separation of applications is assured by means of time and space partitioning. A partition is a logical container created and maintained by the operating system. Resources will be allocated according to partition configuration (e.g. memory, CPU time, I/O access rights).

The resulting RTOS achieved TRL 6 (see [TRL]). Therefore, validation has been performed in a representative platform.

The activity identified and provided analyses to demonstrate the level of security, needed artifacts and guidance for an eventual security certification.

The following companies were involved in this activity:

- SYSGO GmbH (Mainz, Germany) – Main contractor.
- Airbus Defense and Space GmbH (Immenstaad, Germany) - supported the assessment of security threats for specific mission scenarios by describing the basic satellite use cases and data handling architectures.
- Thales Alenia Space (Cannes, France) - supported the extension of these use cases that were considered relevant in the context of NG-ULTRA.

4 Work Performed and Main Results

The work was carried out around the following high-level activities:

- Context and objectives definition resulting in use cases and security objectives derived from typical satellite mission scenarios (§ 4.1).
- Analysis of possible threats and refinement of security objectives and establishment of a security criticality categorization. (§ 4.2)
- Production of the RTOS specific security requirements based on security analysis & treatment (§ 4.3).
- RTOS Requirements Validation and Verification (§ 4.4).
- Guidance security certification of the RTOS and the System (§ 4.4).

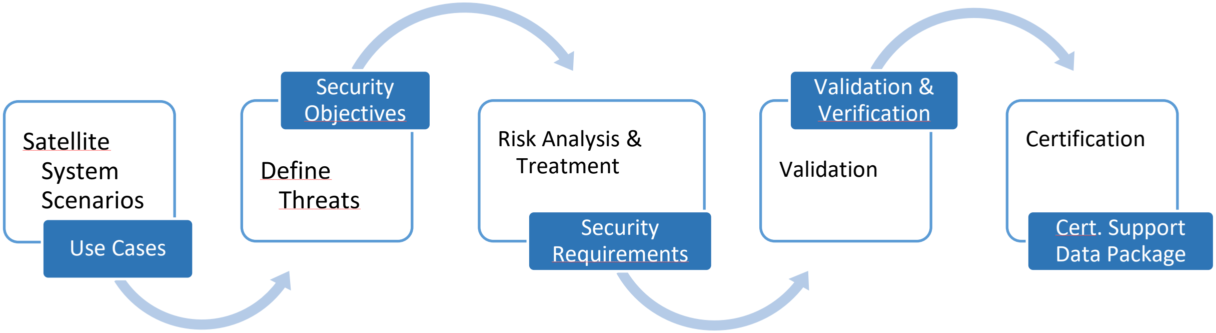

Satellite System Scenarios
Use Cases
Security Objectives
Define Threats
Risk Analysis & Treatment
Security Requirements
Validation & Verification
Validation
Certification
Cert. Support Data Package

Figure 1 High-Level Activities

4.1 Use Case, Usage Scenarios and Security Objectives

In cooperation with ADS and TAS the typical satellite mission usage scenarios e.g.:

- Earth Observation
- Satellite Navigation
- Satellite Telecommunications
- Deep Space

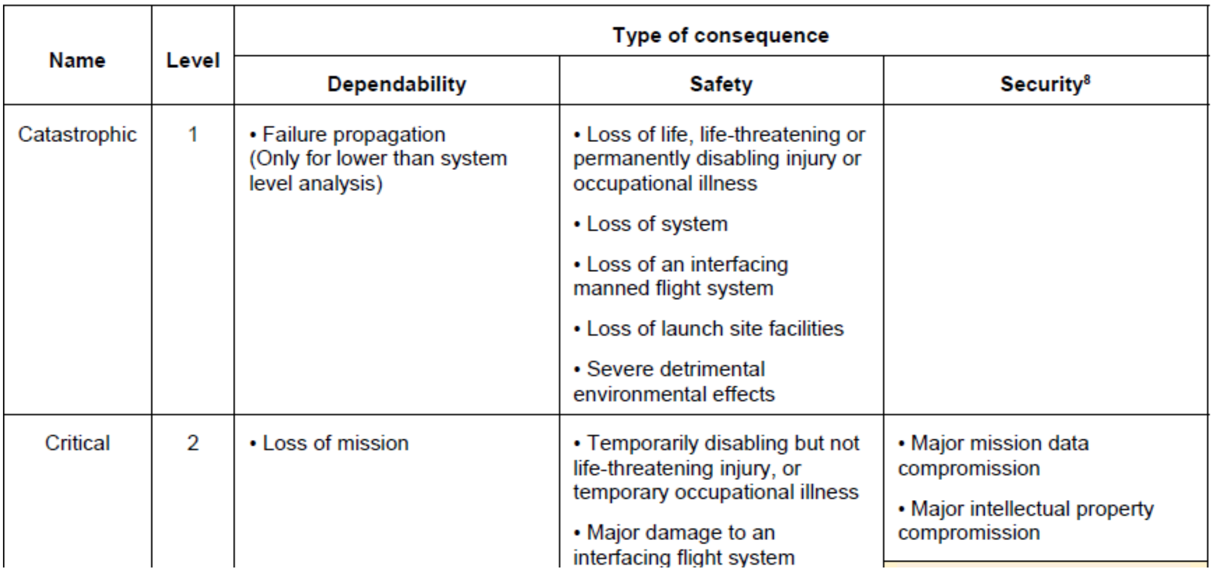
and use cases deemed relevant for security were analyzed and mapped e.g.:

- protection of the OS layer from applications, and applications from other applications.
- Protection of the communications to and from external systems.
- Secure Boot / Secure Update.

Next the security Objectives were derived based on the use cases. e.g.:

- Hardware
- Exclusive access to resources
- Privileged executables

Finally, criticality categorization of security consequences has been discussed e.g.:



Name	Level	Type of consequence		
		Dependability	Safety	Security[8]
Catastrophic	1	• Failure propagation (Only for lower than system level analysis)	• Loss of life, life-threatening or permanently disabling injury or occupational illness • Loss of system • Loss of an interfacing manned flight system • Loss of launch site facilities • Severe detrimental environmental effects	
Critical	2	• Loss of mission	• Temporarily disabling but not life-threatening injury, or temporary occupational illness • Major damage to an interfacing flight system	• Major mission data compromission • Major intellectual property compromission

Figure 1: Severity Categories (augmented with security aspects)

4.2 Security Analyses & Treatment

In the second step, the security objectives of the RTOS were refined based on the analysis of the use cases.

Based on these use cases and refined security objectives, a generic security analysis was performed to identify the RTOS inherent and external (e.g., application driven) security risks.

The identified security risks were analysed in order to determine the cases where dependability and safety are aligned with security and the cases where a trade-off needs to be established between them (risk treatment).

4.3 RTOS Security Requirements and Artifacts

The required security characteristics and functionality of the RTOS were summarized into testable security requirements, mapped to the previous generated risk treatment and complemented by other RTOS artifacts (e.g.: RTOS Requirements, RTOS Design, RTOS User Manuals).

4.4 RTOS Validation & Security Certification Support

The test & validation of the identified security requirements were performed, the results were recorded.

Although a certification was not the goal of this study, a plan of certification aspects was created and a package to support an eventual certification of the RTOS and the system was produced. The package shows which documents and artifacts must be produced, and what evidence must be collected along the lifecycle of the project and throughout all its activities based on proven avionic ([ECSS], [ED-203A], [DO-356A]) and security standards ([CC]).

5 Deliverables

The following deliverables have been produced in the scope of this contract:

5.1 Documents

Ref.	Document ID - Document Title – optional Description
[TP]	21102-0090-TP - Tailoring Plan CYBERSECURITY BY DESIGN FOR MIXED CRITICALITY EMBEDDED SYSTEMS - contains the tailoring of the SYSGO Processes
[ECSS_COMPL]	21102-1002-COMPL_ECSS - Compliance Matrix to ECSS CYBERSECURITY BY DESIGN FOR MIXED CRITICALITY EMBEDDED SYSTEMS - contains the tailoring of the [ECSS] standards.
[D1]	21102-8100-D1 – D1 - Use Cases and Security Objectives Definition Report
[D2_D3]	21102-7002-D2_and_D3 - Security Risks Analysis Report / D3 - Security Risk Treatment Plan
[D4]	21102-7004-D4 – D4 - Security Concept Technical Note
[D5]	21102-7005-D5 – D5 - RTOS User Requirements
[D6]	21102-7006-D6 – D6 - RTOS Design Document
[D7]	21102-7007-D7 – D7 - Software Reuse File
[D8]	21102-7008-D8 – D8 - User Manual
[D9_D10_D11]	21102-7009-D9-D10-D11 – D9 - Software Validation Specification, D10 Software Verification Control Document, D11 Software Validation Reports and Logs
[D12]	21102-7012-D12 – D12 - Certification Aspects Plan
[D13]	21102-7013-D13 – D13 - Certification and Accreditation Support Data Package
[SEC-TR]	21102-1800-ARM8R-TRACE-TR-SEC - PikeOS for MPU Test Results
[SEC_TRACE]	21102-1800-ARM8R-TRACE-TR-SEC - 21102 Trace Data of Security Requirements

Table 2 Delivered Documents

5.2 RTOS & Test Execution Environment

Complementing the above deliverables, the RTOS PikeOS for MPU 1.1 (SW1) and the corresponding test framework including the security test suite (SW2) was delivered.

The SW2 including all necessary components was delivered as docker container so that the execution of the test results can be reproduced by ESA.

6 Conclusion

The results of this activity, based on the existing NG-ULTRA FPGA and the existing RTOS PikeOS for MPU, provide the European space community with a step-by-step approach from the definition of the high-level system view, showing which documents and artifacts must be produced to the final verification for safe & secure embedded systems in space.