This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

Project Number: 871259

Project Acronym: ADMORPH

Project title:

Towards Adaptively Morphing Embedded Systems

Technical Report

Part B

Period covered by the report:
from 1/01/2020 to 30/10/2020

Due Date:	Month 10
Delivery:	Month 10
Lead Partner:	UvA
Editor:	Juliane Steinhardt & Prof. Andy Pimentel, UvA
Dissemination Level:	P
Status:	submitted
Approved:	
Version:	1.0

DOCUMENT INFO

This is not a formal periodic report, but an intermediate technical report upon request of the European Commission. This is not part of the Grant Agreement.

The structure is adapted from that of periodic reports, Part B, in a lighter version. The purpose of this document is to provide the reviewers of the technical review in month 11 an overview of the work done within ADMORPH as well as an outlook of work planned within the remainder of the first reporting period of the project.

DOCUMENT INFO – Revision History

Date and version number	Author/Contributor	Comments
20.02.2020, v0.1	Juliane Steinhardt (UvA)	First draft
09.10.2020, v0.2	Marcus Völp (UNILU), Don Kuzhiyelil (SYSGO)	WP 2 and WP 4 input
12.10.2020, v0.3	Clemens Grelck (UvA)	WP 1 input
13.10.2020, v0.4	Stefanos Skalistis (UTRC-I), Antonio Casimiro (FC.ID)	WP 5 and WP6 input
14.10.2020, v0.5	Andy Pimentel (UvA)	Input WP3, proof read UvA
16.10.2020, v0.6	Juliane Steinhardt (UvA)	Correction of the PM table
23.10.2020, v0.7	Martina Maggio (ULUND) Petr Novobílský (QMA)	Internal review

CONTRIBUTORS

Editor: Juliane Steinhardt, Prof. Andy Pimentel

Authors: All ADMORPH partners have provided contributions. The WP leaders were in charge of collecting the information for their WP:

- WP1: Clemens Grelck (UvA)
- WP2: Marcus Völp (UNILU)
- WP3: Martina Maggio (ULUND)
- WP4: Don Kuzhiyelil (SYSGO)
- WP5: Stefanos Skalistis (UTRC-I)
- WP6: Antonio Casimiro (FC.ID)
- WP7: Juliane Steinhardt (UvA)

TABLE OF CONTENTS

1 Introduction

The domain of Cyber Physical Systems (CPS) is one of the largest information-technology sectors worldwide and a driver for innovation in many other crucial industrial sectors such as health industries, industrial automation, avionics and space. The embedded computer systems in these physically-entangled CPS increasingly rely on complex system architectures. Oftentimes these architectures are heterogeneous multi- core or many-core systems, which are distributed, and connected via complex networks. Highly distributed and networked systems entrusted with the control of physical assets are called Cyber Physical Systems of Systems (CPSoS).

Designers of these CPS(oS) face several daunting challenges as these systems have to meet a range of stringent extra-functional design requirements in terms of, e.g., real-time performance and energy efficiency. Mission- and safety-critical CPS(oS), like those in the avionics and space domains, usually also demand ultra-high levels of dependability. This is becoming even more important as the levels of system autonomy rise. With advanced levels of autonomy, more and more systems that were traditionally not considered safety-critical now become safety-critical. Furthermore, as mission- and safety-critical CPS(oS) become increasingly connected, they receive more and more attention from attackers, which may also render these systems unreliable and unavailable and thus potentially causing dangerous situations. To provide a high degree of reliability, availability, and safety, mission- and safety-critical CPS(oS) need to be able to cope with various disruptive events, which could be related to hardware component failures or cyber-attacks aimed at disrupting the system or worse, attacks compromising software components with the goal of taking over critical system functionality.

System adaptivity, foremost in terms of dynamically remapping of application components to processing cores, represents a promising technique to fuse fault- and intrusion tolerance with the increasing performance requirements of these mission- and safety-critical CPS(oS). The aim of the ADMORPH project is to make various types of complex systems that are controlled by computers more resistant to defects and more secure. The projects goal is, to develop technology to enable more resilient CPS(oS) against disruptive system events caused by either hardware component failures or cyber-attacks.
In the ADMORPH project, we evaluate this hypothesis using a novel, holistic approach to the specification, design, analysis and runtime deployment of adaptive, i.e., dynamically morphing, mission- and safety-critical CPS(oS) that are robust against both component failures and cyber-attacks. To this end, we will address four aspects that are instrumental for the realization of these adaptively morphing systems: (i) the formal specification of adaptive systems, e.g. by means of a coordination language to specify system requirements and adaptivity strategies; (ii) adaptivity methods like strategies for maintaining safe and secure control of CPS(oS); (iii) analysis techniques for adaptive systems to, e.g., perform timing verification of adaptive systems to avoid timing violations after system

reconfigurations; and (iv) run-time systems for adaptive systems that realize the actual run-time system reconfigurations to achieve fault and intrusion tolerance. The developed technology will be evaluated using three industrial use cases taken from the radar surveillance systems, autonomous operations for aircrafts, and transport management systems domains.

1.1 Project objectives

Objective 1: Robustness against component failures

Hardware component failures may be due to the harsh environment the system operates in, cosmic radiation, physical wear-out, manufacturing defects, etc. ADMORPH will develop technology that aims at prolonging the system lifetime and maximizing the system efficiency during this lifetime under the occurrence of hardware component failures.

Objective 1 directly addresses Impact 1, as specified in the H2020-01-2019 call: "*Availability of innovative technologies supporting compute-intensive applications in industrial and professional domains, demonstrating significant and measurable improvement over the state of the art."*

Within ADMORPH, we will develop novel technologies to increase the system robustness against component failures using adaptivity, providing a guaranteed quality- of-service and guaranteed real-time behavior.

We define the following two KPIs for Objective 1:

- **KPI 1.1:** Guaranteed quality of service in the presence of components failures
- **KPI 1.2:** Prolonged system availability despite component failures

Objective 2: Robustness against cyber-attacks

Cyber-attacks such as DoS or compromising system components can cause systems to become unreliable and unavailable. In the case of mission- or safety-critical CPS(oS), unavailability can subsequently lead to severe problems. For example, it can pave the way to coordinated attacks, which exploit the physical entanglement of CPS(oS) to cause harm in the physical world. Within ADMORPH, we will develop technology that aims at prolonging the availability of a system while under attack.

Objective 2 also directly addresses Impact 1: "*Availability of innovative technologies supporting compute- intensive applications in industrial and professional domains, demonstrating significant and measurable improvement over the state of the art."*

ADMORPH will provide novel means to fend off such cyber-attacks, even unknown ones, using a combination of detection and evasion mechanisms and fault tolerance mechanisms to protect highly-critical components.

We define the following two KPIs for Objective 2:

- **KPI 2.1:** Continued safe, fail safe, or fail-operational behavior while under attack
- **KPI 2.2:** Adaptation of the system to return to a state that is at least as robust as the initial one

Objective 3: Robustness of adaptation methodologies

ADMORPH will develop methodologies for dynamic application task coordination, foremost by means of application task re-mapping techniques, to achieve fault and intrusion tolerance of CPS(oS). Objective 3 directly addresses both Impact 1: "*Availability of innovative technologies supporting compute- intensive applications in industrial and professional domains, demonstrating significant and measurable improvement over the state of the art.*" and Impact 2: "*Availability of engineering practices and tools for CPSoS, resulting in a demonstrable improvement in quality and cost of development and operation for large SoS*".

The adaptivity methodologies and the development techniques for adaptive systems themselves constitute an objective of ADMORPH.

We define the following KPI for Objective 3:

- **KPI 3.1:** Adaptivity with bounded down-time and guaranteed robustness

Objective 4: Efficient engineering of robust, adaptive systems

The ADMORPH project aims at developing a holistic and efficient approach for systematically designing, analyzing, and run-time managing robust, adaptive CPS(oS).

Objective 4 directly addresses Impact 2: "*Availability of engineering practices and tools for CPSoS, resulting in a demonstrable improvement in quality and cost of development and operation for large SoS*".

- **KPI 4.1:** High-level means to model and analyse adaptive systems, and to deploy adaptivity methodologies
- **KPI 4.2:** Testing framework to properly quantify the impact of adaptivity

Objective 5: Industrial evaluation and dissemination of research

The methodologies, methods and tools developed within ADMORPH will be evaluated using *three* industrial use cases. As our application domains, we will use: (i) radar surveillance systems, (ii) autonomous aerospace systems, and (iii) transport management systems. These domains have been chosen as representative cyber-physical systems of systems of different sizes, with highly variant requirements on the safety, reliability, energy efficiency and security, and with a high economic impact.

Objective 5 directly addresses Impact 3: "*Increased synergies and collaboration between industrial and academic communities; dissemination of high-quality roadmap for future research and innovation activities in the relevant areas*".

Via the industrial partners of ADMORPH, we will directly apply and evaluate the techniques developed by the academic partners under realistic conditions. This allows us to validate the concepts we will develop within the project, but also to steer the research towards practicability and usefulness. We define the following three KPIs for Objective 5:

- **KPI 5.1:** Use-case implementation, which employs adaptivity to increase system robustness against component failures and cyber-attacks
- **KPI 5.2:** Use-case implementation, where the system adaptivity is developed and proven correct using ADMORPH's holistic approach to system design, analysis and run-time management
- **KPI 5.3:** Successful dissemination of ADMORPH's research results

2 Explanation of the work carried out by the beneficiaries and overview of the progress

2.1 Preamble: COVID-19 related problems

Due to COVID-19, we experienced several problems that have affected, to some extent, the progress of the project so far. For example:

- Setting up home offices;
- Problems related to working from home (working environment);
- Reduced social contacts between consortium partners and other research groups, which impacted collaborations as well as creativity;
- Loss/lack of face-to-face meetings and brainstorming sessions;
- Hiring stops at institutes and companies have led to a delay in staffing;
- Dissemination of the scientific results will likely be delayed/stalled by the lack of event participation. One example here is ECRTS 2020: This was one of the events that had to be held online and we are not sure that the paper we submitted received the same attention it would have received in real life.

The above-mentioned issues have impacted our work in general. Task-specific issues will be discussed in the designated task descriptions in Sections 2.2.1, 2.2.2, 2.2.4,2.2.5, 2.2.6, 2.2.7. To prevent these problems having negative impacts on our deliverables, we have had online meetings periodically since March on WP-level.

2.2 Explanation of the work carried out per WP

2.2.1 Work Package 1 (Effort: 59 PM)

This work package targets the specification of adaptive systems including their functional and non-functional behavior, possible fault and attack models, and formal guarantees of the adaptation layer itself. To this end, we will employ a coordination language that operates on a high level of abstraction. The coordination will describe the interplay between the functional components, the requirements on the non-functional behavior including reliability, time and security, and last but not least, the system of system and its fault model. The specification in the coordination language will be compiled towards a run-time coordination layer, implemented on top of an Operating System like Linux or PikeOS.

Task 1.1: Coordination language design (M01-M36)

Task leader: UvA

Task participants: UvA, ULUND

In this task, we will develop a domain-specific language (DSL) for coordination that enables domain experts to specify the software component interplay at a very high level of abstraction. At the same time, this DSL will support the efficient and effective specification of fault tolerance, timing, security and quality-of-service requirements and expectations. Specifications in this DSL set the scene for component-level timing verification as well as for system-level design-space exploration. This task will develop the entire basic compilation infrastructure, from front-end to back-end, needed for compiling specifications in the DSL towards generating a run-time coordination layer implemented on top of an Operating System like Linux or PikeOS.

I) Task status

Our work in Task 1.1 is based on the coordination language TeamPlay that has been under development since 2018 as part of the H2020 project TeamPlay. TeamPlay is a coordination language that supports the specification of cyber-physical systems on a very high level of abstraction as a system of implementation-wise opaque components and their orderly interaction (or coordination) in a streaming network.

For the ADMORPH project we have substantially extended the language design in two directions:

a) specification support for fault-tolerance giving programmers fine-grained control over the use of resilience techniques such as n-modular redundancy, checkpoint-restart and replication;

b) general improvements in defining abstractions in TeamPlay that are primarily motivated by the wealth of parameters coming with the fault-tolerance extensions in a).

This task has made substantial progress during the reporting period. In addition to the language design we have built a complete compiler and a code generator for a proof-of-concept runtime system. We plan to make this available to the consortium partners and to the general public in the near future.

II) Output

In addition to the language implementation work described above and the corresponding contributions to Deliverable D1.1 the scientific output of Task 1.1 so far are a Master Thesis and a refereed workshop paper:

- W. Loeve: Towards Integrating Fault-Tolerance in the TeamPlay Coordination Language. MSc Thesis, University of Amsterdam, 2020.

- W. Loeve, C. Grelck: Towards Facilitating Resilience in Cyber-physical Systems using Coordination Languages. 13th Seminar on Advanced Techniques and Tools for Software Evolution (SATToSE 2020), Amsterdam/Virtual, 2020.

III) COVID-19-related issues/delays:

Other than the ubiquitous general issues and problems that we all experience every day mentioned in section 1.2, two specific issues caused problems with Task 1.1. While one full-time position at UvA has been assigned to WP1 to work on Task 1.1 and subsequently Task 1.2, we were only able to fill this position with a fresh PhD student as of October 2020. In the mean time we have been compensating for this lack of manpower by a very capable Master student and considerable additional involvement by the WP leader, but this cannot deliver the same quality and quantity of work foreseen.

The other issue is a delay in systematic communication and collaboration between academic WP partners and with the industrial partners. Initially planned meetings were postponed under the assumption that travel would again be possible during summer at the very latest. By now we know that the current situation will likely persist for the foreseeable future and we must live with online communication.

Task 1.3: Specifying formal guarantees for the adaptation layer (M01-M24)

Task leader: ULUND

Task participants: ULUND, UvA

One of the objectives of this work package is to specify what kind of formal guarantees can be provided on the adaptation. An abstract example could be: "in response to event X, the predicate Y is false for a maximum time of T", which in concrete can be "if the temperature measured at the CPU level is higher than 90 degrees, after 30 seconds the system is able to recover and stops missing deadlines". This task will investigate how the guarantees can be specified.

I) Task status

We want to explore two types of formal guarantees: (i) at any point in time during the execution of the control system, what is the maximum amount of downtime that we can tolerate in terms of not harming the system behaviour, (ii) after a downtime of a given duration, what is the time the system needs to have in correct functioning mode to recover.

We have explored some aspects of (i) and found some theoretical results on how to find the maximum tolerable downtime. In (ii), we started looking at the performance degradation caused by the downtime and about how to relate the length of the downtime to the amount of degradation.

II) Output

Our initial investigation into (i) has been covered in a publication presented at the 2020 Euromicro Conference on Real-Time Systems (ECRTS), co-authored by Martina Maggio with Arne Hamann, Dirk Ziegenbein, and Eckart Mayer-John. We have also included some preliminary results in Deliverable D1.1.

Task 1.4: Specification of fault model and threat indicators (M01-M06)

Task leader: UNILU

Task participants: UNILU, UvA, ULUND, UTRC-I, TNL, QMA, SYS, FC.ID

For the DSL to anticipate faults and attacks, domain experts must be able to specify the fault categories (accidental and malicious) that the system should tolerate and the indicators that define the current threat level that the system is exposed to. For example, compromise of a replica of the communication gateway, as first component to pass when intruding the system, indicates an ongoing attack and should trigger the adaptation of the fault-threshold of critical components.

I) Task status

The goal of Task 1.4 was to specify the fault model and threat indicators to allow the DSL to anticipate faults and attacks. This goal has been achieved to the degree that other work packages depend on the results of this task. The results are reported in deliverable D.1.1 Section 4 with application specific aspects being reported as part of deliverable D.5.1. The next steps will be to develop a fault tree analysis (FTA) that is capable of anticipating partial adversarial success in compromising the system to derive the residual safety risks after individual components have been fallen into the hands of an attacker. Since this FTA will only be required at a later stage, we have postponed our work towards this part of deliverable D.1.1 and will report it as part of D.1.2.

III) Output

Deliverable D.1.1, specifying the fault model and threat indicators. The following is an executive summary of the specification in D.1.1:

We anticipate advanced and persistent threats under a common model of accidental faults and targeted attacks and with application of the AVI model. During runtime, we aim to compensate for this pessimism by adjusting the actual defense and tolerance mechanisms to the current threat level. Threats are observed in the environment and internally for interacted components to drive adaptation decisions for evading attacks or improving the internal resilience (e.g., by increasing the replication degree of a component).

- D.1.1 (M09) First report on a coordination language for robust, adaptive systems [UvA], involving Tasks 1.1, 1.3 and 1.4. This deliverable has been submitted on time.

III) COVID-19-related issues/delays

Specifically, for T1.4, COVID-19 related hiring difficulties at UNILU and FC.ID caused a delay in adjusting the fault tree analysis to reason about partially successful adversaries. As other work packages do not at the moment depend on this analysis, we will compensate and report the results as part of D.1.2.

2.2.2 Work Package 2 (Effort: 94 PM)

The prime objective of this work package is to develop the adaptation building blocks that are required to maintain the targeted quality of service guarantees or to gracefully degrade these guarantees if extreme situations force the system to engage in such trade-offs. To this end, we aim for methods, protocols, tools and techniques, to increase the resilience of the controllers of CPS(oS), to optimize the mapping, partitioning and scheduling of system components, to automate the design transformation towards a reliable, resource and physical requirement aware system, and to analyze and limit system reconfiguration times. The developed methods and protocols will guide the adaptation strategies (ensured by Task 2.5) that the runtime system (WP 4) will apply to adjust to unforeseen events and the developed tools will provide essential feed-back to the specification language (WP 1) and design space exploration tasks (WP 3). Task 2.6 provides test methods for this runtime system and its adaptation strategies.

During the first 12 month, only Task 2.1. was supposed to be active. COVID-19 caused late onboarding of students and post-docs delayed the execution of this task to Sept. 2020. We have compensated for this delay by covering in the preliminary version of deliverable D.2.1 (due in M12) the dependencies other

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

tasks have on this work package. Although the task has not yet started, early results of T2.6 are available.

Task 2.1: Control-aware fault and intrusion tolerance (FIT) (M01-M36)

Task leader: UNILU

Task participants: UNILU, FC.ID

The goal of this task is to develop FIT protocols and techniques to increase the resilience of controllers of CPS(oS) against advanced and persistent threats. Making FIT techniques application-aware (i.e., in this case aware of the controllers they should protect), allows us to optimize the resilience techniques to the specific guarantees that these controllers have to provide (e.g., stability, overshoot, reaction times, etc.). For example, masking faults (i.e., the ability to remain operational despite faults) may be sacrificed during recovery (Task 2.2) if the controlled system remains stable during the down-time a non-masked fault may cause during recovery.

I) Task Status:

Delayed start in M09. Cascading compensated by addressing external dependencies in D.2.1.

II) Output:

Preliminary version of D.2.1 is being prepared.

III) COVID-19-related issues/delays

The delayed onboarding of students/postdocs, due to hiring stops and the above-mentioned issues related to COVID-19 (1.2) have caused a delayed start of T2.1 to M09.

Task 2.6: Testing runtime systems and adaptation strategies (M19-M36)

Task leader: ULUND

Task participants: ULUND, QMA

Testing systems that embed adaptation strategies is difficult. Think of a machine learning algorithm: how many and which samples should we give to the system before we can consider its behaviour testable? And what is the correct outcome? Of course, we can apply unit testing to each function in the code, check for coverage, select a few cases in which the ideal behaviour of the code is known. But this does not give us any guarantee that the code is behaving correctly for the task it has to complete in the physical environment. Also comparing (adaptation strategies for) systems whose behaviour varies over time is difficult. One of the objectives of this work package is to develop testing techniques that allow us to test and compare the system together with the adaptation strategy that is embedded into it.

I) Task status:

The task has not formally started yet, but we started a preliminary study on how to test systems with adaptation. We have exploited the scenario theory, coming from the stochastic control domain. We have shown that when a system has some adaptation embedded in it, the scenario theory can provide probabilistic performance guarantees and definitely outperforms other testing strategies like Monte Carlo and Extreme Value Theory.

II) Output:

Our initial investigation has been covered in a publication to be presented at the 2020 Foundations on Software Engineering Conference (FSE-ESEC 2020), co-authored by Claudio Mandrioli and Martina Maggio. The code to reproduce the experiments presented in the publication is open source (and linked in the ADMORPH website). The publication received the ACM Distinguished Paper award.

- D.2.1 (M12) First report on identified adaptation opportunities and methods [UNILU], involving Tasks 2.1, 2.3. A preliminary version of this deliverable will be available with this report.

2.2.3 Work Package 3 (Effort: 75 PM)

The prime objective of this work package is to build robust tools to evaluate and analyze the runtime behavior of adaptive systems. We will work on developing a simulator to evaluate morphing systems, understanding the space of configurations to explore and its characteristics, encoding the designed adaptation strategies, and understanding how to provide formal guarantees and automated validation of safety for a morphing system - in particular with respect to the proposed case studies.
COVID-19 had an impact on the work package, in the sense that meetings and training sessions that were planned to take place physically had to be rescheduled in a purely virtual way. This made them less effective, and we expect that this could cause some delays in the following part of the project.
At the moment, there are three active tasks in the work package: T3.1, T3.3, and T3.4.

Task 3.1: System-level Simulation of Dynamically Evolving Embedded Systems (M01-M12)

Task Leader: UvA

Task Participants: UvA

In this task, we intend to study and develop simulation-based techniques to analyze and evaluate adaptively morphing embedded systems, building upon our extensive system-level modeling and simulation experience. Here, we plan to use a method based on Monte Carlo (MC) simulation to evaluate the ‘goodness’ of an adaptive embedded system instance, in which we expose the system simulation to sequences of disruptive events according to a given fault or attacks model.

This project has received funding from the *European Union’s Horizon 2020 research and innovation programme* under grant agreement No 871259.

I) Task status

Task T3.1 has been active since the beginning of the project and (not surprisingly) is the one that shows the most progress. In deliverable D3.1, we introduce a first version of our novel system-level simulator that has been developed for analyzing the extra-functional requirements (lifetime reliability, power/energy consumption and cost) of adaptive embedded systems. In this deliverable, we explain how our simulator works at a high-level of abstraction and detailed the components/models involved in the simulator and how they interact with each other. At this moment, we consider simplistic models to have the first version of our simulator running. In the future, we plan to replace all models with more accurate ones that fit more to the project needs and case studies as well.

II) Output

As mentioned above, an output of our work so far is a developed simulator, for which we refer the interested readers to Deliverable 3.1 for more details. The simulator is Open Source, and the sources can be found at https://github.com/sea-art/Simuflage. As a result of this simulator, we aim at publishing 1 or 2 papers soon.

Task 3.3: Adaptivity-Aware Real-Time Scheduling Policies (M01-M24)

Task Leader: UAU

Task Participants: UAU, UvA, UNILU, SYS, FC.ID, UTRC-I

In this task, we will develop real-time scheduling techniques and analyses for dynamically evolving systems. The immense state-space of system configurations prohibit an analysis and optimization of the individual system configurations. We will thus develop techniques to analyses the timing behaviour of multiple system configurations at once. To this end, we will extend the concept of sustainable scheduling analysis to hardware components. Starting from a feasible system, where any additional component failure will result in the violation of the timing behavior, we can provision additional resources while ensuring timing correctness of the resulting system configuration. SYS will work with the partners in using the scheduler plug-in framework developed in Task 4.2 for implementing adaptivity-aware scheduling algorithms on the PikeOS separation kernel.

I) Task status

This task is devoted to fault-tolerant scheduling policies. The task has progressed largely as foreseen and planned. A prototype of the runtime environment to test and evaluate fault-tolerant scheduling policies is available for different architectures. The details about the progress of this task have been reported in deliverable D3.1

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

II) Output

Foremost, the prototype was developed for testing and evaluation of scheduling policies only. We will make it available to the other partners and consider to publicly release the prototype by end of the Task 3.3 (M24). The details about the progress of this task have been reported in deliverable D3.1. Paper publications are in preparations.

Task 3.4: Models of Computation and derived Architectures to allow seamless reconfiguration (M07-M16)

Task Leader: UTRC-I

Task Participants: UTRC-I, UvA

This task will propose a set of features for models of computation and their derived constraints for hardware/software architectures (targeting Multi-core, FPGA and distributed) to allow seamless reconfiguration to achieve dynamic adaptation. This task is linked to the architecture definition and physical constraints introduced in WP 5 to implement those constraints specified by the coordination language. The model should include the possibility of task graphs to be updated (including reconfiguration tasks, on-demand redundancies and communications re-mapping) and for certain levels of optimization to be performed at run time.

I) Task status

Task 3.4 aims at defining the appropriate model of computation and architecture model, which will allow all possible reconfigurations, i.e. hardware, software, software-to-hardware mapping, software timing (scheduling), QoS, and any combination, in a seamless manner. The primary focus for now has been to explore state-of-the-art of models for hardware, software, software-to-hardware mapping, software timing (scheduling) and QoS. While an all-encompassing model might seem a good idea, the literature suggests that such models become hard-to-use and are frequently error-prone.

II) Output

First report on analysis techniques for adaptive systems.

- D3.1 (M09) First report on analysis techniques for adaptive systems [ULUND], involving Tasks 3.1, 3.3 and 3.4. Deliverable D3.1 has been submitted on time.

2.2.4 Work Package 4 (effort: 86 PM)

This work package aims at developing the run-time support, as part of (among others) SYS' PikeOS separation kernel, for adaptive CPS(oS) that are robust against both system faults and cyber-attacks. To this end, the work package addresses the dynamic detection of disruptive events such as faults or attacks,

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

as well as the dynamic system reconfiguration support that is required to deal with these disruptive events.

In the reporting period from M1-M10, we have worked on Task 4.1, Tasks 4.4 and Task 4.6. Some preparatory work was also carried out for Task 4.2. The detailed report is presented below.

Task 4.1: Porting PikeOS to boards/platforms used for WP 5 use cases (M04-M12)

Task leader: SYS

Task participants: SYS, UTRC-I, TNL, QMA

In this task, SYS will work together with industrial partners in identifying hardware platform for the use cases and port PikeOS separation kernel to the selected hardware platform(s). We will also develop drivers for the IO devices in the platform and port guest operating systems/runtimes such as virtualized Linux, POSIX, APEX based on the requirements of industrial demonstrators.

I) Task status

In this task, SYSGO has worked together with industrial demonstrator partners to define the hardware and is porting PikeOS separation kernel, runtimes and Board Support Packages (BSP) on the identified hardware platforms. The following are the main activities carried out in this reporting period:

- PikeOS 5.0 separation kernel is ported to armv8 and e500mc architectures
- BSP for UTRC hardware (Xilinx US+) is developed/ported
- BSP for QME hardware is under development and expected to complete in M12
- PikeOS training is provided to the project partners
    - 13 participants from the consortium were present
    - Training was conducted in four sessions on 4.06, 10.06, 17.06 and 18.06
- PikeOS support for heterogeneous SoC
    - PikeOS for microcontrollers (codename: M-Pike) is developed with the following design goals:
        - Certifiability/use in safety-critical application such as the UTRC-I use case
        - Easy migration of PikeOS tasks – during design time and runtime
        - Fully compatible with PikeOS separation mechanisms – resource and time partitioning
    - Currently M-Pike running on R52 MCU simulated using ARM Fixed-Virtual Platform (FVP)
    - Porting of M-Pike to R5 cores (on US+) started, expected to finish by M12

II) Output

- PikeOS 5.0 and the first version of BSPs are delivered to UTRC-I. QMA has received the BSP for their HW platform.
- All partner participated in the PikeOS training received PikeOS separation kernel, development tools and QEMU based simulation platform to get familiarized with the development environment and to reproduce the demos and exercises from the training.

III) COVID-19-related issues/delays

- PikeOS training was conducted online instead on standard on-site training. To make the training comfortable and comprehensive, we have split the training into 4 sessions spanning over 4 days instead on usual 2 days training.

Task 4.2: Extend PikeOS with support for fault detection and adaptation (M13-M36)

Task leader: SYS

Task participants: SYS, UNILU, UvA

Detecting safety and security faults: We will extend the used PikeOS separation kernel with sensors/monitors for detecting HW faults, timing faults, and programming errors. We will investigate separation kernel level introspection mechanisms to extract virtual machine's static and dynamic configurations and to monitor its resource consumption (e.g. bus, memory, file descriptors etc.). The separation kernel security mechanisms will be augmented by communication monitoring infrastructure for detecting anomalies or overload in the inter-partition or external traffic (e.g. enabling partners to use IDS like solutions). For advanced protection, we will research techniques such as Control Flow Integrity (CFI)[1] for detecting runtime code reuse attacks such as return-into-libc[2] or return oriented programming[3].

Separation kernel-level adaptation mechanism: The PikeOS separation kernel will be extended with mechanisms to support dynamism in space and/or in time (e.g. dynamic memory management in user-space, dynamic time partition switching, pluggable dynamic scheduling policies, primitives to implement dynamic information flow channel between partitions). We will investigate mechanisms for reliable reallocation of IO devices and accelerators to partitions during a reconfiguration step and will implement a novel infrastructure for the migration of tasks between different processing elements in a heterogeneous multi-core platform. For preserving assurance, we will research architectures to support modular (re)configuration of virtual machines to enable incremental/compositional

[1] M. Abadi, M. Budiu, ÚlfU.ar Erlingsson, and J. Ligatti. "Control-flow integrity principles, implementations, and applications". ACM Trans. Inf. Syst. Secur. 13, 1, Article 4, November 2009.
[2] H. Shacham. "The geometry of innocent flesh on the bone: return-into-libc without function calls (on the x86)". In Proceedings of the 14th ACM conference on Computer and communications security (CCS'07), 2007.
[3] R. Roemer, E. Buchanan, H. Shacham, and S. Savage. "Return-Oriented Programming: Systems, Languages, and Applications". ACM Trans. Inf. Syst. Secur. 15, 1, Article 2, March, 2012.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

verification/certification when performing a partial software update to respond to a safety/security incident. We will assess different fault tolerant and SMR techniques applicable for the critical infrastructure applications and develop separation kernel infrastructure needed to implementing them such as clock synchronization - synchronizing PikeOS system clock and the clocks on virtual machines with a master clock. Finally, we will implement support for cryptographic primitives for providing authenticated communication channels and support to implement optimized BFT-SMR protocols such as MinBFT (e.g. via TPM usage).

I) Task status:

We started with the preliminary work of Task 4.2 that includes the following:

- Initial discussion on the reconfiguration primitives with UTRC
- Started investigating OpenAMP for Xilinx US+ heterogeneous SoC for life-cycle management of different processing elements (PE), communication between different instances of PikeOS and M-Pike or other OSes running from different PEs
- CFI for detecting RoP like attacks is prototyped
- Certifiable (meaning: lean) inter-PE/OS communication primitives with queuing-port semantics built on top of shared mem and interrupts under design

II) Output

In progress.

Task 4.4: Runtime support for resilient control (M07-M24)

Task leader: UNILU

Task participants: UNILU, FC.ID

Whereas large parts of the resilient control of highly critical functionality happens in the Byzantine fault tolerance protocols and their implementation, the detect + recover schemes for less critical functionality and certain recovery operations of highly critical replicated functionality requires support from the runtime system and, in part also, from the operating system. In this task, we develop the runtime support for resilient control, including for example, the mechanisms required to relocate a replica from a permanently damaged hardware unit and re-integrating it into the active replica set.

I) Task status

When it comes to interfacing a low-level resilient controller with the actuators or a plant, we have to distinguish resilience-aware actuators from resilient-agnostic ones. Whereas the former would offer precautions that prevent faulty or minority signals from becoming effective (such as, separate interfaces and actuator-internal means to counter opposing inputs - e.g., mechanically as found in aircraft elevator control systems), resilient-agnostic actuators require extra care to not propagate software defects to the

physical world. For the latter, the runtime needs to offer at least a trusted voter and, as early results from Task 1.3 indicate, the ability to hold the previous signal in case of voter mismatch, to enforce that updates happen only consensually. The generic voter, in its simplest form is realized as a propose, agree/disagree interface, subsumes resilience patterns such as plausibility checks (monitor disagrees to implausible results), but also full Byzantine agreement (rotate proposer until a healthy replica had the chance to make a proposal). Higher-level resilient control, in particular interaction between low-level and more complex high-level controllers require further investigation of interaction patterns, as highlighted in Aegean[4]. We plan to investigate to which extent such patterns can be supported by PikeOS application-level components (e.g., realizing replica-group to replica-group broadcast and logging of results) and where additional kernel support is required for performance or reliability reasons.

II) Output

In progress.

III) COVID-19-related issues/delays

Hiring difficulties at UNILU and FC.ID caused a delayed start of the task, which did not begin until M10.

Task 4.6: Update framework (M07-M18)

Task leader: TNL

Task participants: TNL

CPS operate outside the perimeter of the internal and safe network. A framework is required to automatically identify and upload software updates to remote locations in such a way that the impact of a cyber-attack is limited. Additionally, a recovery mechanism is required when the software repository is compromised. Updates can contain any kind of artefact (libraries, profiles, files, patches, documentation, etc.).

I) Task status

Task has not yet started.

II) Output

Not applicable.

[4] Remzi Can Aksoy, Manos Kapritsos, "Aegean: Replication Beyond the Client-Server Model", SOSP 2019

III) COVID-19-related issues/delays

We foresee that Covid-19 will have an impact on the progress of task 4.6. Factors mentioned in Section 2.1 have resulted in a 2-month delay for task 4.6. In the current situation this delay cannot be adjusted and will most probably have an impact on D4.1 (M12). At the moment, however, this delay does not have an impact on D4.2 (M24).

2.2.5 Work Package 5 (Effort: 123 PM)

This work package is focused on showing how the technology developed in the previous work packages is applied to industrial scenarios. The work package will show three use cases, (a) Radar Surveillance Systems, (b) Autonomous aerospace systems, and (c) Railway Transportation Systems.

Task 5.1: Requirement analysis and use case specification (M01-M06)

Task leader: UTRC-I

Task participants: ALL

This task will explore dynamic adaptability in case of real-time mission- and safety-critical systems for the three use-case applications. The main focus will be defining fault and attack taxonomies to specify which cases are to be addressed by the adaptation layer. This will include which faults or attacks will be considered, which systems will require fault tolerance; if it is necessary and/or affordable to asses fault removal, and ways to enable fault forecasting. Moreover, hardware / software platforms for proof-of-concept experiments in the context of the three use case applications will be determined and specified. Last but not least, for each particular use case, more concrete and tangible metrics for measuring the success of our Objectives 1-5 and respective KPIs 1-9 (see Section 1.1) will be specified. This task will be performed in close interaction with Tasks 1.3 and 1.4 from WP 1. The work performed in this task also allows for a comparison between the outcomes of the three different use cases, and learn the lessons from this, at the end of the project.

I) Task status

The purpose of the first task of WP5 is to define the requirements and success criteria for the ADMORPH use-cases. In particular the task defined the functional and, most importantly, the non-functional requirements of the use-cases as well as the success criteria.

II) Output

D5.1 Report on requirement analysis and use case specification, has been submitted on time.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

Task 5.2 Aerospace Use Case (M07-M36)

Task leader: UTRC-I

Task participants: ALL

This use case considers increasing aircraft autonomy and will be demonstrated using a 3D simulation environment connected in a Hardware-in-the-Loop (HiL) fashion to the computing system. The system will allow fault injection to mimic operational failures and attacks, as well as changes in the 3D environment conditions to trigger adaptivity. Evaluation of the adaptivity methods and architectures in terms of performance and degradation of Quality of Service (QoS) will also be included.

I) Task status

The Auto-taxi application has been ported and severely extended. The application consists of Simulink models that are responsible for auto-thrust, auto-brake, path-following, ATC communication (from which the taxi path is acquired), steering control, etc. The application has been interconnected with the FlightGear flight simulator where it is able to successfully control the airplane in real-time and taxi it according to a given path.

This model-in-the-loop setup is the current state of the demonstrator. In addition, a couple of fault-detections mechanisms have been developed that are able to identify if there is an error in the taxiing path (due to a fault or an attack on the ATC communication).

II) Output

First version of the prototype available. This a basic demonstrator (solely software) at approx. 70% functionality.

Task 5.3 Radar systems Use Case (M07-M36)

Task leader: TNL

Task participants: ALL

TNL will provide end user feedback to the other partners and participate in the evaluation of the ADMORPH approach throughout the project. The task will involve evaluating specific methods within the context of an industrial embedded software system (or subsystem) used for radar surveillance processing. As command and control decisions require reliable and robust real-time data processing, the ability of the ADMORPH approach to achieve fault tolerance will be substantially assessed and validated. The development flow will be integrated to the TNL development flow and system results will be measured and compared to the traditional systems. The runtime system will consist in using lightweight container virtualization in combination with an orchestration framework. Software updates are automatically identified and installed in a secure way using the update framework.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

I) Task status

The work for task 5.3 has suffered a 2-month delay due to COVID-19 issues (see below). This delay can be made up for, so at the moment this has no impact on D5.2 or D5.3.

II) Output

Not applicable.

III) COVID-19-related issues/delays

COVID-19 has an impacted the work at TNL, due to the factors mentioned in Section 2.1 and has caused a 2-month delay. This delay will be made up in the beginning of 2021.

Task 5.4 Transport systems Use Case (M07-M36)

Task leader: QMA

Task participants: ALL

The transport systems use case will validate the project outcomes in the railway industry with a focus on metro operation or other urban guided transportation management and control systems (UGTMS) according to the standard [IEC62290][5]. It includes a close cooperation with WP 4 to analyze and define requirements on the adaptively morphing platform and extended PikeOS. QMA will integrate the WP 4 outcomes at the predefined HW platform with taking into consideration security and railway specific requirements, i.e. analysis and consideration of requirements of the following standards: [IEC62443][6], [EN50126][7], [EN50159][8] and related. The integration will then be verified and validated in the specific railway test environment.

I) Task status

Based on D5.1, System Requirements (SYS_RQ), HW Requirements (HW_RQ) and SW Requirements (SW_RQ) were specified for the demonstrator prototype (Baseline 1) within T5.4.

These include both WP and application-specific requirements. The demonstrator will be used at the interface of two railway subsystems - train / stationary, so it was necessary to define in addition to functional requirements also non-functional requirements in the field of Cyber Security and environmental requirements that must be accepted when implementing Railway systems. SW

[5] International Electrotechnical Commission. "IEC 62290-1: Railway applications: Urban guided transport management and command/control systems." *Part1: System principles and fundamental concepts* (2007).

[6] IEC 62443-4-2 Ed.1 Security for Industrial Automation and Control Systems (IACS) part 4-2: Technical Requirements for IACS components (IEC/TC57/WG15, SCA45A/WGA9, ISO/IEC JTC1/SC27/WG3 N1178 (2015-07) IT ST - Security Evaluation, Testing and Specification), https://webstore.iec.ch/preview/info_iec62443- 2-4%7Bed1.0%7Db.pdf

[7] CENELEC, EN50126. "Railway Applications–The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)." *The European Standard* (1999).

[8] CENELEC, EN. "50129: Railway applications–Communication, signalling and processing systems–safety related electronic systems for signalling." *Europäische Norm, Okt* (2003).

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

requirements (SW_RQ) were specified mainly for the needs of WP4. The requirements for the other SW components of the demonstrator will be specified in the next stage.

II) Output

Not applicable.

III) COVID-19-related issues/delays

There are some delays, due to COVID-19 related issues (Section 2.1) made work on T5.4 less effective.

- D5.1 (M06) Report on requirement analysis and use case specification [UTRC-I], involving Task 5.1. This deliverable was submitted on time.

2.2.6 Work Package 6 (Effort: 36 PM)

The prime objective of this work package is to oversee and organize the dissemination and exploitation of ADMORPH's results in the scientific community and in relevant European industrial circles. Moreover, this work package coordinates the communication of our findings and of the societal impacts they imply, when reaching out to the general public. The detailed objectives of the work package are the following: definition of the overall exploitation plan for the project and individual exploitation plans for each partner; promotion and dissemination of the results through participation in various events such as workshops and conferences; publication of the main results in scientific journals, conference proceedings and books.

Task 6.1: Dissemination, communication and community building (M01-M36)

Task leader: FC.ID

Task participants: ALL

This task is responsible for the communication of the project and its results, both to the internal audience, the scientific community, affiliated industry partners and the general public. The task will plan and monitor the project's dissemination and communication activities, and will produce specific outreach materials for relevant conferences and forums. The task will set up structures and processes for dissemination activities such as: creation and maintenance of a project visual identity, namely by providing templates for presentations and reports; creation and maintenance of a project website, including project information, news and publications; presentation of the project during conferences or workshops; continuous collection of all dissemination, cooperation and communication activities of the project; preparation of news for social media to raise public awareness of the project and its results.

In order to disseminate main project results, the consortium will organize technical workshops within the project. These workshops will provide broad and in-depth overviews of the project results and findings, and include interactive sessions to capture potential feedback from experts outside of the

consortium. Depending on the target group addressed, the partners will further disseminate the project results by giving talks at conferences and trade shows and by writing articles for technical and academic publications. All partners will contribute in a wide range of different dissemination activities, including the use of closed forums that they have access to, such as science.lu, SnT's partnership day, ICT.OPEN in the Netherlands, etc., involving affiliated industry partners and the general public. Further important communication channels will be press releases, project leaflets, university lectures, invited talks, and presentations of the project results. ADMORPH will also use social media like Twitter or LinkedIn as communication channels to keep interested parties updated about project work.

I) Task status

For task 6.1 dissemination, communication and community building, during this period, included the construction of the project website, a twitter and LinkedIn channel. Also, achieved was the preparation of a dissemination action plan (D6.1) by month 3. The dissemination action plan was submitted to the Commission. The website contains sections on the project, its aims, the consortium partners and personnel, contact details, an active News and Events section, a feed of the project's twitter account.

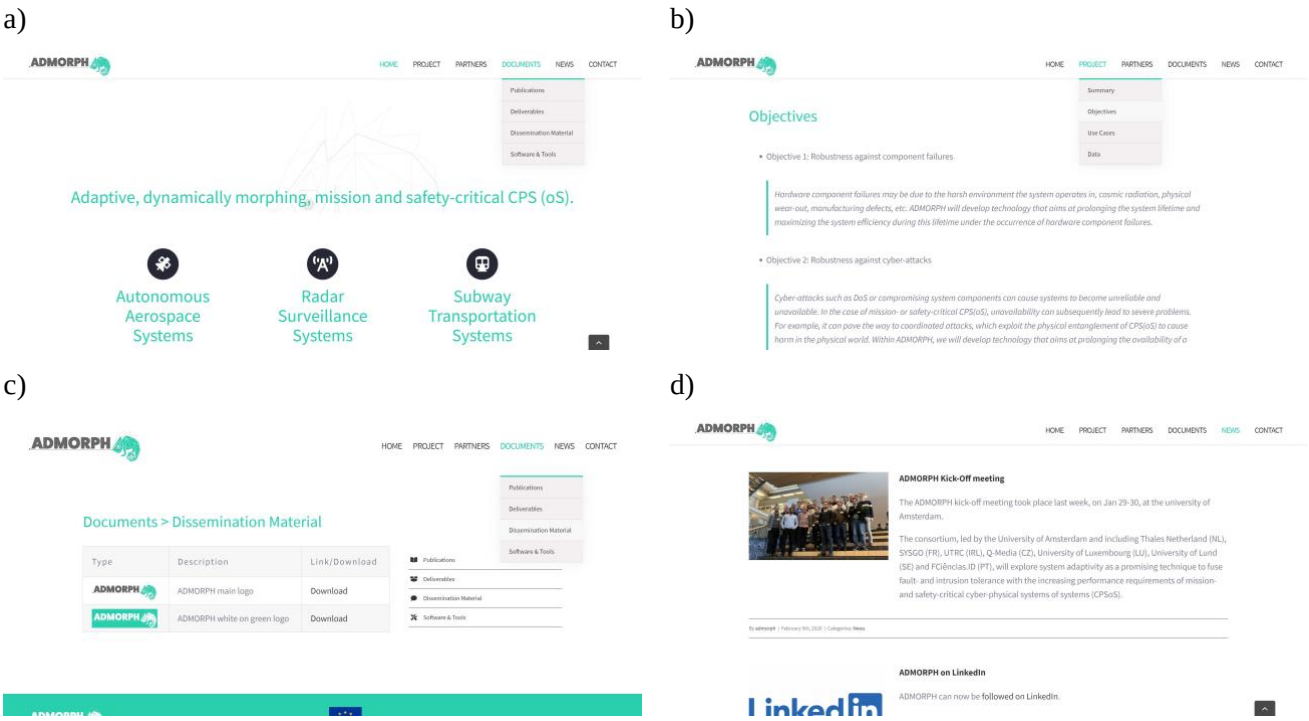

Figure 1: ADMORPH website showing: a) Landing page, b) Objectives page, c) Dissemination materials page and d) News page.

The ADMORPH twitter account is active and in use, and a project documents section, which includes dissemination material (e.g., project logos), a list of publications, a list of public deliverables (to be added when approved by the Commission), and space to add software and tools developed within the project. Since March 2020, there were more than 600 sessions (visits) to the website, by more than 400

different users, which means nearly 100 visits per month. The following image provides the main statistics.

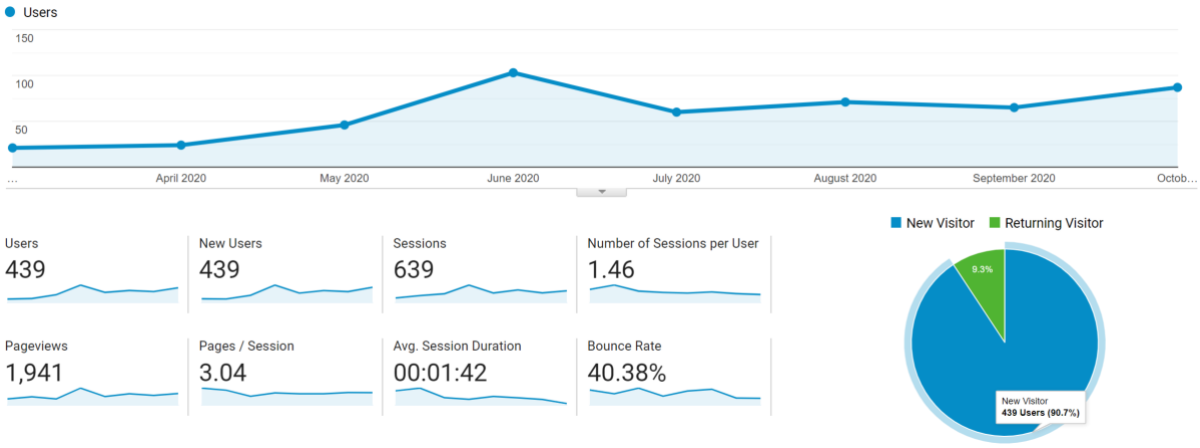

Figure 2: Main statistics of the ADMORPH website.

Most followers are recorded up to date for LinkedIn (24 followers to date). Several posts have been made on this account, and propagated to twitter. In particular, news items added to the ADMORPH web site are propagated to these accounts, for further visibility.

The visual identity of the project was created and has been used in all contents produced by the project, namely on the web page, on presentations and on deliverables. To ensure a consistent use of the image, presentation and deliverable templates have been created, both in Microsoft Word and Powerpoint formats and also in the LaTeX format.

A Git repository has been created and is maintained at the Faculty of Sciences of the University of Lisbon (FCUL), who coordinates this work package. The repository is used for storing project documents, ensuring a consistent view of all partners over shared material, and facilitating collaborative work on shared documents, such as deliverables.

It is also important to mention that an ADMORPH press release was prepared by the project coordinator short after the beginning of the project, under the title “University of Amsterdam receives €4.5M from Horizon 2020”, which was disseminated by the university of Amsterdam and through the project channels.

II) Output

In this initial period of the project, there have been 4 publications accepted for presentation in international events. The list of publications and respective information about the events in which they have been or will be presented is the following:

- **Don Kuzhiyelil, Philipp Zeiris, Marine Kader, Sergey Tverdyshev, Gerhard Fohler**, *Towards Transparent Control-Flow Integrity in Safety-Critical Systems*, 23rd Information

Security Conference (ISC 2020), December 2020. To be held on-line due to the COVID-19 pandemics.

- **Claudio Mandrioli, Martina Maggio**, *Testing Self-Adaptive Software with Probabilistic Guarantees on Performance Metrics*, ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2020), November 2020 – **ACM Distinguished Paper Award.** To be held on-line due to the COVID-19 pandemics.
- **Jan Procházka, Petr Novobilský, Dana Procházková**, *Certification Cycles of Train Cyber Gateway*, **ESREL2020 and PSAM15**, November 2020. Mixed physical and virtual attendance.
- **Martina Maggio, Arne Hamann, Eckart Mayer-John, Dirk Ziegenbein**, *Control System Stability under Consecutive Deadline Misses Constraints*, Euromicro Conference on Real-Time Systems (**ECRTS 2020**), July 2020

In addition, two other publications have been accepted and have been or will be presented at national events:

- **Jan Procházka, Petr Novobilský, Dana Procházková**, *Segmentation of Train Control Systems*, **IRICon2020**, November 2020.
- **Jan Procházka, Petr Novobilský, Dana Procházková**, *Standardization of communication security train-control centre*, **CRISCON2020**, September 2020

III) COVID-19-related issues/delays

Many of the planned events (conferences and workshops) had been cancelled, due to COVID-19. This resulted lesser opportunities for dissemination and outreach activities.

Task 6.2: Exploitation and use (M01-M36)

Task leader: UvA

Task participants: ALL

Given that most of the project work will be done at relatively low values of TRL (up to TRL 5), exploitation of developed tools, technologies and demonstrators will primarily consist in bringing these into further development and use in other activities beyond the project end. Therefore, this task will continuously monitor the work being developed for TRL assessment, and from the perspective of identifying and tracking project results with potential for further use and exploitation. Moreover, these potential uses will be classified by identifying opportunities and shortcomings for this exploitation to be effectively achieved, and planning (and periodically revising this plan) how the partners will use and exploit the results.

I) Task status

Concerning Task 6.2, on exploitation and use, the activity has been essentially related to monitoring the progress of research activities and ensuring that no potentially exploitable results are released into the public without adequate protection of IPR. For that purpose, a process has been set up and agreed by all project participants to ensure that no results are published without the previous consent of all partners.

II) Output

Not applicable.

III) COVID-19-related issues/delays

COVID-19 related cancellation of many planned events (conferences and workshops), resulted lesser opportunities related to exploitation.

Task 6.3: External Expert Advisory Board management (M01-M36)

Task leader: UvA

Task participants: UvA, ULUND, UNILU, SYS, UTRC-I, FC.ID

This task will manage the interactions between ADMORPH and the EEAB, namely ensuring that they are aware of project progresses and results, collecting their advice on project directions, dissemination and exploitation opportunities, and implementing measures within ADMORPH according to the received advice.

I) Task status

Finally, concerning Task 6.3, whose objective is to manage the interactions between ADMORPH and the EEAB, it must be pointed out that the EEAB has been established and two of its members were able to participate in the Kick-Off meeting, while all of them attended the 2nd ADMORPH General Assembly (which was held virtually).

The following people have agreed to take a seat in the ADMORPH's EEAB:

- **Dr. Dirk Ziegenbein**, Chief Expert Engineering Open-Context Systems & SW Systems Engineering, Robert Bosch GmbH, Germany;
- **Prof. Marisol Garcia Valls**, Professor, Department of Communications of Universitat Politècnica de València, Spain;
- **Prof.dr. Leandro Soares Indrusiak,** Reader in Real-time Systems, Dept. of Computer Science, University of York.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

II) Output

Not applicable.

- D6.1.a (M03) Dissemination Plan and Report [FC.ID], involving Task 6.1
  Deliverable D6.1 has been submitted on time.

2.2.7 Work Package 7 (Effort: 18 PM)

Provide full transparency and control of the entire project to the consortium and the EC in terms of time, resources and cost tracking, through the following activities: 1. Establishment and maintenance of the decision-making and management structure; 2. Efficient coordination of the integration of all the work packages and data management; 3. Handling of risks and contingencies; 4. Efficient communication inside and outside the consortium; 5. Reporting, communication and consultation with the European Commission on contractual and financial matters; 6. Monitoring the overall legal and contractual management of the grant agreement; 7. Monitoring and control of the financial budget and corresponding resource usage; 8. Ensuring that IPR, legal and ethical issues are properly dealt with. The tasks of this WP cover the overall technical, financial and administrative management of the consortium and the project's activities. The coordinator, UvA, is the task leader for all its tasks. All partners will contribute to this WP as contributors to the other work packages, therefore no person-months are foreseen for the partners in this specific WP.

For the coordination and management of the ADMORPH project the following tasks were carried out for setting up the project and coordinating the first 10 months of the project:

Task 7.1: Coordination of the activities inside and outside the consortium (M01-36)

Task leader: UvA

Implement internal and external communication mechanisms and administrative measures to ensure the efficiency of the Project and the overall operations of its activities. This will include:

1. Organize the decision-making and management governance and provide administrative support of their procedures (defining standard rules and procedures for the monitoring of the tasks, the use of project documentation, and the production of internal reports);
2. Implement a coherent and efficient communication strategy inside the consortium: mailing lists, collaborative environment, and procedures;
3. Organise consortium wide meetings (in collaboration with other beneficiaries where appropriate);
4. Support the Networking Activities and work package leaders in the communication lines outside the consortium.
5. Representation of the project in European and International relations

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

6. Networking with other projects and organisations

I) Task status

To ensure a consistent implementation of the management of the project, UvA produced a project procedure handbook that is easily accessible to all partners via the projects shared platform on Gitlab, which will describe internal reporting, communication and management procedures, as well as a Quality Assurance Plan to monitor all deliverables before their finalisation. The deliverable also contains a detailed risk analysis and contingency planning.

Meetings:

- Kick-off meeting in Amsterdam from 29-30 January 2020, 25 participants
- 2nd Consortium meeting and GA meeting from 2-3 June 2020 (online), 25 participants
- Online GA meeting, 25 September, 11 participants
- Preparation of 3rd Consortium meeting and GA meeting from 16-17 November 2020 (online)

Communication:

- Through mailing lists

  The mailing lists include a list for: the all consortium members, the EEAB and project coordination team, the GA members, and one for each of the project's work packages.
- Through teleconferences, for the Executive Board and GA meetings as well as consortium meetings.

We have also completed the External Expert Advisory Board (EEAB), after one of its members was not able to sign the Non-disclosure agreement. The newly added member (Prof. Marisol Gracia Valls) was added to the EEAB.

II) Output

Deliverable D7.1, the project handbook, has been submitted on time.

III) COVID-19-related issues/delays

Due to COVID-19 many of the partners had hiring stops or delays, which led to a delay of the full staffing of the consortium until the end of M09.

We were faced with the problems of having to organize remote meetings. This also affected our 2nd consortium meeting, which was originally planned to be taking place in Augsburg.

After finding a suitable platform for remote conferencing, we successfully organized a remote (online) consortium meeting (2nd-3rd June 2020). All WP meetings have now been organized remotely.

In response to COVID-19 we have also organized an additional GA meeting (25th September) to discuss possible issues or delays the project might be facing, due to COVID-19.

Task 7.2: Quality control and work plan monitoring (M01-36)

Task leader: UvA

Manage and support the quality control and timely delivery of project reports and deliverables:

1. Set up and maintenance of an internal quality assurance procedure to monitor deliverables;
2. Monitoring of all project activities and ensuring that they are in line with the project work plan, also through internal reporting;
3. Assuring that necessary actions are undertaken in case of delays or underachievement, and if required executing the appropriate contingency plan, to minimize any delays and their impact on dependent work packages.

I) Task status

To ensure quality control and work plan monitoring, UvA produced a project procedure handbook that is easily accessible to all partners via the projects shared platform on Gitlab, which will describe internal reporting, communication and management procedures, as well as a Quality Assurance Plan to monitor all deliverables before their finalisation. The deliverable also contains a detailed risk analysis and contingency planning. The internal review procedure by two partners, who are not involved in the active deliverable, as well as the management team has proven to be a good measure to assure timely delivery and assured a satisfactory quality assurance.

II) Output

Deliverable D7.1, the project handbook, has been submitted on time.

Task 7.3: Communication with EC, periodic reporting and financial management (M01-36)

Task leader: UvA

1. Interface with the EC administrative offices on behalf of the consortium for the administrative, financial and legal issues;
2. Ensure that necessary audit certificates are delivered as appropriate;
3. Manage progress reporting, specifically collecting information from partners, assembling and forwarding progress reports, ensuring timely delivery to the EC;
4. Financial and accounting management: set up internal reporting procedures, prepare, write and submit financial reports, ensuring compliance with accounting principles and contract rules;
5. Ensure that payments are transferred to participants without delay.

I) Task status

We have set-up a productive remote communication with our EC Project officer. The technical review report is to assess the work carried out under the project over a certain period (first 10 months of the project) and provide recommendations to the Commission.

II) Output

Deliverable D7.3- Progress Report for Technical Review, has been delivered on time.

Task 7.4: IPR, legal and contractual management (M01-36)

Task leader: UvA

Handle all IPR, legal and contractual issues in the project:

1. The negotiation and implementation of the Consortium Agreement weighing the rights and obligations of the beneficiary under the Grant Agreement;
2. The protection of the knowledge and IPR issues that may arise during the project's lifetime;
3. Handling any legal issues arising from the contractual obligations of the consortium towards the EC.

I) Task status

The grant agreement and consortium agreement were agreed upon and signed by all partners. Additionally, we have submitted two amendments to the EC within the first 10 month. This was to add the University of Augsburg (UAU) to the list of consortium members, as Sebastian Altmeyer (former UvA staff) had taken up a new position at UAU. The Amendment included a shift of PersonMonths from the UvA to UAU and the transfer.

In August, we have also initiated an amendment to include a linked third party (Sysgo GmbH) to our consortium partner SYS, who will distribute some of its workload (18PM) towards its daughter company.

II) Output

Not applicable.

Task 7.5: Data management (M01-36)

Task leader: UvA

Set up and implement a data management policy for all the datasets that will be generated by the project, to be included in the Data management plan.

I) Task status

In order to provide an analysis of the main elements of the data management policy that will be used with regard to all the datasets that will be generated by the project, a DMP has been produced. It describes the data management life cycle for all datasets to be collected, processed or generated by the project and it will evolve during the lifetime of the project in order to present the status of the project's reflections on data management.

II) Output

Deliverable D7.2 (M6) Data management plan (first version) has been submitted ahead of time.

- D7.1 (M3) Online Project Handbook [UvA], involving Tasks 7.1-7.4.
- D7.2 (M6) Data management plan (first version) [UvA], involving Task 7.5.
- D7.3 (M10) Technical review report

2.3 Impact

We find it too early to report on impact. Dissemination activities can be found in section 1.2.7.

3 Update of the plan for exploitation and dissemination of result

The COVID-19 situation has had an impact on dissemination activities that we are now starting to perceiving more clearly (e.g., it is not so easy to meet other people, there are less meetings and opportunities to disseminate) and, given that it is still unclear when the situation will improve or end, we will make an update by the end of the year (D6.1b due M12).

4 Update of the data management plan

Not applicable.

5 Follow-up of recommendations and comments from previous review(s)

Not applicable

6 Deviations from Annex 1

After the start of the project we have started an Amendment to add the University of Augsburg (UAU) to the list of consortium members. This was because Sebastian Altmeyer (former UvA staff) had taken up a new position at UAU. The Amendment included a shift of Person Months from the UvA to UAU and the transfer. In August, we have also initiated an amendment to include a linked third party (Sysgo GmbH) to our consortium partner SYS, who will distribute some of its workload (18PM) towards its daughter company.

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.

7 Resources

Person Months overview in the period M01-M09

PM	WP1	WP1 Expected total	WP2	WP2 Expected total	WP3	WP3 Expected total	WP4	WP4 Expected total	WP5	WP5 Expected total	WP6	WP6 Expected total	WP7	WP7 Expected total	PM per partner	Total PM per partner expected
UVA	5	27	0.5	14	4.5	14	0.5	8	0.8	8	1	6	5.2	18	17.4	95
TNT	0	1	0	1	0	1	0.2	5	1	15	0	1	0	0	1.2	24
SYSGO	0	1	0	3	0	1	9.3	24	5.9	10	0.5	3	0	0	15.7	42
Sysgo GMBH*	0	0	0	2	0	2	2.7	8	1	6	0	0	0	0	3.7	18
UNILU	0	1	1	30	0	1	0	16	0	9	0	3	0	0	1.0	60
ULUND	4	6	2	12	8	30	0	0	0	9	0.5	3	0	0	14.5	60
UTRC-I	1.5	10	0.2	2	3.2	10	2.8	10	4.8	30	0.6	3	0	0	13.1	65
QMA	0.4	1	0	1	0.04	1	2.1	5	5.2	26	0.5	3	0	0	8.3	37
FC.ID*	0	2	0	12	0	3	0	4.5	0	4.5	0	4.2	0	0	0	30.2
Ciéncias*	1	2	1	6	0.5	1	0	1.5	0,5	1.5	1	7.8	0	0	4	19.8
UAU	1.8	8	0	11,0	3.9	11	0	4	0,1	4	0.1	2	0	0	5.8	40
TOTAL period/project	13.6	59	4.7	94	20.1	75	17.6	86	19.3	123	4.1	36	5.2	18	84.6	491

* Third linked parties

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 871259.