Distributed Real-time Architecture for Mixed Criticality Systems

Wind Power Evaluation and Monitoring Plan
D 7.1.2

Project Acronym	DREAMS	**Grant Agreement Number**		FP7-ICT-2013.3.4-610640	
Document Version	1.0	**Date**	2015-09-30	**Deliverable No.**	D 7.1.2
Contact Person	Anton Trapman	**Organisation**		ALSTOM	
Phone		**E-Mail**		anton-aart.trapman@power.alstom.com	

Contributors

Name	Partner
Anton Trapman	ALSTOM
Albert Rosado	ALSTOM
David González	IKL
Carlos Fernando Nicolás	IKL
Jon Pérez Maria Cristina Zubia	IKL

Table of Contents

Figure Index

Table Index

Glossary

BVR	Base Variability Resolution
COTS	Commercial Off-The-Shelf
DREAMS	Distributed REal-Time Architecture for Mixed Criticality Systems
DoW	Description of Work [1]
E/E/PES	Electrical/Electronic/Programmable Electronic Safety-related Systems
FCR	Fault-Containment Region
FPGA	Field Programmable Gate Array
FSoE	Fail Safe over EtherCAT
GL	Germanischer Lloyd
GPOS	General Purpose Operating System
HFT	Hardware Fault Tolerance
HMI	Human-Machine Interface
HW	Hardware
I/O	Input / Output
KPI	Key Performance Indicator
MS	Milestone
OS	Operating System
PCIe	Peripheral Component Interconnect Express
PFH	Probability of Failure per Hour
PL	Performance Level
QoS	Quality of Service
RTOS	Real-Time Operating System
SCL	Safety Communication Layer
SIL	Safety Integrity Level
SW	Software
SWOT	Strengths, Weaknesses, Opportunities y Threats
UC	Use Case
SCADA	Supervision, Control And Data Acquisition
SCPU	Safety CPU
WP	Work Package

Executive Summary

The wind power use case is one of the three DREAMS project demonstrators (along with the avionics and healthcare use cases). This use case describes a distributed mixed criticality system, which combines safety, real-time and non real-time functionalities. It is inspired in the current supervision and control solution for wind turbines, which is enhanced by the inclusion of DREAMS technologies.

This document presents the plan to monitor and evaluate the concepts, technologies and tools developed in DREAMS by means of the wind power demonstrator.

1 Introduction

1.1 Context

Alstom Renovables (formerly Alstom Wind and Ecotècnia) is a company which designs, manufactures, deploys and maintains wind turbines all over the world. With a great knowledge of the wind power market and trends, ALSTOM is facing the market push towards off-shore operation. The road to off-shore introduces new technological challenges, stringent safety requirements and new standards to comply with.

ALSTOM is a key partner in the evaluation of DREAMS project, since it leads one out of the three demonstrators where the technology developed in the project will be used, validated and showcased. The experience accumulated through the development process, as well as the results obtained at the end of the way, will allow calibrating the potential of the DREAMS contribution in the wind market.

This document establishes the framework to both monitor and evaluate the demonstrator from technological and business perspectives.

1.2 Revisiting wind power use case

As defined in deliverable D7.1.1 [2], the wind power demonstrator is based on the supervision and control system of the off-shore wind turbines. The original system implements two groups of functionalities:

- Control and supervision.
- Human-Machine Interface (HMI) and communications with the SCADA.

The system is executed in the GALILEO platform, and requires several inputs and outputs that are connected through an EtherCAT fieldbus. GALILEO is a real-time platform developed by ALSTOM and used mainly for the supervision and control system, though it may support other real-time applications such as wind farm control. The last version of this product is GALILEO V5, which is based on a commercial hardware (industrial PC APC 910 [3]) and customized at operating system and software levels. It is based in an x86 dual core processor.

The protection system is in charge of maintaining the wind turbine in a safe state. The main functionality of the protection system is to assure that the design limits of the wind turbine are not exceeded. The protection functions shall be activated as a result of a failure of the control function (running in the supervisory system) or of the effects of an internal or external failure or dangerous event. It should be activated in cases such as:

- Over-speed.
- Generator overload or fault.
- Excessive vibration.
- Abnormal cable twist (due to nacelle rotation by yawing).

Currently, the protection system is implemented in an external module integrated in the EtherCAT ring. This solution lacks the flexibility to implement complex logics since it is only able to handle digital inputs and outputs, and it is mainly a commercial hardware based system.

The demonstrator aims at achieving a higher degree of integration between the supervisory system and the protection system, thus making the overall solution more robust, maintainable, and flexible, while keeping in mind safety and non safety requirements. The demonstrator will integrate the protection system in the GALILEO platform by means of the harmonized platform of DREAMS project. The demonstrator is defined in such a way that it provides great benefit with respect to the state of the art solution in terms of dependability, it allows validating as many project requirements as possible (but only those relevant to the wind power domain), and it reuses the maximum hardware and software components of the current solutions in the wind power domain from ALSTOM.

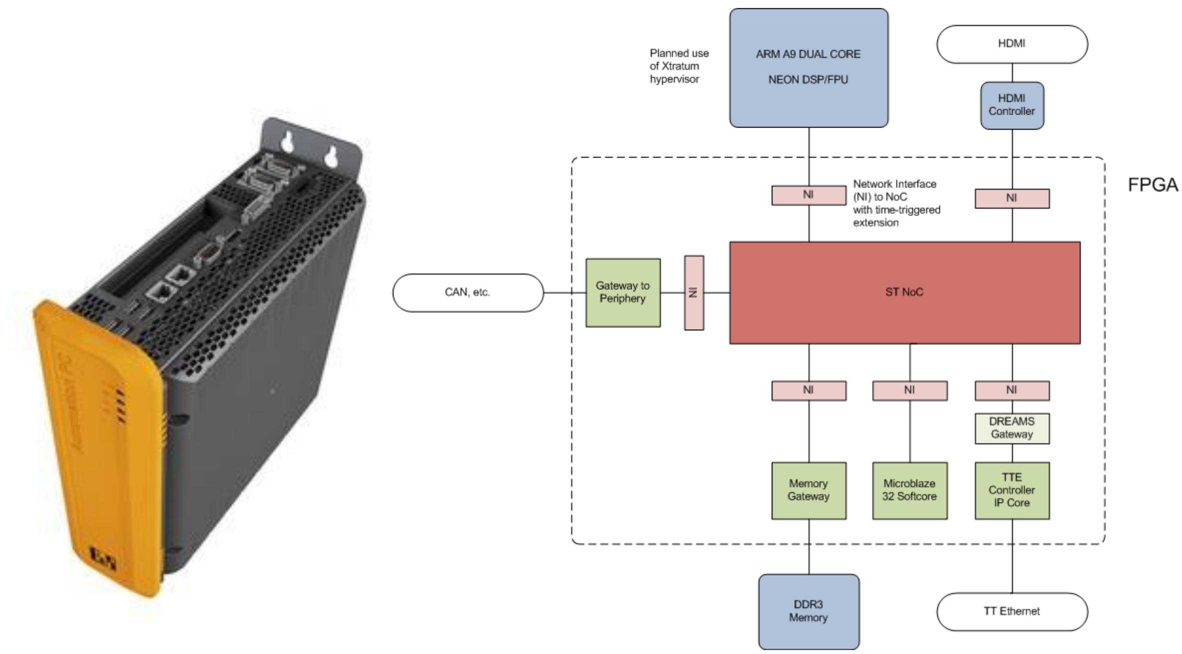

Figure 1: GALILEO V5 and Harmonized Platform

Figure 1 shows the GALILEO V5 platform currently used by ALSTOM for the supervision and control system, along with a diagram of the harmonized platform with the implemented peripherals and services. Both platforms will be interconnected via a PCIe interface.

The harmonized platform is the ZynqTM-7000 board [4], which consist of two ARM Cortex A9 cores and an FPGA where DREAMS technologies and services will be implemented.

As shown in figure 2, the current solution comprises the supervision and control platform (GALILEO), the distributed I/Os connected through EtherCAT, and the protection system, also connected to the fieldbus by using Safety over EtherCAT protocol (FSoE, Fail Safe over EtherCAT [5]). This solution provides a hardware fault tolerance (HFT) of 0, which means that one failure may cause the loss of the safety function.

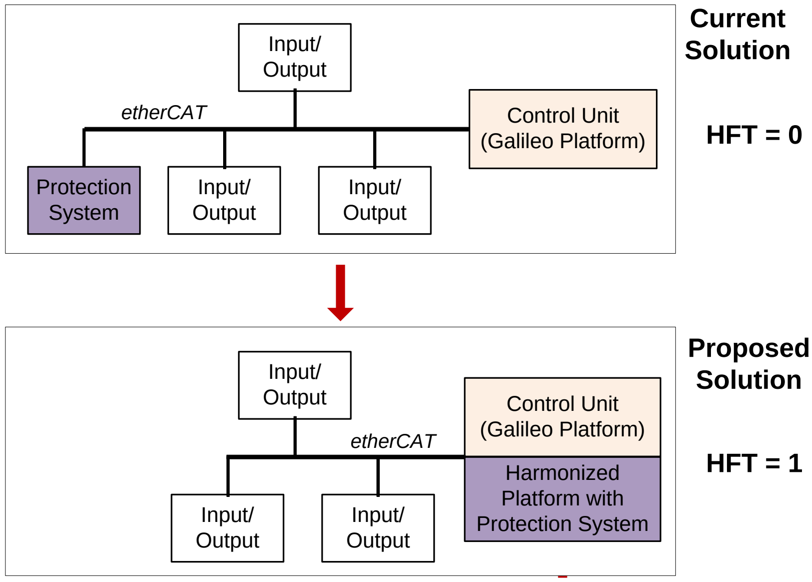

Figure 2: Current solution and proposed solution based on harmonized platform

To achieve higher hardware fault tolerance, the proposed solution integrates the control unit (GALILEO platform) and the harmonized platform via PCIe, keeping the communication with several I/O modules based on EtherCAT fieldbus. This solution, where the protection system is implemented in the harmonized platform, may be used to achieve heterogeneous redundancy, thus providing a HFT of 1. This increase of HFT is theoretical, and the requirements for on-chip redundancy detailed in IEC-61508-2 Annex E [6] must be met in order to achieve certification.

1.3 DREAMS technologies for wind power

Several technologies are being developed in the different technological work packages of DREAMS (WP1-WP5). Though all of them are aligned with project vision and objectives, not all of them are appealing or meaningful to be integrated in a wind power solution. Therefore, the contribution of the wind power demonstrator is limited to validate and evaluate those technologies with potential benefits in this specific domain.

In deliverable D7.1.1 [2], a very preliminary classification of DREAMS requirements was outlined, based on contents of deliverable D1.1.1 [7]. The idea was to reflect a classification of which project outcomes will be potentially used in the wind power sector in general, and in the wind power demonstrator in particular. Three levels of relevance were defined: high, medium and low.

- High relevance

  The most relevant requirements for DREAMS wind power demonstrator are the ones that describe the following features:

  - Architecture
  - Multicore Virtualization Technology
  - Mixed-Criticality Network
  - Mixed-Criticality Certification
  - Wind power Demonstrator

- Medium relevance

  The medium relevant requirements for DREAMS wind power demonstrator are the ones that describe the following features:

  - Tooling, Scheduling and Analysis
  - Modeling and Development Process
  - Resource Management

- Low relevance

  The requirements that have (a priori) the lowest relevance for the DREAMS wind power demonstrator are the ones that describe the following features:

  - Avionics Demonstrator
  - Healthcare Demonstrator
  - Security

At this stage of the project, many of these requirements are already mapped into specific technologies. Next figure summarizes the DREAMS technologies integrated in the case study, showing the dependencies among the work packages that generate the technology and WP7 where the demonstrator is developed.

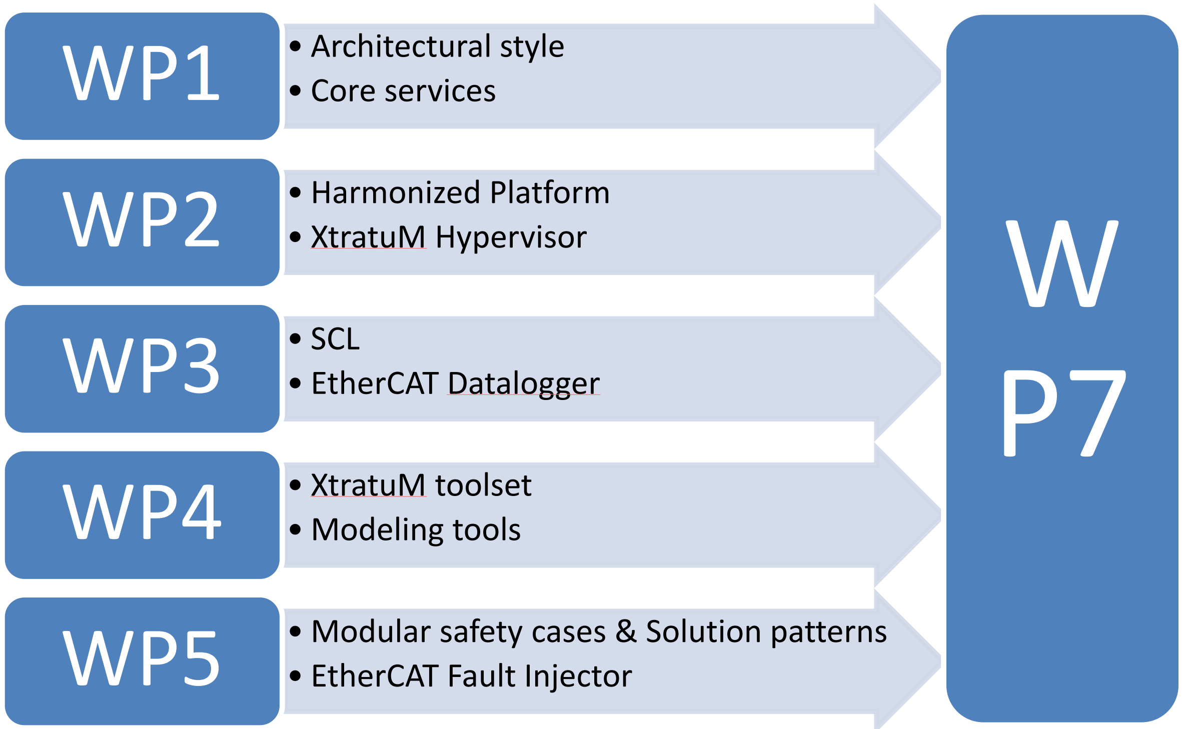

Figure 3: WP7 dependencies with technology WPs

The wind turbine case study integrates a subset of DREAMS technologies listed as follows:

- "WP1: Architectural Style"
  - Subset of core services of the "architectural style" (D1.1.1 [7], D1.2.1 [8])
- "WP2: Multicore Virtualization Technology"
  - Harmonized platform (D2.3.1 [9])
  - XtratuM hypervisor [10] that supports the 'harmonized platform', current GALILEO V5 platform and Windows Embedded CE (D2.4.1 [11])
- "WP3: Mixed-Criticality Network"
  - Safety Communication Layer (SCL) (D3.3.1 [12], D3.3.2 [13]).
  - EtherCAT Datalogger (D3.4.1 [14])
- "WP4: Tooling, Scheduling and Analysis"
  - XtratuM toolset is required to design, develop, verify and validate the case study (D4.1.1 [15], D4.1.2 [16])
  - Subset of modeling meta-models and tools (D4.1.1 [15], D4.1.2 [16])
  - SW component model (D4.1.2 [16])
  - HW platform model (D4.1.2 [16])
  - Hypervisor and partition model (D4.1.1 [15], D4.1.2 [16])
  - Safety model (D4.1.2 [16])
  - Variability model (BVR) (D4.3.1 [17])
- "WP5: Certification, Validation and Verification"
  - Modular safety cases for hypervisor (D5.1.1 [18])
  - COTS multicore device (D5.1.2 [19])

- Mixed-criticality network (D5.1.3 [20])
- Solution patterns (D5.3.1 [21])
- EtherCAT fault injector (D5.2.3 [22])
- Product line validation strategy (D5.5.2 [23])
- Product line certification strategy (D5.5.3 [24])

1.4 Objectives of the document

The objective of this document is to develop an evaluation methodology to be applied to the wind application domain. It shall describe the features of the project innovations to be evaluated in the prototype, and ensure the traceability between the technologies developed in DREAMS and the features of the applications exercising each of them.

The evaluation shall also monitor that requirements are fulfilled in technical work. The plan shall include definition of the measures for success of DREAMS project, such as the following (mentioned in Description of Work [1]):

- Assessment of compliance to relevant standards and norms of the proposed solutions.
- Level of dependability and maintainability of the developed building blocks.
- Increased level of time and space separation between virtual partitions
- Reduction of new applications developing time
- Level of cost-effectiveness in the development of prototypes
- Level of reusability of the developed building blocks
- Level of extensibility of developed building blocks

1.5 Structure of the document

The document is organized as follows. Section 1 provides an introduction to the wind power case study and outlines the dependencies with other DREAMS technological contributions, which will be later evaluated. Section 2 describes the evaluation methodology to be applied during and especially after development process. Section 3 briefly describes the demonstrator monitoring plan, aimed at ensure that it is designed, developed, validated and verified in time, while aligned with project objectives and milestones. Section 4 provides the templates to be filled during preliminary and final evaluations. Finally, section 5 draws conclusions and establishes next steps.

2 Evaluation methodology

This task consists of defining the plan to evaluate the project approach on the basis of the wind power demonstrator. The evaluation will take place in the final phase of the project (validation and verification of overall approach using prototypes and demonstrators), though preliminary report will be delivered in M30.

There are two main objectives to be met in the task:

- Orientation of the use case implementation in order to reach the expected measures for success, which are described in section 2.2. This objective will be achieved by the execution of the monitoring plan and a preliminary evaluation carried out at M30.
- Final evaluation according to the measures for success. Comparing results to expected criteria and producing the report giving the general picture of project technologies interesting for wind power. This includes overall comments on DREAMS technologies and interest for wind power beyond the project selected use cases.

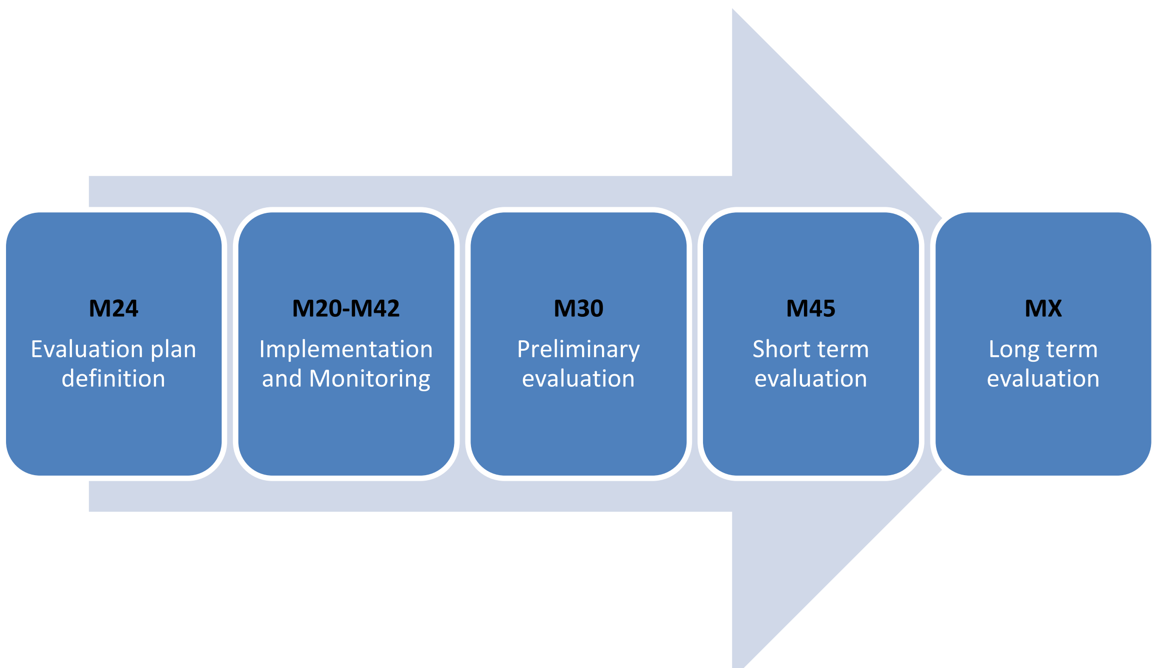

Figure 4: Evaluation process workflow

Figure 4 shows the workflow of the evaluation process. This report aims at defining the details and criteria of the whole process and it is delivered at M24. It creates the basis to monitor the implementation of the wind power demonstrator, and also to produce an intermediate evaluation at M30, which will be provided as feedback to the technology work packages for incorporation into the final version of the DREAMS architecture. This feedback will be used to improve the technological results in WP1-WP5.

The implementation of the demonstrator will be finalized by M42. When this task is completed, the evaluation plan will be executed, producing the corresponding deliverable at M45 with the evaluation results. These results will only incorporate those KPIs that are measurable right after the finalization of the development process. However, some other KPIs (especially business oriented ones), will need to stress the technology and test it in the field, and therefore this information will not be included in this report.

Figure 5 shows the different activities that have been carried out in order to define this evaluation plan. The information presented in the following subsection reflects this workflow.

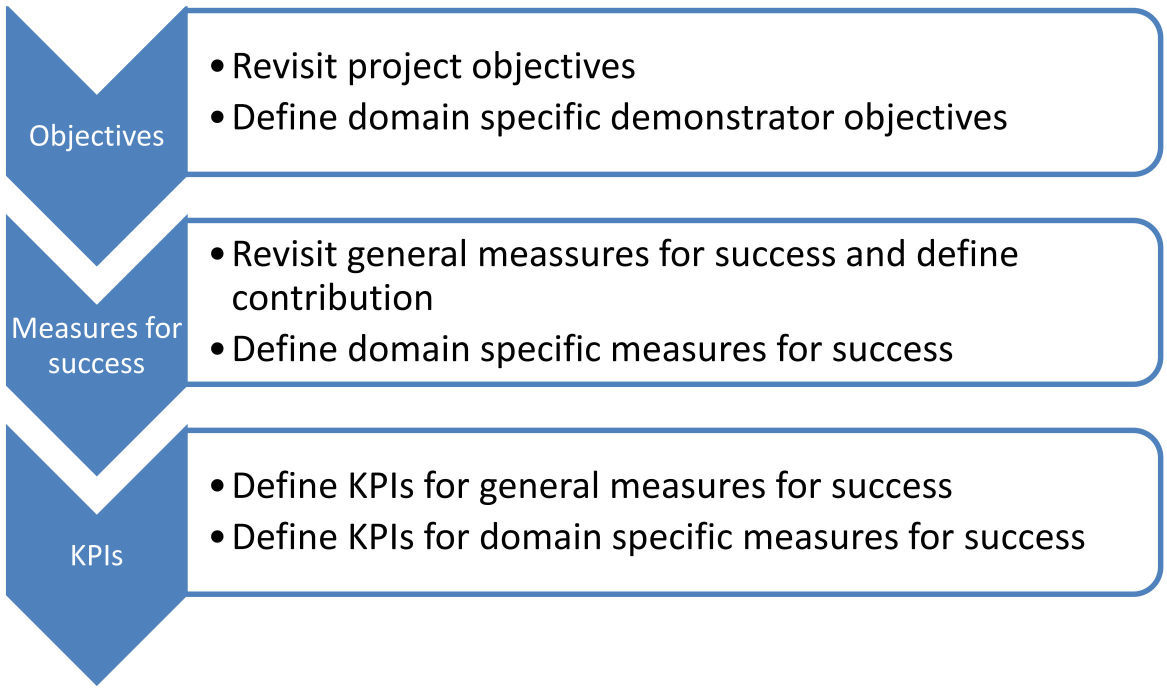

Figure 5: Activities to define the evaluation plan

The first step to evaluate the demonstrator is to clearly define the objectives. There are two kind of objectives to be fulfilled: general project objectives defined in Description of Work [1], and domain specific objectives, defined in section 2.1.2 of this deliverable.

The demonstrator has been specified in such a way that it is strongly aligned with project objectives. By integrating DREAMS technologies coming from WP1-WP5 into a real application use case, the fulfillment of these objectives will be evaluated. Some of the technologies of the project will not be used in the demonstrator since they are not considered interesting for wind power application domain and there are limited resources that should be used in meaningful activities; therefore the wind power demonstrator will not evaluate every single objective. This is not a problem since the validation of the fulfillment of all project objectives shall be done in conjunction by the three project demonstrators (wind power along with avionics and healthcare).

Next step is to define the measures for success. The measures for success are gathered and documented in section 2.2. The measures for success of general project objectives are listed in Description of Work [1], and the contribution of the wind power demonstrator to every of them is described in section 2.2.1. The measures for success of domain specific objectives are described in section 2.2.2 for every domain specific objective.

In order to enable an objective evaluation of all those measures for success, the Key Performance Indicators (KPIs) are defined in section 0. They will be used as quantitative metrics to argue evaluation of the measures for success and project objectives.

This evaluation plan will allow the consortium to gain the knowledge of the advantages and drawbacks of the DREAMS results. These advantages, disadvantages, opportunities and threats will be described in a SWOT matrix.

With all this information, along with the demonstrator, it is expected that potential users could evaluate the usefulness of DREAMS approach and associated technologies. This evaluation plan will serve also as an input for the exploitation and dissemination plans.

2.1 Objectives

As explained before, there are two sources of objectives for wind power demonstrator:

- The project objectives defined in Description of Work [1]: the wind power use case and demonstrator shall be defined in such a way that it is aligned with project objectives, serves as a test bench for project technologies, and in the end, provides the basis to verify fulfillment of project goals. Section 2.1.1 enumerates and briefly explains the project objectives.
- Domain specific objectives: the wind power demonstrator shall aim either at solving some problems detected by experienced engineers in the wind power domain, or at improving the current solutions by using DREAMS technologies and architecture. One of these conditions shall be met so that the wind power demonstrator can be considered realistic and meaningful.

2.1.1 Project objectives

The project objectives are listed in Description of Work [1], Part B, section 1.1, and reproduced next, with a brief extract of the descriptive text:

1. Objective 1: Architectural Style und Modeling Methods based on Waistline Structure of Platform Services:
   "…new architecture style for the seamless virtualization of networked embedded platforms ranging from multi-core chips to the cluster level with support for security, safety and real-time performance…"
2. Objective 2: Virtualization Technologies to Achieve Security, Safety, Real-Time Performance as well as Data, Energy and System Integrity in Networked Multi-Core Chips:
   "Certifiable platform services for virtualization and segregation of resources at cluster and chip-level…"
3. Objective 3: Adaptation Strategies for Mixed-Criticality Systems to Deal with Unpredictable Environment Situations, Resource Fluctuations and the Occurrence of Faults:+
   "Integrated resource management for mixed-criticality systems with monitoring, runtime control and virtualization extensions recognizing system wide, high level constraints…"
4. Objective 4: Development Methodology and Tools based on Model-Driven Engineering:
   "Development process ranging from modeling and design to validation of mixed-criticality systems…"
5. Objective 5: Certification and Mixed-criticality Product Lines
   "Architectural support for the eased definition of mixed-criticality product lines with certification support across product lines"

6. Objective 6: Feasibility of DREAMS Architecture in Real-World Scenarios
   "Practical demonstration of cross-domain applicability of the developed framework and methodology"
7. Objective 7: Promoting Widespread Adoption and Community Building
   "Establish and support a sustainable DREAMS community for system integrators and component developers, who will use the project results for developing mixed-criticality applications…"

2.1.2 Wind power specific objectives

Apart from the general project objectives, some domain specific objectives are defined next, and will also be evaluated through related measures for success and KPIs. Some of the following objectives are somehow contained in the general project objectives, but the following description is given from a domain specific perspective:

8. Objective 8: Enable higher integration of mixed-criticality systems providing scalability and composability.
   There are several electronic systems in the wind turbine which are historically deployed on dedicated hardware platforms due to the heterogeneous criticality requirements. The integration of these systems into the same hardware platform would provide many benefits, especially in terms of scalability and composability, so that the properties of functional groups are not compromised by the integration of new subsystems.
9. Objective 9: Reduce certification cost/effort for safety protection system.
   Certification is a key milestone in the development of wind turbines. By using third party pre-certified components the certification cost and effort can be reduced, but penalizing the flexibility (commercial pre-certified components are able to handle very few digital inputs and outputs, and cannot implement complex logics). This objective establishes that DREAMS project should provide the framework (architecture, method, tools, etc.) to ease certification of custom developed safety protection systems that avoid these limitations. Additionally, if this is the case, it will be possible to eventually certify safety functions in the supervision and control system with reduced effort by reusing this framework.
10. Objective 10: Increase capabilities and programming flexibility of the safety protection system.
    As previously explained, commercial pre-certified components historically used for implementation of the safety protection system imposes many limitations. The objective of the integrated solution developed in the wind power demonstrator is to avoid these limitations in terms of computing resources, programming flexibility, data availability, etc.
11. Objective 11: Incorporate mixed-criticality networks and means for validation.
    The safety protection system requires distributed data variables from the fieldbus. These variables shall communicate in a safe manner, sharing the bus with non-safety information. The combination of different criticality requirements on the same communication medium will allow reusing the infrastructure. In order to ease the validation of this scenario, it is very important to be able to simulate different faults in the communication channel.
12. Objective 12: Obtain a complete methodology to manage system complexity and variability.
    There is a high variability in wind turbines, and many sources of variability. The demonstrator shall be able to be adapted to the specific requirements of a wind farm or wind turbine model. The methodology should cover not only the development process, but also the management of variability and adaptability of the product.

2.2 Measures for success

This sections details the measures for success to evaluate the fulfillment of project objectives, and how the wind power use case and demonstrator can contribute in this task.

2.2.1 Project measures for success

This section defines the use case and demonstrator contribution to every measure for success established for each project objective. In some cases the contribution is relevant and measurable, while in some other cases the contribution is very limited and/or not measurable. As explained in the introduction, the wind power demonstrator is a powerful tool to evaluate DREAMS technologies and the fulfillment of project objectives, but it does not cover every project aspect.

The measures for success are listed in the following subsections and numerated in such a way that the KPIs listed next are easily traced to the related measure for success. In *italics* it can be read the measure for success as defined in Description of Work [1], and following each of them the contribution of the wind power demonstrator is described.

2.2.1.1 Objective 1

Architectural Style and Modeling Methods based on Waistline Structure of Platform Services

The measures for success of the architectural style and the services will be the following architectural properties:

1.1. Safety: Support for safety up to highest criticality levels (10-9 failures per hour)

The use case will provide a safety concept to demonstrate safety certifiability against relevant standards (ISO-13849 [25] [26], IEC-62061 [27], IEC-61508 [28] [6] [29]). The approval of this safety concept by a certification body will serve as a representative proof of concept to discuss the DREAMS contribution and limitations with respect to safety certification.

1.2. Real-time: Real-time support satisfying the timing requirements from the three application domains (e.g., bandwidth/throughput, bounded delays, jitter < 1µs)

The use case consists of a mixed-criticality system which includes three groups of functionalities: human-machine interface and communications, real-time control and supervision, and safety protection. The real-time functionalities will be encapsulated in one or more system partitions, and the validation plan will include some expanded functional tests to ensure that the real-time requirements of the supervision and control system are met under physical/performance extreme conditions, regardless of the state or activities being executed by other system partitions.

1.3. Fault containment: Encapsulation of components and subsystems to ensure data and system integrity providing 100% containment coverage within the DREAMS fault hypothesis

The safety concept of the protection system will include a fault hypothesis which identifies the assumptions regarding faults that the fault-tolerant safety system must tolerate. It shall be demonstrated (and positively assessed by the certification body) that the computing resources where the safety protection system will be deployed (also known as Safety CPU or SCPU) forms a single Fault-Containment Region (FCR).

1.4. Timely adaptation: Adaptation services for adaptivity and energy integrity with bounded reconfiguration time satisfying the requirements from the three application domains

Adaptation services are not used in the wind power use case, thus no action can be taken in order to provide evidences to this measure for success.

1.5. Security: Support for integrity, authenticity and availability based on the attacker and security model of DREAMS, validated using reasonable attacking scenarios and related penetration tests of the implemented security solution, with bounded effects of the implemented security mechanisms (at chip and cluster level) on performance and QoS such as reliability and energy efficiency

Security is not considered relevant in the wind power use case, thus no action can be taken in order to provide evidences to this measure for success.

Measures for success of domain-independence will be as follows:

1.6. Domain-independent core services: Services that ensure the above architectural properties must be domain-independent and useable in all three targeted application domains

The demonstrator will only include a subset of core services of the "architectural style". The list of core services used and discarded by the demonstrator will be analyzed, explained rational for every decision.

1.7. Modular architecture: The modular architecture must support the customization and refinement of the architectural services using domain-specific higher services

As previously mentioned, three groups of functionalities will be included in the wind power demonstrator. Each of this functional group is currently implemented by using a dedicated hardware, and provides a list of domain services. The DREAMS demonstrator shall be analyzed to determine which domain services are able to be implemented on the new architecture by means of customization and refinement, and which domain services cannot be ported to the new approach. The demonstrator itself will not implement all the services since this is not the primary goal, and therefore is not an efficient use of resources, but a short analysis could evaluate the customization capabilities of the modular architecture.

The models shall capture the required information of networked multi-core chips for a model-driven development process to establish the above architectural properties:

1.8. The models should contain sufficient details to support fine-grained analysis/scheduling of mixed criticality systems in WP4 as well as the development of use-cases in WP6-WP8.

1.9. The complexity of the models established in the use-cases will be assessed against experienced data acquired from domain experts from the demonstrator work-packages.

1.10. The completeness of the implementation will be assessed against the requirements collected in the initial phase of the project.

The use case will be modeled by using a subset of the tools generated in WP4. The modeling, transformation and scheduling capabilities of the tools will be evaluated from a wind power domain perspective, providing feedback regarding complexity and completeness of the evaluated toolset.

2.2.1.2 Objective 2

Virtualization Technologies to Achieve Security, Safety, Real-Time Performance as well as Data, Energy and System Integrity in Networked Multi-Core Chips

2.1. Isolation: To achieve the complete spatial and temporal isolation for the chip level QoS. In other words, independently of the amount of non-critical traffic insure that critical traffic can meet the requested QoS target.

The virtualization framework and DREAMS architecture shall provide the means to prevent one application from overwriting code / data in another partition or a memory address not explicitly assigned to this application, and it also shall ensure that an application has sufficient processing time to complete its execution (as configured), regardless of the state of the other applications. The temporal and spatial isolation is one of the challenges that the research community and industry need to solve for the integration of applications of different criticality levels, when safety certification is required. The most critical applications need to be protected against any memory or temporal interference provoked by other applications coexisting on the same platform and sharing resources. The wind power demonstrator provides an excellent scenario to obtain qualitative and quantitative measures of the level of temporal and spatial isolation that DREAMS architecture can achieve:

- As the safety concept will be presented and assessed by a certification body, it will determine whether the architecture and specified safety measures are considered enough to meet the level of isolation required by the standards.
- The verification plan of the demonstrator will include specific tests to analyse the on-chip and off-chip interferences provoked by other applications in terms of processing load, network bandwidth, resources access rate, etc.

The results obtained in the tests, combined with the conclusions of the safety concept assessment, will determine whether theoretical and practical evaluations are aligned and sufficient for safety certification in the wind power domain.

2.2. Reduce bank conflicts: To reduce the chance of bank conflict reducing the average execution times of the workloads by 10%

Bank conflicts decrease the effective bandwidth. As part of the analysis carried out for the evaluation of the temporal and spatial isolation, specific test cases will measure bank conflicts and memory access rates in different situations with parallel on-chip executions.

2.3. Gateways: Availability of gateways for end-to-end segregation as means for integration of mixed criticalities

The wind power demonstrator will base its communications architecture in a combination of on-chip and off-chip (e.g. EtherCAT) communications. Data from sensor shall be available for some of the partitions of the system which are deployed on different chips (e.g. real-time supervision and control system will run on x86 processor while safety protection system will be executed on the harmonized platform). Availability and effectiveness of required gateways to implement this approach will be evaluated, as well as their properties to meet mixed-criticality requirements.

2.4. *Reduction of latencies: Achieved (reduction of) latencies in on-chip and between-chip communication in the wired and wireless networks*
2.5. Reduction of jitter: Achieved (reduction of) jitter in cluster-level and mixed-network communication in the wired and wireless networks

Requirements on latencies and jitters in the wind power demonstrator are not especially demanding, but the demonstrator will provide an excellent framework to characterize communication parameters of the implemented services.

2.6. Reconfiguration: Achieved flexibility of reconfiguration

Adaptation services and reconfiguration are not used in the wind power use case, thus no action can be taken in order to provide evidences to this measure for success.

2.7. Security: Developed security concepts for Ethernet-related protocols (i.e. EtherCAT, TTEthernet and black-channel Ethernet)

The Safety Communication Layer (SCL) will be used in the wind power demonstrator to transport safety related input/output data between EtherCAT slaves and safety protection system deployed in the harmonized platform. However, security is out of the scope of the demonstrator, and no action can be taken in order to provide evidences to this measure for success.

2.2.1.3 Objective 3

Adaptation Strategies for Mixed-Criticality Systems to Deal with Unpredictable Environment Situations, Resource Fluctuations and the Occurrence of Faults

3.1. Variability: support of variability due to faults or fluctuation by maintaining execution of highest criticality level applications

The demonstrator will be comprised of mixed-criticality partitions/applications, being the safety protection system the most critical piece of software. The verification plan will include tests to validate that faults occurring in other partitions/applications do not compromise the safety level of the protection system (but possibly the availability). The Ethernet fault injector will be used as a tool to validate the impact of different faults in the off-chip communication bus.

3.2. Criticality spectrum: coverage of different criticality levels thanks to the combination of offline and online scheduling
3.3. Applicability: multiple system-wide goals and requirements, e.g. end-to-end deadlines, reliability, to be dealt with

Online scheduling is not required by the wind power demonstrator, but only static (offline) scheduling. The scheduling tool shall support the requirements of the functionalities in the whole criticality spectrum (safety-critical, real-time and general purpose). Note that the scheduling tool would require qualification in order to be used in the safety-critical design, and this is out of the scope of the project.

3.4. *Efficiency: degraded performance induced by the algorithms for adaptation strategies will be compensated by the gain of mixing several criticality levels.*

Online adaptation strategies are not used in the wind power use case, thus no action can be taken in order to provide evidences to this measure for success.

3.5. *Scalability: number of resources handled in distributed, networked systems*

Scalability is not to be evaluated in the wind power demonstrator at implementation level. However, it can be evaluated at modeling level through the inclusion of additional supervision and control algorithms allocated in new partitions.

3.6. *Portability: separation of local and global resource management via abstractions, integration in hypervisors and drivers*

The portability will be evaluated by determining:
- The number of specific drivers integrated in the wind power demonstrator to enable porting to the new architecture and platform.
- The effort required to use those drivers at application level. The higher the level of abstraction, the lower the effort.

2.2.1.4 Objective 4

Development Methodology and Tools based on Model-Driven Engineering

4.1. *Development process ranging from modeling and design to validation of mixed-criticality systems. During the implementation of the demonstrators, the development process should be shown to have tackled the major challenges in the design of mixed criticality systems. The usefulness of the development methods, i.e. the savings of development time, will be assessed against experienced data acquired from domain experts from the demonstrator work-packages. The completeness of the implementation will be assessed against the requirements collected in the initial phase of the project.*

The development process will be monitored and evaluated along the whole life of the demonstrator. Acquired data in terms of development time and usefulness of the development methods will be compared against estimations of the engineers responsible of developing the current range of supervision and control solutions. However, it should be taken into account that the demonstrator is being developed along with the technology, and it is quite unlikely that the technology to be integrated is fully validated. This situation is not comparable to the development of the current range of supervision and control solutions, which is based on conventional architecture and consolidated technologies.

4.2. *Percentage of development steps covered by at least one software tool, globally and for each project relevant aspect (safety, timing, energy, variability)*
4.3. *Percentage of data connections between tools for which automatically executable transformations are implemented*

It is not planned to use all the tools developed in the project, since there are some domain and self-imposed constraints to keep using some of the tools currently used for the development and validation of wind power supervision and control solutions. Taking into account this consideration, the percentage of development steps covered by tools will be calculated, providing two different results:

- Percentage of steps covered by DREAMS tools used in the demonstrator.
- Percentage of steps which could be potentially covered by DREAMS tools in the wind power domain (if some self-imposed constraints are avoided).

In both cases, the percentage of automatically executable transformations will also be calculated.

2.2.1.5 Objective 5

Certification and Mixed-criticality Product Lines

5.1. *Modular safety-case for mixed-criticality systems: The approach to use and compose modular safety-cases shall be defined and used in at least one demonstrator. Measures for success are how much more efficient in terms of assessment effort will the modular certification be compared with a series of full certifications. Assessment effort can be measured by how many (additional) tests (or assessments) must be executed to achieve the required coverage.*

The wind power case study safety concept will be defined using previously defined modular safety cases for hypervisors and multicore devices. A measure for success is the effort efficiency in the definition and assessment of an application safety concept (based on previously defined and reusable modular safety cases) and the effort efficiency to update the application safety concept if the hypervisor / device is updated or changed (impact analysis). Because of resource limitations it is not possible to define two complete safety-concepts, one with modular safety cases and the other one without, but it is possible to compare and extrapolate the results with similar safety-concepts previously developed.

5.2. *Safety-case modularity: How well are some given safety-cases susceptible to modular certification? This is measured through the same measurement as for modular certification.*

The modularity of safety-cases will be assessed by what-if scenarios, considering how a particular component (e.g. the virtualization software) could be substituted in the design by other alternatives with equivalent safety properties and functionality. What-if-scenarios will include an impact analysis.

5.3. *Architectural support for the eased definition of mixed-criticality product lines with certification support across product lines: The building blocks for mixed-criticality are available. They are pre-certified and reviewed by the certification body.*

The wind power demonstrator reuses several already existing components of diverse complexity. Yet most of these components are platform-specific, constraining the number of possible deployments. It will be analyzed how the DREAMS optimization of the product line architecture would improve the solution design by using a combination of platform-independent descriptions and transformation components.

5.4. *Configuration optimization: How quickly can a (re)configuration of a mixed-criticality system be calculated such that the configuration is in reasonable vicinity of the overall optimum. The measurement is on algorithmic effort relative to finding the absolute optimum on a selected criterion (such as space, speed or performance). Success could be that with 10% of the time used to reach absolute optimum, our approach reaches 95% of the optimum with 0.95 probability. (What the actual good values are can probably not be determined until we have some initial data)*

Due to the reuse of components mentioned in 5.3, it is unlikely that the wind power demonstrator would pose so a complex optimization as to provided conclusive results about the optimization performance.

5.5. *Variability in applications and platforms as another architectural dimension to handle different criticalities and domains: Specific building blocks for variability of mixed-criticality are defined. Their composition is pre-certified and they are reviewed by the certification body.*

The design for the wind power application under different safety integrity requirements will optimized, and then analyzed whether there are replaceable patterns that provides the safety features, and if it would possible to certify these patterns separately.

5.6. *Different domains and market features, and also optimal selection and configuration of components and platform services for mixed-criticality systems: A study of variability w.r.t. mixed criticality is available and the benefits are obtained from optimal selection and configuration.*

Different what-if scenarios from the business viewpoint will be analyzed, taking into account the product line evolution. Wind power applications are typically long-life systems, thus demanding retro-fitting replacements while introducing new components, technologies or safety requirements. Besides that, also applicable safety standards will evolve, and future products should be designed considering new or more stringent requirements. The adaptability of DREAMS methodology to cope with these business scenarios will be evaluated.

2.2.1.6 Objective 6

Feasibility of DREAMS Architecture in Real-World Scenarios

The measures for success will be the performance indicators from WP6-8, the industrial assessment results from WP6-8 and the meeting of the requirements from the three application domains. In particular the following measures of success have been identified:

6.1. *Separation: Level of time and space separation between virtual partitions, increase up to be able to certificate to the required level.*

The required certification level in the wind power domain is performance level d (PLd) according to ISO-13849 [25] [26] standard (which is equivalent to SIL2 in IEC-62061 [27] and IEC-61508 [28] [6] [29] standards). However, this performance level could be achieved with state of the art solutions, and it would be very interesting to check the possibility to certify to the highest performance level PLe, since DREAMS architecture provides the framework to achieve a Hardware Fault Tolerance (HFT) of ‘1’.

6.2. Standard compliance: Assessment of the compliance to standards and norms of the solutions proposed.

The safety concept evaluated by a certification body will provide the evidences to proof certifiability of the demonstrator, even though the certification process will not be completed. The safety concept will focus on ISO-13849 [25] [26] standard, but the requirements coming from the following standards and guidelines shall also be taken into account:

- ISO-13849 Safety of Machinery [25] [26]
- IEC-62061 Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems [27]
- IEC-61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES) [28] [6] [29]
- GL 2010 Guideline for the Certification of Wind Turbines [30]

6.3. Cost: Level of cost-effectiveness in the development of project prototypes.

This parameter will be determined by comparing the estimated development costs (in terms of development effort and prototyping expenses) of the demonstrator with the sum of the development costs of the subsystems now integrated into the same platform as a mixed-criticality system. The estimation of the DREAMS development costs shall not include the technology related activities such as technology implementation, validation and refinement, but it shall include platform adaptation and customization, as well as application development based on provided services.

6.4. Reusability: Level of reusability (in other application domains related to power generation Tide, Hydro) of the developed building blocks.
6.5. Extensibility: Level of extensibility of developed building blocks.

The supervision and control systems in the hydro and tidal power domains have many similarities with the wind power domain. The applicable safety standards are also the same with the addition of few domain specific requirements, and the protection system’s safety concept could be, in theory, easily adapted. In order to evaluate reusability and extensibility of the approach in other power generation domains, this statement will be more deeply investigated. The differences in terms of system composition, safety requirements and architecture will be enumerated, and the adaptation effort of the DREAMS technologies and wind power demonstrator will be calibrated.

2.2.1.7 Objective 7

Promoting Widespread Adoption and Community Building

7.1. Community Infrastructure available and populated: A populated and active website and repository under www.mixedcriticalityforum.org (already registered) for system integrators and component developers

A reduced version of the wind power demonstrator documentation will be available in the website, and some of the building blocks/components will populate the repository. The information uploaded to website and repository will be evaluated to measure contribution of the wind power demonstrator.

7.2. Training Materials available: Availability of technical training materials for system integrators and component developers

Training material will not be created specifically as part of the demonstrator, but some information generated along development could be used for this purpose. Usefulness of available information will be evaluated.

7.3. Standardization activities performed: Presentations for / Discussions at working groups at standardization bodies (project time will be too short to finalize standardization activities)
7.4. Roadmap: An established European innovation roadmap for research in mixed-criticality systems and provide a community infrastructure and support for H2020 topic definition support.

The wind power demonstrator can be used for presentations and as a base for discussion for standardization purpose. However, this is not the primary goal of the demonstrator and its impact in these activities is not easily measurable.

2.2.2 Wind power specific measures for success

2.2.2.1 Objective 8

Enable higher integration of mixed-criticality systems providing scalability and composability.

8.1. Support for the integration of safety-critical, real-time and general purpose functionalities on the same hardware platform

The demonstrator will integrate these three groups of functionalities. It shall be evaluated whether the development of the demonstrator has been carried out with all facilities and components for the integration of functionalities with heterogeneous criticality requirements (e.g. availability of RTOS and GPOS to be virtualized by means of the hypervisor, tools, modular safety cases, etc.).

8.2. Demonstrator scalability to allocate new functionalities.

The platform shall support new functionalities to be deployed while preserving the properties of the functional groups. The scalability of the resources, the methodology and the system composability shall be prepared to allow integration of new functionalities.

2.2.2.2 Objective 9

Reduce certification cost/effort for safety protection system.

9.1. First-time certification cost/effort

This measure for success shall estimate the cost and effort required to certify the safety protection system integrated in the wind power demonstrator, and compare the obtained values with an estimation of the cost and effort of a certification process of the same system in a situation where the DREAMS technologies, architecture and methodology are not used. It shall be remarked that this comparison will not be made against the certification cost and effort of a commercial system, since due to the limitations of the later, the solutions are not comparable.

9.2. Re-certification cost/effort

Due to the variability of the system, recertification may be needed at some point. The same analysis described in previous measure for success shall be repeated here covering a re-certification process.

9.3. Criticality level up

Some of the components of the system which currently do not have safety requirements may increase the criticality level in the future, requiring certification. The engineering cost an effort to certify according to the new requirements shall be estimated.

2.2.2.3 Objective 10

Increase capabilities and programming flexibility of the safety protection system.

10.1. Safe data availability and logics programming

Traditionally, the safety protection system based on commercial hardware has many limitations in terms of number of variables to handle and programming flexibility. If shall be evaluated if the solution integrated in the wind power demonstrator overcomes these limitations.

2.2.2.4 Objective 11

Incorporate mixed-criticality networks and means for validation.

11.1. Mixed-criticality networks

The wind power demonstrator shall demonstrate that critical and non-critical data can share the same network, and critical information can never be compromised by non-critical traffic.

11.2. Availability of mixed-criticality networks validation means

The validation of the safety protection system shall include communications testing. It shall be evaluated whether the testing framework and equipment are sufficient to validate all communications related safety requirements.

2.2.2.5 *Objective 12*

Obtain a complete methodology to manage system complexity and variability.

12.1. DREAMS methodology compatibility with wind power processes

Currently, a V-Model life-cycle is used for the development of the supervision and control system, as well as for other electronic devices in the wind turbine. The methodology and tools defined in DREAMS shall be as compatible as possible with current practices, so that the learning curve required by engineers and organization is as short as possible.

12.2. Variability management

The electronic devices in a wind turbine must be always adapted to the specific needs of a project (environmental conditions, specific customer requirements, etc.). All these parameters cause a big variability in hardware and software that is very difficult to manage with conventional methods and tools, especially when a certified system is affected. The variability management framework provided by DREAMS will allow engineers to ease the management of these project particularities and shorten the adaptation time.

2.3 Key Performance Indicators (KPIs)

Key Performance Indicators (KPIs) are regarded as a collection of metrics for quantifying the objectives of the project, monitoring its activity progress and assess the expected results.

The collected KPIs should be:

- Objective: it shall be possible to measure them objectively.
- Measurable: it shall be possible to quantify them.
- Relevant to the project: the partners shall confirm their interest.
- Comparable: to the situation of the application use case before using DREAMS approach and technologies.

The performance indicators defined in the following subsections will be traced to one or more measure for success described in section 2.2. During the evaluations (preliminary and final) they will provide quantitative information to support the qualitative evaluation of every measure for success. Some of the measures for success are not traced to any KPI, since there may be no quantitative data that could support the conclusion.

The KPIs are classified into three subsets: KPIs measurable at any time during the execution of the project, KPIs only measurable at the end of the project, and KPIs that may only be obtained years after the project.

Some examples of KPIs which could be calculated during the project are:

- Number of supported core architectures.
- Number of supported operating systems.

KPIs to be calculated at the completion of the project could be such as the following:

- Demonstrator development effort/cost.
- Percentage of DREAMS building blocks used by the demonstrator.

Examples of KPIs to be calculated years after the project could be:

- Time-to-market reduction of a mixed-criticality system based on DREAMS architecture and technologies.
- Cost reduction in variability management of a product developed by using DREAMS architecture and technologies.

Table 1 lists and describes all KPIs of the project, and traces all of them to the measures for success they aim at providing arguments for evaluation. The last column indicates when this metric can be obtained:

- D: During the development of the demonstrator. The KPIs marked with ‘D’ can be evaluated in the preliminary and final reports.
- E: When the development is finished (by the End of the project). These KPIs can only be evaluated in the final report.
- A: After some experience with the technology (After the project). These KPIs cannot be objectively evaluated at the end of the project, since some experience with the technology is needed. Estimation will be provided in the final report.

ID	KPI	Description	Measure for Success	Time
1	Achievable Performance Level	Maximum achievable Performance Level (e.g. PLd, PLe) according to ISO-13849 [25] [26]	1.1, 6.1, 6.2	D
2	Achievable Safety Integrity Level	Maximum achievable Safety Integrity Level (e.g. SIL2, SIL3) according to IEC-61508 [28] [6] [29]	1.1, 6.1, 6.2	D
3	Achievable Hardware Fault Tolerance	Maximum achievable Hardware Fault Tolerance based on DREAMS architecture	1.1, 6.1, 6.2	D
4	Validated support for key real-time OS	(Boolean) The platform supports integration of Windows Embedded CE 6.0 to be used as the OS for the supervision and control system	1.2, 8.1	D
5	Minimum closed-loop cycle time	Minimum period to execute real-time threads of the supervision and control system, containing closed-loop regulation algorithms	1.2	D
6	Minimum fieldbus cycle time	Minimum period to obtain input values and apply output values in the fieldbus modules, in both non-safety and safety data (safety data needs an additional software layer)	1.2	D
7	Maximum jitter	Bounded value for jitter in the execution of the most critical real-time thread	1.2	D
8	Fault containment by construction	(Boolean) The certification body accepts evidences to demonstrate fault containment by construction	1.3, 1.1	D
9	Percentage of integrated core services	Percentage of core services of DREAMS integrated in the wind power demonstrator	1.6	D
10	Percentage of domain services portable to new architecture	Percentage of services of the subsystems that are going to be integrated in the demonstrator which are either ported or portable to the new platform (ideally 100%)	1.6	E
11	Percentage of system architecture/design modeled	Percentage of the system architecture and design that is able to be modeled with the tools developed in DREAMS	1.8	D
12	Percentage of software application modeled	Percentage of the application software that is able to be modeled with the tools developed in DREAMS	1.8	D
13	Models complexity	(Boolean) Wind power domain experts appreciate an easier complexity management by using modeling tools and methods	1.9	D

14	Temporal and spatial isolation by construction	(Boolean) The safety concept (supported by the verification plan) demonstrates that the architecture provides temporal and spatial isolation of partitions by construction	2.1	D
15	Bounded temporal interference (network)	Delay introduced in the safety-related communications when heavy non-safety traffic is generated in the network	2.1	E
16	Bounded temporal interference (processing)	Delay introduced in the critical thread of the safety-related partition when heavy processing load is generated in neighboring non-safety partitions	2.1	E
17	Bounded temporal interference (resources access rate)	Delay introduced in the access to resources (memory) by the safety-related partition when heavy resource consumption is required by neighboring non-safety partitions	2.1, 2.2	E
18	Resources access rate penalty	Access rate penalty measured in the access to resources (memory) by the safety-related partition when heavy resource consumption is required by neighboring non-safety partitions	2.2	E
19	Percentage of out of the box gateways	Percentage of gateways required to connect on-chip and off-chip networks that are provided “out of the box” and not specifically developed for demonstrator	2.3	D
20	Sensor-to-partition latency	Latency between a value is read at the sensor and delivered at the partition where it is going to be processed	0	E
21	Sensor-to-partition jitter	Jitter in the time between a value is read at the sensor and delivered at the partition where it is going to be processed	2.5	E
22	Development time reduction	Reduction in development time of the mixed-criticality system in comparison with the development time of equivalent conventional systems	4.1	E/A
23	Percentage of development steps covered by tools in demonstrator	Percentage of development steps where DREAMS tools provide support in the demonstrator, in one or more of the following aspects: safety, timing, energy, variability	0	D
24	Percentage of development steps potentially covered by tools in wind power	Percentage of development steps where DREAMS tools could potentially provide support in a wind power solution, in one or more of the following aspects: safety, timing, energy, variability	0	E

25	Percentage of automatically executable transformations	Percentage of automatically executed transformations between consecutive development steps provided by tools	4.3	E
26	Effort reduction for addition or modification of features	Estimation of the variation in the assessment effort when changing the safety integrity requirement	5.1	A
27	Effort reduction for replacement of components	Estimation of the re-use of integration evidences, and required additional assessment effort	5.2	D
28	Broadening of the design space	Cost analysis for the rework needed to integrate more abstract descriptions of the components, in order to improve portability and product line evolution	5.3	A
29	Pre-certifiable patterns for aspect features	Percentage of replaceable patterns that provide the safety features	5.5	A
30	Adaptability to evolution of product and standards	(Boolean) The approach provides required adaptability for evolution of product and standards	5.6	A
31	Cost reduction in development of prototype	Cost reduction in the development of the prototype of the demonstrator, compared to the sum of the cost of prototyping the subsystems now integrated	6.3	E
32	Reduction of prototype development time	Development time reduction in the prototype of the demonstrator, compared to the prototyping of the subsystems now integrated	6.3	E
33	Reusability of building blocks in other power generation domain	Percentage of demonstrator building blocks that are straightforward reusable in other domains, and percentage of building blocks that are reusable with small adaptations	6.4, 6.5	E
34	Percentage of public information coming from the demonstrator	Percentage of the contents in website and repository that are part or use demonstrator material	7.1	E
35	Percentage of training material coming from the demonstrator	Percentage of the training material that are part or use demonstrator material	7.2	E
36	Percentage of support for relevant OS (RTOS and GPOS)	Percentage of operating systems that are relevant for the wind power domain (they must be listed) that are available to be deployed on the demonstrator platform	8.1	D
37	Scalability gap	Available resources to scale up the demonstrator to support additional features (in terms of free cores, network throughput, etc.)	8.2	E

38	Reduction in certification cost	Cost reduction in certification due to certification facilities provided (modular safety cases, reference architecture, compliant items, etc.)	9.1	A
39	Reduction in re-certification cost	Cost reduction in re-certification due to certification facilities provided (modular safety cases, reference architecture, compliant items, etc.)	9.2	A
40	Reduction in criticality level up	Cost reduction in the certification of a function which is integrated in the system as a non-safety component and shall be certified (e.g. supervision and control)	9.3	A
41	Safe data availability	Number of variables that the safety partition can safely handle through the mixed-criticality network to use in the safety functions	10.1	D
42	Safe algorithm programming flexibility	(Boolean) The programming of the algorithms of the safety functions does not have any limitation in terms of number of sentences, inputs, outputs, etc.	10.1	D
43	Network flexibility and scalability	(Boolean) Mixed-criticality network allows adding or removing elements and scale the number of nodes	11.1	D
44	Network validation supported by tools	(Boolean) The validation of the mixed-criticality network can be done by using the tools provided in DREAMS	11.2	E
45	Percentage of compatible development steps	Percentage of development steps defined in the DREAMS methodology that are compatible with current process in wind power domain	12.1	E
46	Percentage of variability sources successfully handled	Percentage of variability sources that have been successfully handled through DREAMS methods and tools	12.2	E
47	Reduction of variability adaptation time	Reduction in adaptation time to deliver the system after applying a variability point	12.2	A

Table 1: Key Performance Indicators

2.4 SWOT Analysis

A SWOT analysis (alternatively SWOT matrix) is a structured planning method used to evaluate the strengths, weaknesses, opportunities and threats involved in a project or in a business venture. A SWOT analysis can be carried out for a product, place, industry or person [31].

Figure 6: SWOT analysis template

With the objective of paving the way to exploitation and exposing the advantages of the DREAMS approach, a SWOT analysis is proposed to self-evaluate the validity of DREAMS for future developments.

The usage of this kind of analysis will help to clarify the benefits obtained with DREAMS and to make clear some of the disadvantages. Apart for being useful for the evaluation plan of the use case the results will help in the definition of the next steps and possible improvements of the DREAMS platform.

3 Demonstrator monitoring plan

There are two aspects to be monitored. The first one is the progress of the development process of the demonstrator, which needs to follow a strict scheduled in order to respect project deadlines and provide necessary information to other activities in different work packages. Section 0 provides the criteria to track the status of the different phases of the development, shown in Figure 7.

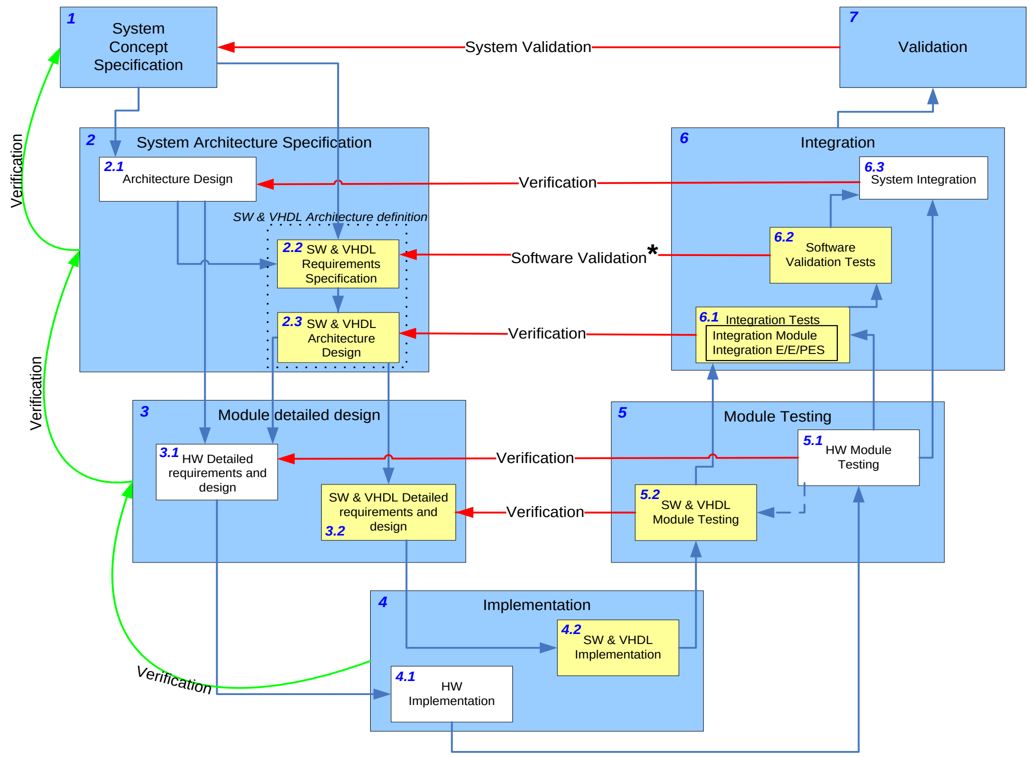

Figure 7: V-model realization according to Ikerlan's IEC-61508 SIL3 FSM [32]

It is very important as well to preliminary check the foreseen degree of fulfillment of the demonstrator with defined objectives, measures for success and KPIs. The sooner a deviation is detected, the earlier it can be corrected while maximizing the possibilities to still achieve expected results. Section 3.1.3 defines the way to perform this monitoring, while the template to complete the preliminary evaluation expected at M30 is provided in section 3.1.3.

3.1.1 Development monitoring

Figure 8 shows the main milestones in the development of the wind power demonstrator that shall be monitored to check the correct progress. This timeline is a simplified linear representation of the V-Model development process shown in Figure 7.

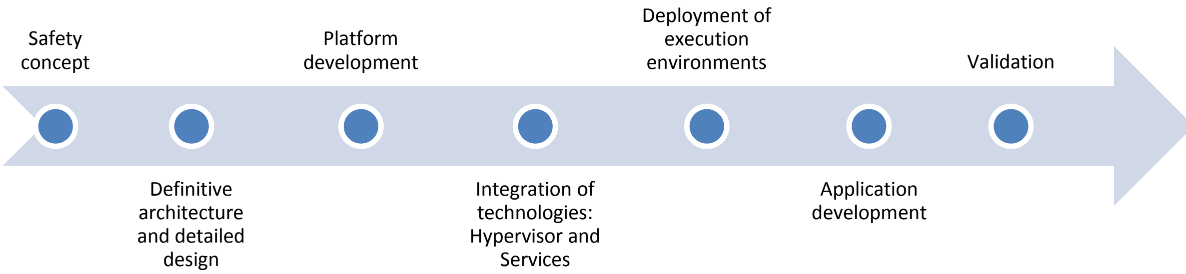

Figure 8: Milestones to be monitored

The first milestone in the development process of the demonstrator is the specification of the safety concept, which shall be assessed by a certification body. This document should present the safety argumentation and outline a first draft of the system architecture, which shall be refined into a detailed document to obtain the definitive architecture and design, reaching the second milestone. The third milestone consists on developing the core hardware, comprised of the DREAMS harmonized platform properly integrated into GALILEO platform.

Milestone	Description	Estimated month
MS1	Safety concept	M22
MS2	Definitive architecture and detailed design	M24
MS3	Platform development (hardware)	M26
MS4	Integration of technologies: Hypervisor and Services	M30
MS5	Deployment of execution environments	M33
MS6	Application software development	M36
MS7	Verification and validation	M40

Table 2: Estimated dates for wind power demonstrator milestones

Once the core hardware is available, the integration of DREAMS technologies will take place (virtualization environment, core services, network drivers, SCL, etc.), giving place to the forth milestone. The virtualization layer will allow creating partitions defined in system architecture to allocate system functionalities with the required properties and resources. The fifth milestone will be reached when the partitions are created and execution environments successfully deployed on them. At this point, the application software reused from current supervision and control system will be allocated in the corresponding partitions, and new application software will be implemented for the safety protection system. When software is developed the sixth milestone will be reached. Finally the verification and validation plans will be executed to complete the demonstrator development (milestone seven).

3.1.2 Level of integration of DREAMS technologies

The following table can be used at any time of the project to check the degree of integration of DREAMS technologies in the wind power demonstrator.

Work Package	Technology	Expected at	Integration status
WP1	Architectural style and core services	M26	
WP2	Harmonized platform	M26	
WP2	XtratuM hypervisor	M26	
WP2	Windows Embedded CE 6.0	M33	
WP3	Safety Communication Layer	M26	
WP3	EtherCAT Datalogger	M33	
WP4	XtratuM toolset	M30	
WP4	Modeling meta-models and tools	M30	
WP4	SW component model	M30	
WP4	HW platform model	M24	
WP4	Hypervisor and partition model	M24	
WP4	Safety model	M22	
WP4	Variability model (BVR)	M24	
WP5	Modular safety cases for hypervisor	M22	
WP5	COTS multicore device	M26	
WP5	Mixed-criticality network	M26	
WP5	Solution patterns	M24	
WP5	EtherCAT fault injector	M36	
WP5	Product line validation strategy	M40	
WP5	Product line certification strategy	M40	

Table 3: Status monitoring of integration of technologies

Integration status can be:

- Not started
- In progress
- Completed
- Validated

It must be taken into account that the development of some technologies can be concluded later than the integration date expected for those technologies in the wind power demonstrator. In those cases, a preliminary version should be integrated to allow continuing with the demonstrator development plan. If this is not possible, an alternative plan should be proposed to minimize the impact of the delays in the demonstrator.

3.1.3 Monitoring of alignment with project objectives

The alignment of the demonstrator with project objectives will be assessed through a preliminary evaluation carried out at M30. The template is presented in section 4.1.

4 Templates

This section includes the templates to be filled for the preliminary evaluation performed at M30, and final evaluation performed at the end of the project (M45), with demonstrator fully implemented and validated.

4.1 Milestones

Table 4 shows the template to be filled in the preliminary evaluation at M30 for the monitoring of milestones achievement.

Milestone	Description	Achieved (Y/N)	Comments
MS1	Safety concept		
MS2	Definitive architecture and detailed design		
MS3	Platform development (hardware)		
MS4	Integration of technologies: Hypervisor and Services		
MS5	Deployment of execution environments		
MS6	Application software development		
MS7	Verification and validation		

Table 4: Template for monitoring milestones at M30

4.2 Integration of technologies

Table 5 shows the template to be filled in the preliminary evaluation at M30 for the monitoring of integration of technologies.

Technology	Expected at	Achieved (Y/N)	Comments
Architectural style and core services	M26		
Harmonized platform	M26		
XtratuM hypervisor	M26		
Windows Embedded CE 6.0	M33		
Safety Communication Layer	M26		
EtherCAT Datalogger	M33		
XtratuM toolset	M30		
Modeling meta-models and tools	M30		
SW component model	M30		
HW platform model	M24		
Hypervisor and partition model	M24		
Safety model	M22		
Variability model (BVR)	M24		
Modular safety cases for hypervisor	M22		
COTS multicore device	M26		
Mixed-criticality network	M26		
Solution patterns	M24		
EtherCAT fault injector	M36		
Product line validation strategy	M40		
Product line certification strategy	M40		

Table 5: Template for monitoring technologies integration at M30

4.3 KPIs

Table 6 shows the template to be filled in both the preliminary and final evaluations at M30 and M45 for the presentation of KPIs. The shaded rows shall be removed in the preliminary evaluation, since those KPIs cannot be calculated until the demonstrator is fully developed and validated (unless there is enough information to provide an early estimation).

ID	KPI	Goal	Value	Comments
1	Achievable Performance Level	SIL3		
2	Achievable Safety Integrity Level	PLe		
3	Achievable Hardware Fault Tolerance	1		
4	Validated support for key real-time OS	Yes		
5	Minimum closed-loop cycle time	1ms		
6	Minimum fieldbus cycle time	1ms		
7	Maximum jitter	10us		
8	Fault containment by construction	Yes		
9	Percentage of integrated core services	50%		
10	Percentage of domain services portable to new architecture	80%		
11	Percentage of system architecture/design modeled	70%		
12	Percentage of software application modeled	50%		
13	Models complexity	Yes		
14	Temporal and spatial isolation by construction	Yes		
15	Bounded temporal interference (network)	10us		
16	Bounded temporal interference (processing)	10us		
17	Bounded temporal interference (resources access rate)	10us		
18	Resources access rate penalty	5%		

19	Percentage of out of the box gateways	50%		
20	Sensor-to-partition latency	100us		
21	Sensor-to-partition jitter	10us		
22	Development time reduction	20%		
23	Percentage of development steps covered by tools in demonstrator	60%		
24	Percentage of development steps potentially covered by tools in wind power	80%		
25	Percentage of automatically executable transformations	10%		
26	Effort reduction for addition or modification of features	30%		
27	Effort reduction for replacement of components	30%		
28	Broadening of the design space	20%		
29	Pre-certifiable patterns for aspect features	50%		
30	Adaptability to evolution of product and standards	Yes		
31	Cost reduction in development of prototype	30%		
32	Reduction of prototype development time	20%		
33	Reusability of building blocks in other power generation domain	25%/25%		
34	Percentage of public information coming from the demonstrator	30%		

35	Percentage of training material coming from the demonstrator	10%		
36	Percentage of support for relevant OS (RTOS and GPOS)	75%		
37	Scalability gap	25%		
38	Reduction in certification cost	30%		
39	Reduction in re-certification cost	60%		
40	Reduction in criticality level up	30%		
41	Safe data availability	>10		
42	Safe algorithm programming flexibility	Yes		
43	Network flexibility and scalability	Yes		
44	Network validation supported by tools	Yes		
45	Percentage of compatible development steps	80%		
46	Percentage of variability sources successfully handled	80%		
47	Reduction of variability adaptation time	60%		

Table 6: Template for collecting KPIs at M30 and M45

4.4 Measures for success and objectives

The following tables are the templates to be filled in both the preliminary and final reports at M30 and M45 for the evaluation of measures for success and project objectives. The completeness and accuracy of the preliminary report will be conditioned by the degree of completeness of the demonstrator.

Objective 1: Architectural Style und Modeling Methods based on Waistline Structure of Platform Services:	
Measure for success	Evaluation
1.1 Safety	
1.2 Real-time	
1.3 Fault containment	
1.4 Timely adaptation	
1.5 Security	
1.6 Domain-independent core services	
1.7 Modular architecture	
1.8 Models with fine grained analysis/scheduling	
1.9 Models complexity	
1.10 Models completeness	
Objective evaluation	

Table 7: Template for evaluation of objective 1

Objective 2: Virtualization Technologies to Achieve Security, Safety, Real-Time Performance as well as Data, Energy and System Integrity in Networked Multi-Core Chips:	
Measure for success	Evaluation
2.1 Isolation	
2.2 Reduced bank conflicts	
2.3 Gateways	
0 Reduction of latencies	
2.5 Reduction of jitter	
2.6 Reconfiguration	
2.7 Security	
Objective evaluation	

Table 8: Template for evaluation of objective 2

Objective 3: Adaptation Strategies for Mixed-Criticality Systems to Deal with Unpredictable Environment Situations, Resource Fluctuations and the Occurrence of Faults:+	
Measure for success	Evaluation
3.1 Variability	
3.2 Criticality spectrum	
3.3 Applicability	
0 Efficiency	
3.5 Scalability	
3.6 Portability	
Objective evaluation	

Table 9: Template for evaluation of objective 3

Objective 4: Development Methodology and Tools based on Model-Driven Engineering:	
Measure for success	Evaluation
4.1 Development process	
0 Development steps covered by tools	
4.3 Automatically executable transformations	
Objective evaluation	

Table 10: Template for evaluation of objective 4

Objective 5: Certification and Mixed-criticality Product Lines	
Measure for success	Evaluation
5.1 Modular safety-case	
5.2 Safety-case modularity	
5.3 Architectural support	
5.4 Configuration optimization	
5.5 Variability	
5.6 Domains and market features	
Objective evaluation	

Table 11: Template for evaluation of objective 5

Objective 6: Feasibility of DREAMS Architecture in Real-World Scenarios	
Measure for success	Evaluation
6.1 Separation	
6.2 Standard compliance	
6.3 Cost	
6.4 Reusability	
6.5 Extensibility	
Objective evaluation	

Table 12: Template for evaluation of objective 6

Objective 7: Promoting Widespread Adoption and Community Building	
Measure for success	Evaluation
7.1 Community infrastructure	
7.2 Training material	
7.3 Standardization	
7.4 Roadmap	
Objective evaluation	

Table 13: Template for evaluation of objective 7

Objective 8: Enable higher integration of mixed-criticality systems providing scalability and composability.	
Measure for success	Evaluation
8.1 Support for integration of criticality levels	
8.2 Demonstrator scalability	
Objective evaluation	

Table 14: Template for evaluation of objective 8

Objective 9: Reduce certification cost/effort for safety protection system.	
Measure for success	Evaluation
9.1 Certification cost	
9.2 Re-certification cost	
9.3 Criticality level up	
Objective evaluation	

Table 15: Template for evaluation of objective 9

Objective 10: Increase capabilities and programming flexibility of the safety protection system.	
Measure for success	Evaluation
10.1 Safe data availability	
Objective evaluation	

Table 16: Template for evaluation of objective 10

Objective 11: Incorporate mixed-criticality networks and means for validation.	
Measure for success	Evaluation
11.1 Mixed-criticality networks	
11.2 Networks validation means	
Objective evaluation	

Table 17: Template for evaluation of objective 11

Objective 12: Obtain a complete methodology to manage system complexity and variability.	
Measure for success	Evaluation
12.1 Methodology compatibility	
12.2 Variability management	
Objective evaluation	

Table 18: Template for evaluation of objective 12

5 Conclusions

This document presents the plan to monitor and evaluate the concepts, technologies and tools developed in DREAMS by means of the wind power demonstrator. Key Performance Indicators have been collected in order to provide quantitative, objective and measurable information to later evaluate measures for success and fulfillment of project objectives. However, some of the collected KPIs do not meet the required properties (objective, measurable, comparable), because of at least one of the following reasons:

- It cannot be precisely measured (e.g. development time and cost). In these cases, estimation will be done by experienced engineers, supporting it with as many evidences and solid arguments as possible.
- It cannot be compared to previous situation because of the lack of information. Again, experienced engineers will provide arguments and estimations to better understand the benefits and cons of the new approach.

The final evaluation will try to minimize the number of estimations and maximize the number of objectively calculated indicators to increase the credit of the document. However, in the preliminary report some of the indicators will need to be estimated.

Finally, it can be concluded that the wind power demonstrator will contribute in the evaluation of a high percentage of project measures for success and objectives. Therefore, the alignment of the demonstrator with the project vision is very high, and this will allow an extensive use of the demonstrator for dissemination activities.

6 Bibliography

1. DREAMS, *Distributed Real-Time Architecture for Mixed-Criticality Systems: Description of Work*, in *DOW*2014. p. 260.
2. DREAMS, *Distributed Real-Time Architecture for Mixed-Critiality Systems: Wind Power Use Cases Specifications*, in *D7.1.1*2014. p. 51.
3. B&R. *Automation PC 910*. 2015 [cited 2015 June]; Available from: http://www.br-automation.com/en/products/industrial-pcs/automation-pc-910/.
4. XILINX, *ZYNQ-7000 All Programmable SoC: Technical Reference Manual*, in *UG585*, 2014
5. EtherCAT, *Safety over EtherCAT*, 2011
6. IEC, *IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*, in *Requirements for electrical/ electronical / programmable electronic safety-related systems*2010, IEC.
7. DREAMS, *Distributed Real-Time Architecture for Mixed-Critiality Systems: Architecture Conceptualization: Requirements, Terms and Principles*, in *D1.1.1*2014. p. 295.
8. DREAMS, *Distributed Real-Time Architecture for Mixed-Critiality Systems: Architecture Style of DREAMS*, in *D1.2.1*2014.
9. DREAMS, *Distributed Real-time Architecture for Mixed Criticality Systems: XtratuM support for enhanced hypervisor layer services: description and interfaces*, in *D2.3.1*2015. p. 92.
10. Fent Innovative Software Solutions, *XtratuM Hypervisor for INTEL x86*, in *fnts-xm-um-x86-21c*, 2013
11. DREAMS, *Distributed Real-Time Architecture for Mixed-Critiality Systems: System Platform Integration*, in *D2.4.1*2016.
12. DREAMS, *Distributed Real-time Architecture for Mixed Criticality Systems: High-Level Design of Cluster-Level Safety and Security Services*, in *D3.3.1*2014. p. 49.
13. DREAMS, *Distributed Real-time Architecture for Mixed Criticality Systems: First Implementation of Cluster-Level Safety and Security Services*, in *D3.3.2*2015. p. 80.
14. DREAMS, *Distributed Real-time Architecture for Mixed Criticality Systems: Integration and Support Report*, in *D3.4.1*2017.
15. DREAMS, *Distributed Real-Time Architecture for Mixed-Critiality Systems: Initial Collection of Offline Adaptation Strategies for Mixed-Criticality*, in *D4.1.1*2014. p. 107.
16. DREAMS, *Distributed Real-time Architecture for Mixed Criticality Systems: Definition of Offline Adaptation Strategies for Mixed-Criticality and Initial Implementation*, in *D4.1.2*2015. p. 102.
17. DREAMS, *Distributed Real-time Architecture for Mixed Criticality Systems: Variability Analysis and Testing for Mixed-Criticality Systems*, in *D4.3.1*2015. p. 54.
18. DREAMS, *Distributed Real-Time Architecture for Mixed-Critiality Systems: Modular Safety Case for Hypervisor*, in *D5.1.1*2015.
19. DREAMS, *Distributed Real-Time Architecture for Mixed-Critiality Systems: Modular Safety Case for COTS processor*, in *D5.1.2*2015.
20. DREAMS, *Distributed Real-Time Architecture for Mixed-Critiality Systems: Modular Safety Case for Mixed-Criticality Network*, in *D5.1.3*2015.
21. DREAMS, *Distributed Real-Time Architecture for Mixed-Criticality Systems: Cross domain mixed-criticality patterns*, in *D5.3.1*2016.

22. DREAMS, *Distributed Real-Time Architecture for Mixed-Criticality Systems: Fault injection framework*, in *D5.2.3*2015.
23. DREAMS, *Distributed Real-Time Architecture for Mixed-Criticality Systems: Validation Techniques for Product-lines of Mixed Criticality Systems*, in *D5.5.2*2015.
24. DREAMS, *Distributed Real-Time Architecture for Mixed-Criticality Systems: Method for certifying mixed-criticality product lines*, in *D5.5.3*2016.
25. ISO, *ISO 13849-1: Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*, 2006. p. 94.
26. ISO, *ISO 13849-2: Safety of machinery — Safety-related parts of control systems — Part2: Validation*, 2012. p. 86.
27. IEC, *IEC 62061 - "Safety of Machinery: Functional safety of electrical, electronic and programmable electronic control systems"*, 2013.
28. IEC, *IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General Requirements*, in *Requirements for electrical/ electronical / programmable electronic safety-related systems*2010, IEC.
29. IEC, *IEC 61508-3: Functional safety of electrical/electronical/programmable electronic safety-related systems - Part 3: Software requirements*, in *Requirements for electrical/ electronical / programmable electronic safety-related systems*2010, IEC.
30. GL, *Guideline for the Certification of Wind Turbines*, 2010.
31. *SWOT analysis*. 25/09/2015]; Available from: https://en.wikipedia.org/wiki/SWOT_analysis.
32. IKERLAN, *Certificate: Functional Safety Management Structure - IEC-61508*, 2013.

Terminology

Access control

Access control includes authorization, identification and authentication (I&A), access approval, and audit. Authorization specifies what a subject can do, e.g., read, write or execute a file. Access approval grants or rejects access to the requested resource. Audit records the access to a resource. For Identification and authentication please refer to the topic on authentication.

Assurance Level

The assurance level is determined from the safety assessment process and hazard analysis by examining the effects of a failure condition in the system.

Authenticity

Authenticity ensures that data is genuine and that the actual origin of the data is the same as the claimed origin.

Authentication of data origin

Authentication of data origin ensures that the actual origin of the data is the same as the claimed origin.

Authentication of a communication partner

Authentication of a communication partner ensures that the actual communication partner is the same as claimed.

Availability

If an Information or access to a service is needed, it must be available. Additionally, it must also function correctly.

Behavior

The behavior of a subsystem is the sequence of message (i.e., intended and unintended) that is produced by the subsystem at its LIF.

Channel

A channel serves for the exchange of messages between ports. A channel is associated with a communication topology, a data-direction (e.g., unidirectional or bidirectional), temporal properties and dependability properties.

Cluster

A cluster is a physically distributed computer system that consists of a set of nodes interconnected by a physical network. Each node can be a multi-core chip with multiple IP cores interconnected by a network-on-a-chip. A cluster can be connected to another cluster using a gateway.

Compliant Item

A compliant item is any item (e.g. an element) on which a claim is being made with respect the clauses of IEC 61508 series.

Component

A component is a constituting element of an application subsystem and forms the basic unit of work. It interacts with other components through the exchange of messages across LIFs in order to work towards a common goal and provide the application services.
A component is regarded as a self-contained building block that can be used in the design of a larger system. The component can have a complex internal structure that is neither visible, nor of concern, to the user of the component. In the context of embedded real-time systems, it is essential that the component behaviour can be specified in the domains of value and time.

Composability

Composability is a concept that relates to the ease of building systems out of subsystems. A system, i.e., a composition of subsystems, is considered composable with respect to a certain property (functional or non-functional) if this property, given that it has been established at the subsystem level, is not invalidated by the integration. Examples of such properties are timeliness or certification.

For example, some embedded systems closely interact with their environment and they have to produce intended results at intended points of time. Temporal composability is a prerequisite for the feasible construction of such temporally predictable systems of high complexity. In architectural styles that support temporal composability, determining the emergent temporal behavior of the resulting system is eased by the fact that the individual subsystems retain their temporal properties after integration.

Confidentiality

Confidentiality ensures the privacy of information. Only authorized users can read the data. This includes the data stored in memory as well as the data transferred over a network.

Core Platform Service

Core platform services (or core services for short) are mandatory in every instantiation of the architecture style. The core platform services provide the foundation for higher-level, optional platform services. For instance, a message-based communication service is a core service. At any given integration level, the core services form a waist that can be realized using a multitude of implementation choices. Also, they form the starting point for the domain-customization using optional services. Exemplary categories of core services are communication services, execution services, time services and resource management services.

Criticality System

Mixed-criticality is the concept of allowing application subsystems that must meet different assurance levels (e.g., ranging from DAL A to DAL E in RTCA DO-178B, SIL1 to SIL4 in EN ISO/IEC 61508) to seamlessly interact and co-exist on the same networked distributed computational platform.

Design Pattern

A Design Pattern is a general reusable solution to a commonly occurring problem within a given context. It is a description or template for how to solve a problem that can be used in many different situations. Patterns are formalized best practices.

Dependability Patterns

Design patterns that focus on finding common links on dependability as a measure of a system's availability, reliability, and its maintainability.

Determinism

A model behaves deterministically if and only if, given a full set of initial conditions (the initial state) at time t0, and a sequence of future timed inputs, the outputs at any future instant t are entailed.

Development Methodology

The development methodology is a framework consisting of a development process, a set of methods, techniques and tools for mixed-criticality systems based on networked multi-core chips.

End-to-End Channel

An end-to-end channel is a channel that can include on-chip and off-chip communication links over hierarchical, heterogeneous and mixed-criticality networks. Gateways enable the horizontal integration at the cluster-level across different off-chip communication networks with different protocols (e.g., TTEthernet, EtherCAT, etc.), different reliabilities (e.g., fault-tolerant networks with media redundancy and active star couplers, low-cost fieldbus networks). Gateways between NoCs and off-chip networks enable the vertical integration through the seamless communication in hierarchical networks respecting mixed-criticality safety and security requirements.

Error

An error is that part of the system state which is liable to lead to a subsequent failure. A failure occurs when the error reaches the service interface.

Event

“An event denotes a distinct form of state change in a running system, taking place at distinct points in time called occurrences of the event. That is, a running system can be observed by identifying certain forms of state changes to watch for, and for each such observation point, noting the times when changes occur. This notion of observation also applies to a hypothetical predicted run of a system or a system model — from a timing perspective, the only information that needs to be in the output of such a prediction is a sequence of times for each observation point, indicating the times that each event is predicted to occur.” – TIMMO-2-USE

Fail-operational System

A fail-operational system is able to tolerate one or several faults. Fail-operational systems send correct messages despite the failure of their subsystems.

Fail-safe System

If a fail-safe system one or more safe states can be reached in case of a system failure. Fail-safeness is a characteristic of the controlled object, not the computer system. In fail-safe systems the computer system must have high error-detection coverage.

Fault

A fault is the adjudged or hypothesized cause of an error. Faults can be internal or external of a system.

Examples of types: An external fault (e.g. a malicious attack) causes an error, and possible a subsequent failure. An internal fault (i.e. vulnerability) allows an external fault to harm the system and has to pre-exist in the system.

Fault-Containment Region

A Fault Containment Region (FCR) is a subsystem that operates correctly regardless of any arbitrary logical or electrical fault outside the region.

Fault Hypothesis

The fault hypothesis is the specification of the faults that must be tolerated without any impact on the essential system services. The fault hypothesis states the assumptions about units of failure (see Fault Containment Region), failure modes, failure frequencies, failure detection, and state recovery.

Failure

A failure occurs when the delivered service deviates from fulfilling its specification.

Integration Level

The integration level denotes the layer in a system-of-systems at which it is composed out of its components. Different integration levels can be distinguished in embedded systems including the chip-level, the cluster-level and the core-level.

Integration Level: Chip-Level

The chip-level is an integration level where IP cores are integrated using an on-chip network.

Integration Level: Cluster-Level

The cluster-level is an integration level where multiple chips are interconnected to a cluster using one or more off-chip communication networks (e.g., ´TTEthernet, EtherCAT). Thereby, applications can be supported that need more resources than are available on a single SoC. In addition, a distributed system with multiple SoCs is a prerequisite for implementing safety-critical application subsystems, because today’s semiconductor technology does not support the manufacturing of chips with a reliability that is suitable for ultra-dependability.

Integration Level: Core-Level

The core-level is an integration level where components are integrated using a hypervisor.

Integrity

Data integrity means that the data cannot be modified unnoticeably. Every intended and unintended modification of the data should be detectable.

Mixed-Criticality Architecture

A mixed-criticality architecture is an architecture that provides platform services and a development methodology supporting mixed-criticality (e.g., temporal and spatial partitioning, modular certification methods).

Optional Platform Services

The optional platform services which are built upon the core platform services can be generic in the sense that they can be used in multiple application domains or specific for a focused domain. These services are optional in the sense that they are not required in every instantiation of the architecture. If needed, developers can pick them out of the architectural style, which includes a set of existing, validated component libraries for the different integration levels. For instance an encryption service could be a generic optional service.

Partition

A partition is the execution environment for a component with corresponding resources (e.g., processor, memory, communication, input/output). The resources for a partition are protected by temporal partitioning and spatial partitioning in order to avoid unintended feature interaction and fault propagation between components.

Periodic Message

Periodic messages are specified by a period and phase, which can be expressed with respect to a system-wide synchronized global time base.

Periodic messages can be exchanged using *time-triggered communication*, where the instants of periodic message transmissions are specified by an a priori planned conflict-free communication schedule. For time-triggered communication, the communication infrastructure is deterministic and guarantees temporal properties such as latency, latency jitter, bandwidth, and message order.

Platform

A platform is the hardware/software foundation for the execution of applications. The platform instantiates the architectural style and implements generic services for the development of applications, which are denoted as platform services (see core platform services and optional platform services).

Platform Services

Platform services facilitate the development of applications subsystems and separate the application functionality from the underlying platform technology to reduce design complexity and to enable design reuse. We differentiate between two different types of platform services: core platform services and optional platform services.

Platform-Independent Model

A Platform Independent Model (PIM) is a model of a system that is independent of the specific technological platform used to implement it.

Platform-Specific Model

A Platform Specific Model (PSM) is a model of a system that is linked to a specific technological platform used in implementation.

Reliability

Reliability is the ability of an application subsystem to perform its required functions under stated conditions for a specified period of time.

Safety manual for compliant items

Safety manual for compliant items is a document that provides all the information relating to the functional safety of an element, in respect of specified element safety functions, that is required to ensure that the system meets the requirements of IEC 61508 series.

Secure End-to-End Channel

Using a secure end-to-end channel means that the communication is uninterruptedly protected between two communicating parties, e.g., PGP (e-mail), ZRTP (VoIP), etc.

Secure Point-to-Point Channel

Using a secure point-to-point Channel means that the communication is uninterruptedly protected between two points/nodes in a network, e.g., VPN, MACsec, IPsec etc.

Security Mechanisms

Security mechanisms are used to provide security services, e.g., encryption is used to ensure confidentiality.

Security Services

Security services define different classes to protect a system against attacks. Security services include authentication, access control, confidentiality, integrity and non-repudiation.

Spatial Partitioning

Spatial partitioning ensures that the service in one partition cannot alter the code or private data of another partition. Spatial partitioning shall also prevent a partition from interfering with control of external devices (e.g., actuators) of other partitions.

Sporadic Message

Sporadic messages establish rate-constrained data-flows with maximum bandwidth use, which helps to guarantee bounded latencies. Successive transfers of sporadic messages belonging to the same rate-constrained dataflow are guaranteed to be offset by a minimum duration (also called minimum inter-arrival time of sporadic messages).

The temporal behaviour of sporadic messages can further be specified by sporadic repetition constraints.

State

The state enables the determination of a future output solely on the basis of the future input and the state the system is in. In other word, the state enables a "decoupling" of the past from the present and future. The state embodies all past history of the given system. Apparently, for this role to be meaningful, the notion of the past and future must be relevant for the system considered.

State Recovery

State recovery is the action of re-establishing a valid state in a subsystem after a failure of that subsystem.

Subsystem

A subsystem is a part of a system that represents a closure with respect to a given property.

System

A system is a set of subsystems.

Temporal Partitioning

Temporal partitioning ensures that a partition cannot affect the ability of other partitions access shared resources, such as the network or a shared CPU. This includes the temporal behaviour of the services provided by resources (latency, jitter, duration of availability during a scheduled access).

Timing Event

Timing Events are identifiable state changes that are possible to constrain with respect to timing. Examples of timing events are: Message Sent, Message Arrived, Task Activation, Task Execution End, Frame Instantiation, Frame Transmission Start, Frame Transmission End.

The most common timing constraints are Latency constraint, Repetition Constraint, Synchronization Constraint.

Task Activation (Event)

A Task Activation is a Timing Event that describes the fact that a recurring task has entered the scheduling queue, i.e. will be considered by the scheduler for allocation of the processing unit.

Task Activations may occur for example periodically, with a certain jitter (see also Repetition Constraint).

Task Execution End (Event)

A Task Execution End is a Timing Event that describes the fact that a recurring task has executed all its instructions and is therefore removed from the scheduling queue.

Synchronization Constraint

A Synchronization constraint describes how tightly the occurrences of a group of events follow each other. This is typically expressed by a temporal window, i.e. an upper bound on the temporal distance between the occurrences of the events of the group.

An example is the reading of input data from different sensors, which must occur in a small time window to ensure a temporally consistent view of the environment.

Worst Case Execution Time (WCET)

The Worst Case Execution Time is the maximal delay needed to execute all instructions of a task, excluding interruption or pre-emption delays.

Worst Case Response Time (WCRT)

The Worst Case Response Time is the worst delay between the occurrence time of the Task Activation and the occurrence time of the Task Execution End. With respect to the WCET, it includes interruption/pre-emption or initial blocking delays (non-pre-emptive scheduling).

Worst Case Traversal Time (WCTT)

The Worst Case Traversal Time is the worst delay between the occurrence time of the Frame Instantiation and the occurrence time of the Frame Transmission End.