Project number: 826276

CPS4EU

Cyber Physical Systems for Europe

D9.1 (2 parts)

Use case 10: Distributed controls for transmission network

Use case 11: Software defined edge Control safety report for critical function

Reviewers: A. Carbonne (Schneider Electric France), E. Rutten (INRIA), M. Arnaud (CEA)

Dissemination level: Public

Requirements for WP9 Use case 10
Distributed controls for transmission network

Deliverable ID:	D9.1
Version:	Rev1.1, 10 September 2020
Due Date:	1 March 2020

CPS4EU
D9.1 – WP 9 Use Case 10 Requirements

Document Manager:	**RTE**		
Project Title:	Cyber Physical Systems for Europe		
Project Acronym:	CPS4EU		
Contract Number:	x		
Project Coordinator:	Valeo		
WP Leader:	RTE		
Task:	T9.1	**Task Leader:**	RTE
Document ID:	D9.1	**Version:**	Rev1.1
Deliverable Title:	Use Case 10 Requirements	**Date:**	10/09/2020
		Approved:	x
Document Classification:	Public		

Approval Status

Prepared by:	**Guillaume GIRAUD**
Approved by (WP Leader):	Guillaume GIRAUD
Approved by (Coordinator):	Philippe. GOUGEON et Antoine DUPRET
	x

Contributors

Name	Partner
Guillaume Giraud	RTE
Mathilde ARNAUD	CEA
Eric RUTTEN	INRIA

Version History

Version#	Date	Reason for change	Released by
Rev0.1	25/10/2019	Initial version	G. Giraud
Rev0.2	13/02/2020	Requirements added	G. Giraud
Rev0.3	27/02/2020	Review by CEA and INRIA	G. Giraud
Rev.1	18/03/2020	Review by Project Coordinators	G. Giraud
Rev.1.1	10/09/2020	Table of contents correction	G. Giraud

Distribution List

Name	Company/Organization	Role / Title
Consortium	CPS4EU Consortium	n/a

TABLE OF CONTENTS

0 Introduction 5
0.1 Purpose 5
0.2 Scope 5
0.3 Link to other documents/TASKS 6
0.4 Definitions, acronyms, and abbreviations 6
1 UC10 - distributed controls for transmission network [RTE] 7
1.1 Overall Description 7
1.1.1 High level Use Case Description 7
1.1.2 Main Features 10
1.1.3 Limits 11
1.1.4 Conclusions 11
1.2 Requirements 12
1.2.1 Functional Requirements 12
1.2.2 Interface Requirements 14
1.2.3 Performance Requirements 15
1.2.4 Security Requirements 16
1.2.5 Operational Requirements 17
1.2.6 Usability Requirements 18
1.2.7 Policies & Compliance Requirements 19
1.2.8 Design Constraints 20
1.2.9 Ethical Requirements 21
2 REQUIREMENTS GATHERING METHODOLOGY 22
2.1.1 Requirements Types 22
2.1.2 Requirement Identification 24
2.1.3 Requirement Principles 25
2.1.4 Requirement Attributes 25

TABLES

Table 1 – UC10 Functional Requirements Description 13
Table 2 – UC10 Functional Requirements interrelations with Modules & Pre-integrated Architectures 13
Table 3 – UC10 Interface Requirements Description 14
Table 4 – UC10 Interfaces Requirements interrelations with Modules & Pre-integrated Architectures 15
Table 5 – UC10 Performance Requirements Description 15
Table 6 – UC10 Performance Requirements interrelations with Modules & Pre-integrated Architectures 15
Table 7 – UC10 Security Requirements Description 16
Table 8 – UC10 Security Requirements interrelations with Modules & Pre-integrated Architectures 16
Table 9 – UC10 Operational Requirements Description 17
Table 10 – UC10 Operational Requirements interrelations with Modules & Pre-integrated Architectures 18
Table 11 – UC10 Usability Requirements Description 18
Table 12 – UC10 Usability Requirements interrelations with Modules & Pre-integrated Architectures 18
Table 13 – UC10 Policies & Compliance Requirements Description 19
Table 14 – UC10 Policies & Compliance Requirements interrelations with Modules & Pre-integrated Architectures . 19
Table 15 – UC10 Design Constraints Requirements Description 20
Table 16 – UC10 Design Constraints Requirements interrelations with Modules & Pre-integrated Architectures 20
Table 17 – UC10 Ethical Requirements Description 21
Table 18 – UC10 Ethical Requirements interrelations with Modules & Pre-integrated Architectures 21

0 INTRODUCTION

0.1 PURPOSE

This document intends to provide a first, general description of WP9 Use Case 10 to WP1-WP6 leaders/participants, so they can better understand the use cases main purposes and the environment where they will be implemented.

0.2 SCOPE

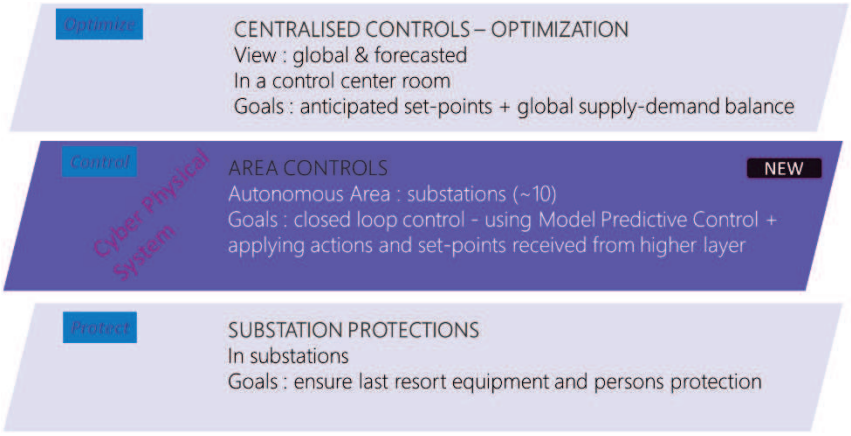
The following document describes Use case 10 of the WP9. A separate document is dedicated to WP9 SME use cases.

This use case is of special interest to electric grid control. Today's architecture has basically two levels:

- substation control, which performs fast, simple controls based on local information (such as voltage and currents in the substation),
- control room, which includes wide area, slower controls, (such as load frequency control or global secondary voltage control).

With the rise of distributed generation, a different control architecture may be needed. If a consensus seems to emerge in the academic community on the use of distributed control to manage complex systems (or systems of systems), the electricity industry is still working on what should be this future control architecture.

RTE R&D is promoting a 3-layer architecture, where "area" controls are supplementing the 2 existing layers.



The centralized level handles the global vision and the heavy forecasting computation and provides lower levels with set-points for optimal operation (OPTIMIZE).

The area level applies actions from higher level and reacts to any unforeseen problems to adapt in real-time (seconds) the strategy (CONTROL).

Substation protection take immediate actions (milliseconds) to guarantee people and assets protection, such as opening breakers when short-circuit is detected (PROTECT).

The use case 10 is the first implementation of this "area" concept on RTE transmission grid.

0.3 LINK TO OTHER DOCUMENTS/TASKS

ID	Description
D9.1	Use case requirements v1

0.4 DEFINITIONS, ACRONYMS, AND ABBREVIATIONS

Acronym / abbreviation	Description
DER	Distributed Energy Resources
ASA	Area Slow Automatons
SSFA	Substation Slow/Fast Automatons
CSA	Centralized Slow Automatons (CSA)
MPC	Model Predictive Control
API	Application Programming Interface
ICCP	Inter Control Centres Protocol
DSO	Distribution System Operator
TSO	Transmission System Operator

1 UC10 - DISTRIBUTED CONTROLS FOR TRANSMISSION NETWORK [RTE]

1.1 OVERALL DESCRIPTION

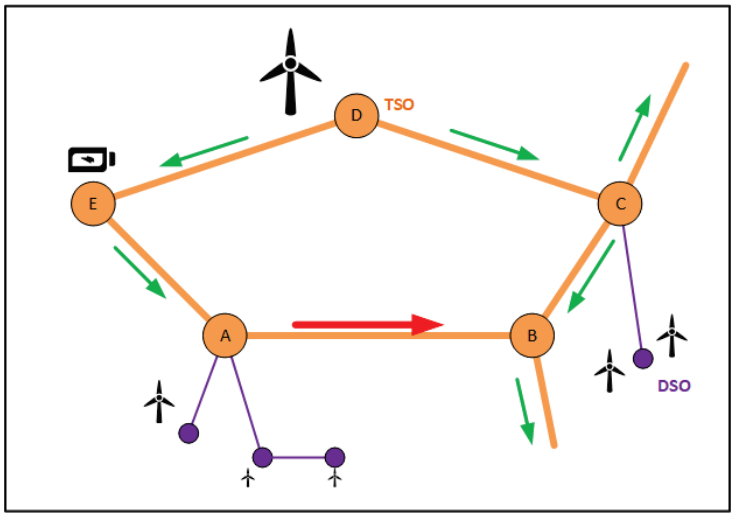
1.1.1 High level Use Case Description

Renewable Energies, and especially Distributed Energy Resources (DER), are increasingly important in electricity generation, especially wind and solar power, and pivotal for the energetic transition. From a system operation point of view, they differ in many points from classical power stations:

- They are often connected to lower voltage networks, not designed to accommodate generation.
- They have very variable outputs, depending on meteorological factors (for example, wind farms produce on average 25% of their peak power).
- Their average unitary power is lower than classic power stations, so system operators will interact with significantly higher number of actors.

An electrical network is dimensioned to manage the peak current, so DER could lead transmission operators to build power lines used only a fraction of the time. A more sober alternative is to manage the flow using new possibilities offered by batteries, power electronics and cyber-physical systems to operate the grid closer to its limits: less physical, more cyber.

For example, on the networks presented on the right, green arrows represent a current under the acceptable limit whereas the red arrow represents an overload on the line between A and B. Transmission network (TSO) is in orange, distribution network (DSO) in purple.



Different levers can be activated to remove this constraint:

- Charging the battery in E,
- Limiting production in D,
- Limiting production at DSO level in grid connected to substation A.

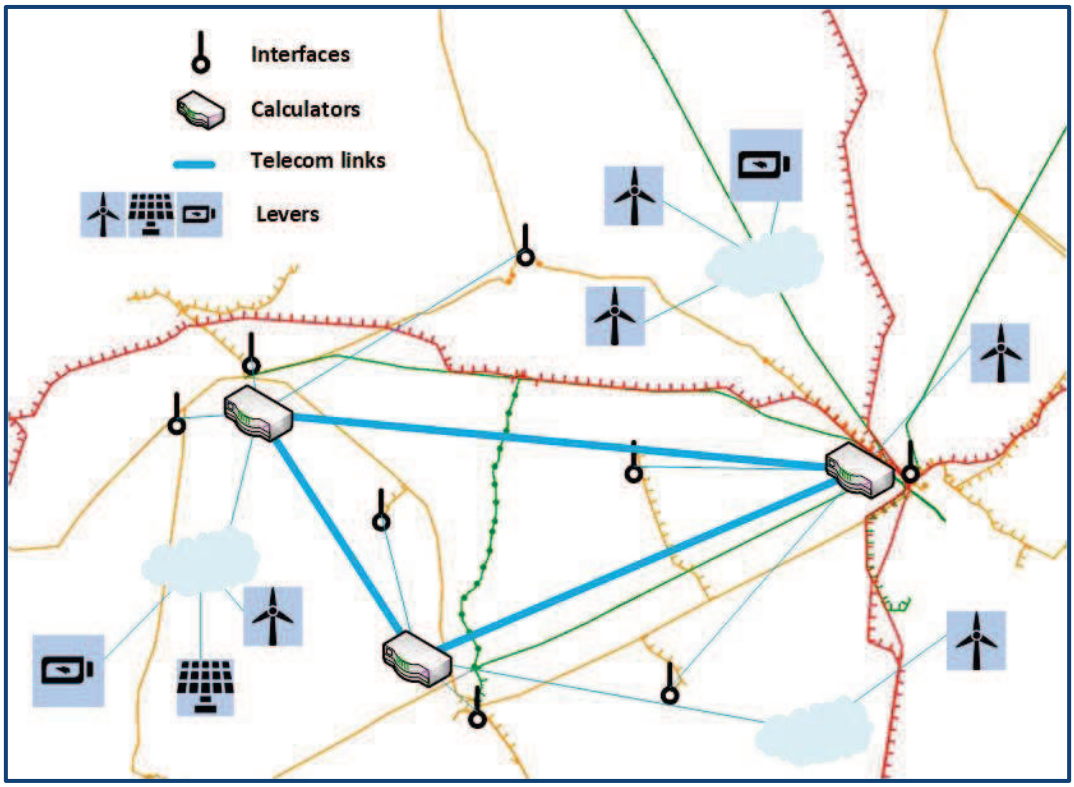
Most of the time, it is a combination of these actions that will be the most relevant, given several parameters: state of battery's charge, time to limit production of the wind farms, severity of the overload, values of currents on the other lines, state of the network after the use of these levers, generation merit order (curtail the cheapest wind farm first), …

The time-to-action is too fast for a human operator (dozens of seconds max) and the complexity of the optimization is also beyond its grasp. That is the reason why we need to install distributed controls, called area automatons, to handle this task.

By monitoring the network and simulating the flows, **area automatons** will ensure the safe operation of the network (in nominal or n-1 situations) by sending:

- topological orders to the network circuit breakers,
- modulation orders to the generators,
- set points to the storage batteries.

These automatons are composed of **interfaces** to monitor and act on the network, of **calculators** who implement the optimisation algorithms, of **telecom links** to ensure communication between its distributed components. They act on the **levers**: wind and solar farms, batteries, network topology …



Those area automatons, also called Area Slow Automatons (ASA), are complemented by Substation Slow/Fast Automatons (SSFA) and Centralized Slow Automatons (CSA).

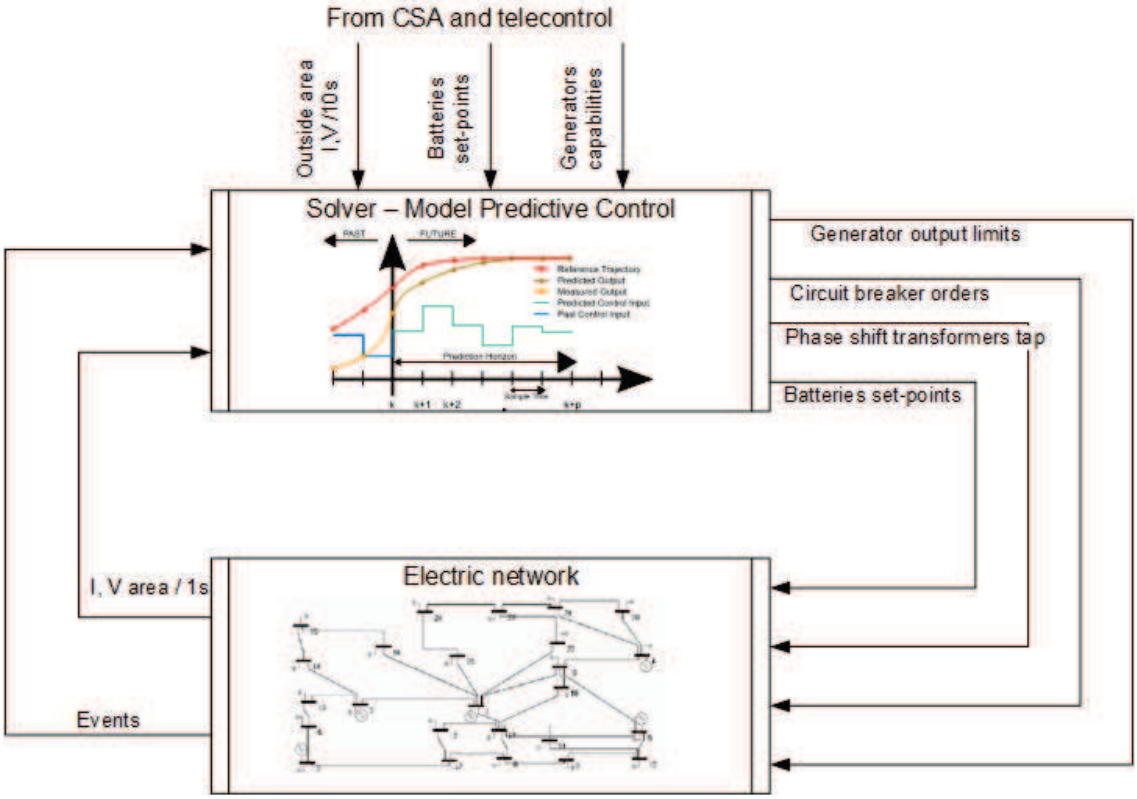
CSA
- Centralized Slow Automata
- Central vision to establish set-points in anticipation and global supply-demand balance
- Implemented in control center

ASA
- Area Slow Automata (an area can be reduced to a single substation)
- Area Automaton receiving set points from higher level for preventive actions and reacting on its own for curative actions using Model Predictive Control
- Distributed implementation – Middleware

SSFA
- Substation Slow Automata in addition to the ASA offer
- Substation Fast Automata : finite states and threshold levels, simple and robust to assure last resort equipment and persons protection
- Implemented in substations

In this use case, **we focus on ASA,** CSA is treated like an input.

The diagram below shows the overall system. Physical constraints (transit limits on the lines, batteries levels, total generation to be curtailed) are associated to the model. The cost function reflects the impact on the grid (deviation from planned transits and batteries set-points) and the cost of the levers (curtailed generation, battery use).

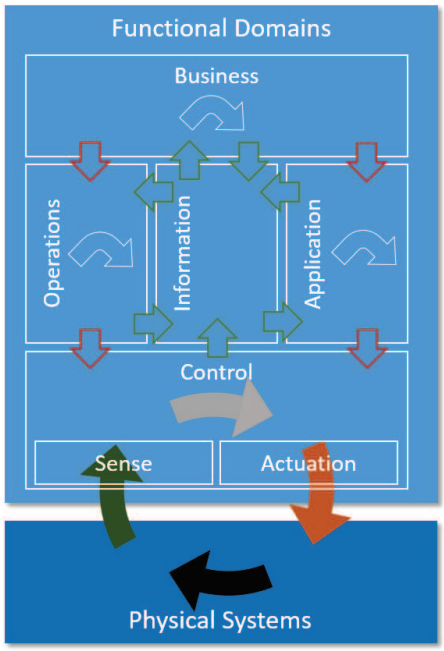


1.1.2 Main Features

We use the functional domains described in the "Industrial Internet of Things Volume G1: Reference Architecture"[1] to describe the area automatons main features.

Control domain

The system **acquires data** (getters) from the sensors (current and voltage transducers, position relays, weather sensors…) installed in the substations of the area. This function can include aggregation or basic combination of acquired data (e.g. turning high frequency Sample Values into RMS values). Rate of acquisition varies from 10s (actual sensors) to 1s or less.



It **writes data** to actuators (setters): Open/close orders to circuit breakers or isolators, set-points to batteries, generation limit value to generators…

It allows **communication** between all these elements (sensors, actuators, gateways, computation units), located in several distant locations. This layer also provides **entity abstraction** so every element of the system can be accessed in a standard way, whatever protocol it uses (IEC 61850, 60850-6-104, Modbus, OPC-UA, ICCP…).

Modelling gives meaning to the retrieved information. It associates a value with a part of the electrical network, i.e. a sensor value to the voltage of the X bus in the Y substation. It maps the data from sensors or actuators to the network model provided to the system (IIDM - iTesla Internal Data Model from the POWSYBL project[2]).

Asset management function includes:

- on boarding (if possible auto discovery) of new components (nodes, gateways),
- basic surveillance of components (NOK/OK), updates of configuration, policy, system or software/firmware updates,
- dynamic resources allocation (for availability or performance issues).

Executor implements the control logic given the states, conditions and behaviour of the system under control and its environment. It relies on Model Predictive Control with a solver that optimize a cost function to use levers such as batteries set-points, generation limit values, … Simple flow charts enforce safety rules in case no solution is found or computation takes too long. For example, they may result in curtailing all necessary generation.

Operations domain

These functions are common to all, or at least several areas that implement automata.

Provisioning and deployment allows to on-board, configure and register assets from a central operation room at scale, for example upgrading all devices from an area at the same time.

Modification of control logic in executor, for example by implementing a new code for optimization, is part of **managements** function.

Monitoring and diagnostics combine:

- Detection of real-time problems by collecting assets health data,
- Advanced diagnosis of the root cause of this problem,

---

[1] https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

[2] *Powsybl (Power system blocks) is an open source framework written in Java that makes it easy to write complex software for power systems' simulations and analysis. Its modular approach allows developers to extend or customize its features.*

Powsybl is part of the LF Energy Foundation, a project of The Linux Foundation that supports open source innovation projects within the energy and electricity sectors. Powsybl in an open source framework licensed under the Mozilla Public License 2.0.

- Alert on abnormal conditions.

Optimization is in charge of global optimization of resources devoted to the different automata, to improve reliability and efficiency.

Information domain

Data from the sensors is sent to the control centre level, possibly after filtering. It may be used by Centralized Slow Automata or other applications. It is also stored in a datalake for subsequent analysis.

Specifically, orders sent to generators and batteries are sent to the back-office for settlement purposes. State of each automaton is also sent to telecontrol system.

All events are available in an execution log for feedback and troubleshooting analysis.

Application domain

Logic and rules are part of the Centralized Slow Automata. They won't be described here, but an example is the batteries pre-calculated program, which is built in application domain by CSA and sent to ASA to be applied by control domain. Weather forecast or any useful data are also transmitted to control domain.

UI shows to control room operator the state of automata APIs, the values measured by sensors and the set-points or limits sent to batteries and generators. Operators can also put in or out of operation a specific automaton. Another UI allows specialists to change the logic of the automata and to deploy it by invoking management function from the operations domain.

API with SCADA system will also be considered in the future.

1.1.3 Limits

The functions of the automata are distributed between several components (from a hardware and software point of view) so it maximizes its capacity to operate under severe conditions (software or hardware breakdowns, communication failure…).

Maximum reliability is expected for control domain functions that must be able to operate even if other functions are unavailable.

Typical application needs a maximum delay between data acquisition and order around 10s, but shorter operation times will be sought.

Coupling with other applications should be loose, so RESTful implementation is preferred.

Fan-less hardware is favoured for use in the substations, with an extended temperature range of operation.

Linux OS is required and the use of a secured CentOS (7.4 in the 14/10/2019) is mandatory.

Java or C++ are currently in use in RTE development teams. Open Source code is mandatory.

Communication protocols common in the electric utility are used at the interfaces: IEC 60870-5-104, 61850, ICCP. Bandwidth between substations can be limited to 500kb/s, so communication sobriety is a plus.

Due to the criticality of the application, security should meet the highest standards. Whenever decided by cybersecurity team, security patches have to be applied.

1.1.4 Conclusions

This automaton focus must first of all be security of operation, with means it should not send **unwanted** commands. By adopting a decentralized or distributed architecture, we aim to boost its **dependability**, ie its ability to issue valid commands, even in non-nominal conditions.

1.2 REQUIREMENTS

This section contains Use Case requirements at a level of detail sufficient to enable CPS4EU designers to design components and pre-integrated architectures to satisfy those requirements, and testers to test that the system satisfies those requirements.

Throughout this section, every stated requirement will be externally perceivable by users, operators, or other external systems.

Important note: In the following requirements, the MPC optimizer is considered with a black box approach: it receives inputs and generates commands. The inner parameters of the MPC are not discussed in this document as many parameters are still under evaluation (for example cost of energy curtailment, cost of using downgraded network topologies).

1.2.1 Functional Requirements

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Functional Requirement	**UC9-FNC-01**	General network situation acquisition	When the middleware receives a new network situation, calculators shall update their databases	High	General use case description
Functional Requirement	**UC9-FNC-02**	Batteries set points acquisition	When the middleware receives a new battery set-point, calculators shall update their databases	High	General use case description
Functional Requirement	**UC9-FNC-03**	Generation forecast acquisition	When the middleware receives a new generation forecast, calculators shall update their databases	Medium	General use case description
Functional Requirement	**UC9-FNC-04**	Area network datapoints acquisition	When the middleware receives a new datapoint from interfaces, calculators shall update their databases	High	General use case description
Functional Requirement	**UC9-FNC-05**	Area events topological events acquisition	When the middleware receives a new topological event from interfaces from interfaces, calculators shall update their databases	High	General use case description
Functional Requirement	**UC9-FNC-06**	Levers setpoints calculation	Every 5 seconds, calculators shall determine new setpoints for all levers (topological orders, modulation orders, batteries setpoints).	High	General use case description
Functional Requirement	**UC9-FNC-07**	Levers setpoints consensus	After levers setpoints calculation, calculators shall determine common levers by using consensus mechanism.	Medium	General use case description
Functional Requirement	**UC9-FNC-08**	Batteries setpoint sending	Every 5 seconds, calculators shall send batteries setpoints to middleware.	Medium	General use case description
Functional Requirement	**UC9-FNC-09**	Topological orders sending	Every 5 seconds, if calculator elaborates a topological order, calculators shall send it to middleware.	High	General use case description
Functional Requirement	**UC9-FNC-10**	Modulation orders sending	Every 5 seconds, calculators shall send modulation orders to middleware.	Medium	General use case description
Functional Requirement	**UC9-FNC-11**	No new upper level data	if no data is received from upper level (UC9-FNC-01, UC9-FNC-02, UC9-FNC-03) then send a warning message "no data from CSA" to other calculators and upper level.	High	General use case description
Functional Requirement	**UC9-FNC-12**	No result from calculation	If no result can be calculated (UC9-FNC-06) then send warning message "no solution found" to upper level and launch back up algorithm after 60s.	High	General use case description

Functional Requirement	**UC9-FNC-13**	No consensus on levers setpoints	If no consensus is achieved between calculators (UC9-FNC-06) then send warning message "Consensus failed" to upper level and launch back-up algorithm OR launch calculation UC9-FNC-07 (to be studied under WP4)	High	General use case description

Table 1 – UC10 Functional Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Functional Requirement	**UC9-FNC-01**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-02**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-03**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-04**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-05**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-06**										MPC module development
Functional Requirement	**UC9-FNC-07**								Consensus mechanism	Collaborative PIARCH ?	
Functional Requirement	**UC9-FNC-08**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-09**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-10**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-11**									Collaborative PIARCH ?	If not RTE NAZA framework
Functional Requirement	**UC9-FNC-12**								Failure modes	Collaborative PIARCH ?	
Functional Requirement	**UC9-FNC-13**								Failure modes	Collaborative PIARCH ?	

Table 2 – UC10 Functional Requirements interrelations with Modules & Pre-integrated Architectures

1.2.2 Interface Requirements

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Interface Requirement	UC9-INT-01	Centralized Slow Automata Interface	Middleware shall use REST API to exchange with CSA.	High	RTE telecontrol architecture
Interface Requirement	UC9-INT-02	SCADA Interface	Middleware shall communicate with OPC-UA SCADA Gateway	High	RTE telecontrol architecture
Interface Requirement	UC9-INT-03	Interface sensors Interface	Middleware shall communicate with IEC 61850 sensors	High	NAZA project
Interface Requirement	UC9-INT-04	Topological event Interface	Middleware shall communicate with IEC 60870-5-104 Remote Transmission Units	High	RTE telecontrol architecture
Interface Requirement	UC9-INT-05	Topological orders Interface	Middleware shall communicate with OPC-UA SCADA Gateway	High	RTE telecontrol architecture
Interface Requirement	UC9-INT-06	Batteries set points Interface	Middleware shall communicate with Battery Management System with IEC 60870-5-104	High	Battery (RINGO) project
Interface Requirement	UC9-INT-07	Generation Modulation Interface	Middleware shall communicate with OPC-UA Generators and Distribution System Operators Gateways (may evolve in next version)	High	NAZA project
Interface Requirement	UC9-INT-08	Communications	All communications are on a private IP MPLS Wide Area Network. Bandwith between calculators should be limited to 500 kb/s.	Medium	RTE telecontrol architecture
Interface Requirement	UC9-INT-09	Language	Java or C++ shall be used.	High	
Interface Requirement	UC9-INT-10	Architecture	Implementation should be RESTful.	Medium	

Table 3 – UC10 Interface Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Interface Requirement	UC9-INT-01								'Collaborative 'Middleware	Collaborative PIARCH ?	RTE NAZA framework
Interface Requirement	UC9-INT-02								'Collaborative 'Middleware	Collaborative PIARCH ?	OPC UA SDK for Java (ProsysOPC)
Interface Requirement	UC9-INT-03								'Collaborative 'Middleware	Collaborative PIARCH ?	OpenMUC framework
Interface Requirement	UC9-INT-04								'Collaborative 'Middleware	Collaborative PIARCH ?	OpenMUC framework

Interface Requirement	UC9-INT-05								'Collaborative 'Middleware	Collaborative PIARCH ?	OPC UA SDK for Java (ProsysOPC)
Interface Requirement	UC9-INT-06								'Collaborative 'Middleware	Collaborative PIARCH ?	OPC UA SDK for Java (ProsysOPC)
Interface Requirement	UC9-INT-07								'Collaborative 'Middleware	Collaborative PIARCH ?	OPC UA SDK for Java (ProsysOPC)
Interface Requirement	UC9-INT-08										
Interface Requirement	UC9-INT-09										
Interface Requirement	UC9-INT-10										

Table 4 – UC10 Interfaces Requirements interrelations with Modules & Pre-integrated Architectures

1.2.3 Performance Requirements

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Performance Requirement	UC9-PRF-01	Levers setpoints calculation	Calculation shall occur in less than 2s	High	NAZA project
Performance Requirement	UC9-PRF-02	Levers setpoints consensus	Consensus shall occur in less than 2s after calculation is available	High	NAZA project

Table 5 – UC10 Performance Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Performance Requirement	UC9-PRF-01										MPC module development
Performance Requirement	UC9-PRF-02								Consensus mechanism	Collaborative PIARCH ?	

Table 6 – UC10 Performance Requirements interrelations with Modules & Pre-integrated Architectures

1.2.4 Security Requirements

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Security Requirement	UC9-SEC-01	Operating system	Use of a secured Linux CentOS (7.4) is mandatory.	High	RTE Cybersecurity rules
Security Requirement	UC9-SEC-02	Idenfication	The use of RTE inudstrial Active Directory is mandatory.	High	RTE Cybersecurity rules
Security Requirement	UC9-SEC-03	Event log	A log shall trace all events linked to identification, access control, resource access and operation.	High	RTE Cybersecurity rules

Table 7 – UC10 Security Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Security Requirement	UC9-SEC-01										RTE framework
Security Requirement	UC9-SEC-02										RTE framework
Security Requirement	UC9-SEC-03										RTE framework

Table 8 – UC10 Security Requirements interrelations with Modules & Pre-integrated Architectures

1.2.5 Operational Requirements

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Operational Requirement	**UC9-OPR-01**	Monitoring	Health of components, firmware or software version should retrieved automatically.	Medium	
Operational Requirement	**UC9-OPR-02**	Advanced monitoring	The system may send an alert to CSA if in abnormal operation conditions and provide an advanced diagnosis based on individual logs.	Low	
Operational Requirement	**UC9-OPR-03**	Remote provisionning	New sensors shall be configured remotely from central control room	High	
Operational Requirement	**UC9-OPR-04**	Remote modelling modification	Control room operator should be able to remotely modify the modelling (configuration) data, for example in case of modification in the substation.	Medium	
Operational Requirement	**UC9-OPR-05**	Remote code management	Control room operator should be able to install remotely a new version of the software on all concerned calculators.	Medium	
Operational Requirement	**UC9-OPR-06**	Maintenance mode	When a substation or part of substation under the supervision of the area automata is in maintenance, data from these sensors shall be ignored or replaced by estimated data.	High	
Operational Requirement	**UC9-OPR-07**	Advanced monitoring	The system should send an alert to CSA if in abnormal operation conditions and provide an advanced diagnosis based on individual logs.	Medium	
Operational Requirement	**UC9-OPR-08**	Auto discovery	New sensors may be automatically detected by the application	Low	
Operational Requirement	**UC9-OPR-09**	Dynamic ressources allocation	Material resources (CPU, bandwidth,, …) may be re-allocated dynamically to enhance performance or availability	Low	

Table 9 – UC10 Operational Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Operational Requirement	**UC9-OPR-01**	Monitoring								Collaborative PIARCH ?	
Operational Requirement	**UC9-OPR-02**	Advanced monitoring								Collaborative PIARCH ?	
Operational Requirement	**UC9-OPR-03**	Remote provisionning								Collaborative PIARCH ?	

Operational Requirement	**UC9-OPR-04**	Remote modelling modification									RTE framework
Operational Requirement	**UC9-OPR-05**	Remote code management									RTE framework
Operational Requirement	**UC9-OPR-06**	Maintenance mode									RTE framework
Operational Requirement	**UC9-OPR-07**	Advanced monitoring									RTE framework
Operational Requirement	**UC9-OPR-08**	Auto discovery							X		
Operational Requirement	**UC9-OPR-09**	Dynamic ressources allocation							X	Collaborative PIARCH ?	

Table 10 – UC10 Operational Requirements interrelations with Modules & Pre-integrated Architectures

1.2.6 Usability Requirements

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Usability Requirement	**UC9-USB-01**	Compact interface	Human Machine Interface shall contain all information in synthetic form on only one screen.	High	
Usability Requirement	**UC9-USB-02**	Internationalization	All Human Machine Interface should support different languages	Low	

Table 11 – UC10 Usability Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Usability Requirement	**UC9-USB-01**										RTE framework
Usability Requirement	**UC9-USB-02**										RTE framework

Table 12 – UC10 Usability Requirements interrelations with Modules & Pre-integrated Architectures

1.2.7 Policies & Compliance Requirements

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Policies&Compliance Requirement	**UC9-P&C-01**	French "Loi de programmation militaire"	Specific security rules apply to operators of essential services.	High	Loi n°2013-1168 article 22
Policies&Compliance Requirement	**UC9-P&C-02**	European NIS Directive	The NIS Directive provides legal measures to boost the overall level of cybersecurity operators of essential services.	High	Directive 2016/1148
Policies&Compliance Requirement	**UC9-P&C-03**	Open Source Software	Software developed by RTE should be Open Source if of interest for the Energy Community.	Medium	Linux Energy Foundation
Policies&Compliance Requirement	**UC9-P&C-04**	Arrêté Technique du 17 mai 2001	Minimum distance between active conductors and ground or installation.	High	ECOI0100130A

Table 13 – UC10 Policies & Compliance Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Policies&Compliance Requirement	**UC9-P&C-01**										RTE framework
Policies&Compliance Requirement	**UC9-P&C-02**										RTE framework
Policies&Compliance Requirement	**UC9-P&C-03**										RTE framework
Policies&Compliance Requirement	**UC9-P&C-04**										RTE framework

Table 14 – UC10 Policies & Compliance Requirements interrelations with Modules & Pre-integrated Architectures

1.2.8 Design Constraints

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Design Constraints	UC9-DSG-01	Hardware	Calculators and sensors gateway shall run on Intel power servers.	High	
Design Constraints	UC9-DSG-02	Substation environnement - Temperature	The operating range of the calculators shall be -10°C + 55°C. It could be restrained to 0°C -40°C if needed.	High	IEC 61850-3
Design Constraints	UC9-DSG-03	Availability	System shall be available at 99.99% of operation time	High	
Design Constraints	UC9-DSG-04	Dependability	No more than one unwanted order shall be sent every 10 years.	High	10 times less than teleprotection

Table 15 – UC10 Design Constraints Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Design Constraints	UC9-DSG-01										RTE infrastructure
Design Constraints	UC9-DSG-02										RTE infrastructure
Design Constraints	UC9-DSG-03										Global
Design Constraints	UC9-DSG-04										Global

Table 16 – UC10 Design Constraints Requirements interrelations with Modules & Pre-integrated Architectures

1.2.9 Ethical Requirements

Requirement Type	Requirement ID *(calculated)*	Short Description	Description	Priority (H/M/L)	Source
Ethical Requirements	**UC9-ETH-01**	Data protection	No personnal data shall be processed by the system. Commercially sensible data, such as load for consumers or production from generator shouldn't be store longer than required to achieve the system proper operation.	High	
Ethical Requirements	**UC9-ETH-02**	Liability	All system operation shall be explainable, ie curtailed generator should have, if asked, all information on why he was curtailed.	High	
Ethical Requirements	**UC9-ETH-03**	Global reliability	Global reliability of the system shall be assessed on a yearly basis to check if the requirements are reached and if not take corrective action.	Medium	

Table 17 – UC10 Ethical Requirements Description

Requirement Type	Requirement ID *(calculated)*	Computing			Connectivity		Sensing		Collaborative	CPS Tools	Non-CPS4EU module / tech
		HP Embedded Computing	AI Computing	Vision Computing	Connectivity (V2X, M2M)	Cyber Security	Ultra precise localisation system	Perception and interpretation of environment	Cooperative algorithms		
Ethical Requirements	**UC9-ETH-01**										
Ethical Requirements	**UC9-ETH-02**										
Ethical Requirements	**UC9-ETH-03**										

Table 18 – UC10 Ethical Requirements interrelations with Modules & Pre-integrated Architectures

2 REQUIREMENTS GATHERING METHODOLOGY

This section reports the methodology adopted in task 9.1 to define the requirements related to the CPS4EU Energy use cases. In the following paragraphs the type of requirements, the adopted notation and the requirement code conventions are described.

Requirements play major roles as they:

- Form the basis of system architecture and design activities
- Form the basis of system integration and verification activities
- Act as reference for validation and stakeholder acceptance
- Provide a means of communication between the various technical staff that interact throughout the project.

2.1.1 Requirements Types

According to the IEEE Standard Glossary of Software Engineering Terminology[3], a requirement is:

- A condition or capability needed by a user to solve a problem or achieve an objective
- A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents
- A documented representation of a condition or capability as in (1) or (2).

CPS4EU Energy and SME (WP9) Use Case requirements are classified into the following types:

Functional Requirement	A requirement that specifies a function that a system, or system component, must be able to perform. A requirement specifying **what** the overall system, or a specific component, will be able to do. Statements of services that the system should provide, how the system should react to particular inputs and how the system should behave in particular situations. Among the functional requirements are also included security requirements relating to the security services offered by the system to users or other systems.
Non Functional Requirement	A requirement specifying **how** the system or component will implement its functionality. In this document the following non-functional types of requirements are considered: • Interface Requirements • Performance Requirements • Security Requirements • Operational Requirements • Usability Requirements • Policies & Compliance Requirements • Design Constraints • Ethical Requirements • Other Requirements.

The following table describe each requirement type:

[3] *https://ieeexplore.ieee.org/document/159342/definitions#definitions*

Requirement Type	Req.ID	Requirement Description
Functional Requirement	**FNC**	Functional Requirements describe the behaviour and information that the solution will manage. In the case of a non-system solution, the behaviour typically refers to a workflow and the information refers to the inputs and outputs of the workflow. Additionally, the requirements describe how the data will be transformed and by whom. In the case of a system solution, the functional requirements describe the features and functionality of the system as well as the information that will be created, edited, updated, and deleted by the system.
Interface Requirement	**INT**	Interface requirements define how the system is required to interact or to exchange information with external systems (external interface), or how system elements within the system interact with each other (internal interface). Interface requirements include physical connections (physical interfaces) with external systems or internal system elements supporting interactions or exchanges. External interface requirements are important for embedded systems and outline how your product will interface with other components. There are several types of interfaces you may have requirements for, including: • Hardware: Describe the logical and physical characteristics of each interface between the software product and the hardware components of the system. • Software: Describe the connections between this product and other specific software components (name and version), including databases, operating systems, tools, libraries, and integrated commercial components. Identify data that will be shared across software components. • Communications: Describe the requirements associated with any communications functions required by this product, including e-mail, web browser, network server communications protocols, electronic forms, and so on. Identify any communication standards that will be used, such as FTP or HTTP. Specify any communication security or encryption issues, data transfer rates, and synchronization mechanisms.
Performance Requirement	**PRF**	If there are performance requirements for the Use Cases under various circumstances, state them here and explain their rationale, to help the developers understand the intent and make suitable design choices. Specify the timing relationships for real time systems. Performance requirements can refer to individual functional requirements or features (e.g. speed of response for a certain functionality).
Security Requirement	**SEC**	Security requirements are related to both the facility that houses the system(s) and the operational security requirements of the system itself. Specify the security and privacy requirements, including access limitations to the system, such as log-on procedures and passwords, and of data protection and recovery methods. This could include the factors that would protect the system from accidental or malicious access, use, modification, destruction, or disclosure. In safety-critical embedded systems this might incorporate a distributed log or history of data sets, the assignment of certain functions to different single systems, or the restriction of communications between some areas of the system. Examples:

		• Access requirements • Integrity requirements • Privacy requirements.
Operational Requirement	**OPR**	Examples: • Delivery mode • Access mode • Availability • Maintainability • Reliability • Capacity • Scalability • Portability • Installation.
Usability Requirement	**USB**	Examples: • Environment of use • Appearance and style • Ease of use • Internationalization • Accessibility.
Policies & Compliance Requirement	**P&C**	These requirements identify relevant and applicable organizational policies or regulatory requirements that could affect the operation or performance of the system(s). Examples: Laws and regulations, standards, business rules.
Design Constraint	**DSG**	Example: Environmental Requirements, which identify the environmental conditions to be encountered by the system in its different operational modes. This should address the natural environment (e.g. wind, rain, temperature, fauna, salt, dust, radiation, etc.), induced and/or self-induced environmental effects (e.g. motion, shock, noise, electromagnetism, thermal, etc.), and threats to societal environment (e.g. legal, political, economic, social, business, etc.).
Ethical Requirement	**P&E**	See §5.1 Ethics of CPS4EU proposal, with particular reference to the document "Ethical Aspects of Cyber-Physical Systems": http://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU%282016%29563501_EN.pdf
Other Requirements	**OTR**	Any other requirement that cannot be classified with the above categories.

2.1.2 Requirement Identification

The CPS4EU Use Case requirements will be uniquely identified by an alphanumeric code consisting of:

<*Use Case number*>-<*classification*>-<*number*>, where:

<Use Case ID>	**UC10**	Distributed controls for transmission network
<classification>	**FNC**	Functional Requirements
	INT	Interface Requirements
	PRF	Performance Requirements
	SEC	Security Requirements
	OPR	Operational Requirements
	USB	Usability Requirements
	P&C	Policies & Compliance Requirements
	DSG	Design Constraints

	ETH	Ethical Requirements
	OTR	Other Requirements
<number>	A progressive number that uniquely identifies the requirement within a requirement type.	

Example:
UC1-USB-01 → Use Case: UC1, Requirement type: Usability Requirement, Requirement number: 01

2.1.3 Requirement Principles

The following principles apply:

Characteristics	Specific requirements should comply with the following characteristics: • unambiguous • complete • consistent • ranked for importance and/or stability • verifiable • modifiable • traceable.
Cross-references	Specific requirements should be cross-referenced to earlier documents that they relate to.
Readability	Careful attention should be given to organizing the requirements to maximize readability.
IDs	All requirements should be uniquely identifiable (via ID).

Each requirement should also be **testable**.

2.1.4 Requirement Attributes

Each requirement will be classified according to the following ***Priority***:

Priority	***Feature***	***How to describe it***
High	A required, must have feature	The system **shall**…
Medium	A desired feature, but may be deferred till later	The system **should**…
Low	An optional, nice-to-have feature that may never make it to implementation	The system **may**…

The ***Source*** field identifies the origin of the requirement i.e. where/whom it comes from.

The ***Computing***, ***Connectivity***, ***Sensing***, ***Collaborative***, ***CPS Tools*** fields describe the relationship between the requirement and the WP1-WP6 module, i.e.

- If/how the requirement will have some impact on WP1-6 modules
- if the requirement foresees the usage of a WP1-6 module

If the requirement foresees a non-CPS4EU module or tech to be used, that is to be specified in the ***Non-CPS4EU module / tech*** field.

Project number: 826276

CPS4EU

Cyber Physical Systems for Europe

D9.1 – Use case 11
Software Defined Edge Control
Safety report for critical function

Reviewer (Carbonne –Schneider Electric France):

Dissemination level: Public

Version	Date	Author (name – company)	Comments
V.0.1	17/01/2020	PAPOZ – Schneider Electric France	
V.1.0	30/03/2020	G. GIRAUD – RTE	remarks from technical Committee

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Table of content

1. Reference 4
   1.1. Reference documents 4
   1.2. Acronyms 5
2. Introduction 6
   2.1. Background 6
   2.2. Purpose of the document 7
3. Methodology 8
4. Step 1: detailed system configuration 10
   4.1. Global sketch of SDEC implementation 10
   4.2. List of equipment used 11
   4.3. Focus on the Merging Unit 11
5. Step 2: detailed failure analysis 12
   5.1. Assumptions for the dependability study 12
   5.2. Failure Mode & Effects Analyses 13
      5.2.1. FMEA table template 13
      5.2.2. List of FMEAs established 14
      5.2.3. Titanium Edge FMEA 14
6. Step 3: SDEC fault tree analysis 17
   6.1. List of basic events used in the FTA 18
   6.2. FTA – UE1 (spurious trip of ANSI 21 – scenario 1) 20
      6.2.1. SDEC solution 20
      6.2.2. Easergy IED 20
   6.3. UE1 FTA - UE2 (loss of ANSI 21 – scenario 1)) 21
      6.3.1. SDEC solution 21
      6.3.2. Easergy IED 22
   6.4. Comments on models 22
7. Results of the dependability study 23
   7.1. Initial results analysis 23
   7.2. Sensitivity studies 23
      7.2.1. Impact of servers' reliability 24
      7.2.2. Impact of operation strategy 24
      7.2.3. Impact of proof tests interval 24
      7.2.4. Impact of (customer dependent) repair times 25
      7.2.5. Impact of Titanium architecture 25
      7.2.6. Impact of Software errors 26
         7.2.6.1. Context 26
         7.2.6.2. Preliminary warning 26
         7.2.6.3. "KerrNet-like" modelling 27
8. Conclusions 30
9. Appendix : electronics FMEA tables template 31

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

1. REFERENCE

1.1. Reference documents

Ref	Doc .Number	Title	Date / Rev	Source
[1]	NHA8953920	STB DI electronics scheme	rev02	Schneider Electric
[2]	NHA8954118	STB DO electronics scheme	rev00	Schneider Electric
[3]	QGH4421323	CEI61850 converter electronics scheme	rev01	Schneider Electric
[4]	NVE1285201	CEI61850 converter power supplies electronics scheme	rev02	Schneider Electric
[5]	NHA8954220	COM_TB module (STB controls) electronics scheme	rev03	Schneider Electric
[6]	MU_SB SCH	CT/VT module electronics scheme	rev01 sept.2015	Schneider Electric
[7]	DFMEA_FUSION_IED_V1	Easergy Fusion v1 protection relay detailed FMEA	A11	Schneider Electric
[8]	WRTSRAM	Titanium Server RAM Modeling Analysis	4.0 jan. 2015	KerrNet Consulting Inc
[9]	IEC 62380	Reliability data handbook for reliability prediction of electronics components, PCBs and equipment	August 2004	IEC
[10]	IMdR – GTR 63	« Démarche et méthodes de Sûreté de Fonctionnement des logiciels »	Ed.2 april 2013	**I**nstitut pour la **M**aîtrise **d**es **R**isques
[11]	ANSI C37.2-2008	IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations	3 October 2008	IEEE

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

1.2. Acronyms

Acronym	**Desription**
ADC	Analogue to digital converter
BoM	Bill of Materials
CPT	Compute
CPS	Compute server
CT	Current Transformer
CTL	Control
FMEA	Failure Modes & Effects Analysis
FPGA	Field Programmable Gate Array
GB	Ground Benign environment
HW	Hardware
IED	Intelligent Electronic Device = digital protection relay
MU	Merging Unit
POC	Proof Of Concept
RAM	Reliability Availability Maintainability
STB DI	Smart Terminal Block Digital Input
STB DO	Smart Terminal Block Digital Output
SW	Software
VT	Voltage Transformer
µP	Microprocessor

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

2. INTRODUCTION

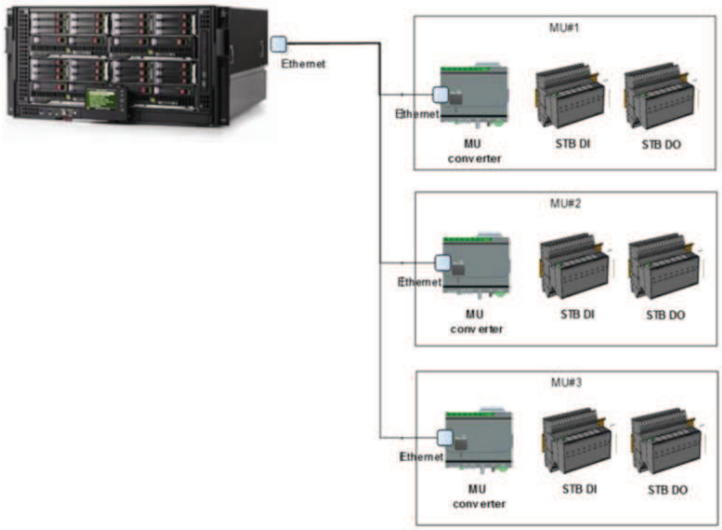
2.1. Background

In CPS4EU, WP9 addresses the other industry sector, more specifically Energy & Energy Networks. The protection relays are critical components to ensure assets and people safety. They are currently implemented in a dedicated equipment (IED) for each important asset (power line, transformer …). With the digitalization of substation automation and the emergence of edge computing, the substitution of the physical architecture of substation protection and automation equipment with a logical architecture of virtual machines seems to become a realistic target. This could lead to equipment minimization, easier hardware replacement and cost efficient use of standard hardware platform. It may also take benefit of the open software platform technology, derived from IT, to address new operation challenges, as cyber threats.

Demonstrating that traditional standalone industrial equipment can be replaced with edge-computing based systems without any loss of availability or safety could benefit to other industrial sectors in CPS4EU, which have the same high requirements.

A Proof Of Concept project is currently ongoing at Schneider Electric, based on virtualization technology.

This innovative approach, named Software Defined Edge Control, consists in replacing in the substation the classical protection relays (i.e. IEDs) by a new distributed solution, minimizing the complexity of the field equipment of an electrical substation, and relocating the complex treatments in servers at the Edge level.

Classical solution based on IEDs (at least one unit per HV circuit breaker)	**SDEC solution** (mutualized servers for the substation, intelligence at EDGE level)
	
Tens of IED in the substation	A few servers for the entire substation.

RTE is in partnership with Schneider Electric in the scope of this virtualization project.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

2.2. *Purpose of the document*

This document summarizes the methodology and the results of the preliminary dependability studies carried out on the SDEC solution.

Indeed, if the benefits of this solution consist in lower costs of acquisition and maintenance, and increased functional flexibility, this new technology raises several questions, and its acceptability partly relies on our capacity to make evidence that the related risks are under control.

These risks are addressed and evaluated through this dependability study, which aims at comparing a classical Easergy protection relay with the SDEC design, from an electrical protection perspective.

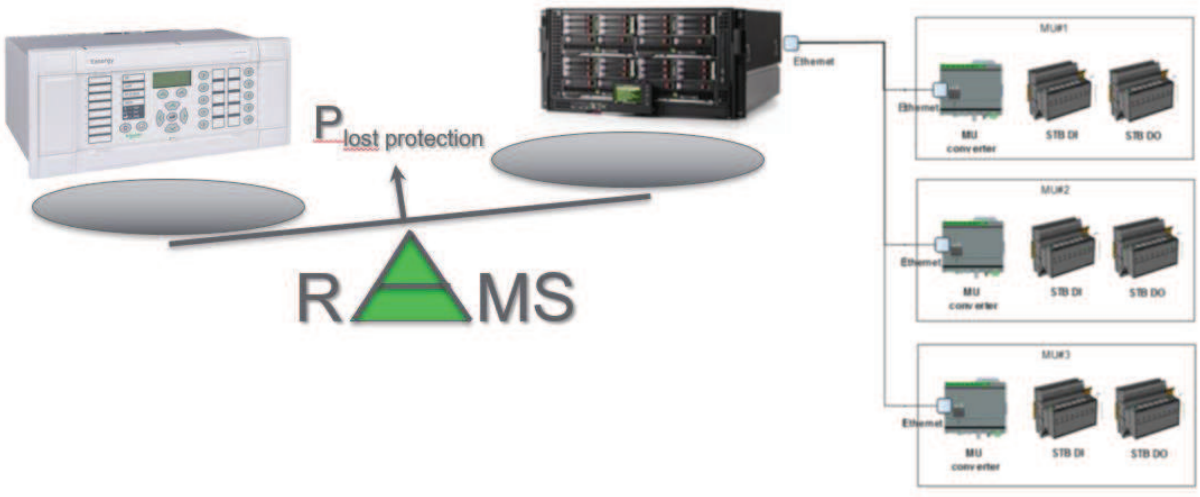
Two types of protection functions are considered here, based on RTE's priority needs:

- Distant protection ANSI21 [11], requiring both three-phase voltage and current measurements
- And the less complex overcurrent protection ANSI 50/51, current based

The dependability metrics studied are those reflecting the customer's questions:

- Distant protection ANSI21, requiring both three-phase voltage and current measurements
- *"how often will the protection trip unduly ?* ➔ this will be measured by the **frequency of spurious actuation** of the ANSI function
- *"what is risk that it does not trip with an electrical fault such as overcurrent ?"* ➔ this will be measured by the mean **unavailability** of the ANSI function ("masking" of the protection)

In the end, the study shall enable to **compare the risks** of spurious trip or loss of the protection function, for a single **Easergy relay vs the SDEC solution**:



Another benefit will be to understand the differences, identify the main contributors to the risks and possibly identify potential tracks of improvement.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

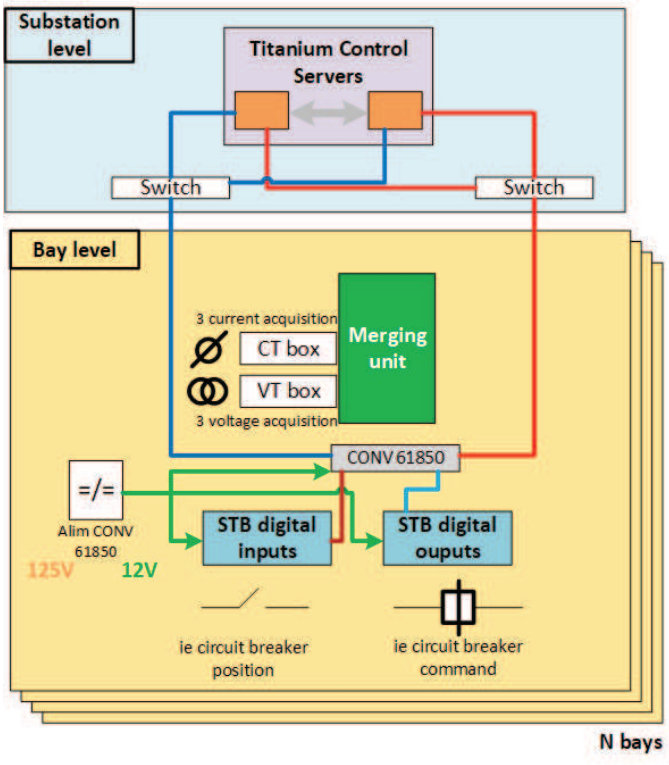
3. METHODOLOGY

The methodology used to perform this dependability analysis is very classic in RAM engineering.

It consists basically in 3 main steps listed below:

1. Gather the detailed documentation related to the POC RTE implementation

- Global sketch of the solution / equipment used
- BoM + detailed schematics of Schneider Electric electronics
  - **CT/VT boxes interfacing the current or voltage sensors**
  - **Merging Unit**
  - **STB DI used to collect status information or commands**
  - **STB DO connected to the breaker's tripping coil**
- Detailed description + RAM Analysis of the Titanium server (WindRiver)



2. Carry-out thorough RAM analyses on each part of the system

- Reliability predictions (generic IEC 62380 models [9] used as reference
- Electronic cards FMEA ➔ failure modes? effects? detection? possible mitigation mechanisms?
- Edge server system FMEA ➔ failure modes? effects? detection? reconfiguration?

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

3. Aggregate the results to build a RAM model for the global SDEC solution

- Model the complete loop from CT/VT boxes up to Titanium server, down to the circuit breaker tripping coil
- Electronic (Fspurious, Pmasking) calculation ➔ comparison with standard Easergy Fusion v1 protection relay
- Weaknesses identification ➔ possible improvements?

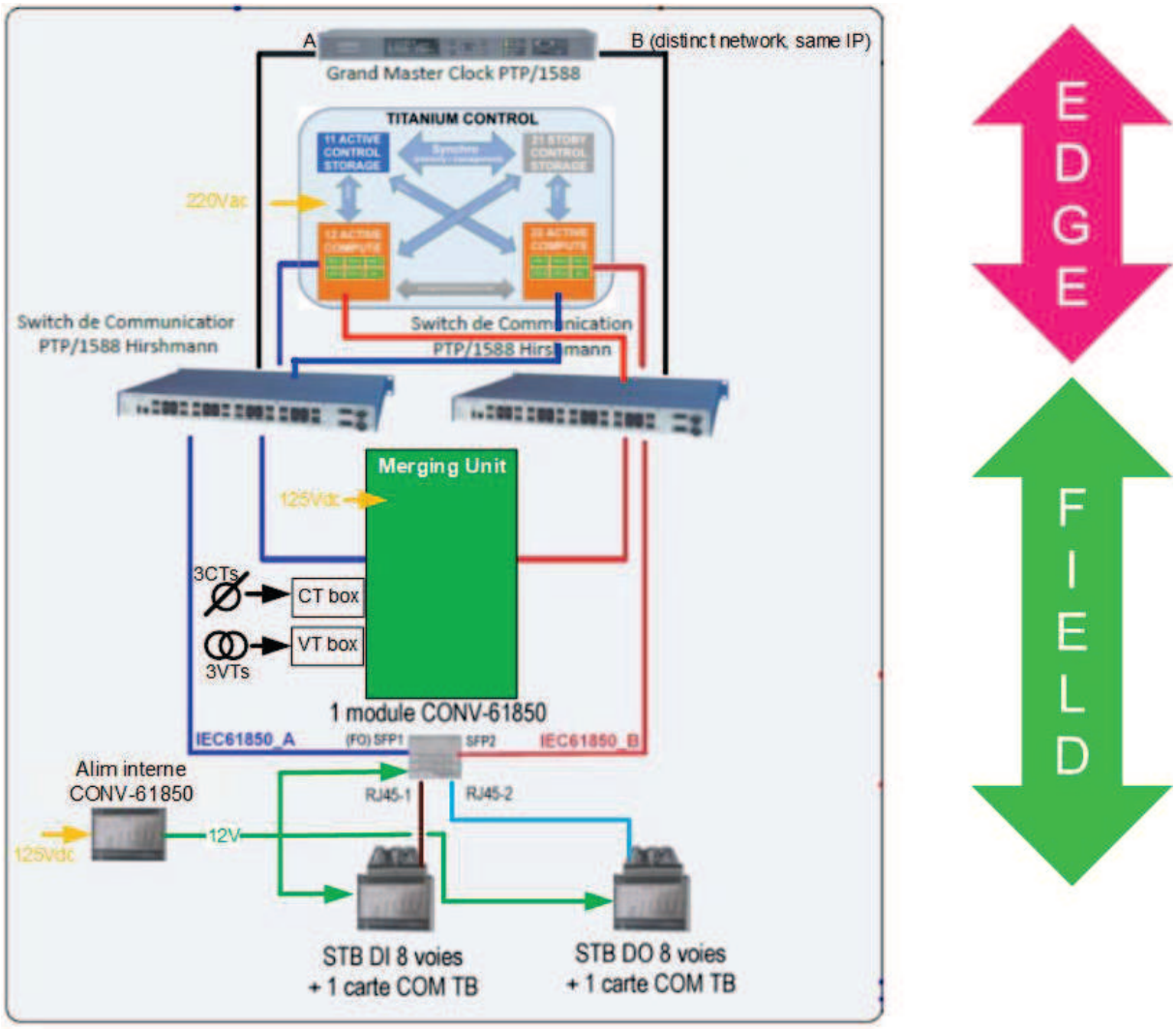
Each of the steps described above is detailed below in a specific section.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4. STEP 1: DETAILED SYSTEM CONFIGURATION

4.1. Global sketch of SDEC implementation

The SDEC solution, as implemented in the POC RTE, is described below:



This picture shows:

- The field equipment, enabling to
  - **send digital current and voltage samples to the Titanium located at the Edge level,**
  - **send digital status information to the Edge as well,**
  - **and receive commands from the Titanium, to actuate the field switchgear in return.**
- The fault tolerant architecture of the Titanium, with
  - **redundant compute servers hosting the virtual machines with their protection algorithms**
  - **redundant control servers ensuring failure detection, Titanium reconfiguration and context data storage.**

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

4.2. List of equipment used

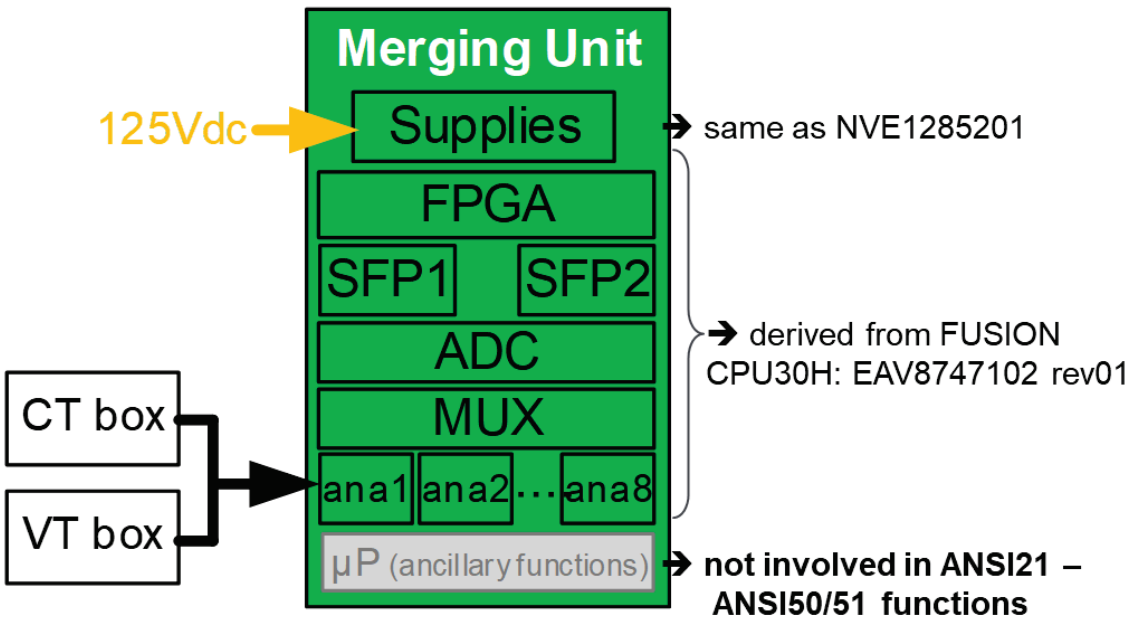
The BOM of the SDEC includes the following:

- STB DI: NHA8953920 rev02
- STB DO: NHA8954118 rev00
- Power supplies CEI61850 converter: NVE1285201 rev02
- Merging Unit power supplies: same as CEI61850 supplies
- CEI61850 converter: QGH4421323 rev01
- COM_TB module (for STB controls): NHA8954220 rev03
- CT/VT module: MU_SB SCH rev01 sept.15
- Titanium server: fault tolerant architecture, with 2 CPT servers + 2 CTL servers
- Communication switches A & B
- Grand Master Clock for synchronization
- Merging Unit

4.3. Focus on the Merging Unit

The Merging Unit currently equipping the POC is not the ultimate one.

The study will thus be based on the design which seems the most appropriate to us, based on the following approach:



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

The main idea behind that is to use the simplest possible design to ensure the tasks related to the protection functions, like merging unit, and let the more complex electronics perform elaborated, but less critical functions.

Hence, this Merging Unit uses:

- Classical analogue input stages, multiplexers, and ADC to perform the analogue to digital conversion
- A single FPGA to control both the analogue to digital conversion and the communication through redundant communication ports SFP1 and SFP2
- And a microprocessor, dedicated to enriched ancillary functions, but playing no role in the ANSI protection functions.

Every part of this Merging Unit is, in fact, a subassembly of the existing Easergy Fusion v1 protection relay. The MU study will thus be based on selected extracts of the Easergy schematics.

5. STEP 2: DETAILED FAILURE ANALYSIS

5.1. Assumptions for the dependability study

The dependability analysis is carried out based on the following assumptions, established with the SDEC project team:

- The mission time considered is 1 year: This is supposedly the interval of time between two periodic proof tests of the ANSIxx electrical protections
- The Merging Unit is built as described in section 4.3, and the µP embedded for advanced functions is not involved in the electrical protection functions
- The MU power supplies are assumed similar to the STB supplies (embedded in the CONV_61850 communication STB)
- The following configuration is considered for RTE use case:
  - **HV circuit breaker equipped with a single shunt opening release,**
  - **no DI is used for the electrical protections (the status of the switchgears is only used for automation functions and status display, not for ANSI21 nor ANSI50/51)**
- SDEC protections dependability is evaluated according to IEC 62380 electronics reliability models, and compared to Easergy Fusion v1 protection relay
- The dependability parameters are evaluated during the useful lifetime of the equipment, with constant failure rates
- Easergy Fusion v1 dependability metrics are evaluated by re-working the FUSION1 FMEAs (see [7]), according to the POC RTE implementation (no DI, one single shunt coil, …)
- In the RTE use case, only 3 CTs are used ➔ the zero-sequence current Io is calculated by summing the 3 phase currents, no dedicated sensor
- If a phase current measurement is lost, then Io = -I1 ➔ the phase to earth protection trips (its setting is generally << In)
- The synchronization by the Grand Master Clock is needed only for differential protections and for the synchro-check function ➔ its loss does not impact ANSI21 nor ANSI50/51 protections

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

- The ANSI21 function is assumed based on impedance measurement ➔ trips when the impedance Z becomes too low, with Z=U/I
- Some failures of electronics impact the gain of both voltage and current measurements ➔ one conservatively considers them as protection masking failures (UE2 “failure to trip” being the most critical event in RTE application)
- Failures causing a voltage signal Ui to be stuck at a DC supply are supposed to cause a spurious ANSI21 tripping
- 2 different scenarios are considered for the analysis:
    - **Scenario 1 : upon failure detection, only an alarm is raised, and the system does not trip the ANSIxx protection**
    - **Scenario 2 : upon failure detection of a non-redundant equipment, a trip command is sent to the breaker shunt coil (when possible)**
- The basic failure rate considered for any server in the Titanium is 2,63E-06h (based on the Tellcordia MTTF prediction sent by Dell : 380 442 h @30°C GB)
- The diagnostic coverage of any server in the Titanium is supposed equal to 99% (source : KerrNet RAM study [8])
- The remaining 1% of undetected failures of a server is assumed to be equally shared between safe and unsafe type ➔ 0,5% spurious actuation + 0,5% protection masking
- The Titanium reconfiguration upon failure detection is as described in the Titanium FMEA (see § 5.2.3)
- The deny of service is assumed to be 1% of the communication switches failures
- The assumed repair time following failure detection (RTE) is 2 days (48h)
- No common mode failure affects redundant equipment
- Human errors are not accounted for (most likely during servers operation / system maintenance)
- Possible troubles by an upgrade of the Operating System are not considered either.

5.2. Failure Mode & Effects Analyses

5.2.1. FMEA table template

As mentioned above, most of the FMEAs performed are related to electronic equipment.

These FMEAs are derived from those established in the scope of Easergy Fusion v1 development, see reference document [7].

So, the same basic FMEA template was used, with the addition of new columns specific to the POC RTE use case.

This FMEA template is shown in Appendix, for illustration purpose.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

5.2.2. List of FMEAs established

This section only lists the different FMEA tables established, and their size.

Almost 2000 lines of FMEA have been established / updated, which is the reason why these detailed documents are not included in this dependability report.

FMEA file	Size
STB DO FMEA	24 rows
CT/VT module FMEA	24 rows
Power supplies CEI61850 converter FMEA	100 rows
CEI61850 converter FMEA	112 rows
COM_TB module (STB controls) FMEA	97 rows
Merging Unit FMEA	813 rows
Titanium server FMEA	16 rows
FUSION FMEA	805 rows

***Notes** :*

1. *no FMEA has been carried out on the STB DI module, as no DI is used in our study case (distance & overcurrent protections only require analogue measurements)*
2. *no detailed FMEA has been made on the communication switches A & B either: their failures have been addressed in a worst-case approach, i.e. any failure is assumed to cause the complete loss of the switch.*

5.2.3. Titanium Edge FMEA

The Titanium has already been studied in a dedicated RAM study, see reference [8].

But this RAM study cannot be used straight away, as:

- The Titanium architecture studied is the common solution used by Telecommunication / Internet Service Providers, which differs from the simplified architecture used in the POC RTE
- The critical events studied in this RAM report do not include service outages lasting less than 10 seconds, which are acceptable in this kind of application.

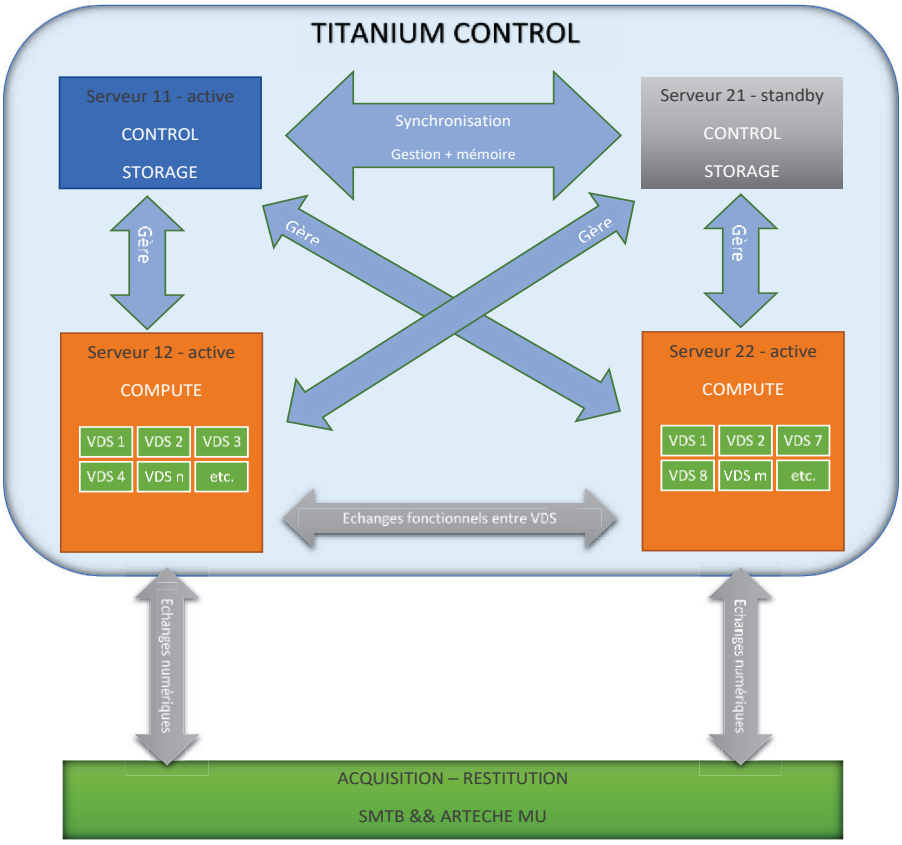
This RAM study is nevertheless useful to understand the respective role of each compute and control server.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

An FMEA was performed on the Titanium architecture used in the POC RTE, and is shown below as:

- The Titanium plays an important role in the execution of the studied ANSIxx protection functions
- And this FMEA is quite short, because the failure modes considered for each server are macroscopic.

The Titanium FMEA table



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

Equipment	Role	Failure modes	Effects		Détection	Comments
			Local	System		
Control server 11 (floating @ IP)	* monitors the status of compute servers 12 & 22 (heartbeat signal) * stores the context data enabling to transfer to control server 21 if needed * ...	complete server crash (power supplies lost, UC failure, ...)	loss of server 11	* compute servers 12 & 22 no more monitored by server 11 * server 21 automatically replaces server 11 * compute servers 12 & 22 managing ANSI protections are not affected	by server 21	* a control server failure cannot affect compute servers treatments * the server can be replaced in less than 3h (spare on site) * MTTR considered = 48h
		lost communication with one of the compute servers (e.g.server 12)	control server 11 communicates only with one of the compute servers (e.g. server 22)	* compute server 12 no more monitored by server 11 * server 21 replaced by server 11 * compute servers 12 & 22 not affected	by server 21	
		lost communication with control server 21	control server 11 only communicates with compute servers 12 & 22	* lost synchronisation between CTL servers * in case of server 11 loss, server 21 takes over without up to date context => possible malfunction of automation functions, but no impact on distance and overcurrent protections	by server 21	
		failure of remote maintenance port OAM	no effect	increased MTTR in case of failure	loss of communication	* this port enables a remote intervention in case of trouble * typical MTTF for a switch ~1E6h
Compute server 12	* receives in IEC 61850 protocole the analogue mesurements (U,I) and the status information (DI) sent by field equipment (MU + SMTB) * supports virtual machines ensuring ANSI protection functions * remotely controls via IEC 61850 links the switchgear manoeuvers (tripping on fault, opening/closing) * ...	server crash (power supplies, UC failure, ...)	loss of server 12 => automation & protection functions no more performed by this server	* server 22 not impacted, goes on ensuring these functions * failure detected by the control servers => alarm and server 12 replacement	active control server 11	* no impactthanks to compute server 22 redundancy * the server can be replaced in less than 3h (spare on site) * MTTR considered = 48h
		lost communication with active control server (e.g. server 11)	compute server 12 no more monitored by active control server 11, but still monitored by standby control server 21	* automatic switch from server 11 to server 21 * compute servers 12 & 22 not impacted	control server 11	
		lost communication with standby control server (e.g. server 21)	compute server 12 remains monitored by active control server 11, but no more by standby control server 22	* no effect on single fault * lost communication is detected by server 21 => alarm & replacement of faulty server 12 (or faulty communication card)	control server 21	
		lost communication with a switch (e.g. network A)	compute server 12 cannot communicate with the field on network A	* communication still valid through IEC 61508 network B => no impact at first fault * lost communication detected by server 12 => alarm, diagnostic, repair	server 12	PRP switch considered
		lostcommunication with compute server 22	compute server 12 cannot communicate with redundant compute server 22	* server 12 functions not impacted => no effect on single fault * lost communication detected by the server => alarm, diagnostic, repair	server 12	
		spurious tripping command to the circuit breaker	switch A receives an undue tripping command	spurious tripping of circuit breaker	no	* very unlikely (IEC 61850 protocole with CRC, etc) * STB_DO module does not check the consistency between switch A vs switch B messages * breaker tripping detected by breaker feedback signal
		lost tripping command to circuit breaker	VM error or HW failure preventing from sending a breaker tripping command	compute server 12 can still send commands through independent switch B, having its own medium (different commands on redundant networks)	no	very unlikely
		communication freezing communication networks A by deny of service	frozen communication network A	no impact on single fault : communication network B remains OK and enables to operate the system	lost of communication network A	very unlikely ; the virtual networks segregation (VLAN) reduces the risks of total network breakdown, with maximum allowable bandwidths for each VLAN.
Ultrafast infrastructure switch	used for VMs migration and backup actuation between compute servers	infrastructure port failure management + infra	lost infrastructure port	loss of VMs migration functions => above listed backups lost	lost of communication	ANSI functions can be affected by dual failure scenario
Grand Master Clock	used for servers synchronisation => critical for certain protectionfunctiond, if different SAMU are used	failure of GPS or lost communication with both switches	lost synchro	lost SOE consistancy.Protections using different Mus are lost	lost communication switches A & B	synchronises the MUs => causes the loss of differential & synchrocheck protections, but no impact on distant and overcurrent protections if a single MU is used

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

6. STEP 3: SDEC FAULT TREE ANALYSIS

Based on the analyses performed in the previous steps, a complete model can be elaborated for the SDEC solution, and for the Easergy relay as well.

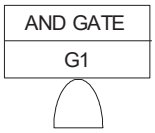
The models are based on the fault tree methodology, which enable:

- To take multiple failure scenarios into consideration (where FMEAs only address individual failures, one by one)
- An easy understanding of the combinations of failures leading to each critical event studied (eases the verification).

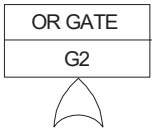
The FTA models are detailed in the following sections.

In order to keep this dependability report simple, only the fault trees related to the distant protection ANSI 21 are given. Those concerning the overcurrent protection function ANSI 50/51 are both simpler, and less critical.

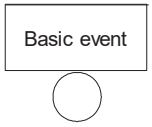
Reminder : Fault Tree Analysis symbols



This symbol represents an AND GATE. The output of this gate is true if all input events are true simultaneously. If all inputs are independents, then $P_{Gate} \approx \prod_i Pi$



This symbol represents an OR GATE. The output of this gate is TRUE if at least one input event is true.
$P_{Gate} \approx \sum_i Pi$



This symbol represents a BASIC EVENT that is the failure of a component with which a statistic law is associated. $P(t) = 1 - R(t) = 1 - e^{-\lambda t}$

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

6.1. List of basic events used in the FTA

Basic event	Definition
com12 A	failure of the communication port A of the server 12
com12 B	failure of the communication port B of the server 12
com22 A	failure of the communication port A of the server 22
com22 B	failure of the communication port B of the server 22
COM61850_DD	detected failure of the STB IEC 61850 communication module
comCPS12->11	loss of communication between servers 11 and 12
comCPS12->22	loss of communication between servers 12 and 22
COMTB_DD	dangerous detected failure of the STB communication module (protection masking)
COMTB_S	safe failure of the STB communication module (spurious trip)
CPS12_DD	dangerous detected failure of the compute server 12 (protection masking)
CPS12_DU	dangerous undetected failure of the compute server 12 (protection masking)
CPS12_SU	safe undetected failure of the compute server 12 (spurious trip)
CPS22_DD	dangerous detected failure of the compute server 22 (protection masking)
CPS22_DU	dangerous undetected failure of the compute server 22 (protection masking)
CPU30_21_DD	dangerous detected failure of Easergy CPU board (ANSI 21 masking)
CPU30_21_DU	dangerous undetected failure of Easergy CPU board (ANSI 21 masking)
CPU30_21_S	safe failure of Easergy CPU board (spurious trip ANSI 21)
crash-CTLS11	complete loss of control server 11
crash-CTLS21	complete loss of control server 21
CTbox1_21_DD	dangerous detected failure of the CT card channel 1 (ANSI 21 masking)
CTbox1_21_S	safe failure of the CT card channel 1 (ANSI 21 tripping)
CTbox2_21_DD	dangerous detected failure of the CT card channel 2 (ANSI 21 masking)
CTbox2_21_S	safe failure of the CT card channel 2 (ANSI 21 tripping)
CTbox3_21_DD	dangerous detected failure of the CT card channel 3 (ANSI 21 masking)
CTbox3_21_S	safe failure of the CT card channel 3 (ANSI 21 tripping)

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

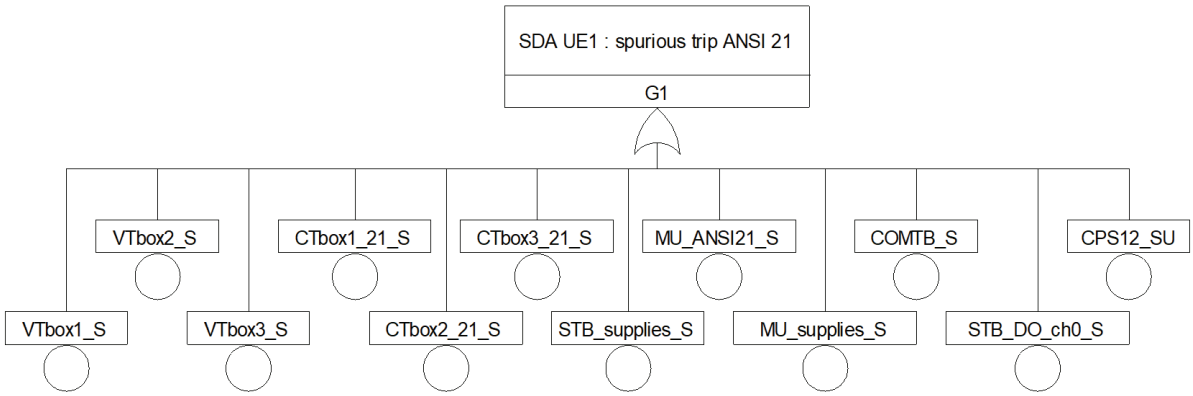
Basic event	Definition
DenSce12 A	failure of the communication port A of the server 12
DenSce12 B	failure of the communication port B of the server 12
DenSce22 A	failure of the communication port A of the server 22
DenSce22B	failure of the communication port B of the server 22
MU_ANSI21_DD	detected failure of the STB IEC 61850 communication module
MU_ANSI21_S	loss of communication between servers 11 and 12
MU_SFP1	loss of communication between servers 12 and 22
MU_SFP2	dangerous detected failure of the STB communication module (protection masking)
MU_supplies_DD	safe failure of the STB communication module (spurious trip)
MU_supplies_S	dangerous detected failure of the compute server 12 (protection masking)
PSU30H_DD	dangerous detected failure of Easergy power supplies (ANSI 21 masking)
PSU30H_DU	dangerous undetected failure of Easergy power supplies (ANSI 21 masking)
PSU30H_S	safe failure of Easergy power supplies (spurious trip ANSI 21)
STB_DO_ch0_DD	dangerous detected failure of STB DO channel 0 (ANSI 21 masking)
STB_DO_ch0_DU	dangerous undetected failure of STB DO channel 0 (ANSI 21 masking)
STB_DO_ch0_S	safe failure of STB DO channel 0 (spurious trip ANSI 21)
STB_supplies_DD	dangerous detected failure of STB power supplies (ANSI 21 masking)
STB_supplies_DU	dangerous undetected failure of STB power supplies (ANSI 21 masking)
STB_supplies_S	safe failure of STB power supplies (spurious trip ANSI 21)
switch A	loss of communication switch A
switch B	loss of communication switch B
switch-infrastr	loss of Titanium infrastructure switch
VTbox1_21_S	dangerous detected failure of the VT card channel 1 (ANSI 21 masking)
VTbox1_S	safe failure of the VT card channel 1 (ANSI 21 tripping)
VTbox2_21_S	dangerous detected failure of the VT card channel 2 (ANSI 21 masking)

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

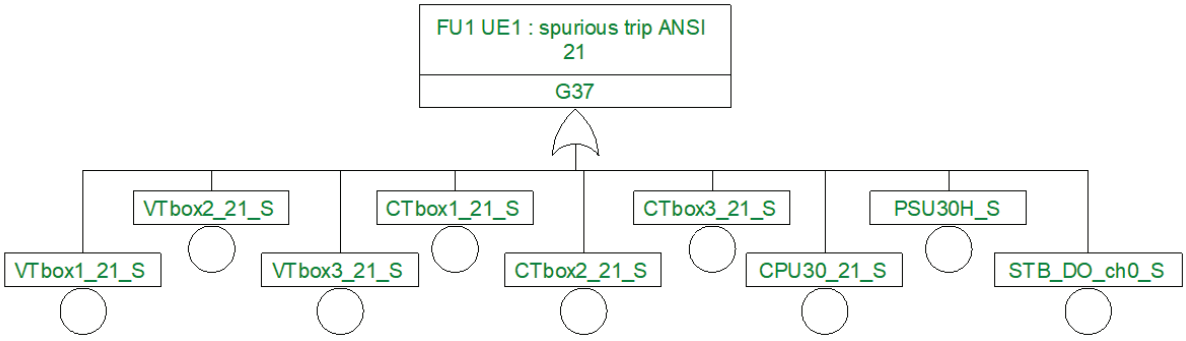
Basic event	Definition
VTbox2_S	safe failure of the VT card channel 2 (ANSI 21 tripping)
VTbox3_21_S	dangerous detected failure of the VT card channel 3 (ANSI 21 masking)
VTbox3_S	safe failure of the VT card channel 3 (ANSI 21 tripping)

6.2. FTA – UE1 (spurious trip of ANSI 21 – scenario 1)

6.2.1. SDEC solution



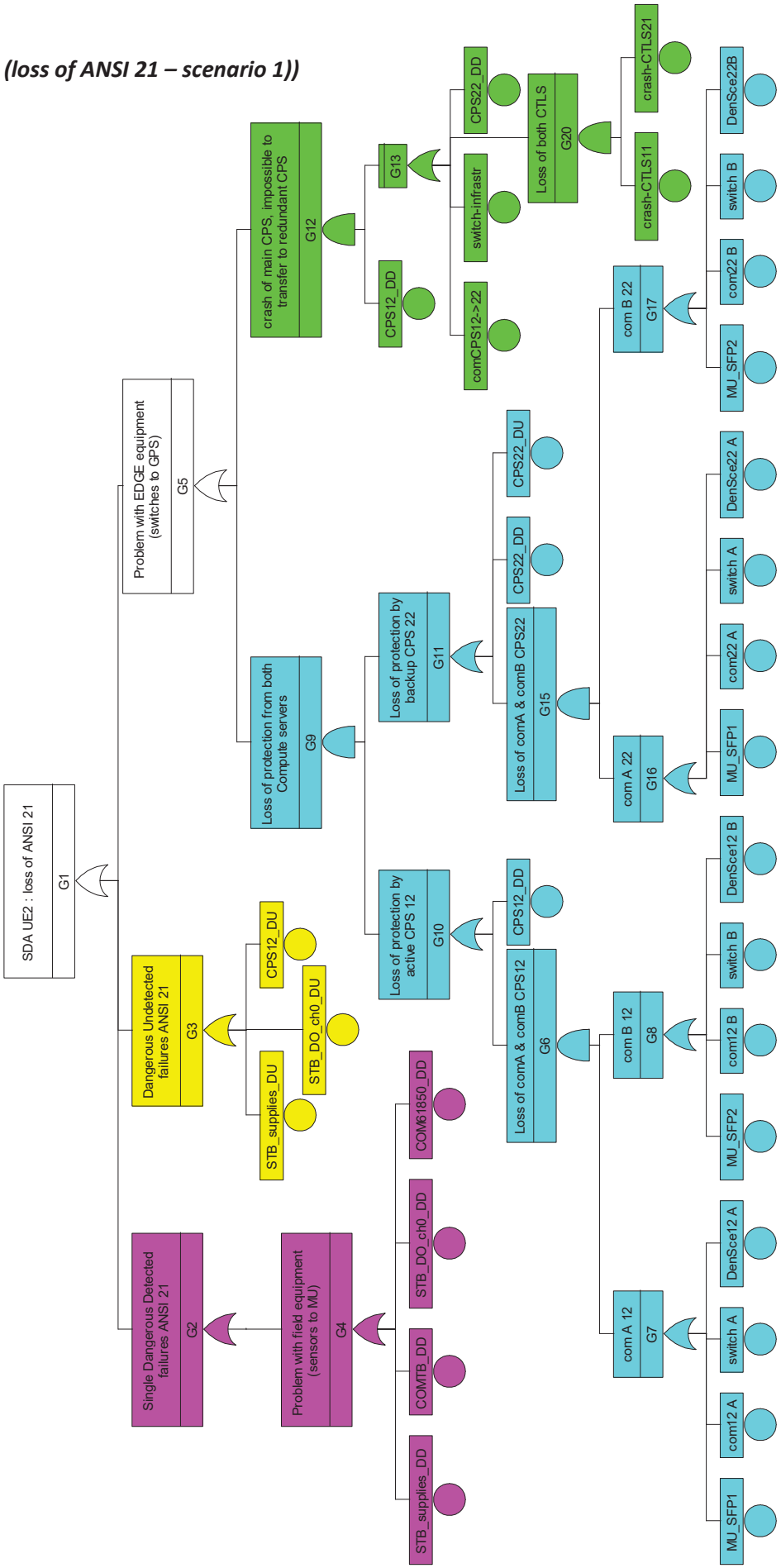
6.2.2. Easergy IED



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

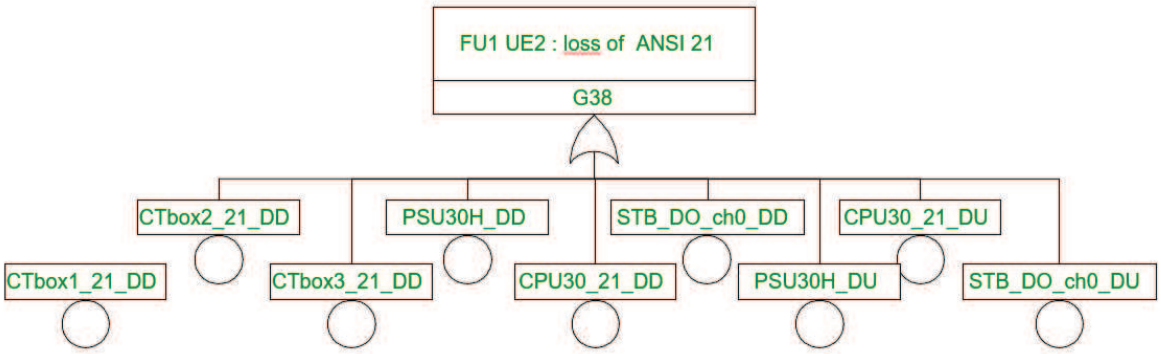
6.3. UE1 FTA - UE2 (loss of ANSI 21 – scenario 1))

6.3.1. SDEC solution



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

6.3.2. Easergy IED



6.4. Comments on models

Regarding the spurious activation, we can see that models for SDEC and Easergy are quite similar, SDEC having a few more components. So any significant difference between their behaviors should come from important differences in “safe” failures probability of single components.

Concerning the availability of the function, the situation is quite different. Easergy IED relies mostly on each component availability, while SDEC has much more redundancies mechanisms in place.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

7. RESULTS OF THE DEPENDABILITY STUDY

7.1. Initial results analysis

The results of the dependability study, under the assumptions listed above and for the scenario 1, are the following:

Scenario 1 (DD faillures => alarm)	unavailability* of ANSI 50/51	F (spurious** actuation of ANSI 50/51) /h	unavailability* of ANSI 21	F (spurious** actuation of ANSI 21) /h
SDEC	1,75E-04	3,00E-07	1,83E-04	3,23E-07
Easergy	1,13E-03	3,85E-07	8,76E-04	3,85E-07

* Unavailability is expressed in % of total time

** Spurious frequency is expressed in number of spurious activation per hour

These results deserve the following comments:

- The mean unavailability of the distant protection ANSI21 is around 1h 36mn per year for SDEC solution. So, the probability of correct behavior of this protection at any time is almost 99,99%
- The two solutions lead to very close frequencies of spurious trips: the gap between them is quite negligible
- The virtualized SDEC solution is almost 5 times more available than the Easergy Fusion1, evaluated on the same reliability predictive models
- This difference can be explained as follows: despite its increased complexity, the SDEC solution is more fault tolerant than the “all in one” protection relay. In particular, Easergy’s single and reliable µP performing the protection calculations is replaced by less reliable, more complex but redundant and replaceable compute servers.
- It is a good engineering practice to secure these preliminary conclusions through sensitivity studies, evaluating the impact of critical parameters changes. This is the aim of the next section.

7.2. Sensitivity studies

The sensitivity studies presented below aim at checking the influence of possible deviations in our assumption, and make sure that the hierarchy between the two solutions is not changed.

In order to keep the report concise, the results are presented only for the most critical and complex ANSI 21 function. Only one parameter is changed at a time in the FTA models.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

7.2.1. Impact of servers' reliability

The table below sums up the effects of changes in the servers MTTF:

	λ_{server} Dell 2,63E-6/h	λ_{server} x2	λ_{server} x3	λ_{server} x5
SDEC: unavailability of ANSI 21	1,83E-04	2,41E-04	2,99E-04	4,15E-04
Easergy Fusion1: unavailability of ANSI 21	8,76E-04			

Decreasing the servers' reliability by a factor of 5 does not change the conclusion: the SDEC solution remains twice more available than the Easergy Fusion 1 relay.

7.2.2. Impact of operation strategy

These tables enable to compare the scenario 1 vs the scenario 2, in terms of protection functions availability:

	Scenario 1 (DD Failures -> alarm)				Scenario 2 (DD Failures -> trip)			
	Unavailability of ANSI 50/51	F (spurious actuation of ANSI 50/51) /h	Unavailability of ANSI 21	F (spurious actuation of ANSI 21) /h	Unavailability of ANSI 50/51	F (spurious actuation of ANSI 50/51) /h	Unavailability of ANSI 21	F (spurious actuation of ANSI 21) /h
SDEC	1,75E-04	3,00E-07	1,83E-04	3,23E-07	1,48E-04	8,61E-07	1,48E-04	1,07E-07
Easergy	1,13E-03	3,85E-07	8,76E-04	3,85E-07	1,11E-03	8,63E-07	8,54E-04	8,41E-07

The scenario 2 seems not to be a good option:

- It increases the spurious trips of distance protection by a factor of 3
- But only generates a minor reduction of the protection unavailability (- 19%).

7.2.3. Impact of proof tests interval

Reducing the frequency of the periodic checking of the electrical protections ANSIxx degrades their availability, for both solutions:

	Tproof = 1 year	Tproof = 2 years	Tproof = 3 years
SDEC: unavailability of ANSI 21	1,83E-04	3,01E-04	4,18E-04
Easergy Fusion1: unavailability of ANSI 21	8,76E-04	1,71E-03	2,54E-03

The SDEC solution is less affected than the Easergy relay by an increase of the period between proof tests: for a three years periodicity, SDEC is 6 times more available than Easergy Fusion v1.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

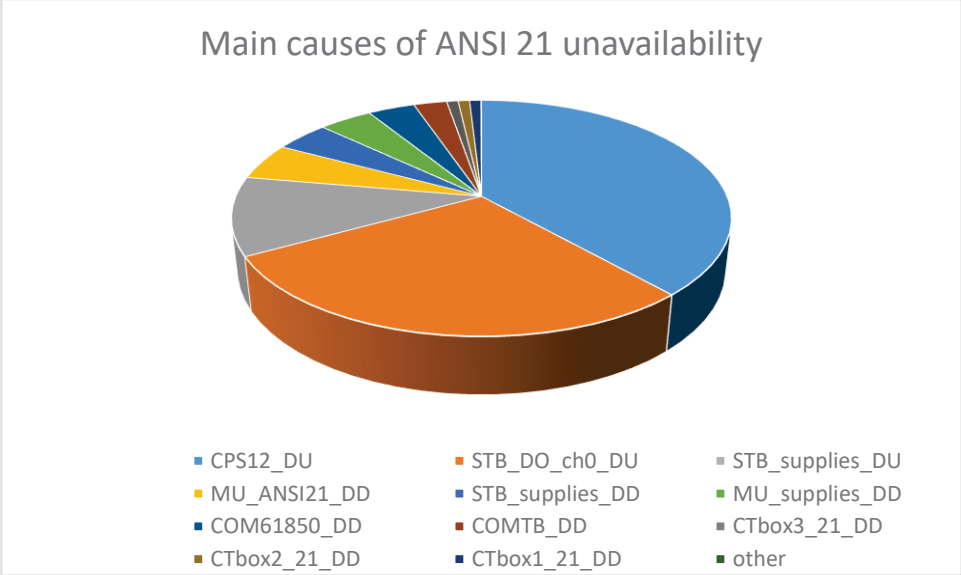
7.2.4. Impact of (customer dependent) repair times

	MTTR 24h	MTTR 48h	MTTR 168h
SDEC: unavailability of ANSI 21	1,50E-04	1,83E-04	3,46E-04
Easergy Fusion1: unavailability of ANSI 21	8,55E-04	8,76E-04	9,79E-04

Increasing the repair time reduces the gap between SDEC et Easergy options, but even with a one week repair time, the virtualized solution remains 3 times more available than the IED.

7.2.5. Impact of Titanium architecture

The analysis of the main contributors to SDEC unavailability show that a predominant failure is the undetected failure of the active compute server, which weights around 40% of the global figure:



Indeed, the Titanium hardware is redundant but the transfers from one server to another can only be launched upon failure detection. So, an undetected failure cannot be circumvented by switching to the backup equipment.

This questions the interest of the Titanium architecture, and deserves some additional investigations with some possible variants at the Edge level.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

The possible alternatives lead to the following results:

	Easergy Fusion1	SDEC Titanium	SDEC with a single CPS	2 CPS + 2 DO channels in 1oo2
unavailability of ANSI 21	8,76E-04	1,83E-04	3,08E-04	1,25E-04

This table shows the benefits of the redundant Titanium, and the possibility to even improve the protection functions availability by simply using 2 independent CPS operating in 1oo2 mode. But this last solution would also double the frequency of spurious trips.

7.2.6. Impact of Software errors

7.2.6.1. Context

The risks generated by the new SDEC architecture are not only related to the random HW failures, but also include the effects of possible errors affecting the software.

The SW is in fact perceived as a threat by many people interested in virtualized architectures.

In the preliminary RAM study performed on the Titanium (see [8]), KerrNet Consulting made an attempt to consider the software errors in the probabilistic evaluations.

RTE technical experts would like to deploy the same approach on this dependability analysis, despite the theoretical limits of such a process (see next section).

7.2.6.2. Preliminary warning

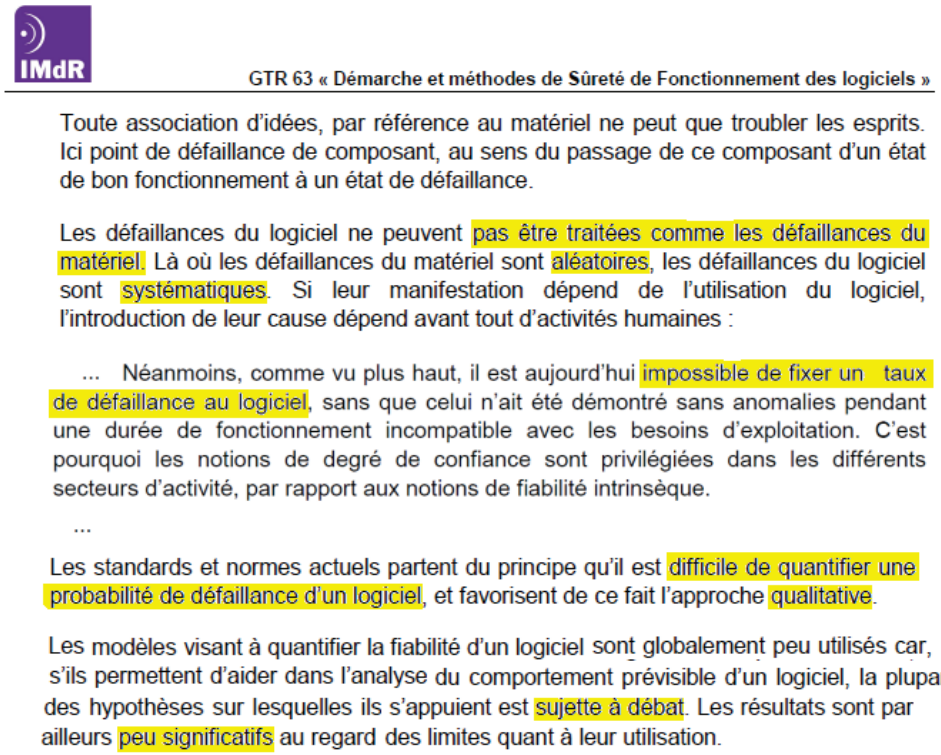
It is important to remind that today, there is no recognized, practicable method in the RAM state of the art to quantify the risks related to SW.

For instance:

- The IEC 61508, which is the reference standard for Functional Safety management, proposes a purely qualitative approach for the software. Tables listing good practices enable to justify the confidence that can be granted to a SW, in terms of systematic errors avoidance. The recommended methods may include some metrics, such as the diagnostic coverage. But the standard does not propose any way to evaluate the SW with a failure rate.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

- The French IDMR (Institute for Risks Management, formerly ISdF Dependability Institute) published a synthesis of the current state of the art in terms of software risks management. In the document IMDR GTR63 "Approach and methods for SW dependability" (ref. [10]), a complete overview is presented. Here are some major points highlighted in this document:



GTR 63 « Démarche et méthodes de Sûreté de Fonctionnement des logiciels »

Toute association d'idées, par référence au matériel ne peut que troubler les esprits. Ici point de défaillance de composant, au sens du passage de ce composant d'un état de bon fonctionnement à un état de défaillance.

Les défaillances du logiciel ne peuvent pas être traitées comme les défaillances du matériel. Là où les défaillances du matériel sont aléatoires, les défaillances du logiciel sont systématiques. Si leur manifestation dépend de l'utilisation du logiciel, l'introduction de leur cause dépend avant tout d'activités humaines :

... Néanmoins, comme vu plus haut, il est aujourd'hui impossible de fixer un taux de défaillance au logiciel, sans que celui n'ait été démontré sans anomalies pendant une durée de fonctionnement incompatible avec les besoins d'exploitation. C'est pourquoi les notions de degré de confiance sont privilégiées dans les différents secteurs d'activité, par rapport aux notions de fiabilité intrinsèque.

...

Les standards et normes actuels partent du principe qu'il est difficile de quantifier une probabilité de défaillance d'un logiciel, et favorisent de ce fait l'approche qualitative.

Les modèles visant à quantifier la fiabilité d'un logiciel sont globalement peu utilisés car, s'ils permettent d'aider dans l'analyse du comportement prévisible d'un logiciel, la plupart des hypothèses sur lesquelles ils s'appuient est sujette à débat. Les résultats sont par ailleurs peu significatifs au regard des limites quant à leur utilisation.

➔ As software bugs lead to systematic errors when a faulty SW branch is run, the behavior is quite different to that of HW failures and can simply not be modelled by an hourly failure rate.

7.2.6.3. "KerrNet-like" modelling

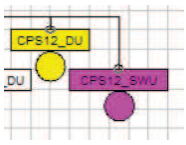
Despite the above-mentioned warning, this section presents an attempt to address SW errors in our dependability study, based on KerrNet Consulting's approach.

- The potential impacts of SW errors in our ANSI 21 application could be seen as follows:
  - **Errors could possibly affect the electrical protection algorithms, leading either to spurious trips or to inoperant protections. It is important to notice that**
- These protection algorithms are stable, well proven and very stable. Unlike in most internet applications, there is no additional functionality added over the years, and the target is really to keep this qualified SW unchanged over decades.
- These algorithms are exactly the same, in Easergy IED and in the VMs used in SDEC solution ➔ so, the risks related to protection algorithm errors are exactly the same in both solutions.
- Therefore, this application software is a common, not discriminating part when comparing the two solutions ➔ it is useless to address it in this section.
  - **Another SW is the Titanium control algorithms, which could possibly cause spurious reconfigurations or an inability to recover upon a server failure ➔ this SW is SDEC specific, and could possibly raise additional risks for the SDEC solution**

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

- Hypothetic SW errors are considered as follows in Titanium RAM study (cf. [8]):
  - **They are accounted for as HW random failures, with an hourly failure rate (/h)**
  - **This SW failure rate is based on a KerrNet custom model, based on telecom field data**
  - **λ_{SW} = f(SW size, upgrades size & frequency, process maturity level), but the equation is not detailed in KerrNet's RAM report**
  - **λ_{SW} = 1,12E-5/h (compute) to 1,34E-5/h (control servers)**
  - **KerrNet assumes that 95% of the SW faults are detected**
  - **Detected SW faults cause a remote controlled system restoration within 20mn**
  - **SW upgrades are assumed to occur once a year, to last 20mn per server.**

- So, the following assumptions can be considered to achieve a "KerrNet-like" modelling of SW errors in our FTA:
  - **VM algorithms, common to both SDEC and Easergy, are out of solutions comparison scope**
  - **Titanium control algorithms: assumed λ_{sw} ~ 1E-05/h for each server**
  - **95% of SW faults are detected ➔ server unavailable for 20mn (manual restoration) ➔ λ_{SW_D}**
  - **5% of SW faults not detected ➔ server lost, no detection until server solicitation ➔ λ_{SW_U}**
  - **λ_{SW_D} and λ_{SW_U} are added in the model, for each server, in addition to the existing HW random failures**

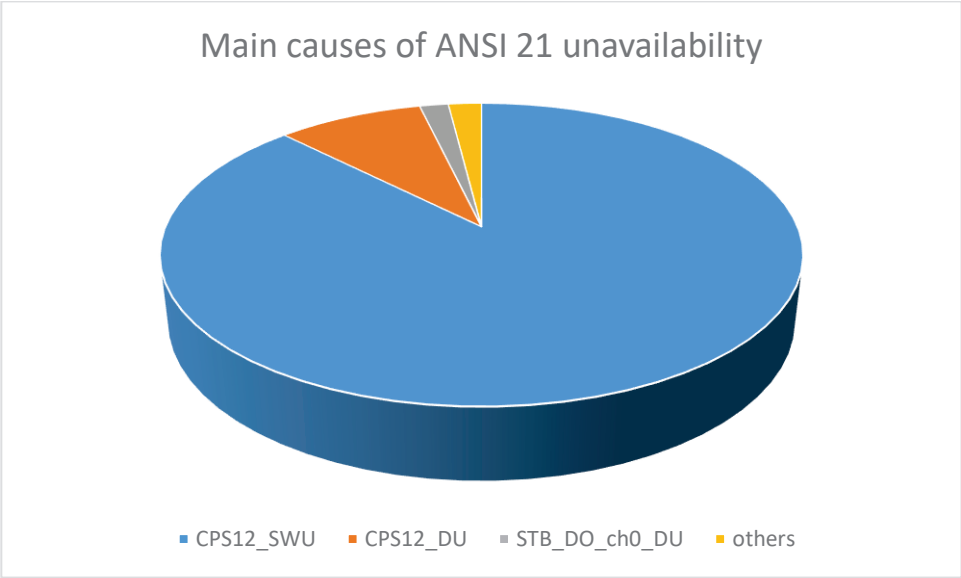


This approach leads to the following results for the distance protection unavailability (other conditions unchanged vs original simulations):

Easergy Fusion1	8,76E-04	478%
SDEC HW failures	1,83E-04	100%
SDEC HW failures + SW faults (95% detected)	2,37E-03	1292%

With their poor "reliability" figures and a 95% detection rate, the SW faults add a drastic contribution to the risks of ANSI 21 protection unavailability, causing the SDEC solution to become twice worse than the Easergy relay:

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276



The 95% detection rate seems quite low to our SW experts. Increasing it to 99% leads to the following results:

SDEC HW failures + SW faults (99% detected)	6,21E-04	339%

SDEC HW failures + SW faults (99% detected)	**6,21E-04**	**339%**

Under these less pessimistic assumptions, the SDEC once again becomes better than the Easergy relay.

The reader should nevertheless keep in mind that this way of modelling the SW is not academic, so these figures lack of confidence justification and can nothing but give rice to controversy.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

8. CONCLUSIONS

This preliminary hardware dependability study only covers the scope of overcurrent and distance protections performed by a single breaker equipped with a shunt coil.

The SDEC solution is quite equivalent to a classical IED in terms of spurious trip.

It also makes the protection functions noticeably more available than the Easergy relay (and this conclusion is robust vs. the servers' reliability figures).

Changing the repair time or the proof tests interval does not change this hierarchy.

The optimal strategy is to simply warn the operator in case of failure detection, and not to systematically trip in such situation.

The SDEC performance could even be improved by simply using two compute servers in 1oo2, without transfer mechanism. But this would double the spurious trip frequency.

The bugs possibly affecting the SW could seriously impact the SDEC performance, with a major influence of the fault detection rate. But what can easily be understood from a qualitative viewpoint is difficult to prove quantitatively, as the KerrNet approach used above is not a recognized one.

Last but not least, this study should be extended from a "product vs product" viewpoint to a "system" viewpoint: it would be interesting to evaluate, in particular, the configuration where a single Titanium manages all the protections in an HV substation, including the main and backup protections, a typical use-case for RTE substations could be defined and studied in a next step.

Though this use case is mostly based on COTS components, the extension of the use of this virtualized infrastructure could be examined for other purposes, for example distributed controls from use case 11. It can also provide technological and methodological inputs for some PIARCH, at least the one supporting collaborative systems from WP4.

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276

9. APPENDIX : ELECTRONICS FMEA TABLES TEMPLATE

		Qualitative part				Quantitative part				POC RTE 2018 (shunt tripping coil)					
Function name	Sub function name	Component identification	Failure mode	Local Effect	$\lambda_{component}$	Repartition of the failures mode	Number of components	λ_{mode}	Unwanted events seen by the customer	Detection (0->1 trip)	loss of ANS2oH	spurious ANS2oH, actuator	loss of ANS2oT	spurious ANS2oT, actuator
FPGA	1V2 decoupling	C109, C112, C115, C118, C121, C124, C127, C128	S.C	Loss of the 1V2 power supply	5.68E-10	90%	8	4.091E-09	UE2: failure to trip	Reset	DD		DD	
FPGA	1V2 decoupling	C109, C112, C115, C118, C121, C124, C127, C128	O.C	Without effects	5.68E-10	10%	8	4.546E-10	UE21: Without effect	NO				
FPGA	3V3 decoupling	C116, C117, C119, C120, C122, C123, C125, C126, C135	S.C	Loss of the 3V3 power supply	5.68E-10	90%	12	6.137E-09	UE2: failure to trip	Reset	DD		DD	
FPGA	3V3 decoupling	C116, C117, C119, C120, C122, C123, C125, C126, C135	O.C	Without effects	5.68E-10	10%	12	6.819E-10	UE21: Without effect	NO				
FPGA	VCCA decoupling	C129, C131, C133	S.C	Loss of the 2V5 power supply	5.68E-10	90%	3	1.534E-09	UE2: failure to trip	Reset	DD		DD	
FPGA	VCCA decoupling	C129, C131, C133	O.C	Without effects	5.68E-10	10%	3	1.704E-10	UE21: Without effect	NO				
FPGA	VCCA filtering	L11	S.C	Without effects	1.34E-09	20%	1	2.677E-10	UE21: Without effect	NO				
FPGA	VCCA filtering	L11	O.C	Loss of the analog FPGA power supply	1.34E-09	80%	1	1.070E-09	UE2: failure to trip	Detected by CPU	DD		DD	
FPGA	VCCD_PLL decoupling	C138, C132, C134	S.C	Loss of the 1V2 power supply	5.68E-10	90%	3	1.534E-09	UE2: failure to trip	Reset	DD		DD	
FPGA	VCCD_PLL decoupling	C138, C132, C134	O.C	Without effects	5.68E-10	10%	3	1.704E-10	UE21: Without effect	NO				
FPGA	VCCD_PLL filtering	L12	S.C	Without effects	1.34E-09	20%	1	2.677E-10	UE21: Without effect	NO				
FPGA	VCCD_PLL filtering	L12	O.C	Loss of the PLL FPGA power supply	1.34E-09	80%	1	1.070E-09	UE2: failure to trip	Detected by CPU	DD		DD	
FPGA	nSTATUS PU	R15	O.C	Without effects	4.70E-11	100%	1	4.704E-11	UE21: Without effect	NO				
FPGA	CONF_DONE PU	R16	O.C	Without effects	4.70E-11	100%	1	4.704E-11	UE21: Without effect	NO				
FPGA	led debug	R17	O.C	Without effects	4.70E-11	100%	1	4.704E-11	UE21: Without effect	NO				
FPGA	FPGA	U2	Safe		1.69E-07	0%	1	0	UE1: Spurious trip	NO		S		S
FPGA	FPGA	U2	Dangerous		1.04E-07	100%	1	1.064E-07	UE2: Failure to trip	CRC..	DD		DD	
FPGA	HRESETn	C283	S.C	Reset	1.88E-10	70%	1	1.325E-10	UE2: Failure to trip	Reset	DD		DD	
FPGA	HRESETn	C283	O.C or daft	Without effects	1.88E-10	30%	1	5.682E-11	UE21: Without effect	NO				
FPGA	FPGA	R277, R278, R279, R280	O.C	Without effects	4.70E-11	100%	1	4.704E-11	UE21: Without effect	NO				

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826276