1. □ ΕΓΚΡΙΝΕΤΑΙ. Εργασίες μπορούν να εκτελεσθούν.
APPROVED. Works may proceed.

2. □ ΑΝΑΘΕΩΡΗΣΗ ΚΑΙ ΕΠΑΝΥΠΟΒΟΛΗ. Δεν μπορούν να εκτελεσθούν εργασίες.
REVISE AND RESUBMIT. Works should not proceed.

3. □ ΔΕΝ ΑΠΑΙΤΕΙΤΑΙ ΕΛΕΓΧΟΣ. Εργασίες μπορούν να εκτελεσθούν.
REVIEW NOT REQUIRED. Works may proceed.

ΑΔΕΙΑ ΕΦΑΡΜΟΓΗΣ ΣΧΕΔΙΟΥ ΔΕΝ ΑΠΑΛΛΑΣΣΕΙ ΤΟΝ ΑΝΑΔΟΧΟ ΑΠΟ ΤΙΣ ΕΥΘΥΝΕΣ ΤΟΥ ΠΟΥ ΑΠΟΡΡΕΟΥΝ ΑΠΟ ΤΗ ΣΥΜΒΑΣΗ ΟΥΤΕ ΑΠΟΤΕΛΕΙ ΑΠΟΔΟΧΗ ΤΗΣ ΕΠΑΡΚΕΙΑΣ ΚΑΙ ΑΚΡΙΒΕΙΑΣ ΤΗΣ ΜΕΛΕΤΗΣ.

PERMISSION TO PROCEED DOES NOT RELIEVE CONTRACTOR FROM HIS RESPONSIBILITIES IMPOSED BY CONTRACT NEITHER DOES IT CONSTITUTE ACCEPTANCE OF THE ADEQUACY AND EXACTNESS OF THE DESIGN.

ΤΕΧΝΙΚΟΣ ΕΛΕΓΧΟΣ ΑΠΟ: TECHNICAL REVIEW BY: ________	ΕΓΚΡΙΘΗΚΕ ΑΠΟ: APPROVED BY: ________
ΥΠΟΓΡΑΦΗ: SIGNED: ________	ΥΠΟΓΡΑΦΗ: SIGNED: ________
ΗΜΕΡΟΜΗΝΙΑ: DATE: ________	ΗΜΕΡΟΜΗΝΙΑ: DATE: ________

F								
E								
D								
C								
B								
A	30.06.16	IFU	N/A	G. Galluzzi		G. Gallo		DFD stage – First issue.
				ΟΝΟΜΑ/N.A.ME	ΥΠΟΓΡ./SIGN.	ΟΝΟΜΑ/N.A.ME	ΥΠΟΓΡ./SIGN.	
ΑΝΑΘ. REV.	ΗΜ/ΝΙΑ DATE	ΣΥΝΤ. INIT.	ΕΛΕΓΧ. CHK.	ΕΓΚΡΙΘΗΚΕ / APPROVED		ΕΠΙΚΥΡΩΘΗΚΕ / AUTHORIZED		ΠΕΡΙΓΡΑΦΗ / DESCRIPTION

ΜΕΤΡΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
THESSALONIKI METRO

ΑΤΤΙΚΟ ΜΕΤΡΟ Α.Ε.

ΜΕΤΡΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
«ΝΕΟΣ ΣΙΔΗΡΟΔΡΟΜΙΚΟΣ ΣΤΑΘΜΟΣ –
ΣΤΑΘΜΟΣ Ν. ΕΛΒΕΤΙΑ ΚΑΙ ΑΜΑΞΟΣΤΑΣΙΟ ΠΥΛΑΙΑΣ»
THESSALONIKI METRO
"NEW RAILWAY STATION – N. ELVETIA STATION AND PILEAS DEPOT"

ΕΡΓΟ / PROJECT: CON-06/004
ΜΕΛΕΤΗ, ΚΑΤΑΣΚΕΥΗ ΚΑΙ ΘΕΣΗ ΣΕ ΛΕΙΤΟΥΡΓΙΑ
ΤΟΥ ΜΕΤΡΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

DESIGN, CONSTRUCTION AND COMMISSIONING
OF THESSALONIKI METRO

ΝΟΜΙΜΟΙ ΕΚΠΡΟΣΩΠΟΙ / AUTHORIZED SIGNATORIES

Κ/Ξ "ΜΕΤΡΟ ΘΕΣΣΑΛΟΝΙΚΗΣ"
ΑΕΓΕΚ - IMPREGILO - ANSALDO T.S.F.
SELI - ANSALDOBREDA

Μ. ΣΙΜΑΣ

ΓΙΑ ΧΡΗΣΗ ΣΕ ΤΕΧΝΙΚΑ ΕΓΓΡΑΦΑ ΜΟΝΟ
FOR TECHNICAL DOCUMENTS ONLY

ΑΝΑΔΟΧΟΣ – ΕΚΔΙΔΟΥΣΑ ΕΤΑΙΡΕΙΑ ΕΓΓΡΑΦΟΥ
CONTRACTOR – DOCUMENT ISSUING COMPANY

ΑΕΓΕΚ Impregilo Ansaldo STS SELI HITACHI

Κοινοπραξία ΜΕΤΡΟ ΘΕΣΣΑΛΟΝΙΚΗΣ ΕΡΓΟ: CON-06/004

ΜΕΛΕΤΗΤΙΚΟ ΓΡΑΦΕΙΟ / DESIGN OFFICE

ΤΙΤΛΟΣ / TITLE

CBACS (Central Building Automation Control System) Safe
DFD – Technical Specification

ΑΝΑΦΟΡΑ ΑΝΑΔΟΧΟΥ / CONTRACTOR'S REFERENCE	ΓΛΩΣΣΑ / LANGUAGE	ΑΡΙΘΜΟΣ ΕΓΓΡΑΦΟΥ – ΣΧΕΔΙΟΥ / DOCUMENT – DRAWING NUMBER
_ _ _ _ _ _ _ _ _ _ _ _ _ _	GR - EN	1 G 0 0 P S 2 5 8 G 1 0 5 A

ΑΡΧΕΙΟ / FILENAME	ΚΛΙΜΑΚΑ / SCALE	ΣΕΛΙΔΑ / SHEET No
1G00PS258G105A_EN.doc	___ : ___	1 of 103

Ψηφιακά υπογεγραμμένο από AIKATERINI CHELMI
Ημερομηνία: 2018.02.05 12:03:51 EET

ENGINEERING

Item Title

CBACS (Central Building Automation Control System) Safe DFD – Technical Specification

Item Code

1G00PS258G105

History of Revisions:

4	30.06.16	R. Palma	C. Agliottone	G. Rizzi	I. Fulgieri	DFD stage – Revision submitted due to coversheet update.
3	30.03.15	R. Palma	C. Agliottone	G. Rizzi	I. Fulgieri	DFD stage – Revision submitted to formal Functional Safety Assessment on safety requirements specification and architectural design specification phases. In particular, some sections have been added: requirements for environmental conditions, subsystem decomposition. Finally, safety functions and SIFs description have been moved into Architecture Description section.
2	15.12.14	R. Palma	C. Agliottone	G. Rizzi	I. Fulgieri	DFD stage – Revision preceding Functional Safety Assessment on safety requirements specification and architectural design specification phases. In particular, some sections have been added: purpose and scope, safety properties, GUI description, safety functions description, safety integrity functions description, software architecture description, subsystem behavioural view. Removed 7-segments display from SafePanel; a new SIF has been defined for automatic workstation fault / error detection, by photo-resistors. Finally, some sections have been removed; their content will be moved to a next safety verification report: SW Design and Implementation Approaches, Architecture Coverage to EN Safety Standards' Requirements, Architecture Coverage to IEC Safety Standards' Requirements.
1	31.12.13	R. Palma	C. Agliottone	G. Rizzi	I. Fulgieri	DFD stage – First issue.
ΑΝΑΘ. **REV.**	**ΗΜ/ΝΙΑ** **DATE**	**ΣΥΝΤ.** **INIT.**	**ΕΛΕΓΧ.** **CHK.**	**ΕΓΚΡΙΘΗΚΕ** **APPROVED**	**Πελάτης ΕΛΕΓΧ.** **Customer CHK.**	**ΠΕΡΙΓΡΑΦΗ** **DESCRIPTION**

Communications and Open Issues:

1						
ΑΝΑΘ. **REV.**	**ΚΩΔΙΚΟΣ** **CODE**	**ΑΠΟΣΤ.** **SENDER**	**ΠΑΡΑΛ.** **RECEIVER**	**ΠΕΡΙΓΡΑΦΗ** **DESCRIPTION**	**ΑΠΌΚΡΙΣΗ** **RESPONSE**	**ΚΑΤΆΣ.** **STATE**

ΦΥΛΛΟ ΤΡΟΠΟΠΟΙΗΣΕΩΝ / MODIFICATION SHEET

ΦΥΛΛΟ SHEET	ΑΝΑΘΕΩΡΗΣΗ / REVISION						ΦΥΛΛΟ SHEET	ΑΝΑΘΕΩΡΗΣΗ / REVISION					
	A	B	C	D	E	F		A	B	C	D	E	F

ΗΜΕΡΟΜΗΝΙΑ / DATE	30.06.16					
ΑΝΑΘΕΩΡΗΣΗ / REVISION	A	B	C	D	E	F

ΤΙΤΛΟΣ / TITLE

CBACS (Central Building Automation Control System) Safe

DFD – Technical Specification

ΑΡΙΘΜΟΣ ΕΓΓΡΑΦΟΥ – ΣΧΕΔΙΟΥ / DOCUMENT – DRAWING

1	G	0	0	P	S	2	5	8	G	1	0	5	A

NUMBER

ΚΛΙΜΑΚΑ / SCALE

_ _ _ _ : _ _ _ _

ΣΕΛΙΔΑ – PAGE 3 / 103

Ansaldo STS DOCUMENT ISSUE

Date	30/06/2016

	Name and Surname	Designation
Author/INIT	I.. Fulgieri	AFC WPL
Verifier/CHK	N/A	N/A
Approver	G. Galluzzi	SCADA&PC Manager
Validator/RAMS	N/A	N/A
Authorizer	G. Gallo	Project Engineer

TRACEABILITY OF THE REVISIONS

Rev.	Ext. Rev.	Date	CO	CO Date	Author	Verifier	Approver	Validator/ RAMS	Authorizer	Revision Description
00.00	A	30-06-2016	--	--	I. Fulgieri	N/A	G.Galluzzi	N/A	G. Gallo	DFD stage First issue

Table of Contents

Management Summary 8

1 Introduction 9

1.1 Context Description 9

1.2 Scope of the Document 9

1.3 Reference Documents 11

1.3.1 Input Documents 11

1.3.2 Applicable Documents 11

1.3.3 Previous Stage Document 12

1.3.4 Literature Documents 12

1.3.5 Customer's Design Review Documents 12

1.3.6 Verification Documents 12

1.4 Reference Standards and Regulations 13

1.5 Glossary of Terms 16

1.6 Glossary of Acronyms 18

2 History of Revisions 19

2.1 Revision A 19

2.1.1 List of Changes 19

2.1.2 List of Open Issues 19

2.1.3 Verification Report 19

3 Subsystem's Purpose and Scope 20

3.1 Subsystem's Overview and Purpose 20

3.2 Subsystem's Scope 22

4 Safety Properties 25

4.1 Summary of Safety Properties 25

4.2 General Safe and Dangerous States 27

4.3 Installation, Operation and Maintenance Assumptions 27

5 Architecture and Functions Description 28

5.1 Subsystem's Structural View 28

5.2 Functions' Coding Rules 28

5.3 OCC Architecture 29

5.4 OCC Functional Requirements 31

5.5 OCC Components Description 34

5.5.1 Workstations' Components 34

5.5.2 OCC Channel A/B Workstation Functional Requirements 37

5.5.3 SafePLCs' Components 43

5.5.4 OCC Channel A/B SafePLC Functional Requirements 46

5.5.5 SafePanel's Components 55

5.5.6 OCC Channel A/B SafePanel Functional Requirements 56

5.6 SMR Architecture 58
5.7 SMR Functional Requirements....59
5.8 SMR Components Description 61
5.8.1 Workstations' Components 61
5.8.2 SMR Workstation Functional Requirements 63
5.8.3 SafePLCs' Components....69
5.8.4 SMR SafePLC Functional Requirements 71
5.8.5 SafePanel's Components....80
5.8.6 SMR SafePanel Functional Requirements....80
5.9 Software Architecture 82
5.10 Graphic User Interface 85
5.11 Safety Protocol 86
5.12 Subsystem Behavioural View....88
5.12.1 Monitoring Function....88
5.12.2 Command Function....90
5.13 Subsystem Decomposition....93
5.13.1 Workstation Decomposition 93
5.13.2 SafePLC Decomposition 99
5.14 Requirements for Environmental Conditions....102
5.14.1 Temperature Range 102
5.14.2 Humidity Range....102
5.14.3 Workstation Power Supply 102
5.14.4 VDU Power Supply 102
5.14.5 SafePLC Power Supply....102
5.14.6 SafePanel Power Supply 102

Index of Figures

Figure 3-1 – CBACS Main Groups and Layers 20
Figure 3-2 – CBACS Safe Parts 22
Figure 3-3 – CBACS Safe Scope 23
Figure 5-1 – CBACS Safe Architecture 28
Figure 5-2 – Deployment of OCC Workstation SW (OCC.WS<k>.SW) on WS Hardware 34
Figure 5-3 – OCC Workstation<A> SW Packages 35
Figure 5-4 – OCC Workstation<B> SW Packages 36
Figure 5-5 – Deployment of OCC SafePLC SW (OCC.SafePLC<k>.SW) on SafePLC Hardware 43
Figure 5-6 – SafePanel’s Layout and Components 55
Figure 5-7 – Deployment of SMR Workstation SW (SMR.WS<k>.SW) on WS Hardware 61
Figure 5-8 – SMR Workstation<A> SW Packages 62
Figure 5-9 – SMR Workstation<B> SW Packages 62
Figure 5-10 – Deployment of SMR SafePLC SW (SMR.SafePLC<k>.SW) on SafePLC Hardware 69
Figure 5-11 – Software Architecture 82
Figure 5-12 – GUI’s Layout and Components 85
Figure 5-13 – Monitoring Function Success Scenario 88
Figure 5-14 – Monitoring Function Exception Scenario 89
Figure 5-15 – Command Function Success Scenario 91
Figure 5-16 – Command Function Exception Scenario 92

Index of Tables

Table 1-1 – Input Documents 11
Table 1-2 – Applicable Documents 11
Table 1-3 – Previous Stage Document 12
Table 1-4 – Literature Documents 12
Table 1-5 – Customer’s Design Review 12
Table 1-6 – Verification Documents 12
Table 1-7 – Reference Standards and Regulations 13
Table 1-8 – Glossary of Terms 16
Table 1-9 – Glossary of Acronyms 18
Table 2-1 – Revision A – List of Changes 19
Table 2-2 – Revision A – List of Open Issues 19
Table 2-3 – Revision A – Verification Report 19
Table 4-1 – Summary of Safety Properties 25
Table 5-1 – SafePLC I/O Signals List 44
Table 5-2 – Example of Structure of a Safety Telegram 86

Management Summary

This document is the 'Safety Concept Design' (SCD) of **CBACS Safe** subsystem and describes the relevant safety architecture.

The SCD records the safety architectural design information for the subsystem; this includes:

- **Architecture Description**, then:
  - The selected Safety Architecture of subsystem;
  - Safety Architecture partitioning in HW and high-level SW components;
  - Safety Architecture's HW and SW interfaces (internal and external).

- **Functions Description**, then:
  - The description of the Safety Functions;
  - The mapping of the Safety Functions to the Safety Architecture;
  - The description of the Safety Integrity Functions / Measures for detection and reaction to subsystem faults / errors (such as redundancy, diversity, comparison, voting, monitoring, data validation / integrity checks);
  - The mapping of the Safety Integrity Functions / Measures to the Safety Architecture.

- If applicable:
  - The report of outstanding issues;
  - The architectural variants, for safety improvements.

1 Introduction

1.1 Context Description

This document is relevant to the Central Building Automation Control System (CBACS) Safe of Thessaloniki Metro Project.
The CBACS Safe is the safety-related HMI layer of the Building Automation Control System (BACS); thus, it doesn't include BACS' Field layer.

The CBACS Safe allows monitoring and, where applicable, command building automation equipment, involved in safety functions, located in the stations, tunnels and along the railway.

The building automation equipment involved in safety functions can be grouped in the two below listed types:

- Fire detection (**FD**);
- Emergency ventilation (**EV**) – exhaust fans, over-track exhaust fans, supply air fans, blast shaft fans, jet fans.

1.2 Scope of the Document

This specification is the 'Safety Concept Design' (SCD) of **CBACS Safe** subsystem and describes the relevant safety architecture.
It records the safety architectural design information for the subsystem; this includes:

- **Architecture Description**, then:
  - The selected Safety Architecture of subsystem;
  - Safety Architecture partitioning in HW and high-level SW components;
  - Safety Architecture's HW and SW interfaces (internal and external).

- **Functions Description**, then:
  - The description of the Safety Functions;
  - The mapping of the Safety Functions to the Safety Architecture;
  - The behaviour of the subsystem in performing the Safety Functions;

- The description of the Safety Integrity Functions / Measures for detection and reaction to subsystem faults / errors (such as redundancy, diversity, comparison, voting, monitoring, data validation / integrity checks);
- The mapping of the Safety Integrity Functions / Measures to the Safety Architecture.
- The behaviour of the subsystem in performing Safety Integrity Functions / Measures (in case of faults / errors detection), including error handling.

Its scope is to:

- Provide an understandable description of subsystem architecture;
- Specify consistently the allocation and implementation of the Safety Functions;
- Specify consistently the allocation and implementation of the Safety Integrity Functions / Measures.

The used specification language is UML (semi-formal) and, where necessary, SysML extensions profile.

1.3 Reference Documents

1.3.1 Input Documents

Table 1-1 – Input Documents

Item #	Code	Title	Date	Rev #
ID.01	1G00PS258G104	CBACS Safe. DFD Safety Requirements Specification.		A

1.3.2 Applicable Documents

Table 1-2 – Applicable Documents

Item #	Code	Title	Date	Rev #
AD.01	1G00PS258K111	CBACS Safe. DFD Bill of Materials.		A
AD.02	1G00PS258G211	CBACS Safe. DFD Components Datasheets.		A
AD.03	1G00PS250O111	CBACS. DFD Racks and Equipment Description.		A
AD.04	1G00PS250C702	CBACS. DFD System Architecture Block Diagrams.		A
AD.05	1G00PS250C106	CBACS. DFD OCC Server Rack Electrical Schemes and Diagrams.		A
AD.06	1G00PS250C114	CBACS. DFD OCC Power Supply Cabinet Electrical Schemes and Diagrams.		A
AD.07	1G00PS258C112	CBACS Safe. DFD OCC PLC Box Electrical Schemes and Diagrams.		A
AD.08	1G00PS258C113	CBACS Safe. DFD SMR PLC Box Electrical Schemes and Diagrams.		A

1.3.3 Previous Stage Document

This paragraph defines if this document has been already issued in previous project's stages GFD1 or GFD2. If yes, the revision 'A' of this document takes as input the previous stage document, in the last issued revision, and relevant open issues.

<u>This document has no previous stage related document</u>.

Table 1-3 – Previous Stage Document

Item #	Code	Title	Date	Rev #
PD	None.	None.	None.	None.

1.3.4 Literature Documents

Table 1-4 – Literature Documents

Item #	Code	Title	Date	Rev #
LD.01		Real-Time Design Patterns: Robust Scalable Architecture for Real-Time Systems. Author(s): Bruce-Powel Douglass. Publisher: Addison-Wesley.	2002	
LD.02		Design Patterns: Elements of Reusable Object-Oriented Software. Author(s): Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides. Publisher: Addison-Wesley.	1994	

1.3.5 Customer's Design Review Documents

First issue of this document, then no Customer's design review document referred.

Table 1-5 – Customer's Design Review

Item #	Code	Title	Date	Rev #
DD.01	None.	None.	None.	None.

1.3.6 Verification Documents

Table 1-6 – Verification Documents

Item #	Code	Title	Date	Rev #
VD.01	1G00PS258G314	CBACS Safe. DFD Architecture Safety Analysis.		A

1.4 Reference Standards and Regulations

Table 1-7 – Reference Standards and Regulations

Item #	Code	Title	Date	Rev #
ST.01	EN 50126-1:1999	European Standard, EN 50126. Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Part 1: Basic requirements and generic process.	Sep-1999	
ST.02	EN 50128:2011	European Standard, EN 50128. Railway Applications: Communications, signalling and processing systems. Software for railway control and protection systems.	Jun-2011	
ST.03	EN 50129:2003	European Standard, EN 50129. Railway Applications: Communications, signalling and processing systems. Safety related electronic systems for signalling.	Feb-2003	
ST.04	EN 50159:2010	European Standard, EN 50159. Railway Applications: Communications, signalling and processing systems. Safety-related communication in transmission systems.	Sep-2010	
ST.05	ODVA CIP	Open DeviceNet Vendors Association (ODVA) Standard. The CIP Networks Library Volume 1: Common Industrial Protocol (CIP).		3.8
ST.06	ODVA EIP	Open DeviceNet Vendors Association (ODVA) Standard. The CIP Networks Library Volume 2: EtherNet/IP Adaptation of CIP.		1.9
ST.07	ODVA CSY	Open DeviceNet Vendors Association (ODVA) Standard. The CIP Networks Library		2.2

		Volume 5: CIP Safety.		
ST.08	IEC 61508-2:2010	International Standard, IEC 61508. Functional safety of Electrical/Electronic/Programmable Electronic safety-related systems. Part 2: Requirements for Electrical/Electronic/Programmable Electronic safety-related systems.	Apr-2010	2.0
ST.09	IEC 61508-3:2010	International Standard, IEC 61508. Functional safety of Electrical/Electronic/Programmable Electronic safety-related systems. Part 3: Software requirements.	Apr-2010	2.0
ST.10	IEC 61508-6:2010	International Standard, IEC 61508. Functional safety of Electrical/Electronic/Programmable Electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.	Apr-2010	2.0
ST.11	IEC 61131-3:2013	International Standard, IEC 61131. Programmable controllers. Part 3: Programming languages.	Feb-2013	3.0
ST.12	IEC 61131-6:2012	International Standard, IEC 61131. Programmable controllers. Part 6: Functional safety.	Oct-2012	1.0
ST.13	ISO/IEC 23270:2006	International Standard, ISO/IEC 23270. Information technology – Programming languages – C#.	Sep-2006	2.0
ST.14	ISO/IEC 14882:2011	International Standard, ISO/IEC 14882. Information technology – Programming languages – C++.	Sep-2011	3.0
ST.15	UML	Object Management Group (OMG) Unified Modeling Language (UML) Specification.	Aug-2011	2.4.1
ST.16	SysML	Object Management Group (OMG) Systems Modeling Language (SysML)	Jun-2012	1.3

		Specification.		

1.5 Glossary of Terms

Table 1-8 – Glossary of Terms

Term	Description
Fail-Operational	A characteristic of a system for which one failure is tolerated, i.e. the system stays operational after one failure. This is required if **no safe state exists** after the failure of a system component.
Fail-Safe	(or preferably de-energize to trip) A characteristic of a system which causes that system to move to a safe state when it loses electrical or pneumatic energy. After one (or several) failure(s) the system posses a safe state (**passive fail-safe**, without external power) or is brought to a safe state, by a special action (**active fail-safe**, with external power). EN50128 defines it as “a concept which is incorporated into the design of a product such that, in the event of a failure, it enters or remains in a safe state”.
Safe State	Condition that the system reaches **to preserve safety** after internal error. Thus, the state of the process **after acting** to **remove the hazard resulting in no significant harm**.
Fault Tolerance	Ability of a system to **continue to perform a required function** in the presence of random faults or errors. For example a 1oo2 voting system can tolerate one random component failure and still perform its function. Fault tolerance is one of the specific requirements for safety integrity level (SIL) and is described in more detail in IEC61508-2:2010 Tables 2 and 3.
Human-Machine Interface (HMI) or Man-Machine Interface (MMI)	Refers to the software that the process operator "sees" the process with. An example HMI / MMI screen may show a tank with levels and temperatures displayed with bar graphs and values. Valves and pumps are often shown and the operator can "click" on a device to turn it on, off or make a set point change.
Safety Function (SF)	EN50128 defines a Safety Function as a “function that implements a part or whole of a safety requirement”. IEC61508 defines a Safety Function as a “function to be

Term	Description
	implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the Equipment Under Control (EUC), in respect of a specific hazardous event”.
Safety Integrity Function (SIF)	The techniques and measures for detection and reaction to subsystem faults / errors, that guarantee a given probability of successful execution for a safety function.
Safety Requirements Specification (SRS)	Specification containing all the requirements of the safety functions those have to be performed by the safety-related system. It includes both what the functions must do and also how well they must do it. It is often a contractual document between companies and is one of the most important documents in the safety lifecycle process.
Safety Management Plan (SMP)	The Safety Plan or Safety Management Plan (SMP) is a key document in any IEC61508 / IEC61511 / EN50126 development project. It specifies how functional safety will be ensured throughout the entire development project and in production. The Safety Plan must identify the various roles and responsibilities as they apply to the development process. The Safety Plan lists the various techniques and measures that will be implemented as part of the development project to ensure that the targeted SIL is achieved. The deliverable of this task is the draft Safety Plan that the Customer must subsequently refine and implement in their development process.
Safety Case (SCS)	The documented demonstration that the system complies with the safety requirements specification (SRS). The Safety Case is based on structured arguments, supported by evidences, intended to justify that a system is acceptably safe.
Safety Manual (SOM)	Document required for safety-related equipment in accordance with IEC61508 / EN50128 / EN50129 that describes the conditions of use for that equipment in safety applications. It typically includes usage requirements / restrictions, environmental limits, optional settings, failure rate data, useful life data, common cause beta estimate, inspection and test procedures. The Safety Manual may be part of another document.

1.6 Glossary of Acronyms

Table 1-9 – Glossary of Acronyms

Acronym	Description
BACS	Building Automation Control System.
CASE	Computer-Aided Software Engineering.
CBACS	Central Building Automation Control System.
DFD	Detailed Final Design.
Depot-BACS	Depot Building Automation Control System.
Depot-CBACS	Depot Central Building Automation Control System.
EN	European Norm.
EV	Emergency Ventilation.
FD	Fire Detection.
FMEA	Failure Mode and Effect Analysis.
FTA	Fault-Tree Analysis.
GFD1	General Final Design 1.
GFD2	General Final Design 2.
HMI	Human-Machine Interface.
HW or H/W	Hardware.
IEC	International Electrotechnical Commission.
IPC	Industrial Personal Computer.
LAN	Local Area Network.
LED	Light Emitter Diode.
MMI	Man-Machine Interface.
MTBF	Mean Time Between Failures.
MTTR	Mean Time To Restoration.
OCC	Operation Control Centre.
PLC	Programmable Logic Controller.
SCD	Safety Concept Design.
SCS	Safety Case.
SFF	Safety Function or Safe Failure Fraction.
SIF	Safety Integrity Function.
SIL	Safety Integrity Level.
SMP	Safety Management Plan.
SOM	Safety Manual.
SRS	Safety Requirements Specification.
STF	Standard (NON-safety) Function.
SMR	Station Master Room.
SW or S/W	Software.
SysML	System Modeling Language.
UML	Unified Modeling Language.
UPS	Un-interruptible Power Supply.
VDU	Visual Display Unit.
WAN	Wide Area Network.
WBACS	Wayside Building Automation Control System.

2 History of Revisions

2.1 Revision A

2.1.1 List of Changes

First issue of this document, then no list of changes is defined.

Table 2-1 – Revision A – List of Changes

Item #	Reference	Remark / Question / Deficiency	Response	Changed Sections
RA.01	None.	None.	None.	None.

2.1.2 List of Open Issues

First issue of this document, then no list of open issues is defined.

Table 2-2 – Revision A – List of Open Issues

Item #	Reference	Remark / Question / Deficiency	Response
OA.01			

2.1.3 Verification Report

Table 2-3 – Revision A – Verification Report

Item #	Reference	Verification Description	Result
VA.01	VD.01	• All SIFs, defined in this document have been addressed in the VD.01 document. No further SIFs are necessary for detection and reaction to subsystem faults / errors.	Success.

3 Subsystem’s Purpose and Scope

3.1 Subsystem’s Overview and Purpose

The CBACS Safe subsystem is the safety-related HMI layer of the main Building Automation Control System (BACS).

Its purpose is to allow relevant operators to monitor and, where applicable, command building automation equipment, involved in safety functions, located in the stations, tunnels and along the railway.

The building automation equipment involved in safety functions can be grouped in the two below listed types:

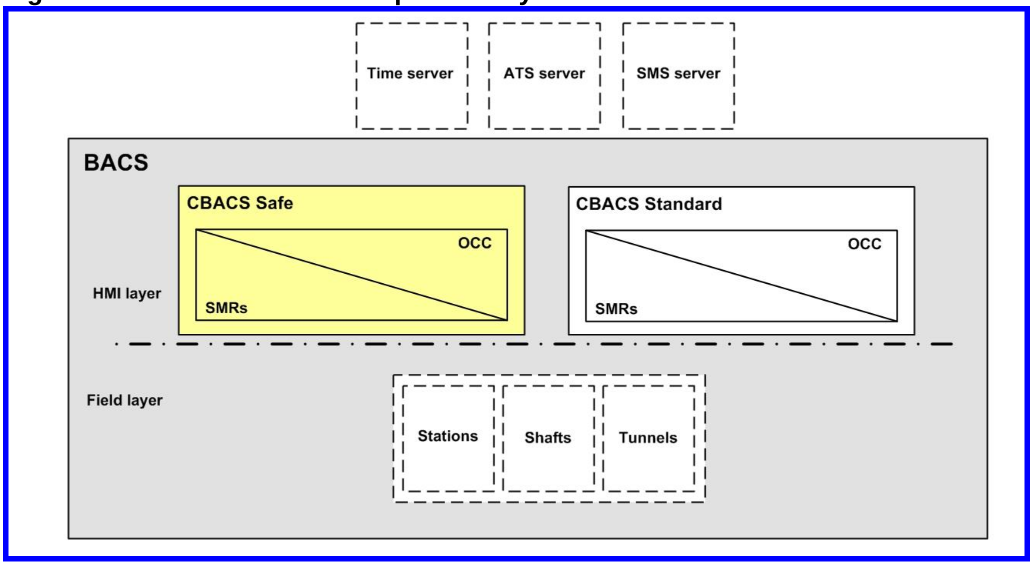
- Fire detection (**FD**);
- Emergency ventilation (**EV**) – exhaust fans, over-track exhaust fans, supply air fans, blast shaft fans, jet fans.

Equipment not involved in safety functions are not controlled by CBACS Safe but from CBACS (Standard) subsystem; this guarantees separation of safety-related subsystems and functions from non safety-related systems.

The **Figure 3-1** shows the main groups and layers of BACS, with its partitions in:

- Human Machine Interface layer (HMI layer), thus the CBACS Safe;
- Field layer, composed by PLCs and all relevant components (FieldPLCs), directly controlling plant equipment.

Figure 3-1 – CBACS Main Groups and Layers



The field layer (thus FieldPLCs) is not in the scope of this safety concept (represented in the **Figure 3-1** by dashed lines).

The CBACS Safe is composed by workstations installed at the OCC and in the SMRs; on each workstation runs the HMI application, which:

- Communicates data with FieldPLCs, in monitoring and command direction;
- Provides a set of interactive graphic screens (the GUI), which allows the operator to execute the monitoring and command functions of plant equipment.

The CBACS Safe, in addition to communicating with FieldPLCs, also communicates with three external systems (represented in the **Figure 3-1** by dashed lines):

- Security Management System (SMS) server PC; CBACS Safe sends to it alarm messages, including and EV equipment alarms, both stations and tunnels;
- Signalling System, in particular the Automatic Train Supervision (ATS) server PC; CBACS Safe receives from it train-board alarm messages (including fire alarms) and train position information (track identification code, where train positioned);
- Clock Synchronization & Time Distribution System (CSTD), in particular the Time server; CBACS Safe requests and receives from it date & time messages for its time synchronization.

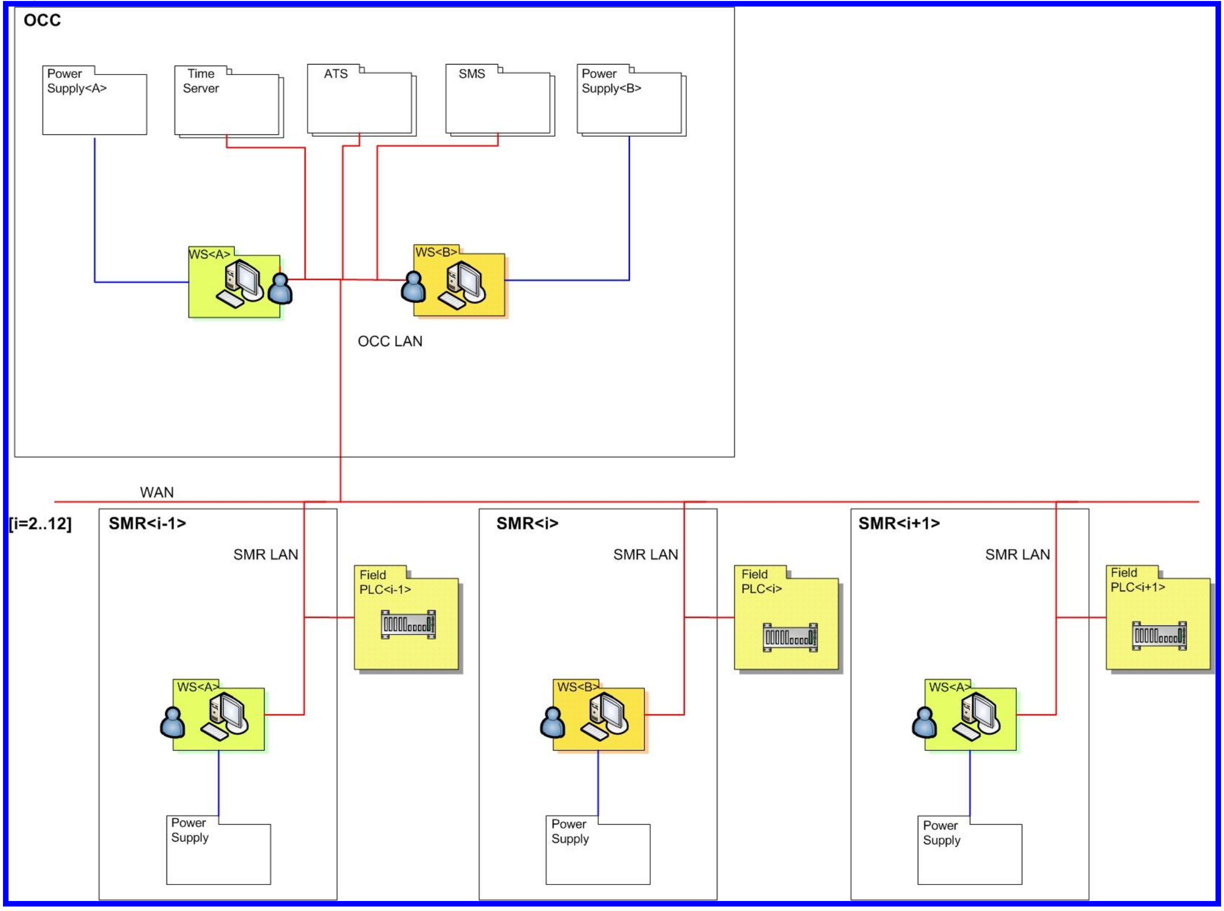
Notice that, ATS alarms and time synchronization messages, in a next system level variant, could also be indirectly received from FieldPLC.

3.2 Subsystem’s Scope

The CBACS Safe subsystems is deployed at the OCC and in the 13 (thirteen) SMRs.

The **Figure 3-2** shows all subsystem’s interfaces, then its parts and external systems, including power supply inputs also:

Figure 3-2 – CBACS Safe Parts



The couple of CBACS Safe workstations at the OCC are fed by different power supplies and are connected to the OCC LAN, so that, they are able to directly communicate with the three external systems (Time server, SMS server PC and ATS server PC) connected on the same LAN.

The communication between workstation at the OCC and the FieldPLC of a station <i> is physically supported by WAN infrastructure.

The WAN supports the communication between the FieldPLC of the station <i> with the FieldPLC of the adjacent stations <i-1> (previous station) and <i+1> (next station).

The LAN that are present in each site (OCC LAN, station LANs, depot LAN) are completely interconnected via WAN.

The CBACS Safe workstation in the SMR is fed by local station power supply and is connected to the station LAN, so that, it's able to directly communicate with the FieldPLC, "independently" to the OCC CBACS Safe; at last it can communicate, through the WAN, with the three external systems (Time server, SMS server PC and ATS server PC).

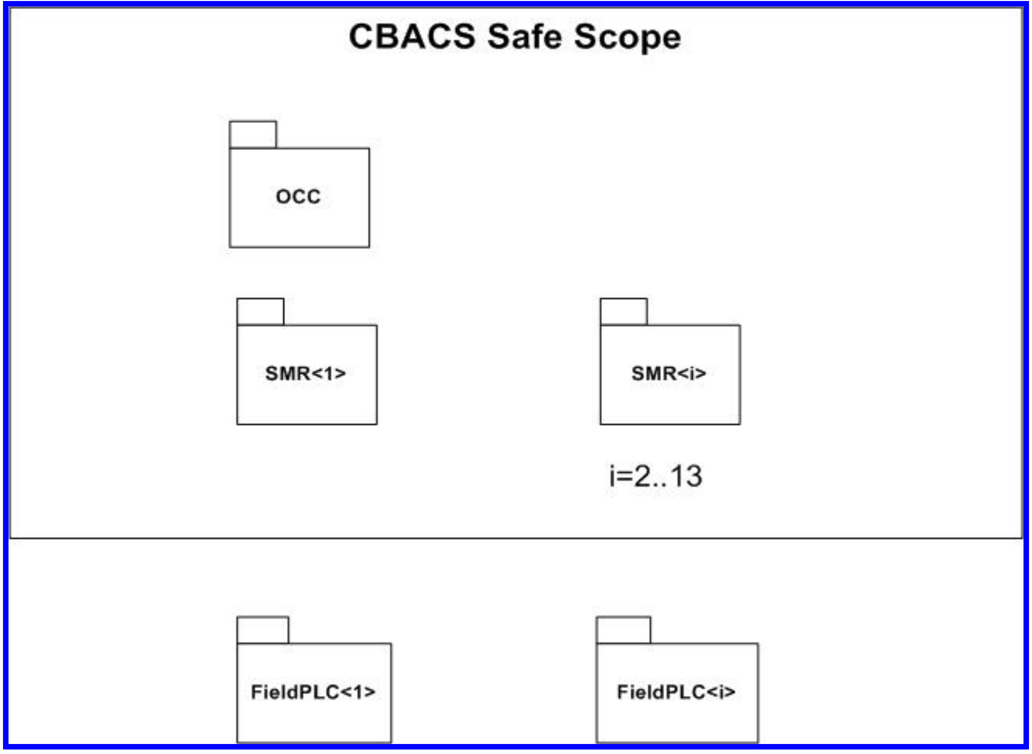
The workstation in the SMR allows the operator to locally execute the monitoring and command functions of plant equipment in case of WAN or OCC failures also.

Moreover, because the FieldPLC of the station <i> allows the SMR workstation to access to the FieldPLCs of the two linked adjacent stations (<i-1> and <i+1>), thus the workstation in the SMR allows the operator to execute the monitoring and command functions of plant equipment of the two linked adjacent stations.

Considering **Figure 3-2**, we define the scope of the safety system being the CBACS Safe.

The next **Figure 3-3** shows the OCC and SMR<i> (for 2 ≤ i ≤ 13) composing the CBACS Safe are in the scope of the present safety concept while the FieldPLCs are not.

Figure 3-3 – CBACS Safe Scope



It is worth nothing that we assume a safety protocol communication between CBACS Safe and the FieldPLCs.

4 Safety Properties

All safety requirements of CBACS Safe are specified in the safety requirements specification document (**ID.01**).

4.1 Summary of Safety Properties

Table 4-1 – Summary of Safety Properties

SIL (IEC 61508)	See safety functions (SFF) in par. 5.5.2 and 5.8.2.
Safety Mode of Operation	Low demand mode.
Safety Related Input	Principal input types: Operator (keyboard and mouse, or touch-screen); Safety Protocol; SafePanel key-switch, push-button and photo-resistors. SafePLC digital inputs.

Safety Related Output	Principal output types:
	Visual Display Unit (VDU), buzzer (speaker);
	Safety Protocol;
	SafePanel LED-lamps;
	SafePLC digital outputs.

Safety Related Interfaces	Principal communication interface(s): Safety Protocol.
Type of Subsystem (IEC 61508)	Type B – complex.
Hardware Fault Tolerance	Minimum HFT = 1.
Architecture	1oo2D for each site (OCC or SMRs), 1oo4D for the whole system (OCC and SMRs), diagnosed by presence of SafePLCs (see par. 5.5.3 and 5.8.3).
Mean Time To Restoration (MTTR)	≤ 8 hours.
Safe Failure Fraction (SFF)	60%.
Test Cycle Time Ranges for Runtime Tests (normal operation)	Tests are done at: 1/ Normal operation; 2/ Cyclically. See SIFs at par. 5.5.2, 5.5.4, 5.5.6, 5.8.2, 5.8.4 and 5.8.6.

4.2 General Safe and Dangerous States

CBACS Safe has not a fail-safe state, but it is rather a fail-operational system.

In case of detected non correct working, CBACS Safe shall:

- Inhibit execution of incorrect commands by SafePLC;
- Inform operators about malfunctioning by SafePanel.

The following CBACS Safe components are to execute the safety functions:

- OCC workstations, SafePLC and FieldPLC;

or

- SMR workstations, SafePLC and FieldPLC.

Dangerous states (undetected malfunctioning that leads to the inability of executing safety functions on demand) of CBACS Safe are:

- Inability to properly execute monitoring and command safety functions (see par. 5.5.2 and 5.8.2).

4.3 Installation, Operation and Maintenance Assumptions

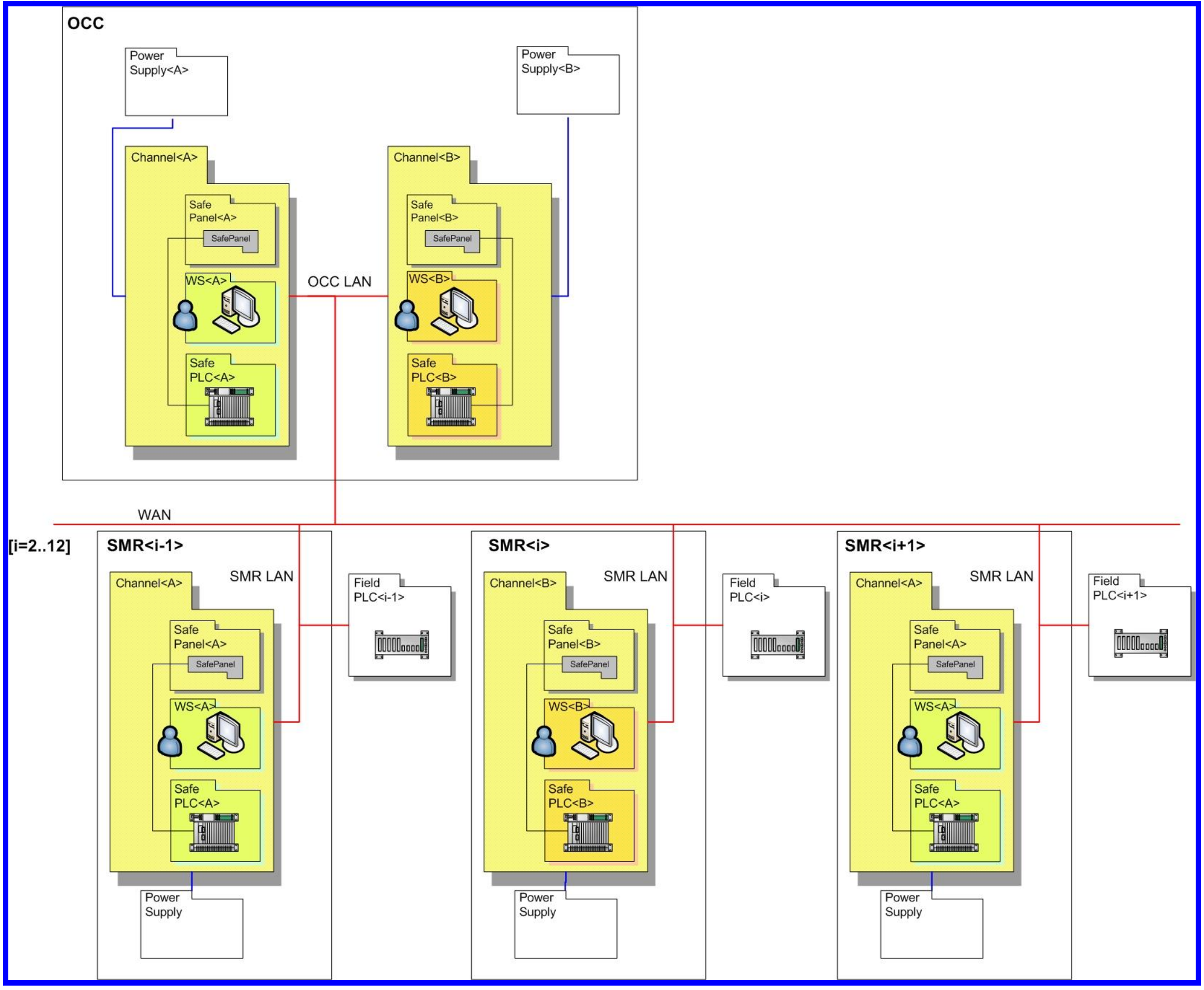
Notice that the Safety Manual will explain all assumptions including installation assumptions to be considered by the user or maintenance / service personnel.

5 Architecture and Functions Description

5.1 Subsystem's Structural View

The safety architecture (static view) of the CBACS Safe subsystems at the OCC and in the SMRs is shown in the **Figure 5-1** below:

Figure 5-1 – CBACS Safe Architecture



Comparing the safety architecture with the previous **Figure 3-2** is possible to notice the additional components named SafePLC and SafePanel. Their functions are defined in the next paragraphs.

5.2 Functions' Coding Rules

Before starting with functional description of CBACS Safe items, this paragraph defines the coding rules applied to the relevant functions.

The functions are uniquely identified by code which is based on the format below described:
CBACSS.<location code>**.**<function class>**.**<function acronym>

The applicable location codes are:

- **OCC** for Operation Control Centre;
- **SMR** for Station Master Room;
- **ALL** for both Operation Control Centre and Station Master Room.

The functions classes are:

- Safety Functions, **SFF**;
- Safety Integrity Functions (Measures), **SIF**.

The function acronym will be a string, having 12 characters maximum length.

5.3 OCC Architecture

The OCC CBACS Safe architecture, shown in **Figure 3-2**, is based on **dual channel with diagnostic** architectural pattern (1oo2D).

Both channels can independently execute the same functions (peer channels) and, for this specific implementation of the pattern, the below listed rules have been applied:

- Both channels are made up the same number of components;
- Each component of a channel have correspondent, on the peer channel, which executes the same function(s);
- Each channel have its own fault detection and reaction components (the D-components), which have the same hardware and software implementation both channels;
- Corresponding components of both channels, except D-components, have diverse hardware and software implementation.

Then, both channels and peer components **implement the same safety requirements specification** but, to reduce hardware common cause failures and systematic failures, diversity measures have been applied between corresponding hardware and software components (except D-components).

For each channel, the main components and relevant functions are below described:

- **Workstation**. It provides the HMI which allows the operator to execute the safety monitoring and command functions. It's made up by one Industrial PC (IPC) equipped with network interface card, graphic card, audio card, visual display unit (VDU), keyboard and mouse (or touch-screen). The workstation alone is an "unsafe" component, which hardware faults and software errors need to be detected.
- **SafePLC**. It's the required "safe" component in the architecture. Executes three main functions:
  - Fault detection of workstation, which consists in **comparison** and **data validation / integrity checks**, applied to data exchanged with workstation;
  - Fault reaction on workstation fault(s) detected which consists in **enabling / disabling of workstation command functions** (using fail-safe characteristic of PLC) and **activation / de-activation of signalisations** to subsystem's operator (through the SafePanel);
  - Communication mediator between workstation and FieldPLC. Thus, acts as data filter which **avoids** (a) workstation command sending without data validation / integrity checks and (b) workstation visualization of incorrect data without error signalisation.
- **SafePanel**. It's the auxiliary hardware component, directly controlled by SafePLC (through I/O modules) which provides signalisations and control facilities, to subsystem's operator. It has to be used in combination with the HMI to support successful execution of safety monitoring and command functions. It's made up by set of LED-lamps, one key-switch, one push-button and a number of photo-resistors.

In case of workstation fault(s) detected by SafePLC, the operator realizes anomaly condition by SafePanel indications and moves the other workstation to continue execution of safety monitoring and command functions.

Diversity measures between both channels are in workstations components, which have different IPC, VDU and software implementation. Whilst, both channels' D-components:

- SafePLCs have the same hardware and software implementation;
- SafePanel have the same hardware implementation.

Diversity measures within each channel have also been applied; in fact, SafePLC and SafePanel are different to the relevant workstation, in terms of hardware and software implementation.

Even though diversity measures have been defined in implementation, it's here important to specify that HMI layout has to be the same both workstations, including graphic objects properties (form, position, dimension) and behaviour (colouring rules); this measure allows operator to independently use one of both channels, without addition of potential operator errors deriving from use of a dual HMI (such as error of cognition, perception, decision, omission, timing and inadequacy).

Measures against communication threats between architecture's components have been applied by adoption of safety protocols; in particular:

- SafePLC and relevant I/O modules communicate by CIP Safety over EtherNet/IP (**ST.07**). CIP Safety is certified for applications up to SIL 3, according to IEC615F8 standard.
- SafePLC and relevant workstation communicate by specifically implemented safety protocol over EtherNet/IP (SafeCommLayer), where SafePLC and workstation respectively act as TCP server and TCP client. It's based on EtherNet/IP standard messaging (**ST.06**) but adds it measures against communication threats, according to EN50159:2010. The applied measures are additional message's fields (as minimum: sequence number, timestamp, source and destination identifiers, control & status data, hash code), specific data exchange sequences and specific data check procedures.
- SafePLC and FieldPLC communicate by SafeCommLayer.

Finally, communication interfaces between OCC CBACS Safe and external subsystems at the OCC are below listed:

- OCC CBACS Safe (through SafePLC) and OCC SMS communicate by EtherNet/IP standard messaging (**ST.06**).
- OCC CBACS Safe (through SafePLC) and OCC ATS communicate by SafeCommLayer.

5.4 OCC Functional Requirements

Acquire the state changes of individual emergency ventilation equipment and show to the operator	
Input:	State changes of emergency ventilation equipment (received from FieldPLC).
Output:	Visual notification to the operator.
Description/Behavior:	The OCC CBACS Safe shall acquire the state of changes of the emergency ventilation equipment from the FieldPLCs and provide a visual notification to the operator, to allow the management of the emergency ventilation equipment

	accordingly.
Safe State/Reaction:	Visual notification to the operator and disabling of the command.
Operating mode:	Normal operation.
SIL:	2

Acquire the fire detection alarm and show to the operator	
Input:	Fire detection alarm (received from FieldPLC).
Output:	Visual notification to the operator.
Description/Behavior:	The OCC CBACS Safe shall acquire the alarm of fire detection from the FieldPLC and provide a visual notification to the operator, to allow the management of the emergency ventilation equipment accordingly.
Safe State/Reaction:	Visual notification to the operator and disabling of the command.
Operating mode:	Normal operation.
SIL:	2

Provide the command to the FieldPLC for the emergency ventilation equipment	
Input:	Command request of the operator.
Output:	Command to the FieldPLCs.
Description/Behavior:	The OCC CBACS Safe shall provide the command to the FieldPLCs to perform the emergency ventilation equipment action requested by the operator.
Safe State/Reaction:	Visual notification to the operator and disabling of the command.
Operating mode:	Normal operation.
SIL:	2

Provide the command to the FieldPLC to execute a scenario of emergency ventilation equipment	
Input:	Command request of the operator.
Output:	Scenario command to the FieldPLCs.
Description/Behavior:	The OCC CBACS shall provide the command to the FieldPLCs to execute the emergency ventilation equipment scenario requested by the operator.
Safe State/Reaction:	Visual notification to the operator and disabling of the command.
Operating mode:	Normal operation.
SIL:	2

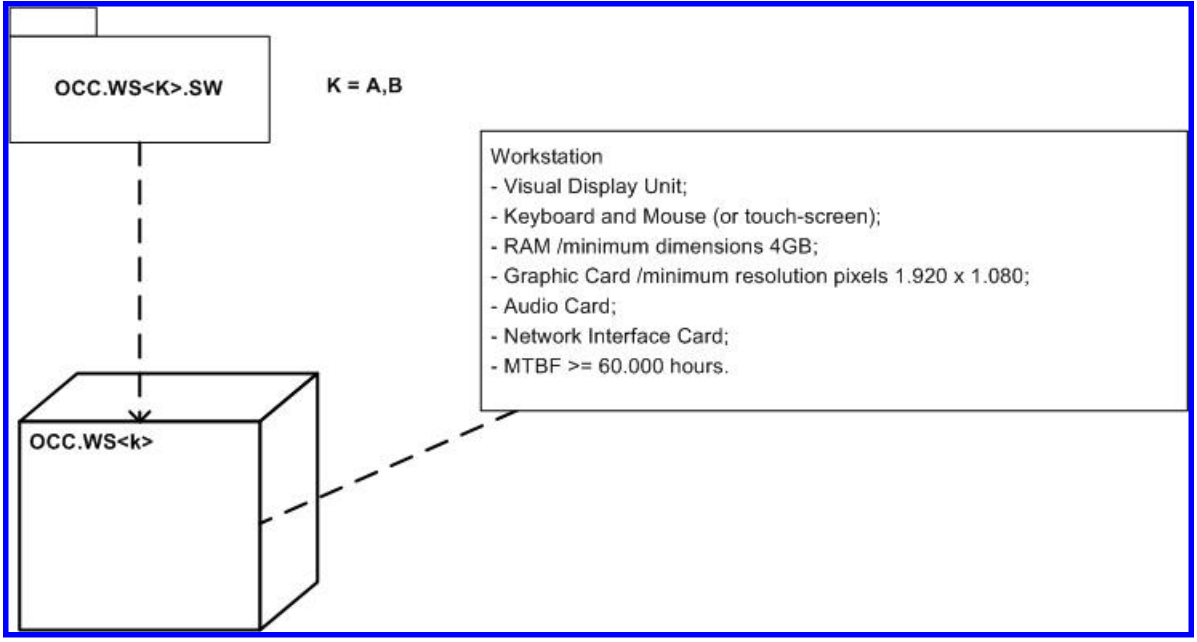
5.5 OCC Components Description

5.5.1 Workstations' Components

This paragraph describes WS<A> (first channel) and WS<B> (second channel) components.
The workstations have different hardware (IPC and VDU), operating system and SW application framework. In term of HW reliability parameters, workstations has MTBF >= 60.000 hours.

In **Figure 5-2** the UML diagram is showing the deployment of the software package OCC.WS<k>.SW (the whole software to be executed) on the hardware node OCC.WS<k>, where k = A or B. The UML diagram is also showing the main hardware features of the OCC.WS<k> node.

Figure 5-2 – Deployment of OCC Workstation SW (OCC.WS<k>.SW) on WS Hardware


OCC.WS<K>.SW
K = A,B
Workstation
- Visual Display Unit;
- Keyboard and Mouse (or touch-screen);
- RAM /minimum dimensions 4GB;
- Graphic Card /minimum resolution pixels 1.920 x 1.080;
- Audio Card;
- Network Interface Card;
- MTBF >= 60.000 hours.
OCC.WS<k>

On WS<A>'s Industrial PC basically runs:

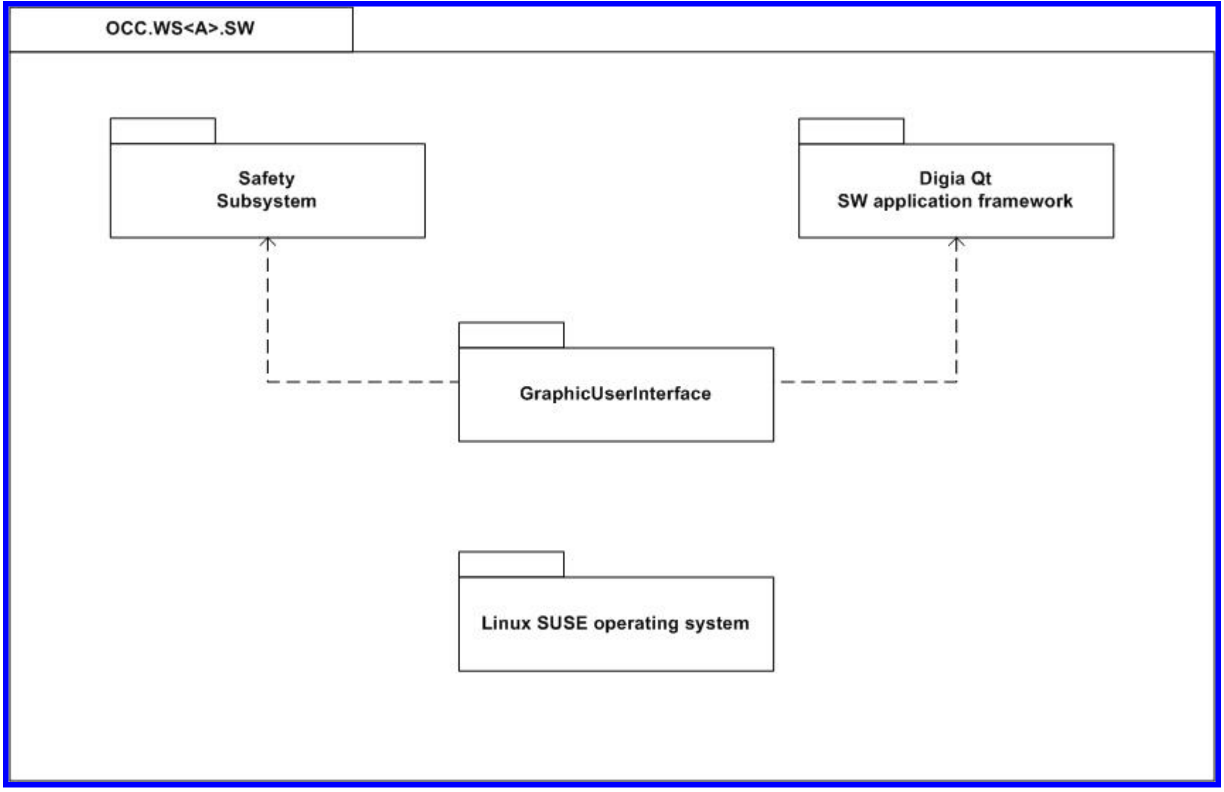
- **Linux SUSE** operating system;
- **Digia Qt** SW application framework.

On WS<B>'s Industrial PC basically runs:

- **Microsoft Windows 7** operating system**;**
- **Microsoft .Net** SW application framework.

The next **Figure 5-3** shows the main architectural software packages of OCC Workstation<A>.

Figure 5-3 – OCC Workstation<A> SW Packages

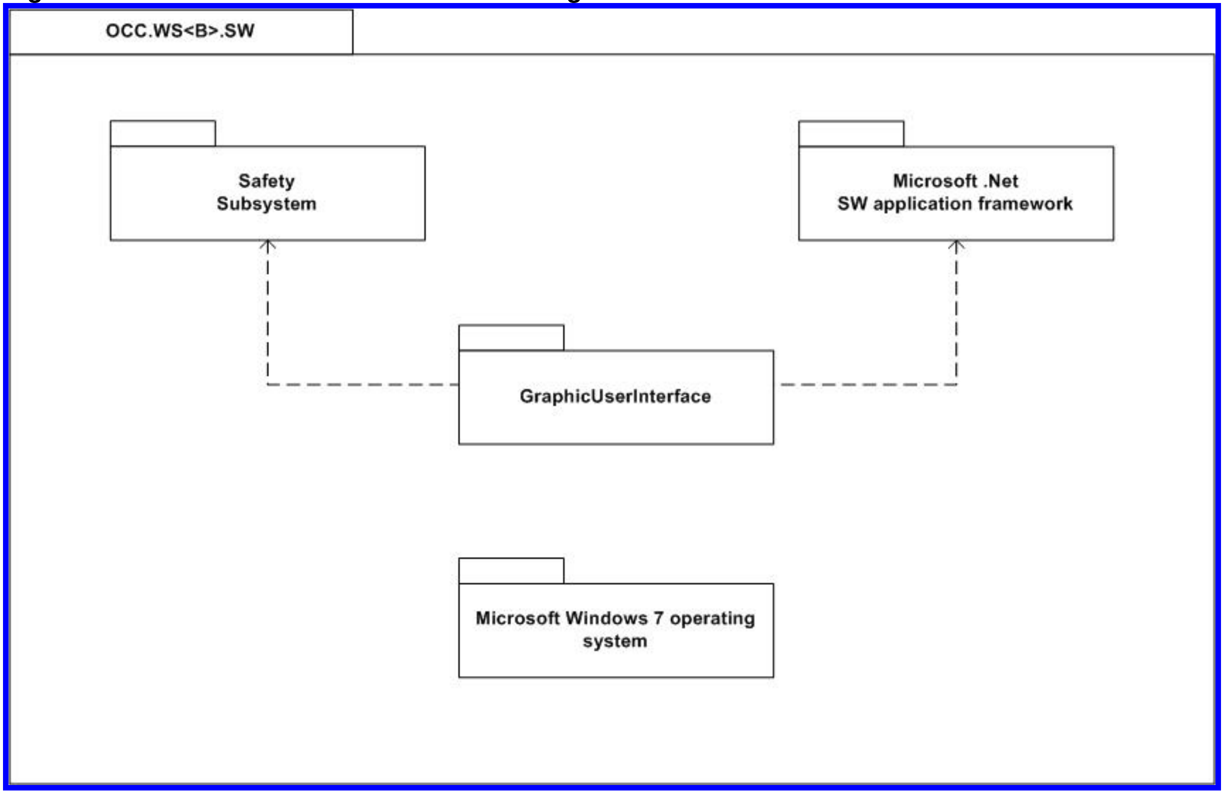

OCC.WS<A>.SW
Safety Subsystem
Digia Qt SW application framework
GraphicUserInterface
Linux SUSE operating system

Over **Linux SUSE** operating system and **Digia Qt** SW application framework there are two additional packages:

- GraphicUserInterface: It's the set of interactive graphic screens and related objects, which allows the operator to execute the safety monitoring and command functions. It includes an event handling module which defines, for a limited set of detectable events (e.g. mouse-clicked, key-pressed), the specific behaviour of graphic objects (e.g. background colour change) or other actions to do.
- Safety Subsystem: is the group of all modules that guarantee the safety of OCC CBACS Safe. It's described in detail at par. 5.9.

The next **Figure 5-4** shows the main architectural software packages of OCC Workstation<B>.

Figure 5-4 – OCC Workstation<B> SW Packages


OCC.WS<B>.SW
Safety Subsystem
Microsoft .Net SW application framework
GraphicUserInterface
Microsoft Windows 7 operating system

Also here, over **Microsoft Windows 7** operating system and **Microsoft .Net** SW application framework there are two additional packages:

- GraphicUserInterface: It's the set of interactive graphic screens and related objects, which allows the operator to execute the safety monitoring and command functions. It includes an event handling module which defines, for a limited set of detectable events (e.g. mouse-clicked, key-pressed), the specific behaviour of graphic objects (e.g. background colour change) or other actions to do.
- Safety Subsystem: is the group of all modules that guarantee the safety of OCC CBACS Safe. It's described in detail at par. 5.9.

5.5.2 OCC Channel A/B Workstation Functional Requirements

OCC WS Monitor State Changes of EV Equipment [Id: CBACSS.OCC.SFF.MON_EV_STS]	
Input:	State changes of emergency ventilation equipment (received from FieldPLC).
Output:	Signals to the VDU.
Description/Behavior:	The Workstation of the OCC Channel A/B shall acquire the state changes of emergency ventilation equipment from the FieldPLCs via EtherNet/IP and shall show it to the operator. The safety function is base on two steps: 1) The OCC WS collects state changes information (digital inputs) of emergency ventilation equipment from the FieldPLC of the involved station. 2) The OCC WS GUI screens show the collected information to the operator.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MON_EV_STS

OCC WS Monitor Alarms of FD Equipment [Id: CBACSS.OCC.SFF.MON_FD_ALM]	
Input:	Fire alarm (received from FieldPLC).
Output:	Signals to the VDU.
Description/Behavior:	The Workstation of the OCC Channel A/B shall acquire the fire detection from the FieldPLCs via EtherNet/IP and shall show it to the operator. The safety function is base on two steps: 1) The OCC WS collects fire alarm information (digital inputs) of fire detection equipment from the FieldPLC of the involved station. 2) The OCC WS GUI screens show the collected information to the operator.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MON_FD_ALM

OCC WS Command State Changes of EV Equipment [Id: CBACSS.OCC.SFF.CMD_EV_IND]	
Input:	ID of the pressed button. Back-computed graphic information (from graphic inverter). Results of signal validity from SafePLC.
Output:	Command signal (to the SafePLC).
Description/Behavior:	The workstation shall acquire the request from the button pressed by the operator and shall transmit the associated command to the FieldPLCs via EtherNet/IP, in order to control the emergency ventilation equipment. The safety function is based on five steps below listed: 1) The OCC WS operator receives fire alarm information from the FieldPLC. 2) The operator opens the GUI screen of involved station. 3) The operator from the GUI screen can push the command button to send a command towards individual emergency ventilation equipment. 4) The operator from the GUI screen has to push a Confirm or a Cancel button to respectively send or abort the command to the FieldPLC. 5) The FieldPLC sends to the operator the execution feedbacks for the scenario command, then “command started”, “command failed”, “command timed-out”, “command succeeded”. The command can be sent out to the FieldPLC only after the command validation of the SafePLC.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.CMD_EV_IND

OCC WS Command Scenario of EV Equipment [Id: CBACSS.OCC.SFF.CMD_EV_SCN]	
Input:	ID of the pressed button. Back-computed graphic information (from graphic inverter). Results of signal validity from SafePLC.
Output:	Command signal (to the SafePLC).
Description/Behavior:	The workstation shall acquire the request from the button pressed by the operator and shall transmit the associated command to the FieldPLCs via EtherNet/IP, in order to control the emergency ventilation equipment. The safety function is based on six steps below listed: 1) The OCC WS operator receives fire alarm information from the FieldPLC. 2) The operator opens the GUI screen of involved station. 3) The GUI screen highlights the suggested scenario command to the operator, e.g. by changing colour of a shape near to the suggested command button. 4) The operator from the GUI screen can push the suggested scenario command button or a different scenario command. 5) The operator from the GUI screen has to push a Confirm or a Cancel button to respectively send or abort the scenario command to the FieldPLC. 6) The FieldPLC sends to the operator the execution feedbacks for the scenario command, then “command started”, “command failed”, “command timed-out”, “command succeeded”. The command can be sent out to the FieldPLC only after the command validation of the SafePLC.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.CMD_EV_SCN

OCC WS Diverse Redundancy [Id: CBACSS.OCC.SIF.ARC_DR_WKS]	
Input:	-
Output:	-
Description/Behavior:	Workstation in OCC has dual redundancy that tolerates the failure of one WS to keep the safety functions executable on demand. In fact, at the OCC are present two workstations WS<A> and WS<B>. Moreover, at the OCC, WS have diverse hardware (IPC and VDU) and software implementation (operating system and SW application framework) of the same safety requirements specification. Finally, at the OCC, WS<A> and WS<B> are fed by different power lines. In case of workstation fault(s) detected by SafePLC, the operator realizes anomaly condition by SafePanel indication and moves the other workstation to continue execution of safety monitoring and command functions.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.ARC_DR_WKS

OCC WS Commands Proof-Test [Id: CBACSS.OCC.SIF.CMD_PT_WKS]	
Input:	-
Output:	-
Description/Behavior:	Periodically (e.g. every 1 year) operator has to send a command to FieldPLC for execution of safety functions **CBACSS.OCC.SFF.CMD_EV_IND** and **CBACSS.OCC.SFF.CMD_EV_SCN**.
Safe State/Reaction:	-
Operating mode:	Cyclically.
SIL:	-

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.CMD_PT_WKS

OCC Operator Periodic Test of VDU [Id: CBACSS.OCC.SIF.MNT_MD_VDU]	
Input:	-
Output:	-
Description/Behavior:	Periodically (e.g. every 6 months) operator has to test VDU components by visual inspection. Thus, it has to: 1) Set the key-switch KeySwEnablingDisabling in “Disable” position (workstation commands are disabled). 2) Access to the “Test Page” on GraphicUserInterface. 3) Push the “Test VDU” button on GraphicUserInterface, which change colour of VDU screen following several test patterns, e.g. all red, all green and all blue (with exception of a limited control area).
Safe State/Reaction:	Replacement of the VDU with a working one.
Operating mode:	Cyclically.
SIL:	-

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MNT_MD_VDU

5.5.3 SafePLCs' Components

This paragraph describes SafePLC<A> and SafePLC<B> components, which are equal both channels.

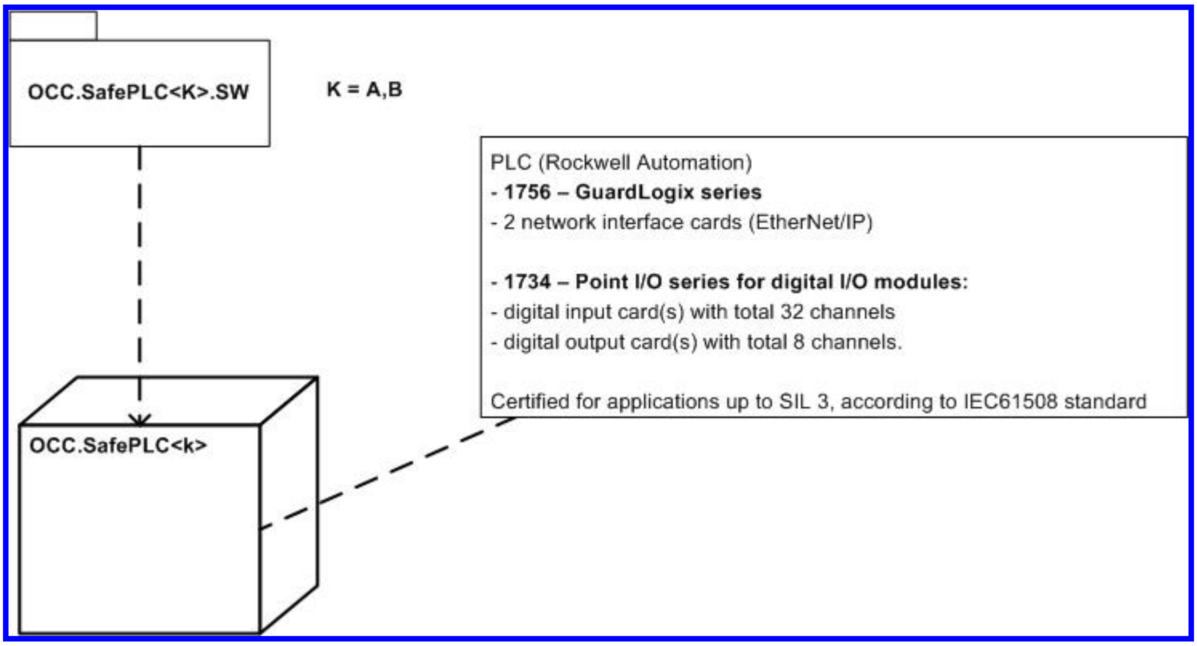
Both SafePLCs are **fail-safe** and are based on **Rockwell Automation** products series below listed:

- GuardLogix series (1756);
- Point I/O series (1734), for digital and analogue I/O modules.

These product series are certified for applications up to SIL 3, according to IEC61508 standard.

In **Figure 5-5** the UML diagram is showing the deployment of the software package OCC.SafePLC<k>.SW (the whole software to be executed) on the hardware node OCC.SafePLC<k>, where k = A or B. The UML diagram is also showing the main hardware features of the OCC.SafePLC<k> node.

Figure 5-5 – Deployment of OCC SafePLC SW (OCC.SafePLC<k>.SW) on SafePLC Hardware



PLC (Rockwell Automation)
- **1756 – GuardLogix series**
- 2 network interface cards (EtherNet/IP)

- **1734 – Point I/O series for digital I/O modules:**
- digital input card(s) with total 32 channels
- digital output card(s) with total 8 channels.

Certified for applications up to SIL 3, according to IEC61508 standard

Notice: The choice of Rockwell Automation products is justified to simplify interoperability with FieldPLC, which use Rockwell Automation products also, then EtherNet/IP communication protocol. It allows implementation of safety protocol over EtherNet/IP (SafeCommLayer).

The SafePLC is equipped with:

- One CPU, with safety diagnostic unit;
- Two network interface cards (EtherNet/IP), one for data exchanging with workstation the second for data exchanging with FieldPLC and external subsystems (ATS and SMS).
- One (or more depending on modularity) digital input card with total 32 channels;
- One (or more depending on modularity) digital output card with total 8 channels.

Using of two network interface cards guarantees “data filtering” function of SafePLC; in fact, workstation is physically separated from FieldPLC and external subsystems.

In case the SafePLC is un-powered, the failure shall be notified to the Operator through the SafePanel. The notification shall be a lamp or an audio buzzer.

Table 5-1 – SafePLC I/O Signals List

Channel#	Digital Input	Digital Output	Description
DO.0		**X**	SafePanel, lighting-on red lamp IndLampFailed.
DO.1		**X**	SafePanel, lighting-on green lamp IndLampRun.
DO.2		**X**	SafePanel, lighting-on red lamp IndLampDisabled.
DO.3		**X**	SafePanel, lighting-on green lamp IndLampEnabled.
DO.4		**X**	Output 1 for disabling flag of workstation command.
DO.5		**X**	Output 2 for disabling flag of workstation command.
DO.6		**X**	Free spare available.
DO.7		**X**	Free spare available.
DI.0	**X**		SafePanel, Line 1 photo-resistor 1.
DI.1	**X**		SafePanel, Line 1 photo-resistor 2.
DI.2	**X**		SafePanel, Line 1 photo-resistor 3.
DI.3	**X**		SafePanel, Line 1 photo-resistor 4.
DI.4	**X**		SafePanel, Line 1 photo-resistor 5.
DI.5	**X**		SafePanel, Line 1 photo-resistor 6.
DI.6	**X**		SafePanel, Line 1 photo-resistor 7.
DI.7	**X**		SafePanel, Line 1 photo-resistor 8.

Channel#	Digital Input	Digital Output	Description
DI.8	**X**		SafePanel, Line 2 photo-resistor 1.
DI.9	**X**		SafePanel, Line 2 photo-resistor 2.
DI.10	**X**		SafePanel, Line 2 photo-resistor 3.
DI.11	**X**		SafePanel, Line 2 photo-resistor 4.
DI.12	**X**		SafePanel, Line 2 photo-resistor 5.
DI.13	**X**		SafePanel, Line 2 photo-resistor 6.
DI.14	**X**		SafePanel, Line 2 photo-resistor 7.
DI.15	**X**		SafePanel, Line 2 photo-resistor 8.
DI.16	**X**		SafePanel, Line 3 photo-resistor 1.
DI.17	**X**		SafePanel, Line 3 photo-resistor 2.
DI.18	**X**		SafePanel, Line 3 photo-resistor 3.
DI.19	**X**		SafePanel, Line 3 photo-resistor 4.
DI.20	**X**		SafePanel, Line 3 photo-resistor 5.
DI.21	**X**		SafePanel, Line 3 photo-resistor 6.
DI.22	**X**		SafePanel, Line 3 photo-resistor 7.
DI.23	**X**		SafePanel, Line 3 photo-resistor 8.
DI.24	**X**		SafePanel, “Disable” position by Key-switch KeySwEnablingDisabling.
DI.25	**X**		SafePanel, “Enable” position by Key-switch KeySwEnablingDisabling.
DI.26	**X**		SafePanel, “Failure Reset” pressed by Push-button PushBtnReset.
DI.27	**X**		Feedback 1 for disabling flag of workstation command.
DI.28	**X**		Feedback 2 for disabling flag of workstation command.
DI.29	**X**		Free spare available.
DI.30	**X**		Free spare available.
DI.31	**X**		Free spare available.
DI.32	**X**		Free spare available.

5.5.4 OCC Channel A/B SafePLC Functional Requirements

OCC Diversity between WS and SafePLC [Id: CBACSS.OCC.SIF.ARC_DD_WKS]	
Input:	-
Output:	-
Description/Behavior:	Workstation in OCC has its own SafePLC, which is the diagnostic monitoring unit of workstation. One of SafePLC functions is fault detection of workstation, which consists in comparison and data validation / integrity checks, applied to data exchanged with workstation. As per “diverse monitor techniques”, required by IEC61508 standard, SafePLC implements separation between the monitor computer and the monitored computer (workstation). SafePLC, is the monitoring channel is certified for applications up to SIL 3, according to IEC61508 standard.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.ARC_DD_WKS

OCC SafePLC Automatic Fault Detection for WS Command [Id: CBACSS.OCC.SIF.CMD_AD_WKS]	
Input:	ID of the pressed button. Back-computed graphic information (from graphic inverter).
Output:	Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the signals provided by the workstation each time a button is pressed. When operator has to send a command to FieldPLC it pushes a command button from the GUI screen; thus two information are sent to the SafePLC: 1) The command unique identifier (integer number), associated to the pressed command button. 2) The back-computed graphic information, detected by GraphicInverter, relevant to colour changing of pressed button. The SafePLC compares the two information above listed and, if differs, SafePLC itself reacts disabling workstation command functions and activating signalisations to operator (through the SafePanel). A retry mechanism could be applied to avoid disabling workstation command on transient faults.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.CMD_AD_WKS

OCC SafePLC Automatic Fault Detection for WS Monitoring [Id: CBACSS.OCC.SIF.MON_AD_WKS]	
Input:	Requested information (state changes or fire detection). Message received from the FieldPLCs. Back-computed graphic information (from graphic inverter).
Output:	Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the notification performed by the workstation to the operator. After the plant data transmission from SafePLC to WS, the GraphicInverter software component, running on the workstation, accesses to graphic card's memory, through related application programming interfaces (APIs), and back-computes the received graphic information in a message to be sent to the SafePLC (through SafeCommunicator). The SafePLC compares this message with the plant data sent from SafePLC and, if they're different, SafePLC itself reacts disabling workstation command functions and activating signalisations to operator (through the SafePanel), turning off the IndLampRun and turning on the IndLampFailed.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MON_AD_WKS

OCC SafePLC to FieldPLC Safety Protocol [Id: CBACSS.OCC.SIF.IFC_SP_SPC]	
Input:	Message received from the FieldPLCs. Back-computed graphic information (from graphic inverter).
Output:	Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the communication between itself and the FieldPLC, by means of the safety protocol. FieldPLC and SafePLC communicate by safety protocol over EtherNet/IP (SafeCommLayer), where they respectively act as TCP server and TCP client. It's based on EtherNet/IP standard messaging but adds it measures against communication threats, according to EN50159:2010. The applied measures are additional message's fields (as minimum: sequence number, timestamp, source and destination identifiers, control & status data and hash code). The typical (standardized) errors affecting communication are: • Repetition (old and obsolete messages are repeated at an inopportune time causing disturbance at the receiver's end); • Loss (one or more messages are transmitted, but never received; messages are deleted); • Insertion (unexpected messages are introduced in the communication path); • Incorrect sequence (the sending order of messages does not correspond to the reception order); • Corrupted data (the integrity of transmitted data is not preserved; sent data are different from the received ones); • Delay (a message arrives at receiver site with unacceptable delay; the elapse time from sending to receiving is too long); • Erroneous addressing (wrong the receiver of a message was not the intended one). A safety protocol is there to introduce measures able to reinforce a normal communication protocol to avoid the above listed failure. In case the SafePLC detects a failure in the communication the following action shall be performed: - Disable the workstation command; - Turn on the IndLampFailed; - Turn off the IndLampRun.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.IFC_SP_SPC

OCC WS to SafePLC Safety Protocol [Id: CBACSS.OCC.SIF.IFC_SP_WKS]	
Input:	Message received from the WS.
Output:	Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the communication between itself and the Workstation, by means of the safety protocol. SafePLC and workstation communicate by safety protocol over EtherNet/IP (SafeCommLayer), where they respectively act as TCP server and TCP client. It's based on EtherNet/IP standard messaging but adds it measures against communication threats, according to EN50159:2010. The applied measures are additional message's fields (as minimum: sequence number, timestamp, source and destination identifiers, control & status data and hash code). The typical (standardized) errors affecting communication are: • Repetition (old and obsolete messages are repeated at an inopportune time causing disturbance at the receiver's end); • Loss (one or more messages are transmitted, but never received; messages are deleted); • Insertion (unexpected messages are introduced in the communication path); • Incorrect sequence (the sending order of messages does not correspond to the reception order); • Corrupted data (the integrity of transmitted data is not preserved; sent data are different from the received ones); • Delay (a message arrives at receiver site with unacceptable delay; the elapse time from sending to receiving is too long); • Erroneous addressing (wrong the receiver of a message was not the intended one). A safety protocol is there to introduce measures able to reinforce a normal communication protocol to avoid the above listed failure. In case the SafePLC detects a failure in the communication the following action shall be performed: - Disable the workstation command; - Turn on the IndLampFailed; - Turn off the IndLampRun.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.IFC_SP_WKS

OCC SafePLC Automatic Fault Detection for VDU of Workstation [Id: CBACSS.OCC.SIF.MON_AD_VDU]	
Input:	Sequence number from photo resistor.
Output:	Sequence number to WS. Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the VDU, in order to detect fault in the notification to the operator. A number of photo-resistors, each one connected to SafePLC's digital input module, for detection of incorrect alignment of data transmitted from SafePLC and data shown from workstation's VDU. In particular, SafePLC cyclically compares two counters, the first local of SafePLC's (e.g. the sequence number of data transmitted to the workstation) and the second local of workstation and shown on the GraphicUserInterface (e.g. the sequence number of data received from SafePLC). The GraphicUserInterface shows workstation's counter in binary format on eight adjacent little square where photo-resistors are positioned; e.g. white colour square indicates "on", whilst, black colour square indicates "off". When SafePLC compares the two counters, its local and feedback detected from photo-resistors, if they have the same value, then workstation is properly operating, else workstation fault / error is detected from SafePLC, then commands are automatically disabled and IndLampFailed lights-on. To improve reliability of feedback, 3 lines of eight photo-resistors can be used and 2oo3 voting can be executed by SafePLC. Notice that photo-resistors cover a limited area of VDU screen, but is necessary to force refreshing of all GUI's monitoring areas when workstation's counter is updated. Thus, to force workstation's to graphic card's to update VDU screen, each LED-lamps a little changing, not tedious for operator eyes and not interfering with GraphicInverter, updated by new values of workstation's counter. A retry mechanism could be applied to avoid disabling workstation command on transient faults.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MON_AD_VDU

OCC SafePLC Enabling / Disabling of Workstation Commands [Id: CBACSS.OCC.SIF.ARC_DD_DIS]	
Input:	-
Output:	Workstation disables command.
Description/Behavior:	SafePLC, in case of workstation fault(s) detected, as safe reaction, disables workstation command functions, using its fail-safe characteristic. In particular, SafePLC de-energize two its digital outputs channels, which are fed-back in two its digital input channels (for fault tolerance). The digital input channels are the flags that disable the command messages sending towards the FieldPLC. At least on digital input channel has to go “off” to disable workstation command. When fault is cleared SafePLC doesn’t automatically enable workstation command functions, but is necessary push SafePanel’s button PushBtnReset. Digital outputs channels, alternatively, could also de-energize workstation or SafePLC’s network interface card for data exchanging with FieldPLC.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.ARC_DD_DIS

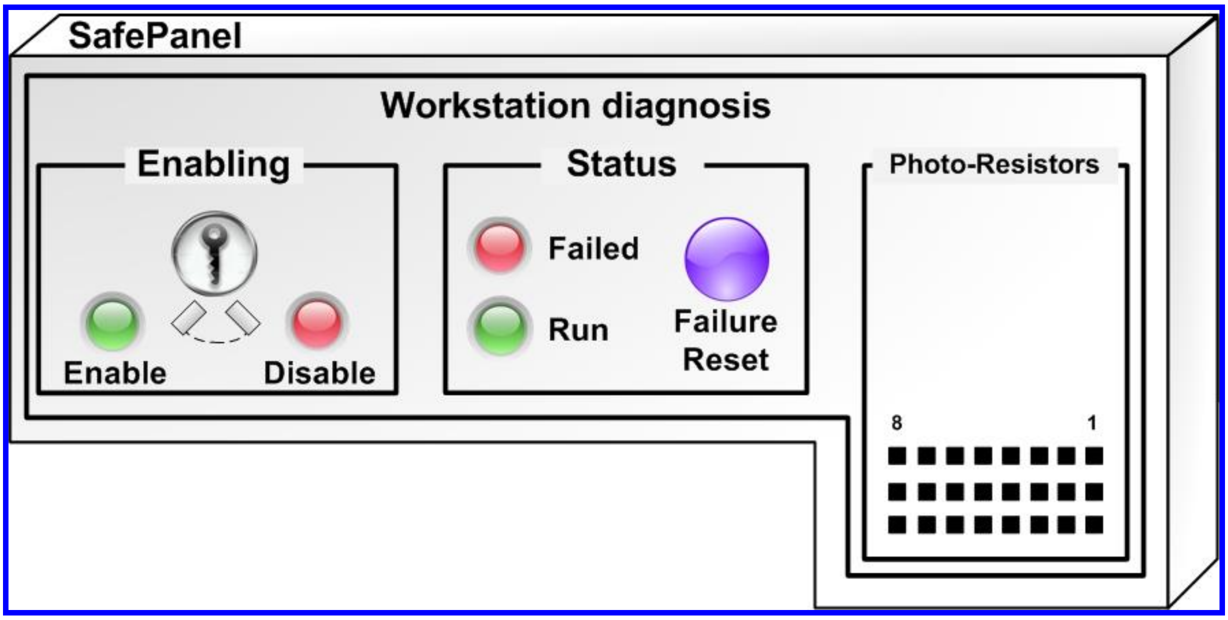
OCC SafePanel Signalisation of Workstation Fault / Error [Id: CBACSS.OCC.SIF.ARC_DD_SPN]	
Input:	-
Output:	Signal to control the IndLampFailed. Signal to control the IndLampRun.
Description/Behavior:	When SafePLC detects workstation fault(s), over to disable workstation command functions, it activates one red lamp IndLampFailed on SafePanel.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.ARC_DD_SPN

5.5.5 SafePanel's Components

This paragraph describes SafePanel's components and next **Figure 5-6** shows the relevant layout.

Figure 5-6 – SafePanel's Layout and Components



It's composed by:

- One red lamp IndLampFailed (see "Failed" in the figure above), which indicates that workstation fault / error has been detected from SafePLC, then commands have been automatically disabled.
- One key-switch KeySwEnablingDisabling, which have to be selected in "Disable" position by operator when workstation fault / error has been detected or maintenance procedures have to be initiated. When it's selected in "Disable" position workstation commands are disabled.
- One red lamp IndLampDisabled (see "Disable" in the figure above), which indicates that workstation fault / error has been detected from operator or maintenance procedures are progressing, then commands have been manually disabled by KeySwEnablingDisabling.
- One green lamp IndLampEnabled (see "Enable" in the figure above), which is complementary to IndLampDisabled, then KeySwEnablingDisabling is selected in "Enable" position.
- One green lamp IndLampRun (see "Run" in the figure above), active only when both IndLampFailed and IndLampDisabled are de-activated, which indicates that workstation is properly operating and then commands are enabled.

- One push-button PushBtnReset (see "Failure Reset" in the figure above), which have to be pressed to restore commands enabling after automatic or manual disabling, then IndLampRun lights-on.

- A number of photo-resistors (see "Photo-Resistors" in the figure above), each one connected to SafePLC's digital input module, for detection of incorrect alignment of data transmitted from SafePLC and data shown from workstation's VDU. In particular, SafePLC cyclically compares two counters, the first local of SafePLC's (e.g. the sequence number of data transmitted to the workstation) and the second local of workstation and shown on the GraphicUserInterface (e.g. the sequence number of data received from SafePLC). The GraphicUserInterface shows workstation's counter in binary format on eight adjacent little square where photo-resistors are positioned; e.g. white colour square indicates "on", whilst, black colour square indicates "off". When SafePLC compares the two counters, its local and feedback detected from photo-resistors, if they have the same value, then workstation is properly operating, else workstation fault / error is detected from SafePLC, then commands are automatically disabled and IndLampFailed lights-on.

  To improve reliability of feedback, 3 lines of eight photo-resistors can be used and 2oo3 voting can be executed by SafePLC.

5.5.6 OCC Channel A/B SafePanel Functional Requirements

OCC SafePanel Shows to the Operator the Status of the WS [Id: CBACSS.OCC.SIF.ARC_SS_SPN]	
Input:	Signals from SafePLC to control the LED.
Output:	Command to the LED.
Description/Behavior:	The SafePanel shall notify the WS fault to the operator when requested by the SafePLC. When the SafePLC detects an error in the WS, the IndLampFailed shall be turned ON and the IndLampRun shall be turned OFF.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

OCC SafePanel WS Enabling and Disabling [Id: CBACSS.OCC.SIF.ARC_DS_SPN]	
Input:	Operator request (by pressing the PushBtnReset button).
Output:	Activation of the WS command.
Description/Behavior:	The SafePanel shall allow the reactivation of the WS command to the operator after the WS disabling, by pressing the PushBtnReset button. The operator can enable or disable the WS commands via the KeySwEnablingDisabling. When a failure in the WS occurs, an audio buzzer shall be played, in order to have a more effectiveness notification to the operator.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

OCC Operator Periodic Test of SafePanel [Id: CBACSS.OCC.SIF.MNT_MD_SPN]	
Input:	-
Output:	-
Description/Behavior:	Periodically (e.g. every 6 months) operator has to test SafePanel components by visual inspection. Thus, it has to: 1) Set the key-switch KeySwEnablingDisabling in “Disable” position (workstation commands are disabled). 2) Access to the “Test Page” on GraphicUserInterface. 3) Push the “Test SafePanel” button on GraphicUserInterface, which lights-on and off all LED-lamps, through SafePLC. 4) Move key-switch and push-button of SafePanel and check on “Test Page” that relevant graphic objects change (copy of physical objects). 5) Push the “Test SafePanel” button on GraphicUserInterface, which lights-on and off little square where photo-resistors are positioned and check on “Test Page” that relevant graphic objects change (copy of physical objects).
Safe State/Reaction:	-
Operating mode:	Cyclically.
SIL:	-

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MNT_MD_SPN

5.6 SMR Architecture

SMR CBACS Safe architecture, shown in **Figure 3-2**, is based on dual channel with diagnostic architectural pattern (1oo2D), similar to OCC, then the same components and measures (diversity, fault detection and reaction) defined at the par. 5.1 are applied to the SMR.

Anyway, some details have to be described:

- Each SMR has a single workstation, SafePLC and SafePanel, resulting alone 1oo1D architecture;
- Each SMR can monitor and command adjacent station' equipment, because the FieldPLC of a station communicates with FieldPLC of the adjacent stations, through the WAN.

It means that SMR architecture becomes 1oo2D.

In case of workstation fault(s) detected by SafePLC, the operator realizes anomaly condition by SafePanel indication. Thus, it informs (by phone or other media) the SMR operator in the adjacent stations (<i-1> or <i+1>), so the other operator continue execution of safety monitoring and command functions by its own workstation.

Diversity measures between adjacent SMRs (both channels) are in workstations components, which have different IPC, VDU and software implementation. Whilst, both channels' D-components:

- SafePLCs have the same hardware and software implementation;
- SafePanel have the same hardware implementation.

The workstation of SMR<1> is the same of OCC WS<A>, whilst workstation of SMR<2> is the same of OCC WS<B>, and so on until SMR<13>.

Finally, it's important to underline that SMR SafePLC is different to OCC SafePLC, whilst SafePanel remains equal.

5.7 SMR Functional Requirements

Acquire the state changes of individual emergency ventilation equipment and show to the operator	
Input:	State changes of emergency ventilation equipment (received from FieldPLC).
Output:	Visual notification to the operator.
Description/Behavior:	The SMR CBACS Safe shall acquire the state of changes of the emergency ventilation equipment from the FieldPLCs and provide a visual notification to the operator, to allow the management of the emergency ventilation equipment accordingly.
Safe State/Reaction:	Visual notification to the operator and disabling of the command.
Operating mode:	Normal operation.
SIL:	2

Acquire the fire detection alarm and show to the operator	
Input:	Fire detection alarm (received from FieldPLC).
Output:	Visual notification to the operator.
Description/Behavior:	The SMR CBACS Safe shall acquire the alarm of fire detection from the FieldPLC and provide a visual notification to the operator, to allow the management of the emergency ventilation equipment accordingly.
Safe State/Reaction:	Visual notification to the operator and disabling of the command.
Operating mode:	Normal operation.
SIL:	2

Provide the command to the FieldPLC for the emergency ventilation equipment	
Input:	Command request of the operator.
Output:	Command to the FieldPLCs.
Description/Behavior:	The SMR CBACS Safe shall provide the command to the FieldPLCs to perform the emergency ventilation equipment action requested by the operator.
Safe State/Reaction:	Visual notification to the operator and disabling of the command.
Operating mode:	Normal operation.
SIL:	2

Provide the command to the FieldPLC to execute a scenario of emergency ventilation equipment	
Input:	Command request of the operator.
Output:	Scenario command to the FieldPLCs.
Description/Behavior:	The SMR CBACS shall provide the command to the FieldPLCs to execute the emergency ventilation equipment scenario requested by the operator.
Safe State/Reaction:	Visual notification to the operator and disabling of the command.
Operating mode:	Normal operation.
SIL:	2

5.8 SMR Components Description

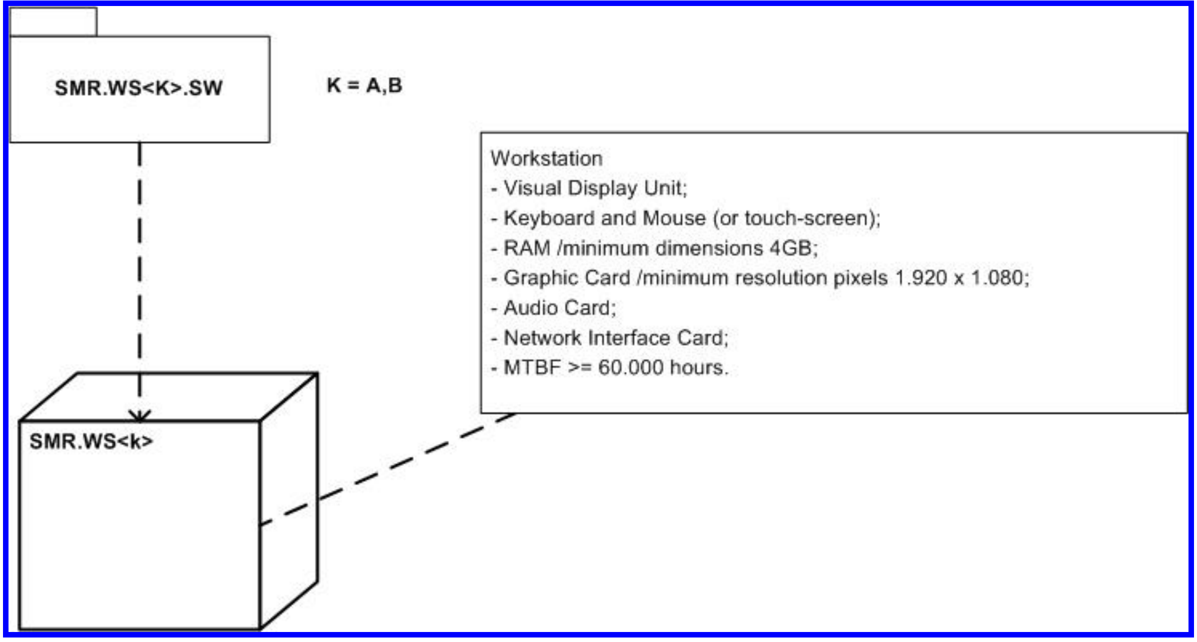
5.8.1 Workstations’ Components

The workstation in SMR architecture has the same composition of that used in OCC architecture, with alternations.

Please, refer to par. 5.5.1 for detailed description.

In **Figure 5-7** the UML diagram is showing the deployment of the software package SMR.WS<k>.SW (the whole software to be executed) on the hardware node SMR.WS<k>, where k = A or B. The UML diagram is also showing the main hardware features of the SMR.WS<k> node.

Figure 5-7 – Deployment of SMR Workstation SW (SMR.WS<k>.SW) on WS Hardware


SMR.WS<K>.SW
K = A,B
SMR.WS<k>
Workstation
- Visual Display Unit;
- Keyboard and Mouse (or touch-screen);
- RAM /minimum dimensions 4GB;
- Graphic Card /minimum resolution pixels 1.920 x 1.080;
- Audio Card;
- Network Interface Card;
- MTBF >= 60.000 hours.

The next show the main architectural software packages of SMR Workstation<A> and Workstation<B>, respectively.

Figure 5-8 – SMR Workstation<A> SW Packages

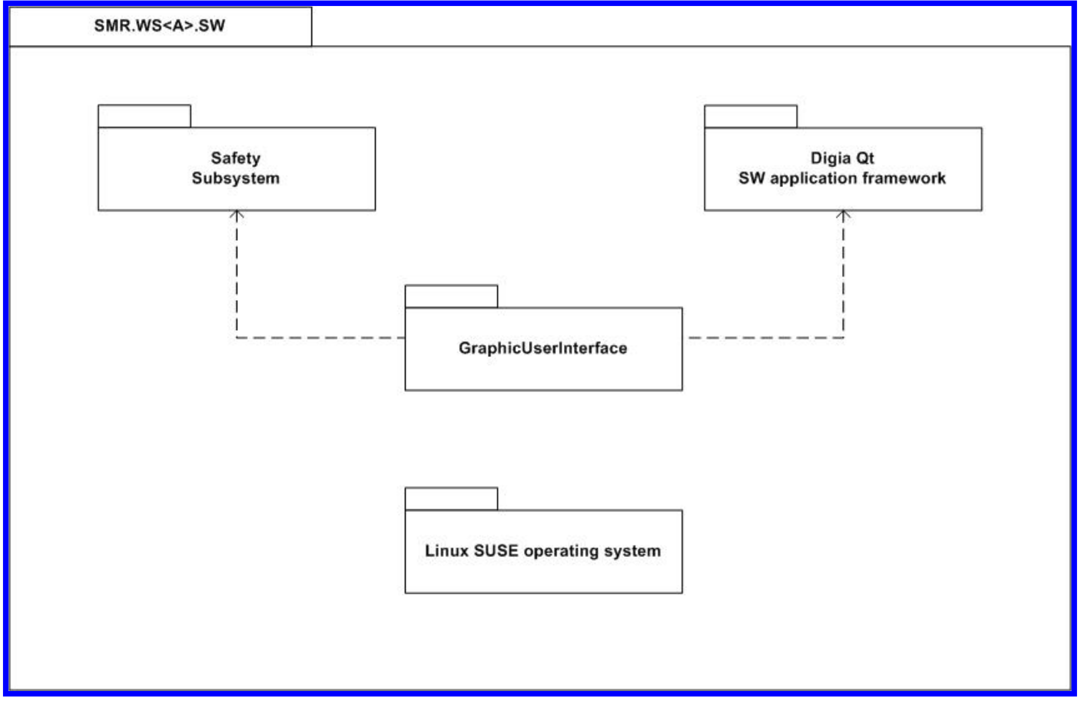
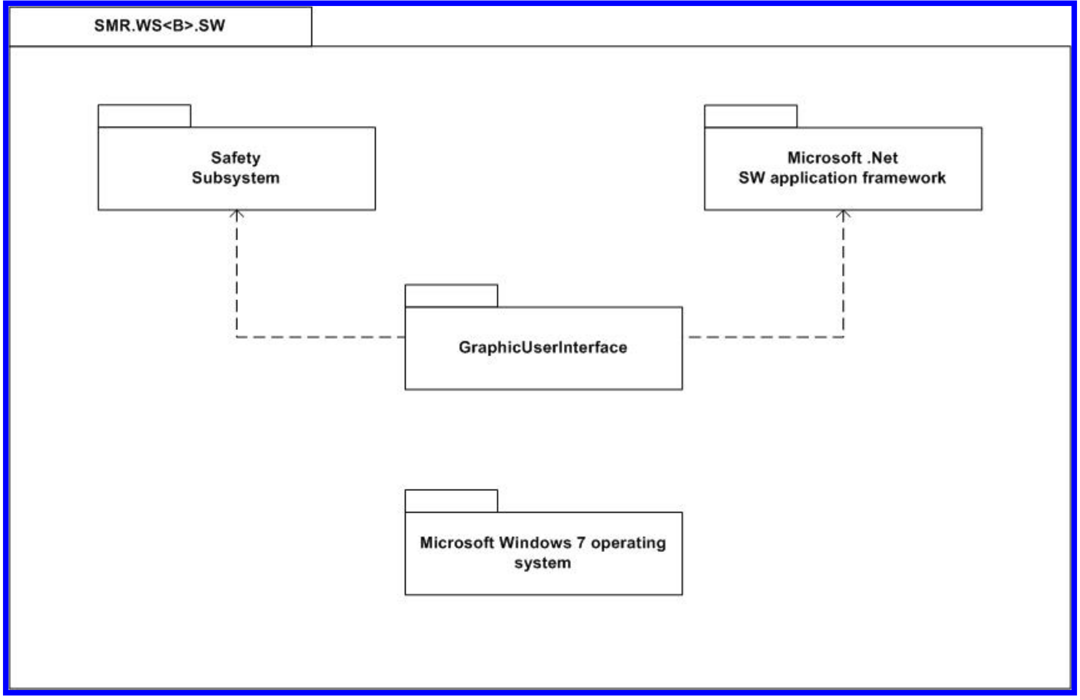

SMR.WS<A>.SW
Safety Subsystem
Digia Qt SW application framework
GraphicUserInterface
Linux SUSE operating system

Figure 5-9 – SMR Workstation<B> SW Packages


SMR.WS<B>.SW
Safety Subsystem
Microsoft .Net SW application framework
GraphicUserInterface
Microsoft Windows 7 operating system

5.8.2 SMR Workstation Functional Requirements

SMR WS Monitor State Changes of EV Equipment [Id: CBACSS.SMR.SFF.MON_EV_STS]	
Input:	State changes of emergency ventilation equipment (received from FieldPLC).
Output:	Signals to the VDU.
Description/Behavior:	The Workstation of the SMR shall acquire the state changes of emergency ventilation equipment from the FieldPLCs via EtherNet/IP and shall show it to the operator. The safety function is base on two steps: 1) The SMR WS collects state changes information (digital inputs) of emergency ventilation equipment from the FieldPLC of the involved station. 2) The SMR WS GUI screens show the collected information to the operator.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MON_EV_STS

SMR WS Monitor Alarms of FD Equipment [Id: CBACSS.SMR.SFF.MON_FD_ALM]	
Input:	Fire alarm (received from FieldPLC).
Output:	Signals to the VDU.
Description/Behavior:	The Workstation of the SMR shall acquire the fire detection from the FieldPLCs via EtherNet/IP and shall show it to the operator. The safety function is base on two steps: 1) The SMR WS collects fire alarm information (digital inputs) of fire detection equipment from the FieldPLC of the involved station. 2) The SMR WS GUI screens show the collected information to the operator.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MON_FD_ALM

SMR WS Command State Changes of EV Equipment [Id: CBACSS.SMR.SFF.CMD_EV_IND]	
Input:	ID of the pressed button. Back-computed graphic information (from graphic inverter). Results of signal validity from SafePLC.
Output:	Command signal (to the SafePLC).
Description/Behavior:	The workstation shall acquire the request from the button pressed by the operator and shall transmit the associated command to the FieldPLCs via EtherNet/IP, in order to control the emergency ventilation equipment. The safety function is based on five steps below listed: 1) The SMR WS operator receives fire alarm information from the FieldPLC. 2) The operator opens the GUI screen of involved station. 3) The operator from the GUI screen can push the command button to send a command towards individual emergency ventilation equipment. 4) The operator from the GUI screen has to push a Confirm or a Cancel button to respectively send or abort the command to the FieldPLC. 5) The FieldPLC sends to the operator the execution feedbacks for the scenario command, then “command started”, “command failed”, “command timed-out”, “command succeeded”. The command can be sent out to the FieldPLC only after the command validation of the SafePLC.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.CMD_EV_IND

SMR WS Command Scenario of EV Equipment [Id: CBACSS.SMR.SFF.CMD_EV_SCN]	
Input:	ID of the pressed button. Back-computed graphic information (from graphic inverter). Results of signal validity from SafePLC.
Output:	Command signal (to the SafePLC).
Description/Behavior:	The workstation shall acquire the request from the button pressed by the operator and shall transmit the associated command to the FieldPLCs via EtherNet/IP, in order to control the emergency ventilation equipment. The safety function is based on six steps below listed: 1) The SMR WS operator receives fire alarm information from the FieldPLC. 2) The operator opens the GUI screen of involved station. 3) The GUI screen highlights the suggested scenario command to the operator, e.g. by changing colour of a shape near to the suggested command button. 4) The operator from the GUI screen can push the suggested scenario command button or a different scenario command. 5) The operator from the GUI screen has to push a Confirm or a Cancel button to respectively send or abort the scenario command to the FieldPLC. 6) The FieldPLC sends to the operator the execution feedbacks for the scenario command, then “command started”, “command failed”, “command timed-out”, “command succeeded”. The command can be sent out to the FieldPLC only after the command validation of the SafePLC.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.CMD_EV_SCN

SMR WS Diverse Redundancy [Id: CBACSS.SMR.SIF.ARC_DR_WKS]	
Input:	-
Output:	-
Description/Behavior:	Workstation in SMR has dual redundancy that tolerates the failure of one WS to keep the safety functions executable on demand. In fact, in each SMR is present one workstation only but, it workstation can monitor and command adjacent station' equipment, because the FieldPLC of a station communicates with FieldPLC of the adjacent stations, through the WAN. Moreover, for two adjacent sites (SMRs), WS have diverse hardware (IPC and VDU) and software implementation (operating system and SW application framework) of the same safety requirements specification. In case of workstation fault(s) detected by SafePLC, the operator realizes anomaly condition by SafePanel indication and moves the other workstation to continue execution of safety monitoring and command functions.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.ARC_DR_WKS

SMR WS Commands Proof-Test [Id: CBACSS.SMR.SIF.CMD_PT_WKS]	
Input:	-
Output:	-
Description/Behavior:	Periodically (e.g. every 1 year) operator has to send a command to FieldPLC for execution of safety functions **CBACSS.SMR.SFF.CMD_EV_IND** and **CBACSS.SMR.SFF.CMD_EV_SCN**.
Safe State/Reaction:	-
Operating mode:	Cyclically.
SIL:	-

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.CMD_PT_WKS

SMR Operator Periodic Test of VDU [Id: CBACSS.SMR.SIF.MNT_MD_VDU]	
Input:	-
Output:	-
Description/Behavior:	Periodically (e.g. every 6 months) operator has to test VDU components by visual inspection. Thus, it has to: 1) Set the key-switch KeySwEnablingDisabling in “Disable” position (workstation commands are disabled). 2) Access to the “Test Page” on GraphicUserInterface. 3) Push the “Test VDU” button on GraphicUserInterface, which change colour of VDU screen following several test patterns, e.g. all red, all green and all blue (with exception of a limited control area).
Safe State/Reaction:	Replacement of the VDU with a working one.
Operating mode:	Cyclically.
SIL:	-

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MNT_MD_VDU

5.8.3 SafePLCs' Components

This paragraph describes SafePLC components, which are equal for all SMRs.

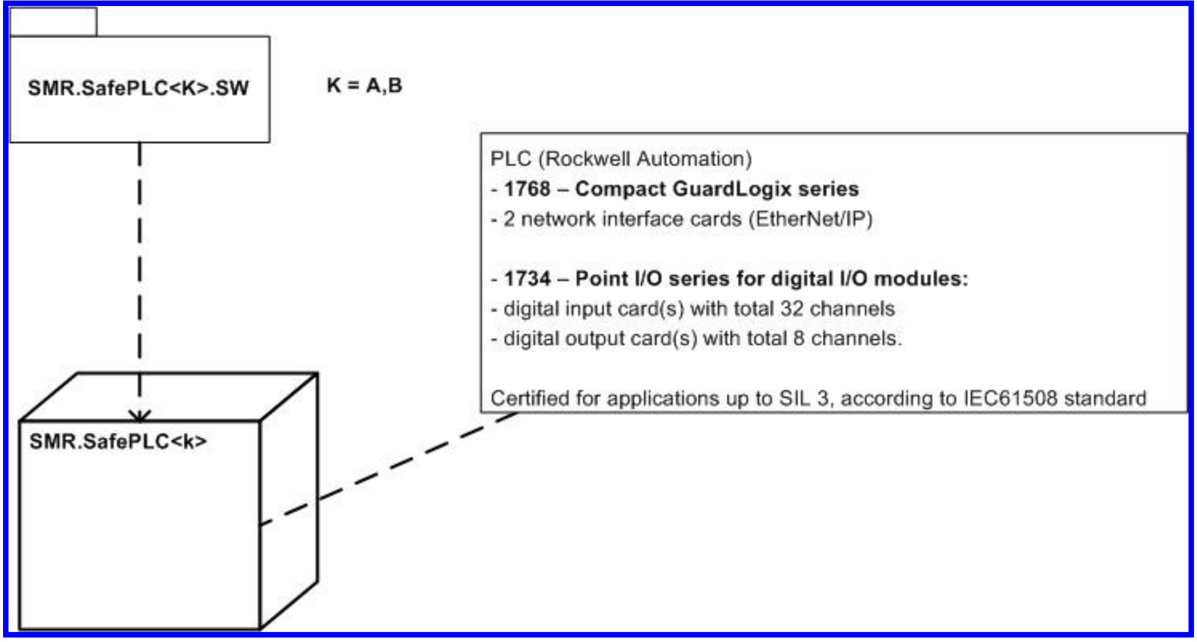
All SafePLCs are **fail-safe** and are based on **Rockwell Automation** products series below listed:

- Compact GuardLogix series (1768);
- Point I/O series (1734), for digital and analogue I/O modules.

These product series are certified for applications up to SIL 3, according to IEC61508 standard.

In **Figure 5-10** the UML diagram is showing the deployment of the software package SMR.SafePLC<k>.SW (the whole software to be executed) on the hardware node SMR.SafePLC<k>, where k = A or B. The UML diagram is also showing the main hardware features of the SMR.SafePLC<k> node.

Figure 5-10 – Deployment of SMR SafePLC SW (SMR.SafePLC<k>.SW) on SafePLC Hardware



PLC (Rockwell Automation)
- **1768 – Compact GuardLogix series**
- 2 network interface cards (EtherNet/IP)

- **1734 – Point I/O series for digital I/O modules:**
- digital input card(s) with total 32 channels
- digital output card(s) with total 8 channels.

Certified for applications up to SIL 3, according to IEC61508 standard

Notice: The choice of Rockwell Automation products is justified to simplify interoperability with FieldPLC, which use Rockwell Automation products also, then EtherNet/IP communication protocol. It allows implementation of safety protocol over EtherNet/IP (SafeCommLayer).

The SafePLC is equipped with:

- One CPU, with safety diagnostic unit;
- Two network interface cards (EtherNet/IP), one for data exchanging with workstation the second for data exchanging with FieldPLC and external subsystems (ATS and SMS).
- One (or more depending on modularity) digital input card with total 32 channels;
- One (or more depending on modularity) digital output card with total 8 channels.

Using of two network interface cards guarantees “data filtering” function of SafePLC; in fact, workstation is physically separated from FieldPLC and external subsystems.

The I/O signals list is the same of that defined for OCC SafePLC. Please, refer to **Table 5-1** for detailed description.

In case the SafePLC is un-powered, the failure shall be notified to the Operator through the SafePanel. The notification shall be a lamp or an audio buzzer.

5.8.4 SMR SafePLC Functional Requirements

SMR Diversity between WS and SafePLC [Id: CBACSS.SMR.SIF.ARC_DD_WKS]	
Input:	-
Output:	-
Description/Behavior:	Workstation in SMR has its own SafePLC, which is the diagnostic monitoring unit of workstation. One of SafePLC functions is fault detection of workstation, which consists in comparison and data validation / integrity checks, applied to data exchanged with workstation. As per “diverse monitor techniques”, required by IEC61508 standard, SafePLC implements separation between the monitor computer and the monitored computer (workstation). SafePLC, is the monitoring channel is certified for applications up to SIL 3, according to IEC61508 standard.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.ARC_DD_WKS

SMR SafePLC Automatic Fault Detection for WS Command [Id: CBACSS.SMR.SIF.CMD_AD_WKS]	
Input:	ID of the pressed button. Back-computed graphic information (from graphic inverter).
Output:	Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the signals provided by the workstation each time a button is pressed. When operator has to send a command to FieldPLC it pushes a command button from the GUI screen; thus two information are sent to the SafePLC: 1) The command unique identifier (integer number), associated to the pressed command button. 2) The back-computed graphic information, detected by GraphicInverter, relevant to colour changing of pressed button. The SafePLC compares the two information above listed and, if differs, SafePLC itself reacts disabling workstation command functions and activating signalisations to operator (through the SafePanel). A retry mechanism could be applied to avoid disabling workstation command on transient faults.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.CMD_AD_WKS

SMR SafePLC Automatic Fault Detection for WS Monitoring [Id: CBACSS.SMR.SIF.MON_AD_WKS]	
Input:	Requested information (state changes or fire detection). Message received from the FieldPLCs. Back-computed graphic information (from graphic inverter).
Output:	Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the notification performed by the workstation to the operator. After the plant data transmission from SafePLC to WS, the GraphicInverter software component, running on the workstation, accesses to graphic card's memory, through related application programming interfaces (APIs), and back-computes the received graphic information in a message to be sent to the SafePLC (through SafeCommunicator). The SafePLC compares this message with the plant data sent from SafePLC and, if they're different, SafePLC itself reacts disabling workstation command functions and activating signalisations to operator (through the SafePanel), turning off the IndLampRun and turning on the IndLampFailed.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MON_AD_WKS

SMR SafePLC to FieldPLC Safety Protocol [Id: CBACSS.SMR.SIF.IFC_SP_SPC]	
Input:	Message received from the FieldPLCs. Back-computed graphic information (from graphic inverter).
Output:	Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the communication between itself and the FieldPLC, by means of the safety protocol. FieldPLC and SafePLC communicate by safety protocol over EtherNet/IP (SafeCommLayer), where they respectively act as TCP server and TCP client. It's based on EtherNet/IP standard messaging but adds it measures against communication threats, according to EN50159:2010. The applied measures are additional message's fields (as minimum: sequence number, timestamp, source and destination identifiers, control & status data and hash code). The typical (standardized) errors affecting communication are: • Repetition (old and obsolete messages are repeated at an inopportune time causing disturbance at the receiver's end); • Loss (one or more messages are transmitted, but never received; messages are deleted); • Insertion (unexpected messages are introduced in the communication path); • Incorrect sequence (the sending order of messages does not correspond to the reception order); • Corrupted data (the integrity of transmitted data is not preserved; sent data are different from the received ones); • Delay (a message arrives at receiver site with unacceptable delay; the elapse time from sending to receiving is too long); • Erroneous addressing (wrong the receiver of a message was not the intended one). A safety protocol is there to introduce measures able to reinforce a normal communication protocol to avoid the above listed failure. In case the SafePLC detects a failure in the communication the following action shall be performed: - Disable the workstation command; - Turn on the IndLampFailed; - Turn off the IndLampRun.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.IFC_SP_SPC

SMR WS to SafePLC Safety Protocol [Id: CBACSS.SMR.SIF.IFC_SP_WKS]	
Input:	Message received from the WS.
Output:	Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the communication between itself and the Workstation, by means of the safety protocol. SafePLC and workstation communicate by safety protocol over EtherNet/IP (SafeCommLayer), where they respectively act as TCP server and TCP client. It's based on EtherNet/IP standard messaging but adds it measures against communication threats, according to EN50159:2010. The applied measures are additional message's fields (as minimum: sequence number, timestamp, source and destination identifiers, control & status data and hash code). The typical (standardized) errors affecting communication are: • Repetition (old and obsolete messages are repeated at an inopportune time causing disturbance at the receiver's end); • Loss (one or more messages are transmitted, but never received; messages are deleted); • Insertion (unexpected messages are introduced in the communication path); • Incorrect sequence (the sending order of messages does not correspond to the reception order); • Corrupted data (the integrity of transmitted data is not preserved; sent data are different from the received ones); • Delay (a message arrives at receiver site with unacceptable delay; the elapse time from sending to receiving is too long); • Erroneous addressing (wrong the receiver of a message was not the intended one). A safety protocol is there to introduce measures able to reinforce a normal communication protocol to avoid the above listed failure. In case the SafePLC detects a failure in the communication the following action shall be performed: - Disable the workstation command; - Turn on the IndLampFailed; - Turn off the IndLampRun.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.IFC_SP_WKS

SMR SafePLC Automatic Fault Detection for VDU of Workstation [Id: CBACSS.SMR.SIF.MON_AD_VDU]	
Input:	Sequence number from photo resistor.
Output:	Sequence number to WS. Workstation disables command. Signal to turn on the IndLampFailed. Signal to turn off the IndLampRun.
Description/Behavior:	The SafePLC shall detect fault in the VDU, in order to detect fault in the notification to the operator. A number of photo-resistors, each one connected to SafePLC's digital input module, for detection of incorrect alignment of data transmitted from SafePLC and data shown from workstation's VDU. In particular, SafePLC cyclically compares two counters, the first local of SafePLC's (e.g. the sequence number of data transmitted to the workstation) and the second local of workstation and shown on the GraphicUserInterface (e.g. the sequence number of data received from SafePLC). The GraphicUserInterface shows workstation's counter in binary format on eight adjacent little square where photo-resistors are positioned; e.g. white colour square indicates "on", whilst, black colour square indicates "off". When SafePLC compares the two counters, its local and feedback detected from photo-resistors, if they have the same value, then workstation is properly operating, else workstation fault / error is detected from SafePLC, then commands are automatically disabled and IndLampFailed lights-on. To improve reliability of feedback, 3 lines of eight photo-resistors can be used and 2oo3 voting can be executed by SafePLC. Notice that photo-resistors cover a limited area of VDU screen, but is necessary to force refreshing of all GUI's monitoring areas when workstation's counter is updated. Thus, to force workstation's to graphic card's to update VDU screen, each LED-lamps a little changing, not tedious for operator eyes and not interfering with GraphicInverter, updated by new values of workstation's counter. A retry mechanism could be applied to avoid disabling workstation command on transient faults.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MON_AD_VDU

SMR SafePLC Enabling / Disabling of Workstation Commands [Id: CBACSS.SMR.SIF.ARC_DD_DIS]	
Input:	-
Output:	Workstation disables command.
Description/Behavior:	SafePLC, in case of workstation fault(s) detected, as safe reaction, disables workstation command functions, using its fail-safe characteristic. In particular, SafePLC de-energize two its digital outputs channels, which are fed-back in two its digital input channels (for fault tolerance). The digital input channels are the flags that disable the command messages sending towards the FieldPLC. At least on digital input channel has to go “off” to disable workstation command. When fault is cleared SafePLC doesn’t automatically enable workstation command functions, but is necessary push SafePanel’s button PushBtnReset. Digital outputs channels, alternatively, could also de-energize workstation or SafePLC’s network interface card for data exchanging with FieldPLC.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.ARC_DD_DIS

SMR SafePanel Signalisation of Workstation Fault / Error [Id: CBACSS.SMR.SIF.ARC_DD_SPN]	
Input:	-
Output:	Signal to control the IndLampFailed. Signal to control the IndLampRun.
Description/Behavior:	When SafePLC detects workstation fault(s), over to disable workstation command functions, it activates one red lamp IndLampFailed on SafePanel.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.ARC_DD_SPN

5.8.5 SafePanel's Components

The SafePanel in SMR architecture has the same composition of that used in OCC architecture. Please, refer to par. 5.5.5 for detailed description.

5.8.6 SMR SafePanel Functional Requirements

SMR SafePanel Shows to the Operator the Status of the WS [Id: CBACSS.SMR.SIF.ARC_SS_SPN]	
Input:	Signals from SafePLC to control the LED.
Output:	Command to the LED.
Description/Behavior:	The SafePanel shall notify the WS fault to the operator when requested by the SafePLC. When the SafePLC detects an error in the WS, the IndLampFailed shall be turned ON and the IndLampRun shall be turned OFF.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

SMR SafePanel WS Enabling and Disabling [Id: CBACSS.SMR.SIF.ARC_DS_SPN]	
Input:	Operator request (by pressing the PushBtnReset button).
Output:	Activation of the WS command.
Description/Behavior:	The SafePanel shall allow the reactivation of the WS command to the operator after the WS disabling, by pressing the PushBtnReset button. The operator can enable or disable the WS commands via the KeySwEnablingDisabling. When a failure in the WS occurs, an audio buzzer shall be played, in order to have a more effectiveness notification to the operator.
Safe State/Reaction:	-
Operating mode:	Normal operation.
SIL:	2

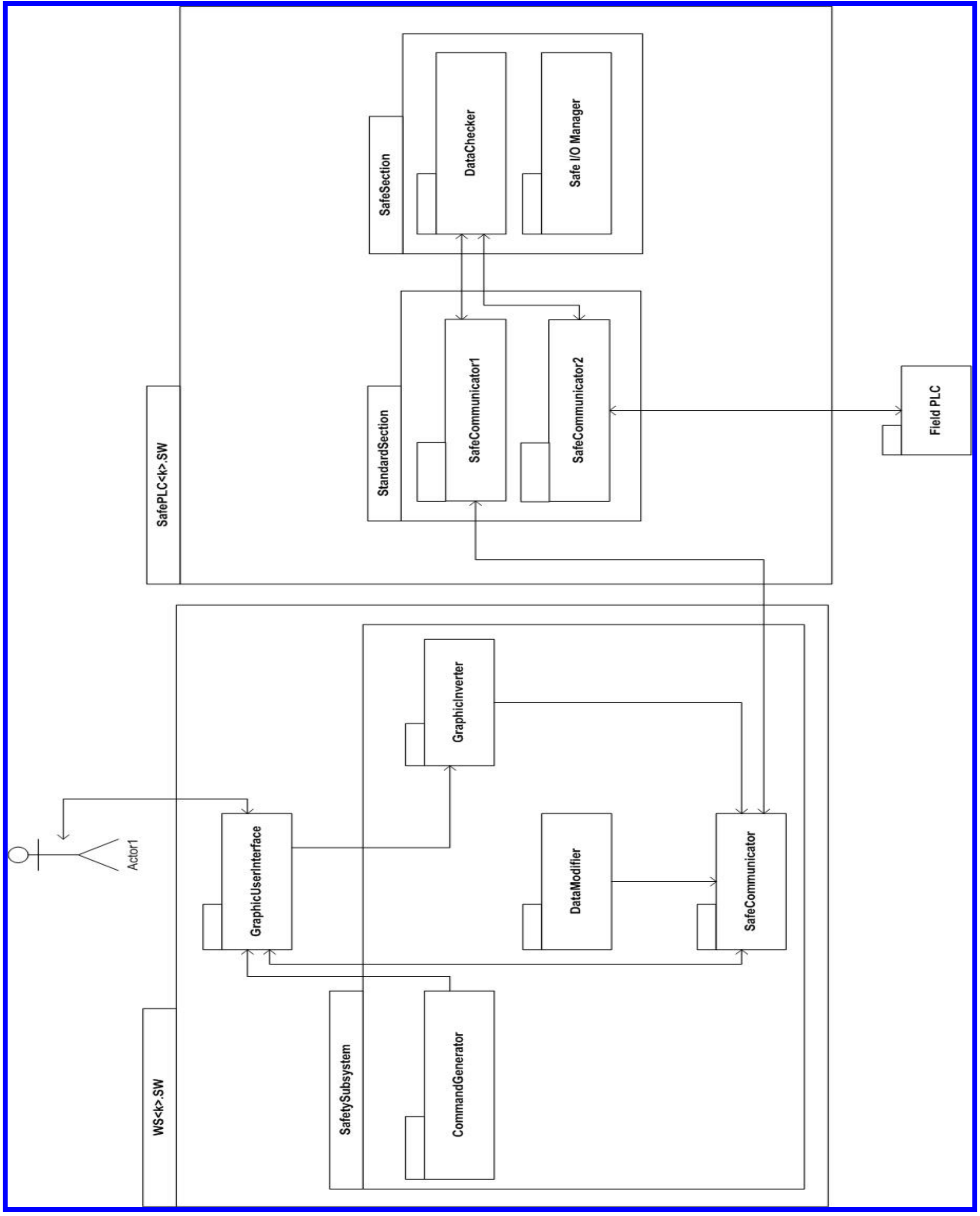
SMR Operator Periodic Test of SafePanel [Id: CBACSS.SMR.SIF.MNT_MD_SPN]	
Input:	-
Output:	-
Description/Behavior:	Periodically (e.g. every 6 months) operator has to test SafePanel components by visual inspection. Thus, it has to: 1) Set the key-switch KeySwEnablingDisabling in “Disable” position (workstation commands are disabled). 2) Access to the “Test Page” on GraphicUserInterface. 3) Push the “Test SafePanel” button on GraphicUserInterface, which lights-on and off all LED-lamps, through SafePLC. 4) Move key-switch and push-button of SafePanel and check on “Test Page” that relevant graphic objects change (copy of physical objects). 5) Push the “Test SafePanel” button on GraphicUserInterface, which lights-on and off little square where photo-resistors are positioned and check on “Test Page” that relevant graphic objects change (copy of physical objects).
Safe State/Reaction:	-
Operating mode:	Cyclically.
SIL:	-

Ref. Requirement: 1G00PS258G104 / CBACSS.ALL.SRS.MNT_MD_SPN

5.9 Software Architecture

The software architecture of CBACS Safe is shown in the **Figure 5-11**; it's applicable both OCC and SMR and either WS<A> or WS<B>.

Figure 5-11 – Software Architecture



For each workstation, within relevant SW application framework, are implemented and runs the software components, which forms the HMI application. They're below listed:

- **GraphicUserInterface**. It's the set of interactive graphic screens and related objects, which allows the operator to execute the safety monitoring and command functions. It includes an event handling module which defines, for a limited set of detectable events (e.g. mouse-clicked, key-pressed), the specific behaviour of graphic objects (e.g. background colour change) or other actions to do. It interfaces:
  - SafeCommunicator (subsequently described), to collect and send plant data (through SafePLC);
  - Graphic event manager, which detects and notifies events to the handling module, including operator's actions.

and the next components, which are parts of SafetySubsystem:

- **SafeCommunicator**. It implements the SafeCommLayer to exchange data with SafePLC, then acts as TCP client;
- **DataModifier**. It's used to test fault detection capability of the SafePLC during monitoring function. It interfaces SafeCommunicator and, when requested from SafePLC, "modifies" the data (e.g. adding an offset) to be fed-back to the SafePLC itself.
- **CommandGenerator**. It's used to automatically test part of the command loop when no concrete command has to be sent towards the plant. It interfaces SafeCommunicator and GraphicUserInterface and, when requested from SafePLC, "activates" the pressed event for command request button on the GraphicUserInterface. This test covers the graphic event handling module and GraphicInverter (subsequently described).
- **GraphicInverter**. It's used to detect workstation errors either in monitoring or command functions. It accesses to graphic card's memory, through related application programming interfaces (APIs), and back-computes the received graphic information in a message to be sent to the SafePLC (through SafeCommunicator). The SafePLC compares this message with the "expected result", and if they're different, SafePLC itself reacts disabling workstation command functions and activating signalisations to operator (through the SafePanel).

The "expected result" has different meanings, depending on the tested function:

- For monitoring function, "expected result" is the plant data sent from SafePLC.

- For command function, “expected result” is the command unique identifier (integer number), associated to the pressed request button, and sent to SafePLC.

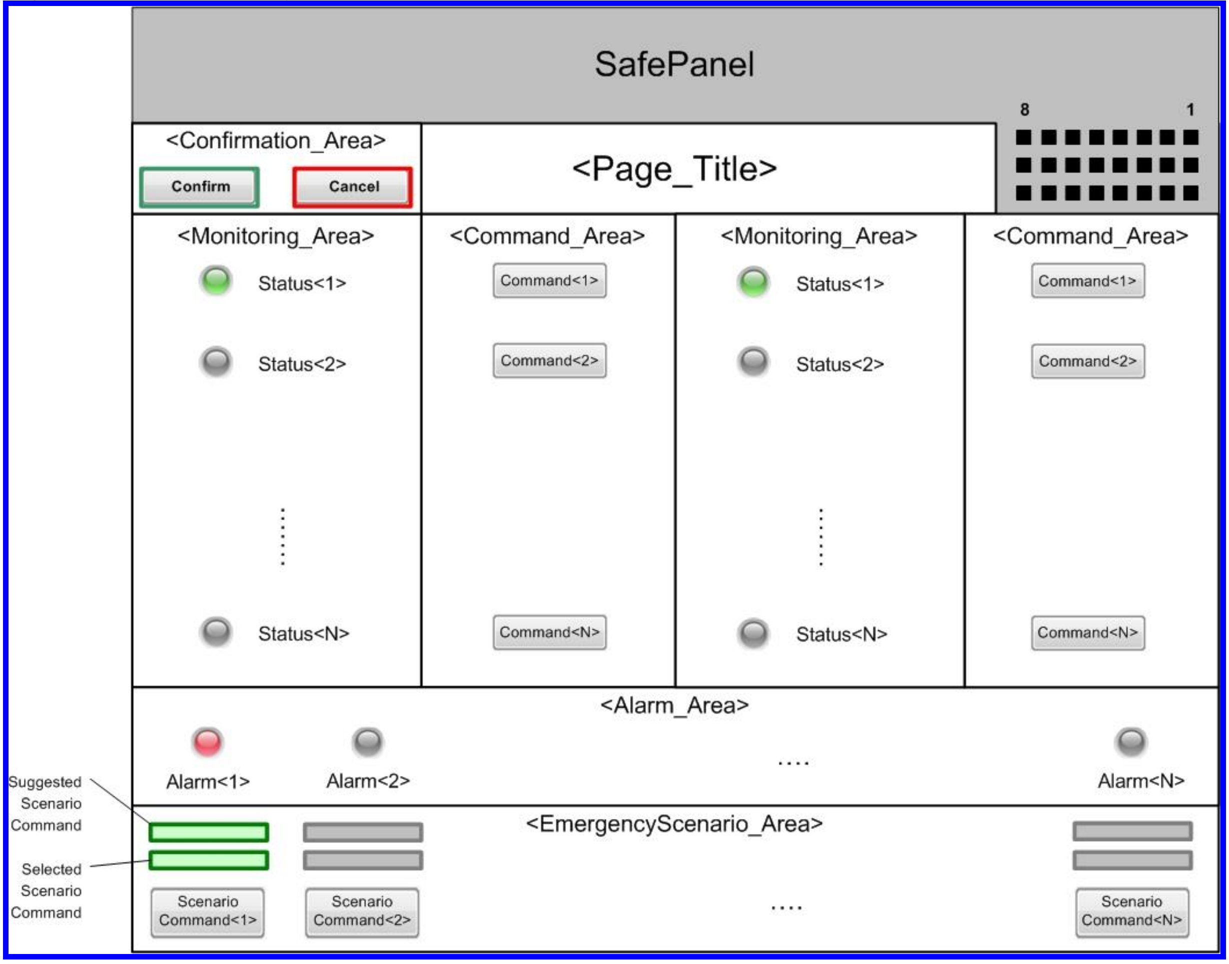
For each SafePLC, runs the software components below listed:

- **SafeCommunicator1**. It implements the SafeCommLayer to exchange data with workstation, then acts as TCP server;
- **SafeCommunicator2**. It implements the SafeCommLayer to exchange data with relevant FieldPLC;
- **DataChecker**. It execute the checks on SafetyCommunicator data, e.g. CRC checks, thus uses safety instructions subset of SafePLC;
- **Safe I/O Manager**. It manage the safety digital I/O, including that controlling SafePanel.

5.10 Graphic User Interface

This paragraph describes Graphic User Interface (GUI) format and composing objects; the next **Figure 5-12** shows the relevant layout:

Figure 5-12 – GUI's Layout and Components



Main characteristic of GUI are:

1) The form and animation of monitoring objects is very simple, no rotating and no translating, we propose LED-lamps and shapes that change colour.
2) The colour of monitoring objects is clear, no gradients, we propose red, green, blue and grey.
3) Data entry objects are command buttons only.

The meaning of (1) and (2) is to simplify operator interaction and GraphicInverter component workload, which acts on monitoring areas, on shapes for visualization of selected command and suggested command.

The meaning of (3) is to limit variability of operator data entry.

To avoid unintentional sending of commands, each command need subsequent pressing of confirmation button in confirmation area.

Notice that **Figure 5-12** also shows SafePanel, which covers the top-right area of screen; at the top-right area of screen there are eight adjacent little square that represents workstation's counter in binary format. Finally, an additional page named "Test Page" is included in GUI, it supports operator for periodic checking of SafePanel and VDU components by visual inspection.

5.11 Safety Protocol

Safety Protocol is a module implementing a safe communication. This is obtained by build up safety measures over and above the means that already exist in the communication protocol to permit the necessary residual error.

An example of typical structure of a safety telegram for supporting the measures against typical communication faults is provided in Table 5-2 where the first (from left to right) fields are usually called safety parameters. The receiver ID and sender ID are used to identify uniquely the source and destination of the telegram. This allows a receiver to understand if a given telegram has been sent by an eligible sender and it is the expected receiver of such telegram. In this way we can avoid insertion and erroneous addressing.

Table 5-2 – Example of Structure of a Safety Telegram

Receiver ID	Sender ID	Consecutive Number	Hash Code	Control / Status	DATA

The consecutive number is a number that is increased, say + 1, by the sender each time it issues a new telegram for a given receiver. Assuming that one byte is give for the consecutive number, we have that for the same receiver and a new telegram, the sender increases from 0 to 255, the consecutive number then wraps over back to 0 and starts again. The consecutive number allows a receiver to effectively detect if some telegram have been lost or repeated. If it receives a telegram with a bigger than expected consecutive number it can mean that some messages were lost. In case it receives a telegram with a smaller than expected consecutive number, it can mean that such telegram is a repetition. The consecutive number as provide data flow monitoring since it allows to detect the receiving of telegrams in wrong orders. In some cases consecutive number allows also to detect insertion although in general it does not guarantee this. The hash coded is usually calculated over all other telegram data and it is for ensuring data integrity. Ideally, the hash code should always change with the changing of the data it is calculated from, therefore different data should provide different hash codes. In practice there are different hash algorithms from check sum to CRC 32 each one with different capability of ensuring that a change in data (from which the hash code is calculated) gives rise to a change in the hash code. Status and Control data are optional and usually included to inform the receiver about the status of the sender (e.g. it recognized a failure) or to provide commands to be executed by the receiver. Finally, the field DATA is to contain the “application data” that the sender wants to pass to the receiver. It is worth nothing that the definition of the telegram structure is the first step towards the definition of the Safe Communication, time monitoring is the other key ingredient for such a specification. Time monitoring consists in the verification of the arrival of a new correct telegram at the receiver side within the watchdog time.

5.12 Subsystem Behavioural View

This paragraph provides a dynamic view of CBACS Safe subsystem, during execution of monitoring and command functions, either in success or in exception scenario.

5.12.1 Monitoring Function

The main monitoring function is classified in two separates safety functions, depending on monitored equipment: state changes of EV or fire alarms of FD.

The sequence diagrams shown in the next **Figure 5-13** and **Figure 5-14** provides CBACS Safe behaviour both safety functions, either in success or in exception scenario. The same diagram is applicable to OCC SMR workstations.

Figure 5-13 – Monitoring Function Success Scenario

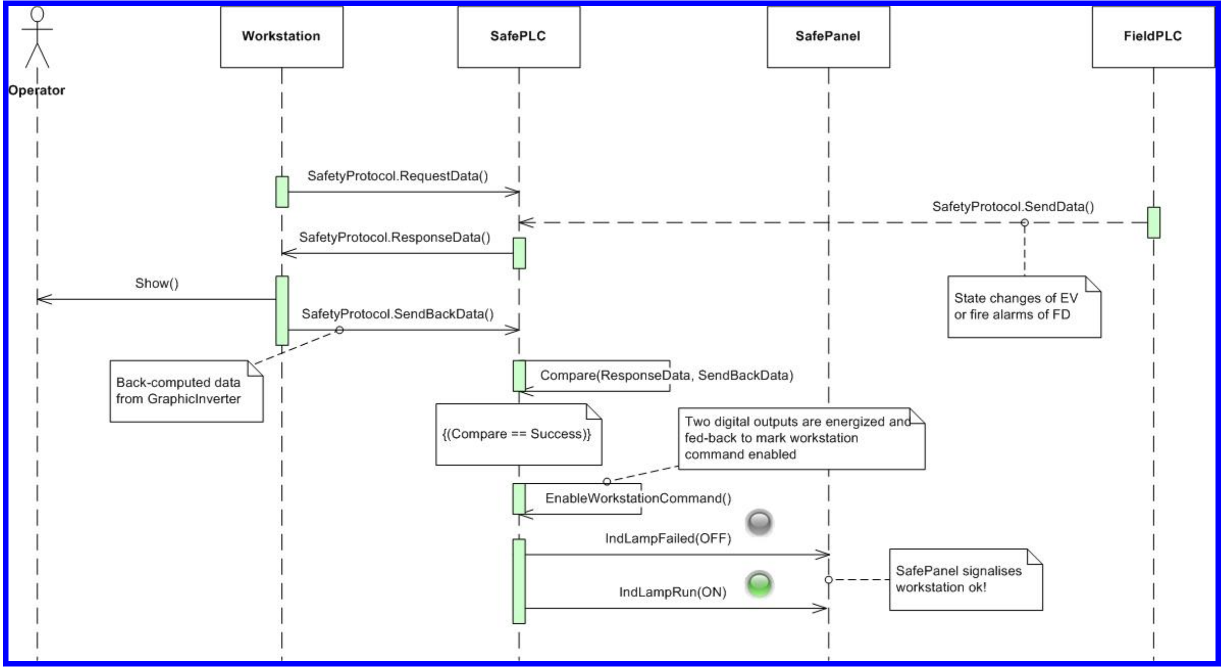
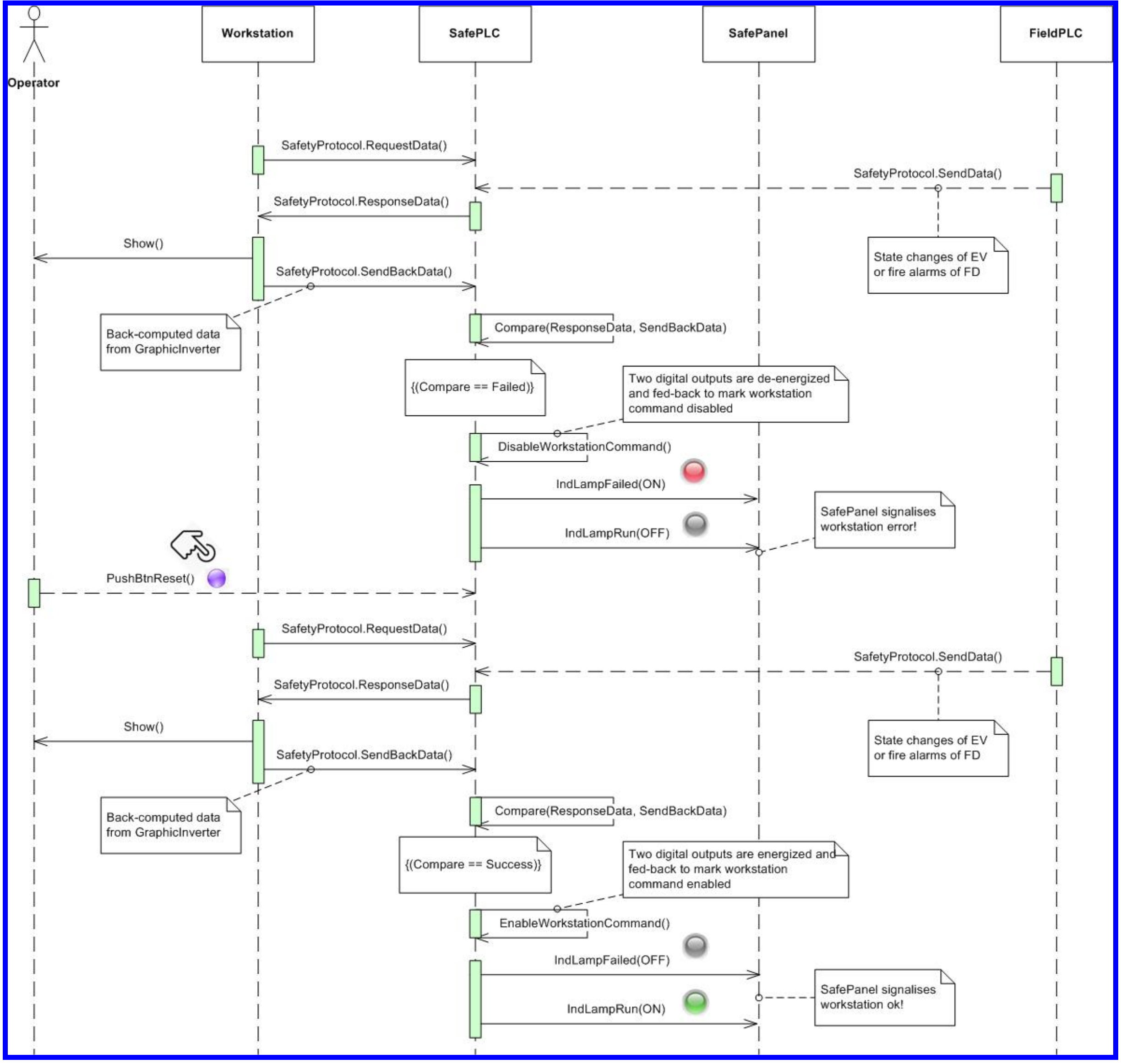

Operator
Workstation
SafePLC
SafePanel
FieldPLC
SafetyProtocol.RequestData()
SafetyProtocol.SendData()
SafetyProtocol.ResponseData()
Show()
SafetyProtocol.SendBackData()
State changes of EV or fire alarms of FD
Back-computed data from GraphicInverter
Compare(ResponseData, SendBackData)
{(Compare == Success)}
Two digital outputs are energized and fed-back to mark workstation command enabled
EnableWorkstationCommand()
IndLampFailed(OFF)
IndLampRun(ON)
SafePanel signalises workstation ok!

Figure 5-14 – Monitoring Function Exception Scenario


Operator
Workstation
SafePLC
SafePanel
FieldPLC
SafetyProtocol.RequestData()
SafetyProtocol.SendData()
SafetyProtocol.ResponseData()
Show()
State changes of EV or fire alarms of FD
SafetyProtocol.SendBackData()
Back-computed data from GraphicInverter
Compare(ResponseData, SendBackData)
{(Compare == Failed)}
Two digital outputs are de-energized and fed-back to mark workstation command disabled
DisableWorkstationCommand()
IndLampFailed(ON)
SafePanel signalises workstation error!
IndLampRun(OFF)
PushBtnReset()
SafetyProtocol.RequestData()
SafetyProtocol.SendData()
SafetyProtocol.ResponseData()
Show()
State changes of EV or fire alarms of FD
SafetyProtocol.SendBackData()
Back-computed data from GraphicInverter
Compare(ResponseData, SendBackData)
{(Compare == Success)}
Two digital outputs are energized and fed-back to mark workstation command enabled
EnableWorkstationCommand()
IndLampFailed(OFF)
SafePanel signalises workstation ok!
IndLampRun(ON)

The SafePLC communicates (through safety protocol) with all relevant FieldPLCs then, in the SMR it communicates with local FieldPLC, whilst in OCC it communicates with all 13 FieldPLCs (one per station).

The workstation communicates with SafePLC (through safety protocol), then first request data **it needs to show** to the relevant SafePLC, periodically (every 1 second), and second shows them on GUI screen. At third step, the GraphicInverter component, running on the workstation, back-computes the shown data in a message to be sent back to the SafePLC (always through safety protocol); subsequently the SafePLC compares: sent back data from workstation and initially responded data to workstation.

If comparison fails then SafePLC itself reacts disabling workstation command functions and activating signalisations to operator (through the SafePanel).
Notice that compare function is part of safety instructions subset of SafePLC.

5.12.2 Command Function

The main command function is classified in two separates safety functions, depending on command mode: individual command to (single) EV equipment or scenario command to (multiple) EV equipment.
The sequence diagrams shown in the next **Figure 5-15** and **Figure 5-16** provides CBACS Safe behaviour both safety functions, either in success or in exception scenario. The same diagram is applicable to OCC SMR workstations.

The operator from the GUI screen pushes a command button to send a command towards plant equipment (select command).
Then first sends to SafePLC (through safety protocol) two differently computed data:

1) The request command, that is the unique identifier (integer number), associated to the pressed command button;
2) The back-computed graphic information, detected by GraphicInverter, relevant to colour changing of selected button.

Subsequently, the SafePLC compares both data above; if comparison fails then SafePLC itself reacts disabling workstation command functions and activating signalisations to operator (through the SafePanel). Whilst, if comparison succeeds, further checks are done on request command value, e.g. if included in acceptable values range.
If last check fails then, in the same way, SafePLC itself reacts disabling workstation command functions and activating signalisations to operator (through the SafePanel).
Else, if last check succeeds, operator from the GUI screen has to push a Confirm or a Cancel button to respectively send or abort the command to the FieldPLC.
The FieldPLC sends to the operator the execution feedbacks for the command, then "command started", "command failed", "command timed-out", "command succeeded".

Figure 5-15 – Command Function Success Scenario

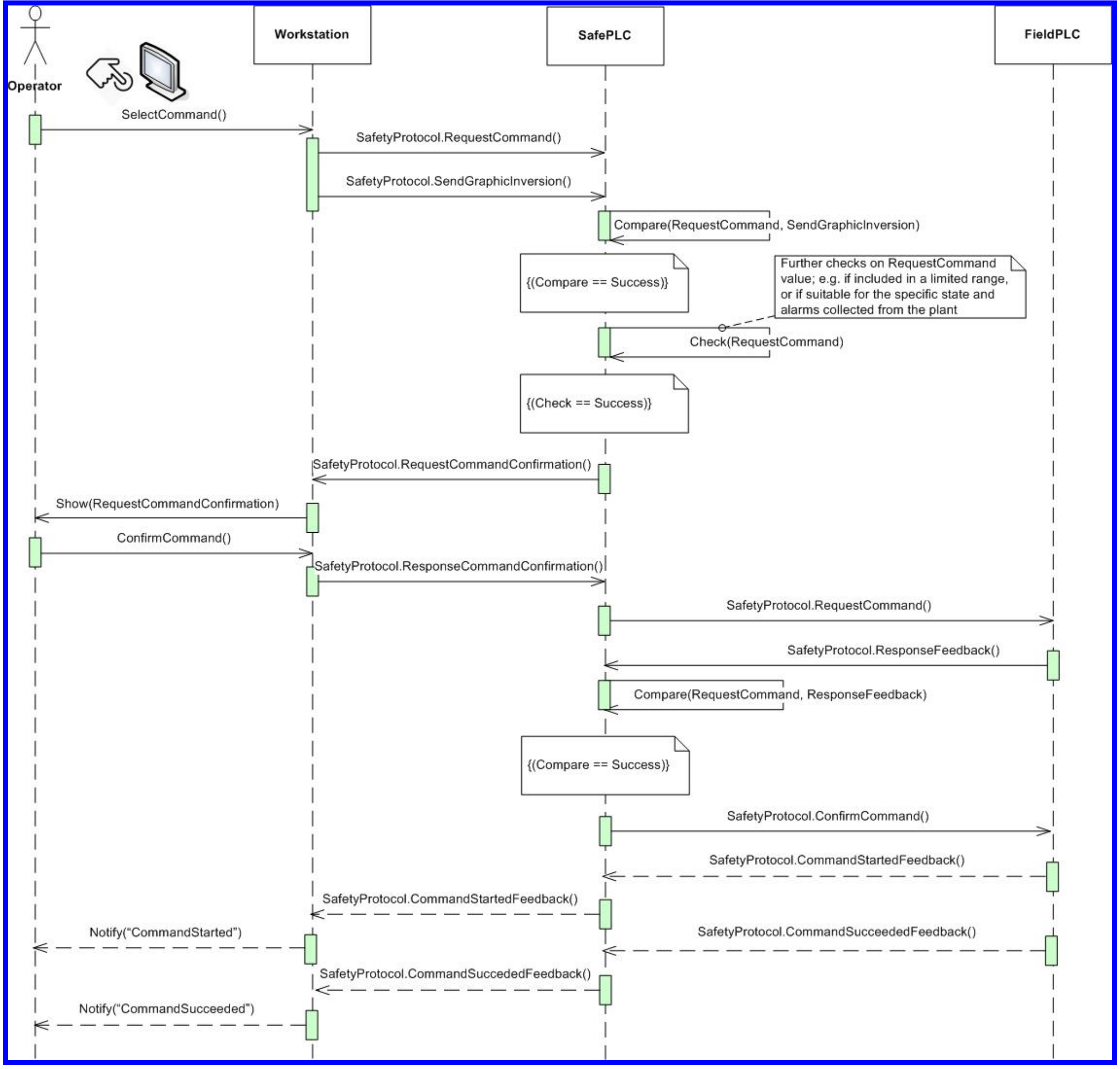
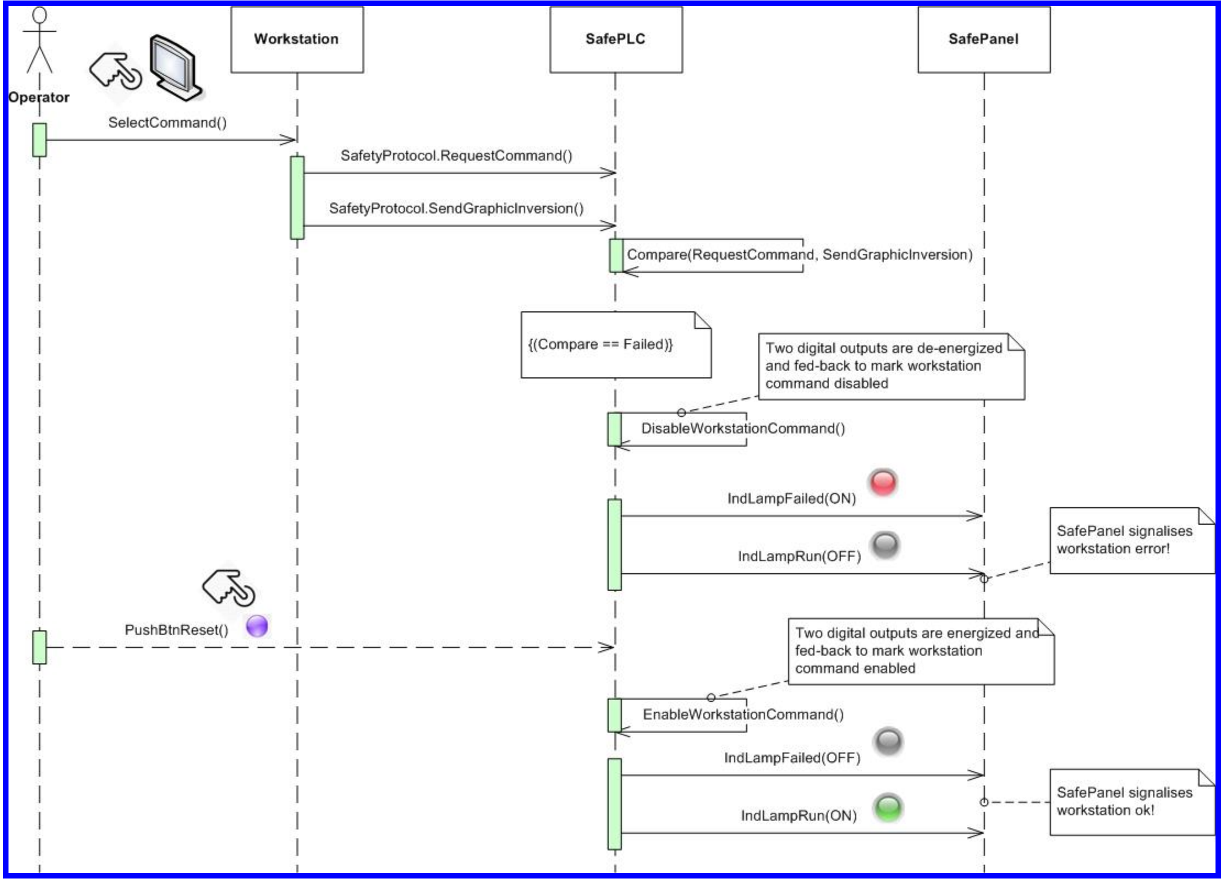

Operator
Workstation
SafePLC
FieldPLC
SelectCommand()
SafetyProtocol.RequestCommand()
SafetyProtocol.SendGraphicInversion()
Compare(RequestCommand, SendGraphicInversion)
{(Compare == Success)}
Further checks on RequestCommand value; e.g. if included in a limited range, or if suitable for the specific state and alarms collected from the plant
Check(RequestCommand)
{(Check == Success)}
SafetyProtocol.RequestCommandConfirmation()
Show(RequestCommandConfirmation)
ConfirmCommand()
SafetyProtocol.ResponseCommandConfirmation()
SafetyProtocol.RequestCommand()
SafetyProtocol.ResponseFeedback()
Compare(RequestCommand, ResponseFeedback)
{(Compare == Success)}
SafetyProtocol.ConfirmCommand()
SafetyProtocol.CommandStartedFeedback()
SafetyProtocol.CommandStartedFeedback()
Notify("CommandStarted")
SafetyProtocol.CommandSucceededFeedback()
SafetyProtocol.CommandSuccededFeedback()
Notify("CommandSucceeded")

Figure 5-16 – Command Function Exception Scenario


Operator
Workstation
SafePLC
SafePanel
SelectCommand()
SafetyProtocol.RequestCommand()
SafetyProtocol.SendGraphicInversion()
Compare(RequestCommand, SendGraphicInversion)
{(Compare == Failed)}
Two digital outputs are de-energized and fed-back to mark workstation command disabled
DisableWorkstationCommand()
IndLampFailed(ON)
IndLampRun(OFF)
SafePanel signalises workstation error!
PushBtnReset()
Two digital outputs are energized and fed-back to mark workstation command enabled
EnableWorkstationCommand()
IndLampFailed(OFF)
IndLampRun(ON)
SafePanel signalises workstation ok!

5.13 Subsystem Decomposition

This is intended to list the requirements of the subsystem decomposition.

5.13.1 Workstation Decomposition

According to the SW architectural overview and to the list of HW component used in the Workstation it is possible to identify the following functional blocks:

- **Network Management Block:** It manages the communication between the WS and the SafePLC.
- **GUI Management Block:** It allows the interaction between the FieldPLC and the operator, by showing the received signals and allowing the command to be actuated. It also allows the interpretation of the graphic information.
- **SIF management block:** manage the execution of the functions that check the integrity of the WS.

These blocks are all applicable to the OCC and SMR Workstation.

5.13.1.1 WS Network Management Block

Acquire the signals from the SafePLC and provide to the signal to the GUI Management Block	
Input:	Emergency ventilation state changes (from SafePLC). Fire detection alarm (from SafePLC).
Output:	Emergency ventilation state changes (to GUI Management Block). Fire detection alarm (to GUI Management Block).
Description/Behavior:	The Network Management Block shall acquire the emergency ventilation equipment status and the fire detection alarm information from the SafePLC and shall transmit them to the GUI Management Block, in order to show them to the operator.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Acquire the pressed button information from the GUI Management Block and provide it to the SafePLC	
Input:	ID of the requested command (from GUI Management Block). Graphic inverted information (from GUI Management Block).
Output:	ID of the requested command (to SafePLC). Graphic inverted information (to SafePLC).
Description/Behavior:	Every time the operator request the activation of the emergency ventilation equipment by pressing the associated button, the Network Management Block shall acquire from the GUI Management Block the ID of the pressed button and the graphic inverted information and shall transmit them to the SafePLC. Between the ID of the button and the graphic inverter information shall be applied a differentiation, using for example the hamming distance approach.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

5.13.1.2 WS GUI Management Block

Show the information acquired from the Network Management block in the VDU	
Input:	Emergency ventilation state changes (from Network Management Block). Fire detection alarm (from Network Management Block).
Output:	Emergency ventilation state changes (to VDU). Fire detection alarm (to VDU).
Description/Behavior:	The GUI Management Block shall acquire the signals from the SafePLC (emergency ventilation equipment state changes and fire detection alarm) through the Network Management Block and shall show them in the VDU, in order to be visible to the operator.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Provide the information of the operator request to the Network Management Block	
Input:	Button press of the operator.
Output:	ID of the requested command (to Network Management Block). Graphic inverted information (to Network Management Block).
Description/Behavior:	Every time the operator request the activation of the emergency ventilation equipment by pressing the associated button, the GUI Management Block shall interpret the operator request and shall provide the ID of the pressed button and the graphic inverted information, by means of the graphic inverter. These information shall be provided to the Network Management Block, in order to be transmitted to the SafePLC.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

5.13.1.3 WS SIF Management Block

Check the CPU Integrity	
Input:	SafePLC triggering message.
Output:	Message corruption.
Description/Behavior:	A mechanism to detect faults in CPU, and to guarantee the proper working of it, shall be implemented. The CPU self-test module performs a cyclic test of the CPU instructions. Its objective is to detect wrong results or possible errors during the execution of instructions. If a failure has been detected, the WS shall corrupt the messages to be sent to the SafePLC. So the SafePLC can manage the error by disabling the WS command and by notifying the fault to the operator. A feedback message on executed test shall be sent from WS to the SafePLC.
Safe State/Reaction:	Corrupt the message to the SafePLC.
Operating mode:	Cyclically.

SIL:	2

Check the Memory Integrity	
Input:	SafePLC triggering message.
Output:	Message corruption.
Description/Behavior:	An appropriate effectiveness memory test shall be implemented in the system, in order to detect faults that can occur in the memory used by safety SW. This module shall be based on algorithms capable to detect the permanent hardware or transient software faults. To test the memory items many test patterns, based on memory fault models, are needed. If a failure has been detected, the WS shall corrupt the messages to be sent to the SafePLC. So the SafePLC can manage the error by disabling the WS command and by notifying the fault to the operator. A feedback message on executed test shall be sent from WS to the SafePLC.
Safe State/Reaction:	Corrupt the message to the SafePLC.
Operating mode:	Cyclically.
SIL:	2

Program Flow Monitoring	
Input:	-
Output:	Message corruption.
Description/Behavior:	The correct program execution sequence shall be verified by means of spy points inserted in the supervised entity code. This mechanism is useful to detect a defective program sequence. This can occur if an individual element of a program is processed in wrong sequence. This failure can be either due to software or due to hardware failures. If a failure has been detected, the WS shall corrupt the messages to be sent to the SafePLC. So the SafePLC can manage the error by disabling the WS command and by notifying the fault to the operator.
Safe State/Reaction:	Corrupt the message to the SafePLC.
Operating mode:	Normal operation.
SIL:	2

Temporal Flow Monitoring	
Input:	-
Output:	Message corruption.
Description/Behavior:	The correct program execution timing shall be verified by means of temporal flow monitoring. This mechanism is used to monitor the execution time and frequency of a configurable number of so called Supervised Entities (pieces of code under temporal supervision). The time base shall be provided by a dedicated timer. If a failure has been detected, the WS shall corrupt the messages to be sent to the SafePLC. So the SafePLC can manage the error by disabling the WS command and by notifying the fault to the operator.
Safe State/Reaction:	Corrupt the message to the SafePLC.
Operating mode:	Normal operation.
SIL:	2

5.13.2 SafePLC Decomposition

According to the SW architectural overview and to the list of HW component used in the SafePLC it is possible to identify the following functional blocks:

- **Verification Management Block:** It manages the execution of the Safety Integrity Functions, including the safety protocol.
- **Network Management Block:** It manages the communication with the WS and with the FieldPLC.
- **Digital Input/Output Management Block:** it manages the digital input and the output signals.

These blocks are all applicable to the OCC and SMR SafePLC.

5.13.2.1 SafePLC Verification Management Block

Manage the execution of the SIF	
Input:	-
Output:	-
Description/Behavior:	The Verification Management Block shall schedule the execution of the Safety Integrity Functions, in order to ensure the integrity of the system. The Safety Integrity Functions to be executed are specified in the chapters titled “OCC Channel A/B SafePLC Functional Requirements” and “SMR SafePLC Functional Requirements”.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

5.13.2.2 SafePLC Network Management Block

Manage the acquisition of the messages from the FieldPLC	
Input:	Emergency ventilation state changes (from FieldPLC). Fire detection alarm (from FieldPLC).
Output:	Emergency ventilation state changes (to Verification Management Block). Fire detection alarm (to Verification Management Block). Emergency ventilation state changes (to WS). Fire detection alarm (to WS).
Description/Behavior:	The Network Management Block shall acquire the emergency ventilation equipment status and the fire detection alarm information from the FieldPLC and shall transmit them to Verification Management Block, in order to check their validity. If the Verification Management Block does not detect any error in the messages, the Network Management Block shall provide these messages to the Workstation.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Manage the acquisition of the messages from the Workstation	
Input:	ID of the pressed button (from WS). Graphic inverter information (from WS).
Output:	ID of the pressed button (to Verification Management Block). ID of the pressed button (to FieldPLC).
Description/Behavior:	The Network Management Block shall acquire the ID of the pressed button and the graphic inverter information from the Workstation and shall transmit them to Verification Management Block, in order to check their validity. If the Verification Management Block does not detect any error in the messages, the Network Management Block shall provide these messages to the FieldPLC.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

5.13.2.3 Digital Input/Output Management Block

Manage the acquisition of the digital input signals	
Input:	Digital input signals.
Output:	SafePanel information (to Verification Management Block).
Description/Behavior:	The Digital Input/Output Management Block shall acquired the digital input data coming from the SafePanel, to test the proper working of the VDU and to enable/disable the workstation. The Digital Input/Output Management Block shall provide these data to the Verification management block, to perform the associated SIF.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

Manage the control of the digital output signals	
Input:	Digital output signal request (from Verification Management Block).
Output:	Digital output signals.
Description/Behavior:	The Digital Input/Output Management Block shall provide the digital output signals in order to manage the SafePanel and to disable the workstation.
Safe State/Reaction:	Disable the workstation commanding and report the failure in the SafePanel.
Operating mode:	Normal operation.
SIL:	2

5.14 Requirements for Environmental Conditions

This section lists and defines the environmental conditions the CBACS Safe is used in.

5.14.1 Temperature Range

All HW components of CBACS Safe are located in technical rooms and then related operating temperature shall be in the range from +5°C to +45°C.

5.14.2 Humidity Range

All HW components of CBACS Safe are located in technical rooms and then related operating humidity shall be in the range from 55% ± 5%.

5.14.3 Workstation Power Supply

The power supply of the Workstation shall be 230VAC.

5.14.4 VDU Power Supply

The power supply of the VDU shall be 230VAC.

5.14.5 SafePLC Power Supply

The power supply of the SafePLC shall be +24VDC.

5.14.6 SafePanel Power Supply

The supply of the SafePanel shall be +24VDC.

ΠΑΡΑΡΤΗΜΑΤΑ / APPENDICES

Α/Α R/N	ΚΩΔΙΚΟΣ CODE	ΤΙΤΛΟΣ TITLE	ΑΝΑΘΕΩΡΗΣΗ REVISION