| | |
|---|---|
| 1. ☐ | ΕΓΚΡΙΝΕΤΑΙ. Εργασίες μπορούν να εκτελεσθούν.<br>*APPROVED. Works may proceed.* |
| 2. ☐ | ΑΝΑΘΕΩΡΗΣΗ ΚΑΙ ΕΠΑΝΥΠΟΒΟΛΗ. Δεν μπορούν να εκτελεσθούν εργασίες.<br>*REVISE AND RESUBMIT. Works should not proceed.* |
| 3. ☐ | ΔΕΝ ΑΠΑΙΤΕΙΤΑΙ ΕΛΕΓΧΟΣ. Εργασίες μπορούν να εκτελεσθούν.<br>*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:<br>TECHNICAL REVIEW BY: | ΕΓΚΡΙΘΗΚΕ ΑΠΟ:<br>APPROVED BY: |
| ΥΠΟΓΡΑΦΗ:<br>SIGNED: | ΥΠΟΓΡΑΦΗ:<br>SIGNED: |
| ΗΜΕΡΟΜΗΝΙΑ:<br>DATE: | ΗΜΕΡΟΜΗΝΙΑ:<br>DATE: |

| ΑΝΑΘ.<br>REV. | ΗΜ/ΝΙΑ<br>DATE | ΣΥΝΤ.<br>INIT. | ΕΛΕΓΧ.<br>CHK. | ΕΓΚΡΙΘΗΚΕ / APPROVED ΟΝΟΜΑ/Ν.Α.ΜΕ | ΕΓΚΡΙΘΗΚΕ / APPROVED ΥΠΟΓΡ./SIGN. | ΕΠΙΚΥΡΩΘΗΚΕ / AUTHORIZED ΟΝΟΜΑ/Ν.Α.ΜΕ | ΕΠΙΚΥΡΩΘΗΚΕ / AUTHORIZED ΥΠΟΓΡ./SIGN. | ΠΕΡΙΓΡΑΦΗ / DESCRIPTION |
|---|---|---|---|---|---|---|---|---|
| F | | | | | | | | |
| E | | | | | | | | |
| D | | | | | | | | |
| C | | | | | | | | |
| B | 17.11.17 | GRI | IFU | Ch. Panou | | G. Valavanis | | Second Issue |
| A | 13.03.17 | GRI | IFU | Ch. Panou | | G. Valavanis | | First issue. |

**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 SIGN.A.TORIES

ΓΙΑ ΧΡΗΣΗ ΣΕ ΤΕΧΝΙΚΑ ΕΓΓΡΑΦΑ ΜΟΝΟ
FOR TECHNICAL DOCUMENTS ONLY

ΑΝΑΔΟΧΟΣ – ΕΚΔΙΔΟΥΣΑ ΕΤΑΙΡΕΙΑ ΕΓΓΡΑΦΟΥ
CONTRACTOR – DOCUMENT ISSUING COMPANY

ΑΕΓΕΚ ΚΑΤΑΣΚΕΥΑΣΤΙΚΗ Α.Ε. – salini impregilo – Ansaldo STS – SELI – HITACHI Hitachi Rail Italy, Spa
Κοινοπραξία ΜΕΤΡΟ ΘΕΣΣΑΛΟΝΙΚΗΣ — ΕΡΓΟ: CON - 06 / 004

ΜΕΛΕΤΗΤΙΚΟ ΓΡΑΦΕΙΟ / DESIGN OFFICE

ΤΙΤΛΟΣ / TITLE

# BACS (Σύστημα Ελέγχου Αυτοματισμού Κτιρίων)
ΜΕ – Περιγραφή της Ολοκληρωμένης Αρχιτεκτονικής

# BACS (Building Automation Control System)
DFD – Integrated Architecture Description

| ΑΝΑΦΟΡΑ ΑΝΑΔΟΧΟΥ / CONTRACTOR'S REFERENCE | ΓΛΩΣΣΑ / LANGUAGE | ΑΡΙΘΜΟΣ ΕΓΓΡΑΦΟΥ – ΣΧΕΔΙΟΥ / DOCUMENT – DRAWING NUMBER |
|---|---|---|
| _ _ _ _ _ _ _ _ _ _ _ _ _ _ | GR/EN | 1G00PS250R789B |
| **ΑΡΧΕΙΟ / FILENAME** | **ΚΛΙΜΑΚΑ / SCALE** | **ΣΕΛΙΔΑ / SHEET No** |
| 1G00PS250R789B | _ _ _ : _ _ _ | 1 of 61 |

Ψηφιακά υπογεγραμμένο από AIKATERINI CHELMI
Ημερομηνία: 2018.02.05 12:02:32 EET

**Item Title**

# BACS (Building Automation Control System) DFD - Integrated Architecture Description

**Item Code**

## 1G00PS250R789B

### History of Revisions:

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| **B** | 17.11.17 | L.Marino/A.Piccolo | C.D'Apice | G.Rizzi/F.Nudo | I.Fulgieri | Second Issue |
| **A** | 13.03.17 | C. D'Apice | F. Nudo/R. Palma | G. Rizzi | I. Fulgieri | First issue. |
| **ΑΝΑΘ.**<br>**REV.** | **ΗΜ/ΝΙΑ**<br>**DATE** | **ΣΥΝΤ.**<br>**INIT.** | **ΕΛΕΓΧ.**<br>**CHK.** | **ΕΓΚΡΙΘΗΚΕ**<br>**APPROVED** | **Πελάτης ΕΛΕΓΧ.**<br>**Customer CHK.** | **ΠΕΡΙΓΡΑΦΗ**<br>**DESCRIPTION** |

### Communications and Open Issues:

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| **1** | | | | | | |
| **ΑΝΑΘ.**<br>**REV.** | **ΚΩΔΙΚΟΣ**<br>**CODE** | **ΑΠΟΣΤ.**<br>**SENDER** | **ΠΑΡΑΛ.**<br>**RECEIVER** | **ΠΕΡΙΓΡΑΦΗ**<br>**DESCRIPTION** | **ΑΠΟΚΡΙΣΗ**<br>**RESPONSE** | **ΚΑΤΆΣ.**<br>**STATE** |

**ΤΟΜΕΑΣ Α**

**Ελληνική Γλώσσα**

**SECTION B**

**English Language**

## Table of Contents

## Index of Tables



## Index of Figures

# 1 Introduction

## 1.1 Context Description

This document is relevant to the Building Automation Control System (BACS) and the Depot Building Automation Control System of Thessaloniki Metro Project. This description covers the main components of architecture of BACS and Depot-BACS.

The purpose of the BACS (in its complete architecture) is to control and monitor all Ventilation and HVAC systems and E&M systems within the stations, shafts and tunnels under all normal and emergency conditions. The building automation equipment managed by the BACS, can be grouped in the three below listed types:

- Electro-Mechanical (escalators, lifts, UPS, pumps, fire detection, etc…);
- Heating, Ventilation and Air Conditioning (HVAC);
- Tunnel Ventilation (over-track exhaust fans, supply air fans, blast shaft fans, jet fans).

Both subsystems, BACS and Depot-BACS, are composed by:

- The HMI Layer (CBACS and Depot-CBACS);
- The Field Layer (Local BACS) that is distributed in 13 (thirteen) stations, tunnel and depot area.

The CBACS subsystem is composed of two parts:

- CBACS No Safe
- CBACS Safe

They are two systems completely separated. The CBACS No Safe is composed of Server and Workstation component; the CBACS Safe is composed of Workstation, Safe Panel and Safe PLC. This difference is for maintain the segregation of the functionality managed.

The system allow monitoring and, where applicable, command building automation equipment in the stations, tunnels and along the railway. The BACS shall also be capable to perform other software functionality (like historical data storage and real-time trending) that will be described in specific technical documents (**ID.05**, **ID.06**).

The Depot-CBACS allows monitoring and, where applicable, command building automation equipment at the depot and is independent.

## 1.2 Scope of the Document

The present document contains an architectural description for the realization of the BACS (Building Automation Control System) within the project "Thessaloniki Metro Project". The aim of this document is to define the description of integrated architecture of all subsystems that the BACS is composed, from HMI layer to field components, particularly in the safe aspect and describes the relevant safety architecture.

The scope of this document is to describe how to integrate (among them) the subsystems that comprise the BACS system. For the single subsystem are indicated the follows points:

- The HW architecture;
- The SW architecture;
- The interfaces with other BACS components and external systems;

CBACS No Safe and Depot-CBACS technical specifications are here defined to comply with:

- Subsystems' requirements (**ID.02**);

All safety requirements of CBACS Safe are specified in the safety requirements specification document (**ID.04**) and are compliant with the referenced standard (Table 1-7 – Reference Standards and Regulations) for the demonstration of SIL2.

## 1.3 Reference Documents

### 1.3.1 Input Documents

**Table 1-1 – Input Documents**

| Item # | Code | Title | Date | Rev # |
|---|---|---|---|---|
| **ID.01** | T_DP15450 | Thessaloniki Metro.<br>Design, Performance and Workmanship Specification.<br>Building Automation Control System. | 01.12.04 | A |
| **ID.02** | 1G00PS250G108 | CBACS.<br>Requirements' Compliance Matrix. | | B |
| **ID.03** | 1G00PS258G314 | CBACS Safe.<br>DFD Architecture Safety Analysis. | | A |
| **ID.04** | 1G00PS258G104 | CBACS Safe.<br>DFD Safety Requirements Specification. | | A |
| **ID.05** | 1G00PS250G105 | CBACS Architecture Description (Technical Specification) | | B |
| **ID.06** | 1G00PS258G105 | CBACS Safe Technical Specification | 30.06.16 | A |
| **ID.07** | 1G00GE270B104 | System & Subsystem Safety Requirements | | |
| **ID.08** | RFP-110/03 | Design, Construction and<br>Commissioning of Thessaloniki Metro<br>System.<br>Technical Description of the Project. | | |
| **ID.09** | 05-724-TRA4-H1 | CBACS - Review of DFD Specifications | 12.2015 | 0 |
| **ID.10** | 05-724-TRA4-H2 | CBACS - Review of Safety Analysis and<br>Verification Report | 12.2015 | 0 |
| **ID.11** | 1G00PS250G306 | Local BACS.<br>DFD – Interface Specification. | | |
| **ID.12** | 1G00PS258G105 | CBACS Safe.<br>DFD Technical Specification | | A |

### 1.3.2 Applicable Documents

**Table 1-2 – Applicable Documents**

| Item # | Code | Title | Date | Rev # |
|---|---|---|---|---|
| | | | | |

### 1.3.3 Previous Stage Document

First issue of this document, then no Previous stage design review document referred.

**Table 1-3 – Previous Documents**

| Item # | Code | Title | Date | Rev # |
|---|---|---|---|---|
| **LD.01** | None. | None. | None. | None. |

### 1.3.4 Literature Documents

**Table 1-4 – Literature Documents**

| Item # | Code | Title | Date | Rev # |
|---|---|---|---|---|
| **LD.01** | None. | None. | None. | None. |

### 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** | 1G00PS250G103 | CBACS.<br>Requirements' Compliance Matrix. | | B |

## 1.4 Reference Standards and Regulations

**Table 1-7 – Reference Standards and Regulations**

| Item # | Code | Title | Date | Rev # |
|---|---|---|---|---|
| **ST.01** | EN 50126:2000 | European Standard, EN 50126. Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). | 2000 | |
| **ST.02** | EN 50128:2002 | European Standard, EN 50128. Railway Applications: Communications, signalling and processing systems. Software for railway control and protection systems. | 2002 | |
| **ST.03** | EN 50129:2009 | European Standard, EN 50129 Railway applications. Communication, signaling and processiong systems. Safety related electronic system for signaling. | 2009 | |
| **ST.04** | IEC 61508:2010 | Functional safety of electrical/electronic/programmable electronic safety-related systems. | 2010 | |

## 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.<br>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.<br>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).<br>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.<br>For example a 1oo2 voting system can tolerate one random component failure and still perform its function.<br>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)<br>or<br>Man-Machine Interface (MMI) | Refers to the software that the process operator "sees" the process with.<br>An example HMI / MMI screen may show a tank with levels and temperatures displayed with bar graphs and values.<br>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”.<br>IEC61508 defines a Safety Function as a “function to be 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 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.<br>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.<br>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.<br>The deliverable of this task is the draft Safety Plan that the Customer must subsequently refine and implement in their development process. |

## 1.6 Glossary of Acronyms

Table 1-9 – Glossary of Acronyms

| Acronym | Description |
|---|---|
| **BACS** | Building Automation Control System. |
| **BSF** | Blast Shaft Fan. |
| **B/W** | Black and White. |
| **CBACS** | Central Building Automation Control System. |
| **MCR** | Main Control Room |
| **DCR** | Depot Control Room. |
| **Depot-BACS** | Depot Building Automation Control System. |
| **Depot-CBACS** | Depot Central Building Automation Control System. |
| **DFD** | Detailed Final Design. |
| **E&M** | Electro-Mechanical. |
| **ECR** | Emergency Control Room |
| **EQP** | Equipment Room |
| **GUI** | Graphic User Interface. |
| **HMI** | Human Machine Interface. |
| **H/W - HW** | Hardware. |
| **HVAC** | Heating, Ventilation and Air Conditioning. |
| **IP** | Internet Protocol. |
| **IEC** | International Electrotechnical Commision |
| **IPC** | Industrial Personal Computer |
| **LAN** | Local Area Network. |
| **MNT** | Maintenance Room |
| **NIC** | Network Interface Card. |
| **OCC** | Operation Control Centre. |
| **OTE** | Over Track Exhaust. |
| **PLC** | Programmable Logic Controller. |
| **SAF** | Supply Air Fan. |
| **SCADA** | Supervisory Control and Data Acquisition. |
| **SIL** | Safety Integrity Level. |

| | |
|---|---|
| **SMR** | Station Master Room. |
| **SMS** | Security Management System. |
| **SPC** | Statistical Process Control. |
| **SQL** | Structured Query Language. |
| **SW** | Software. |
| **TCP** | Transmission Control Protocol. |
| **UML** | Unified Modelling Language |
| **UPS** | Uninterruptible Power Supply. |
| **VDU** | Visual Display Unit |
| **WAN** | Wide Area Network. |
| **WS** | Workstation. |

# 2 History of Revisions

## 2.1 Revision

### 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 | CON-06/004-AIASA-10672/07.03.2017 | Particular attention should be given to the communication among the PLCs (manner of communication, protocol of communication), the communication of the PLCs with the servers of the system at local and central level, the communication among the servers at local and central level, etc. | We agreed. All requests are reported in the Changed Section. | § 4.1 |
| | | Moreover, provide references as detailed as possible to the two different software programs that will be used for the safe CBACS (Microsoft, Unix) | We are reported in the Changed Section. | § 3.5.4 |
| | | as regards the communication between the safe CBACS of the OCC and the safe CBACS in the SMR and their cases of failure. | We agreed. All requests are reported in the Changed Section. | § 4.1<br>§ 4.2 |
| | | Describe the operation in case of failure between one of the two servers, as well as of the safe PLCs inside the OCC, as well as in case of complete failure of the OCC or the SMR | We agreed. All requests are reported in the Changed Section. | § 3.5.3.1<br>§ 3.5.3.2<br>§ 4.1 |
| | | Provide more information on the safe PLCs and the safe panels for better understanding. | We agreed. All requests are reported in the Changed Section. | §3.5.3 |
| | | Make separate submittals for the BACS and for the Depot BACS. | There described in are different paragraphs. So the submission is only one. | |
| RA.02 | Internal Review | On page 22/49 the Jet Fans PLCs in the Track to Depot – 1A14 (Tunnel Nea Elvetia) are two (1A14/JFA & 1A14/JFB) and not six, according to the LBACS DFD. The Jet Fans PLCs in the Forestation near New Railway Station- 1T01 will be named 1T01/JFA & 1T01/JFB. | Reported in the Changed Section. | §3.6.2 |
| | | On page 34/49 in the notice the Field PLC will be Schneider Electric products and not Rockwell | Reported in the Changed Section. | § 3.5.2 |

| | | | | |
|---|---|---|---|---|
| | | Automation products. | | |
| | | On page 41/49 in paragraph 3.6.2 in first sentence the PLC cabinets up to now are 95 and not 85 according to the Local BACS DFD. | Reported in the Changed Section. | § 3.6.2 |
| | | On top of page 42/49 the Jet Fans PLCs in the Forestation near New Railway Station- 1T01 will be named 1T01/JFA & 1T01/JFB and the Jet Fans PLCs in the Track to Depot – 1A14 (Tunnel Nea Elvetia) are two (1A14/JFA & 1A14/JFB) and not six. Correction of figure 3-14 accordingly. | Reported in the Changed Section. | § 3.6.2 |
| | | On page 49/49 the double connection of the LAN to the station TLC WAN is realized from the OTE/SAF PLC cabinet while on page 22/49 is realized from two different PLC cabinets which AM prefers. | Reported in the Changed Section. | § 3.6.2 |
| **RA.03** | Internal Review | Update the Overall to DFD Stage | Figure 3-3 | § 3.3.1 |
| | | Update the Architecture of LBACS equipment to DFD Stage | Pg. 35<br>Figure 3-9 | § 3.5.3 |
| | | Changes of image for more clarification of the distribution of Local BACS' PLC in the station | Figure 3-14 | § 3.6 |
| **RA.04** | Internal Review | "The Field PLCs are connected to form local optical ring and have two redundant and physically separated connections to the L3 LAN/WAN Switch (OmniSwitch 9907) with highly resilient and redundant architecture supplied by TLC in the telecom room (3.4t). The BACS workstations in the SMR (Safe and no Safe) are connected to a L2 Switch in the SMR (2.3), which in turn connects via two redundant links to the same L3 LAN/WAN Switch (OmniSwitch 9907) in the Telecom Room (3.4t).<br><br>In case of loss of WAN communication (e.g. due to F.O. fault) or fault of the OCC BACS, the LAN part of the OmniSwitch 9907 continues to operate, thus the local communication of the BACS workstations with the Field PLCs at station level is maintained, independently of the gateway connection to the OCC via WAN. Further to this provision, the Field PLCs can be also controlled from the local switchboard as described in § 3.6.4." | Reported in the Changed Section. | § 3.1 |

| | | | | |
|---|---|---|---|---|
| | | Other parts of the document (e.g. Ch.3.3.1, 3.5.1, 4.3, ) to be updated accordingly. | Reported in the Changed Section. | § 3.3.1<br>§ 3.5.1<br>§ 3.6.4<br>§ 4.3 |

### 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 | None. | None. | None. |

# 3 BACS Architecture Description

## 3.1 General Description

The BACS System, as showed in the "**Figure 3-1**", is made of the:

- CBACS no Safe (OCC or SMR)
  - To control and monitor all Ventilation, HVAC systems and E&M systems within the stations, shafts and tunnels under normal conditions;
  - To perform real-time trending and Statistical Process Control (SPC) for some critical parameters.

- Depot-CBACS
  - To control and monitor all HVAC systems and E&M systems within the Administration Building, the Operation Control Centre (OCC) and the Depot Area under normal conditions.

- CBACS Safe (OCC or SMR)
  - To monitoring and command equipment involved in Tunnel Ventilation located in the stations, tunnels and along the railway in emergency scenario.

- Local BACS (Field Components of the three previous listed subsystems)
  - To control and monitor all E&M, HVAC, Jet Fans, BSF, OTE and SAF equipment systems within the Administration Building, the Operation Control Centre (OCC) and the Depot Area, stations, shafts, tunnel and recesses under normal conditions and emergency condition.

The BACS System communicates with three External Systems (represented in the "**Figure 3-1**" by dashed lines): Time Server, for the clock synchronization, SMS and ATS for exchange of relevant alarms and events.

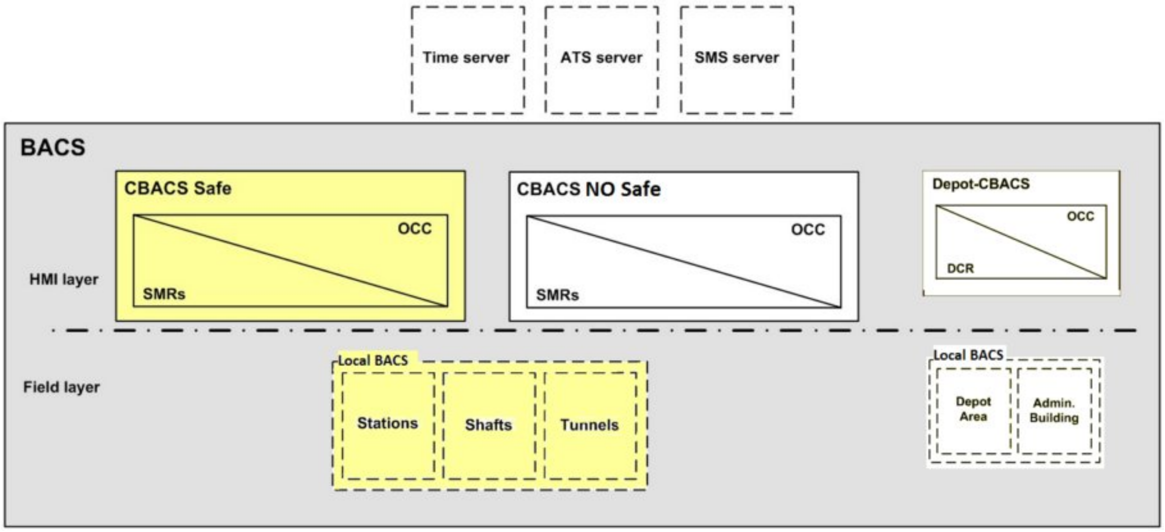



**Figure 3-1 – Layer of Building Automation Control System (BACS)**

The general architectures of the BACS is realized by integration of two levels:

- Human Machine Interface Layer (Central BACS).
- Field Layer (Local BACS);

The CBACS are based on the servers, workstations and printers installed at the OCC, in the SMRs, in the DCR and in the ECR.

The HMI Layer is a distributed Client-Server Architecture based on SCADA System Framework, including:

- SCADA System Server application that communicates with the PLCs of the Field Layer and collects, processes, stores, distributes data towards the SCADA System Client application.

- SCADA System Client application that collects the data distributed by the SCADA System Server and shows them by appropriately developed Graphic User Interface (GUI).
  The GUI allows also sending data towards the connected SCADA System Server.

Then, from the workstation where the SCADA System Client runs, the operator can interact either in monitoring or in control with the Field Layer and plant equipment through the connected SCADA System Server.

The Field PLCs are connected to form  local optical ring and have two redundant and physically separated connections to the L3 LAN/WAN Switch (OmniSwitch 9907) with highly resilient and redundant

architecture supplied by TLC in the telecom room (3.4t). The BACS workstations in the SMR (Safe and no Safe) are connected to a L2 Switch in the SMR (2.3), which in turn connects via two redundant links to the same L3 LAN/WAN Switch (OmniSwitch 9907) in the Telecom Room (3.4t).
In case of loss of WAN communication (e.g. due to F.O. fault) or fault of the OCC BACS, the LAN part of the OmniSwitch 9907 continues to operate, thus the local communication of the BACS workstations with the Field PLCs at station level is maintained, independently of the gateway connection to the OCC via WAN. Further to this provision, the Field PLCs can be also controlled from the local switchboard as described in § 3.6.4."

The independency concept between the OCC and SMR allows the management of the Station by SMR if there isn't any communication with the OCC (OCC fault).

The Local BACS (represented in the "Figure 3-1" by dashed lines) it's constituted by the Field Layer PLCs and all related components (i.e. fiber optic LAN ring). The Local BACS is described in the next paragraph 3.6.

A block diagram that summarizes the limits of BACS components involved is shown in follow **Figure 3-2**:

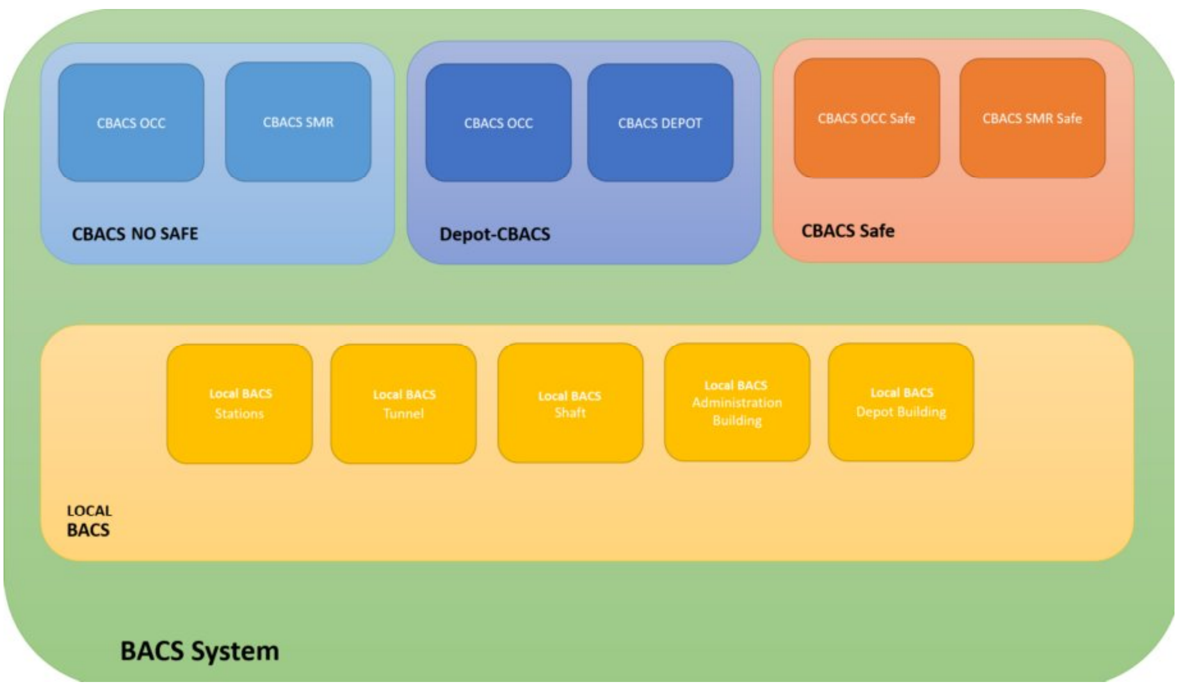



**Figure 3-2 – Block Diagram of Subsystem Components of BACS**

## 3.2 Interfaces components of BACS and other Subsystem

In the table below, the block diagram that summarizes the limits of BACS components involved (shown in Figure 3-2) and the external interfaces are combined for better shown the main component interface:

| | | Internal interfaces **(LOCAL BACS)** | | External interfaces | | |
|---|---|---|---|---|---|---|
| | | DEPOT LBACS (**administration** and **depot building**) | LOCAL BACS (**tunnel**, **station** and **shaft**) | ATS | SMS | Time Server |
| CBACS no Safe | OCC | | ✓ | ✓ | ✓ | ✓ |
| | SMR | | ✓ (only with the Local BACS of SMR) | | | ✓ |
| CBACS Safe | OCC | | ✓ | ✓ | ✓ | ✓ |
| | SMR | | ✓ (Local BACS required from the Tunnel Ventilation scenario) | | | ✓ |
| DEPOT-CBACS | OCC | ✓ | | | ✓ | ✓ |
| | Depot | ✓ | | | ✓ | ✓ |

**Table 3-1 -** Main component interface

## 3.3 Overall Architecture of BACS System Components

### 3.3.1 Integrated H/W solution

The general architecture of the entire BACS system, formed by components in Line Area (Technical Room, SMR) and Administration - Depot Building (OCC, DCC) are summary in the follow figure (refer to "**Figure 3-3**").

The "TLC" boxes and the "cloud" simbols represents the networking equipment and is out of scope of the BACS..

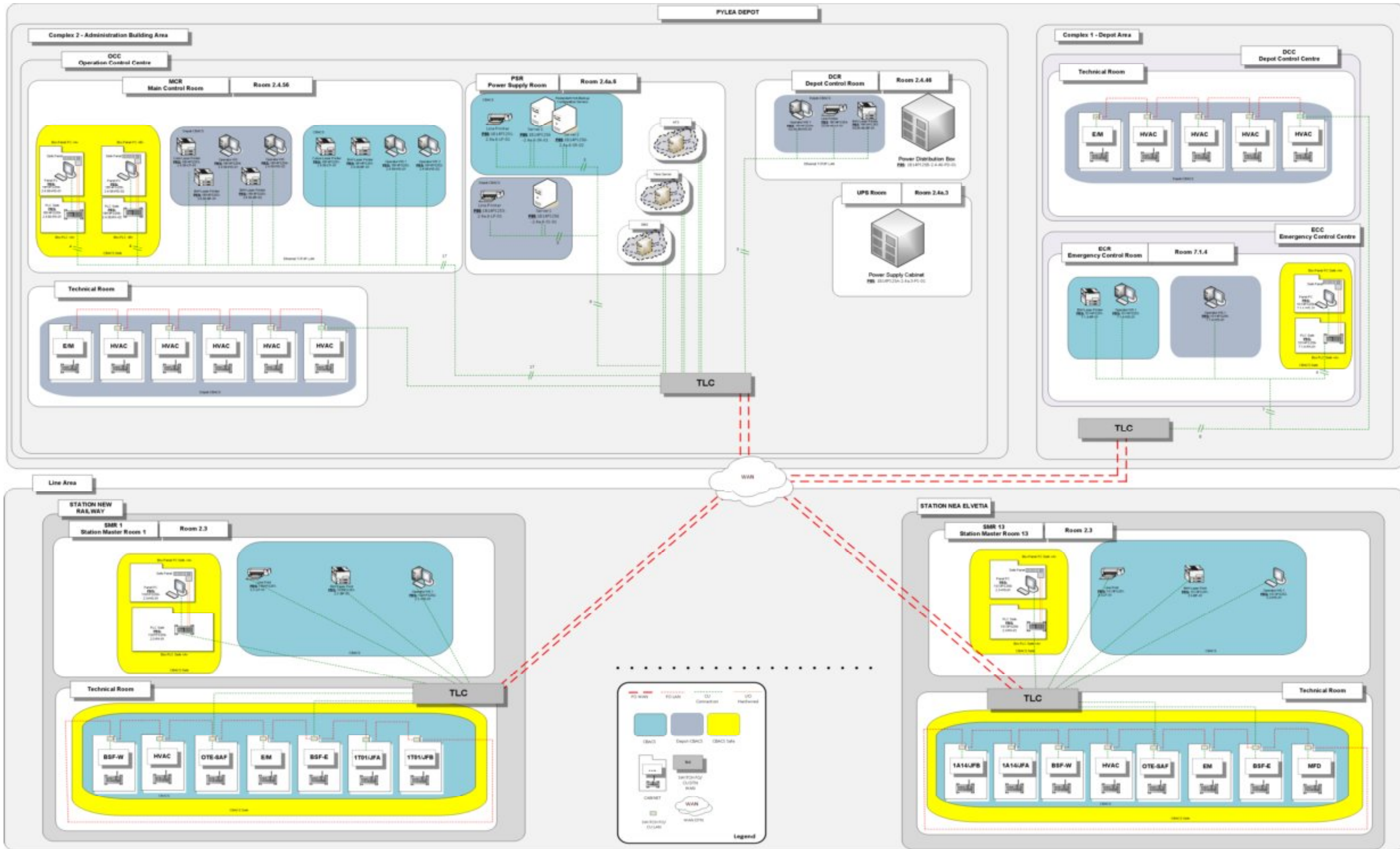



**Figure 3-3 – Overall BACS System H/W Architecture**

## 3.4 CBACS no Safe and Depot-CBACS H/W & S/W Architecture

### 3.4.1 Subsystem's Overview

The Building Automation Control System (BACS), as showed in the "**Figure 3-1**", is made of the:

- CBACS no Safe
  - To control and monitor Ventilation, HVAC systems and E&M systems within the stations, shafts and tunnels under normal conditions;
  - To perform real-time trending and Statistical Process Control (SPC) for some critical parameters.

- Depot-CBACS
  - To control and monitor all HVAC systems and E&M systems within the Administration Building, the Operation Control Centre (OCC) and the Depot Area under normal conditions.

The BACS communicates with three External Systems (represented in the "**Figure 3-4**" by dashed lines): Time Server, for the clock synchronization, SMS and ATS for exchange of relevant alarms and events (for more details, refer to the **ID.05** document).

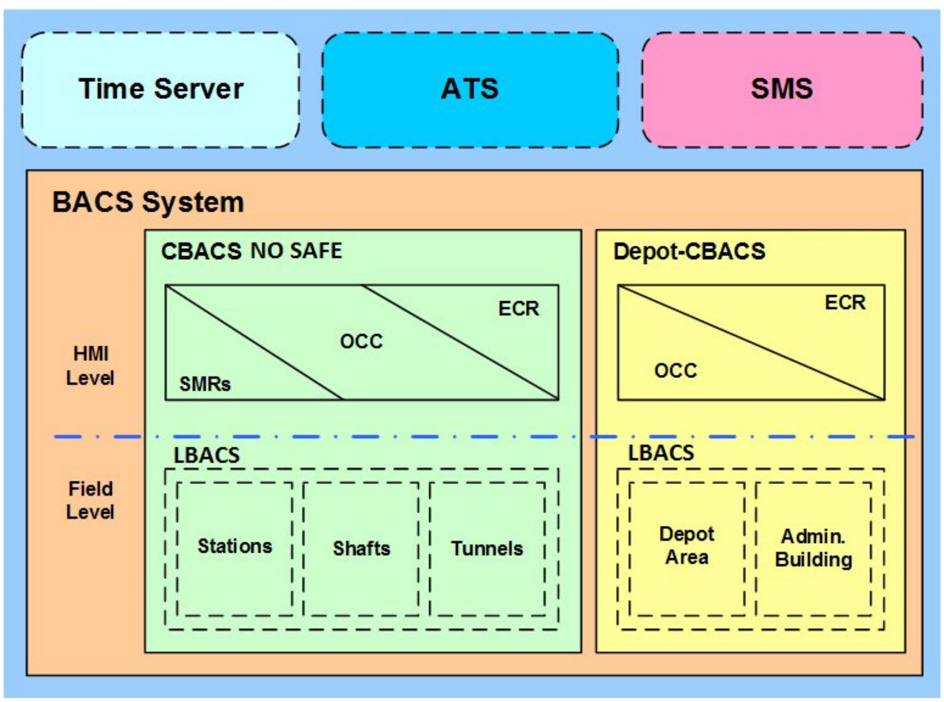



**Figure 3-4 - Building Automation Control System (BACS)**

The general architectures of the CBACS no SAFE and the Depot-CBACS are realized by integration of two levels:

- Human Machine Interface-Level (HMI-Level).
- Field-Level;

The HMI-Level is based on the servers, workstations and printers installed at the OCC, ECR, in the SMRs and in the DCR.

More details about Filed-Level are present in the **3.6** paragraph

### 3.4.2 CBACS no Safe H/W Architecture

The OCC CBACS no Safe H/W architecture (refer to “**Figure 3-5**”) is based on:

- One couple of industrial grade Servers, in redundant hot-backup configuration, acting as SCADA Servers (PWS room);
- Two industrial grade Operator Workstations, acting as SCADA Clients (MCR);
- One industrial grade PC for Emergency Room purpose (ECR);
- Four Printers: one Line Printer (PSR), two B/W Laser Printers (MCR and ECR) and one Color Laser Printer (MCR).

The SMR CBACS no Safe H/W architecture (refer to **Figure 3-5**), is based on:

- One industrial grade Workstations, acting as stand-alone SCADA Server and Client;
- Two Printers: one Line Printer and one B/W Laser Printer.

For more details regarding the mentioned components refer to **ID.05** documents.

The other components in the “**Figure 3-5**”, highlighted in yellow, are part of the BACS Safe

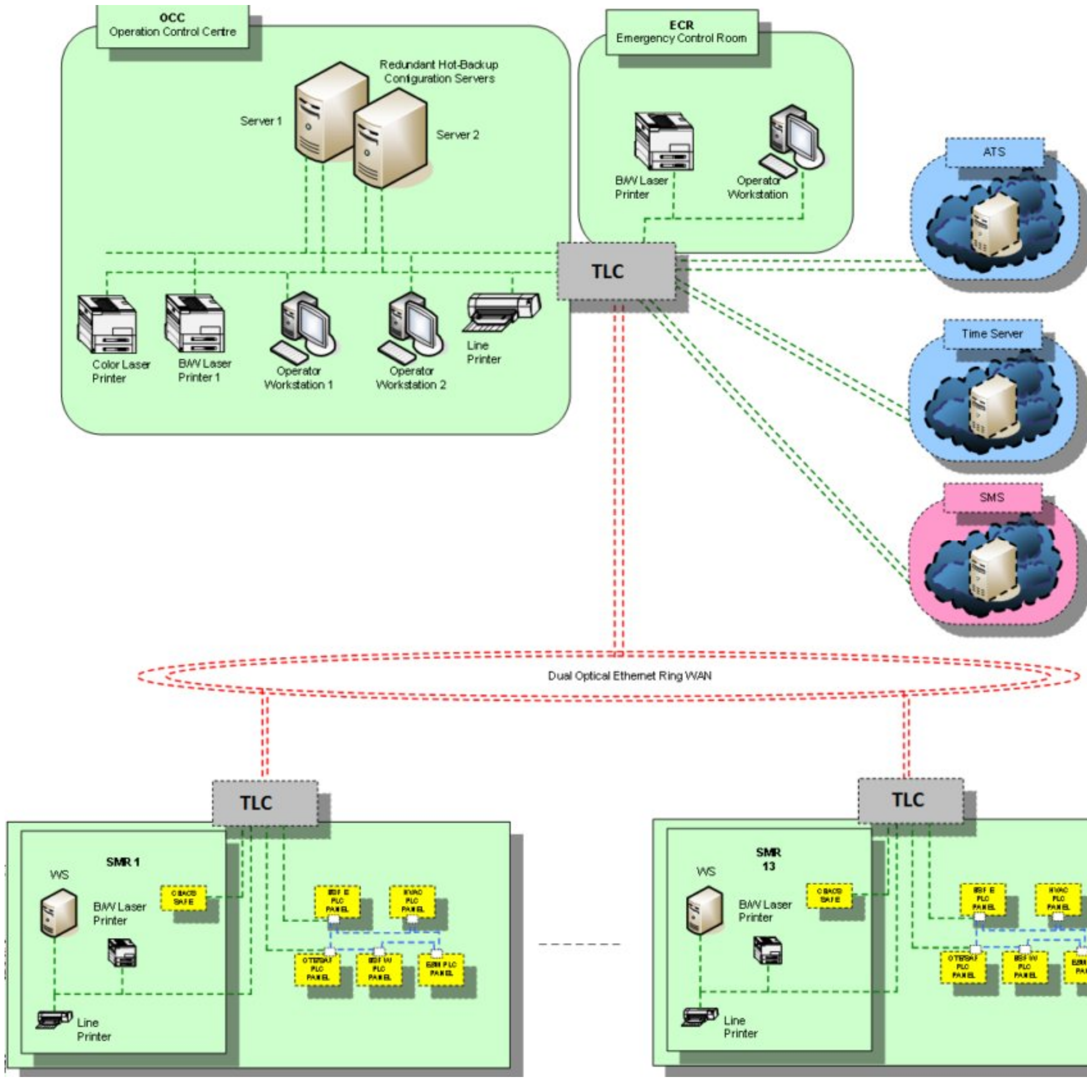



**Figure 3-5 – CBACS H/W Architecture**

The operator workstations act as SCADA Clients in the distributed Client-Server Architecture of the CBACS no Safe at the OCC. They are designed to carry out the main functions below listed:

- To collect in real-time the events/status/alarms distributed by the OCC CBACS no Safe Server application;
- To send data towards the OCC CBACS no Safe Server application;
- To provide the GUI for monitoring and control the Field Layer and plant equipment.

By default, the SCADA Client GUI act as client is configured to attach to either Primary server or Secondary server and will automatically switch to the Secondary server when the primary server fails.
For detail of OCC CBACS no Safe and SMR CBACS no Safe refer the Technical Specification **ID.05.**

### 3.4.3 CBACS no Safe S/W Architecture

The OCC CBACS S/W architecture is based on the components listed in the "**Table 3-2**":

| Computer | Installed S/W |
|---|---|
| **Server 1-2** | Operating System (OS): Server Operating System |
| | Database Management System (DBMS): SQL-based relational DBMS Server Edition |
| | SCADA Server application |
| **Operator Workstation 1-2** | Operating System (OS): Workstation Operating System |
| | SCADA Client application |

**Table 3-2 – OCC CBACS S/W components**

The ECR CBACS S/W architecture is based on the components listed in the "**Table 3-3**":

| Computer | Installed S/W |
|---|---|
| **Operator Workstation** | Operating System (OS): Workstation Operating System |
| | SCADA Client application |

**Table 3-3 – ECR CBACS S/W components**

The SMR CBACS S/W architecture is based on the components listed in the "**Table 3-4**":

| Computer | Installed S/W |
|---|---|
| **Workstation** | Operating System (OS): Workstation Operating System |
| | Database Management System (DBMS): SQL-based relational DBMS Workstation Edition |
| | SCADA Server application |
| | SCADA Client application |

**Table 3-4 – SMR CBACS S/W components**

For more details regarding the mentioned components refer to the **ID.05** documents.

### 3.4.4 Depot-CBACS H/W Architecture

The OCC Depot-CBACS H/W architecture (refer to “Figure 3-5”) is based on:

- One industrial grade Server acting as SCADA Server (PSR);
- One industrial grade Operator Workstation, acting as SCADA Client (MCR);
- One industrial grade Operator Workstation, acting as SCADA Client (ECR);
- Three Printers: one Line Printer (PSR), one B/W Laser Printer (MCR) and one Color Laser Printer (MCR).

The DCR Depot-CBACS H/W architecture (refer to “**Figure 3-6**") is based on:

- One industrial grade workstation acting as stand-alone SCADA Server and Client (DCR);
- One Line Printer (DCR);
- One B/W laser printer used for printing logs on-demand (DCR).

For more details regarding the mentioned components refer to the **ID.05** documents.

The other components in the “**Figure 3-6**", are part of the field component of the LBACS.
The “TLC” box represent the networking equipment and mean that is a independent LAN interconnected through WAN.

.

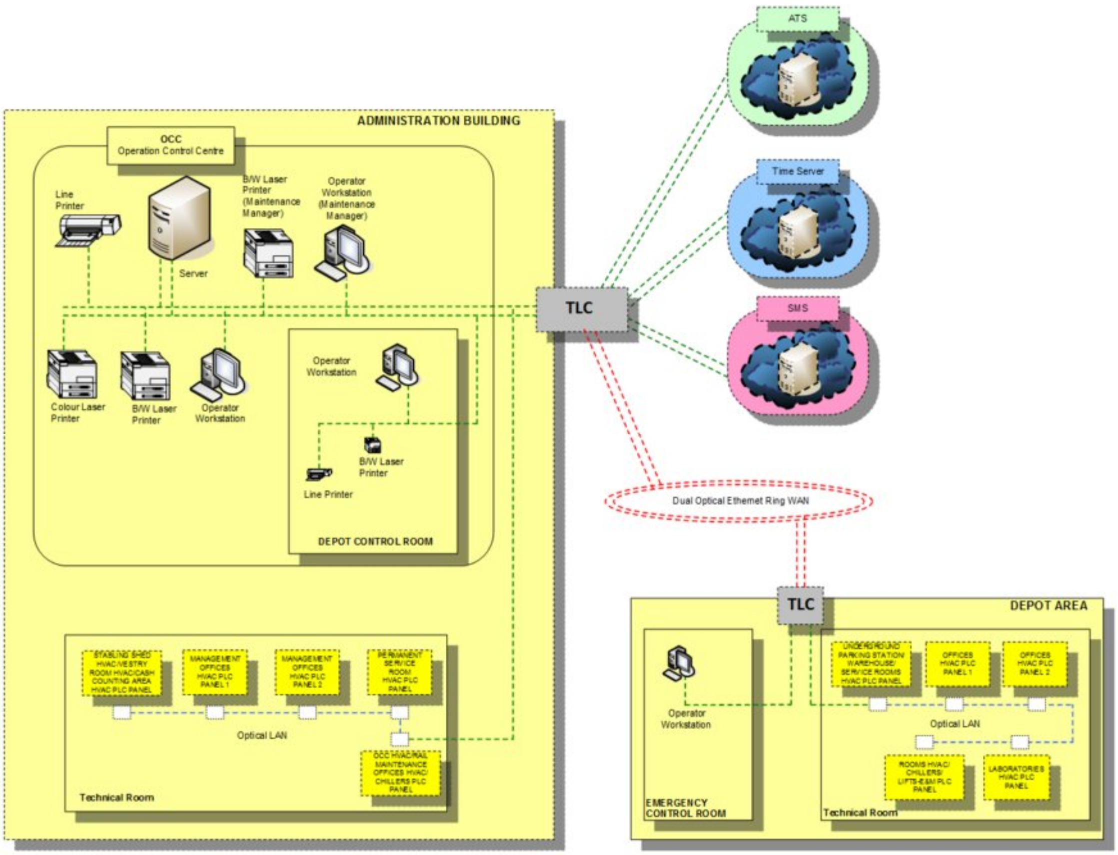



**Figure 3-6 – Depot CBACS H/W Architecture**

There are two operator workstation acts as SCADA Client in the distributed Client-Server Architecture of the Depot-CBACS at the OCC. The Depot BACS is designed to carry out the main functions below listed:

- To collect in real-time the events/status/alarms distributed by the Depot-CBACS server application;
- To send data towards the OCC Depot-CBACS server application;
- To provide the GUI for monitoring and control the Field Layer and plant equipment.

For detail of DEPOT CBACS refer the Technical Specification **ID.05.**

### 3.4.5 Depot-CBACS S/W Architecture

The Depot-CBACS S/W architecture is represented in the "**Figure 3-6**", where the External Systems S/W and the components out of the scope of this technical description are highlighted by dashed lines.

The PC for maintenance purpose is not represented because it's not a part of the S/W architecture.

The OCC Depot-BACS S/W architecture is based on the components listed in the "**Table 3-5**":

| Computer | Installed S/W |
|---|---|
| **Server** | Operating System (OS): Workstation Operating System |
| | Database Management System (DBMS): SQL-based relational DBMS Workstation Edition |
| | SCADA Server application |
| **Operator Workstation 1-2** | Operating System (OS): Workstation Operating System |
| | SCADA Client application |
| **PC for maintenance purpose** | Operating System (OS): Workstation Operating System |
| | Utility Package: Office Software Suite |

**Table 3-5 – OCC Depot-BACS S/W components**

The ECR Depot-BACS S/W architecture is based on the components listed in the "**Table 3-6**":

| Computer | Installed S/W |
|---|---|
| **Operator Workstation** | Operating System (OS): Workstation Operating System |
| | SCADA Client application |

**Table 3-6 – ECR Depot-BACS S/W components**

The DCR Depot-CBACS S/W architecture is based on the components listed in the "**Table 3-7**":

| Computer | Installed S/W |
|---|---|
| **Workstation** | Operating System (OS): Workstation Operating System |
| | Database Management System (DBMS): SQL-based relational DBMS Workstation Edition |
| | SCADA Server application |
| | SCADA Client application |

**Table 3-7 – DCR Depot-CBACS S/W components**

## 3.5 CBACS Safe H/W & S/W Architecture

### 3.5.1 Subsystem's Overview

The CBACS Safe subsystem is the safety-related HMI layer of the main Building Automation Control System (BACS).
Its purpose is to operate fire scenarios for tunnel ventilation, involving equipment, located in the stations, tunnels and along the railway.
The building automation equipment involved in safety functions is listed below:

- Tunnel ventilation (**TV**): over-track exhaust fans (OTE), supply air fans (SAF), blast shaft fans (BSF), jet fans (JF) and Motorized Fire Damper (MFD).

Operation and monitoring of equipment for purpose other than fire scenarios for tunnel ventilation is not through CBACS safe but from CBACS no Safe subsystem; this guarantees separation of safety-related subsystems and functions from non safety-related systems.

The "**Figure 3-7**" 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 (Local BACS), directly controlling plant equipment.

The Field Layer (Local BACS) is described in the next paragraph **3.6**.

The CBACS Safe is composed of Workstation, Safe Panel and Safe PLC (boxes safe). The workstations is stand-alone client/server installed at the OCC and in the SMRs; in any case in every boxes safe runs the HMI application, which:

- Communicates data with Local BACS (is connected to the LAN's Field PLCs through Switch TLC in the SMR), in monitoring and command direction;
- Provides a set of interactive graphic screens (the GUI), which allows the operator to monitoring and command the scenarios of tunnel ventilation.

The HMI-Level safe is based on a stand-alone SCADA system (Server and Client), the boxes safe in OCC (WS, Safe Panel and Safe PLC) are able to communicate with the external systems: data are collected from Safe PLC. In SMR are able to communicate with server clock.

The CBACS Safe in OCC and SMR, in addition to communicating with Local BACS also communicates with some external systems (represented in the Figure 3-7 by dashed lines) like this schema:

- Security Management System (SMS) server: CBACS Safe (in OCC) sends to it alarm messages;
- Signalling System, in particular the Automatic Train Supervision (ATS) server: CBACS Safe (in OCC) 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 (in OCC and SMR) requests and receives from it date & time messages for its time synchronization.

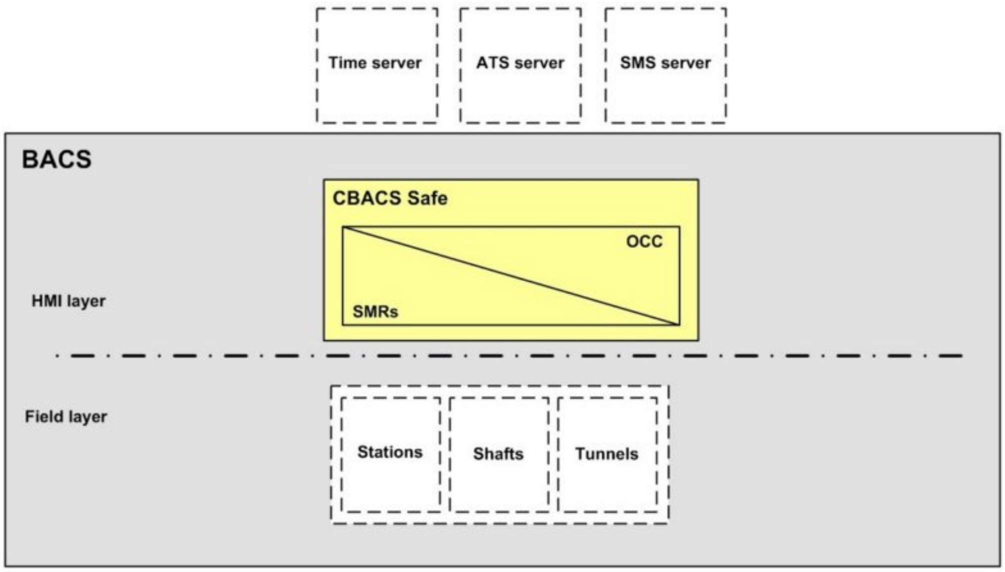



**Figure 3-7 – CBACS Safe Main Group and Layers**

The L3 LAN/WAN Switch supports the communication between the device in the SMR of the station “N” with the PLCs of the adjacent stations “N-1” (previous station) and “N+1” (next station) and others PLCs along the line area involved in the emergency scenario.

### 3.5.2 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 Safe PLC;
- Inform operators about malfunctioning by Safe Panel.

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

- OCC boxes safe (WS, Safe Panel and Safe PLC) and Local BACS;
- SMR boxes safe (WS, Safe Panel and Safe PLC) and Local BACS.

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.

### 3.5.3 CBACS Safe H/W Architecture

The safety architecture (static view) of the CBACS Safe subsystems at the OCC and in the SMRs is shown in the **Figure 3-8** below:

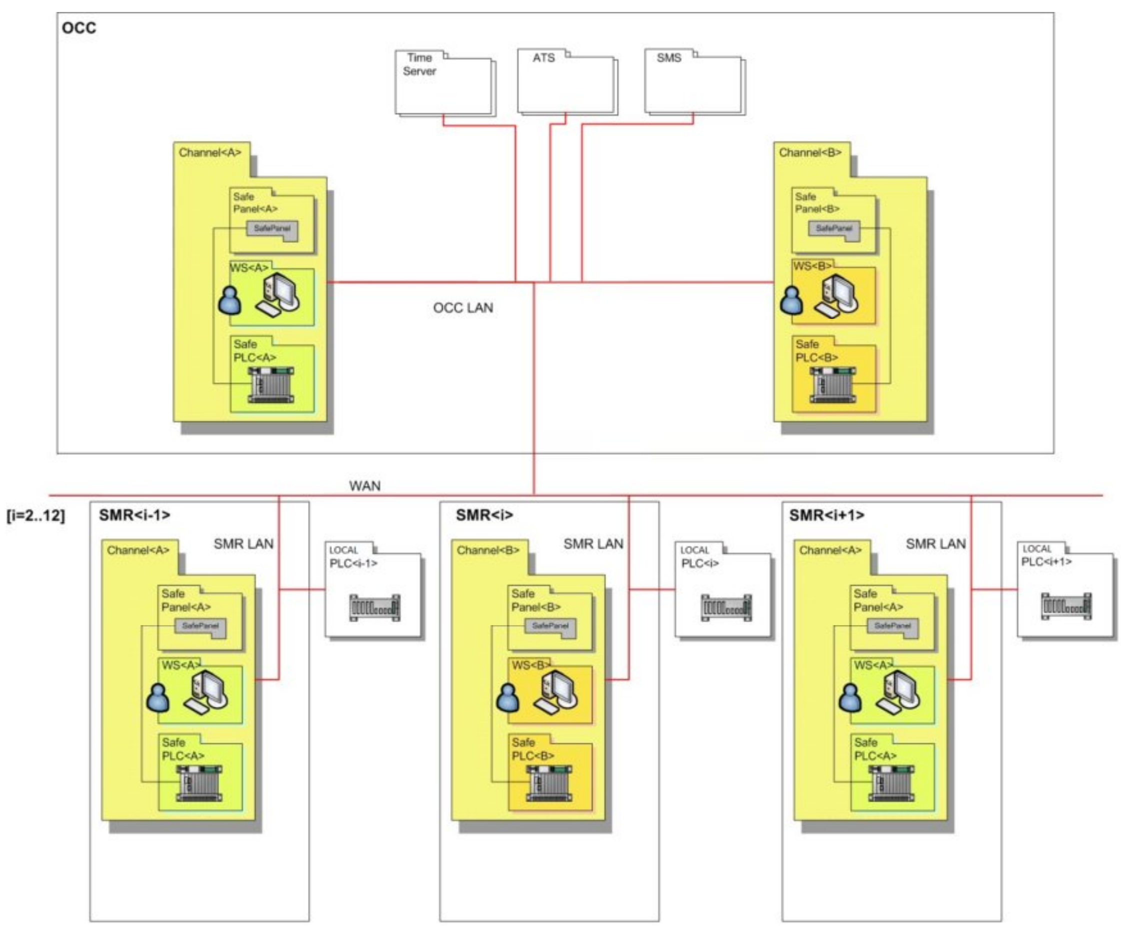



**Figure 3-8 – CBACS Safe Architecture**

The additional components named **Safe PLC** and **Safe Panel** are defined in the next paragraphs. The "Local PLC" package represents the Local BACS (Field Layer).

#### *3.5.3.1 OCC Architecture*

The OCC CBACS Safe architecture, shown in **Figure 3-8**, is based on **dual channel with diagnostic** architectural pattern (Fault Tolerance, 1oo2D).

Both channels can independently execute the same functions, then, both channels and peer components implement the same **safety requirements specification** (SRS) but, to reduce hardware common cause failures and systematic failures, diversity measures have been applied between corresponding hardware and software components.

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

- **WS**. 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.
- **Safe PLC**. This section describes SafePLC<A> and SafePLC<B> components, which are equal both channels. Both Safe PLCs are **fail-safe** and are based on **Schneider Electric** products series below listed:
  - BMEP584040S M580 SIL3 CPU
  - BMEP58CPROS3 M580 SIL3 COPROCESSOR
  - BMENOC0301 MODBUS TCP/IP - ETHERNET/IP MODULE
  - PMXUCM0302 ETHERNET UNIVERSAL COMM TCPOPEN MODULE for communication with external system (no SIL).
  - BMXSDI1602 SAFETY DIG 16I 24VDC SINK
  - BMXSDO0802 SAFETY DIG 8Q TRANS SOURCE 24VDC, 0.5A

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

In **Figure 3-9** 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.

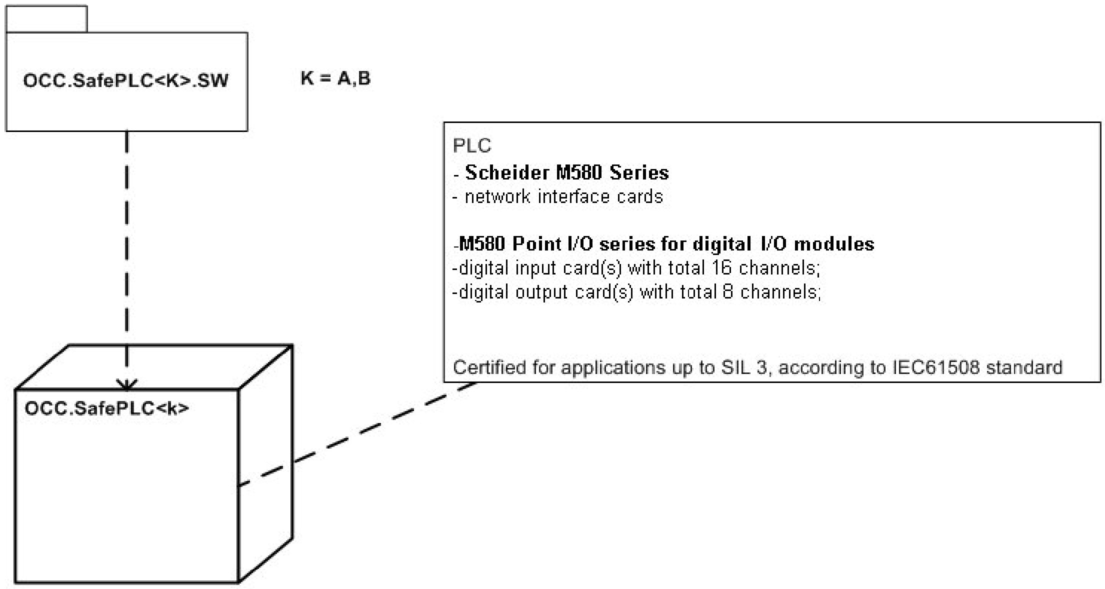



**Figure 3-9 - Deployment of OCC SafePLC SW (OCC.SafePLC<k>.SW) on SafePLC Hardware**

**Notice:** The choice of Schneider Electric products is justified to simplify interoperability with Field PLC, which use Schneider Electric products also, then TCP/IP communication protocol. It allows implementation of safety protocol over TCP/IP (SafeCommLayer). In particular the TLC system must ensure one NTP Server with 20 milliseconds tolerance to ensure the correct safety protocol working. For the communication (via peer to peer) between two PLCs in Safe modality it's necessary have an NTP synchronization. For this synchronization, the PLC's through Ethernet module (BMENOC0301) obtains the synchronization from the centralized NTP Server.

The Safe PLC is equipped with:

- One CPU, with safety diagnostic unit;
- One Coprocessor CPU with safety diagnostic unit;
- Two network interface cards (EtherNet Module BMENOC0301), one for data exchanging with workstation, and one for data exchanging with Field PLC
- One programmable module for external subsystems (ATS and SMS).
- One (or more depending on modularity) digital input card with total 16 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 Safe PLC; in fact, workstation is physically separated from Field PLC and external subsystems.

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 Safe Panel);
- Communication mediator between workstation and Local BACS. 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.

- **Safe Panel.**

This paragraph describes SafePanel's components and next **Figure 3-10** shows the relevant layout.

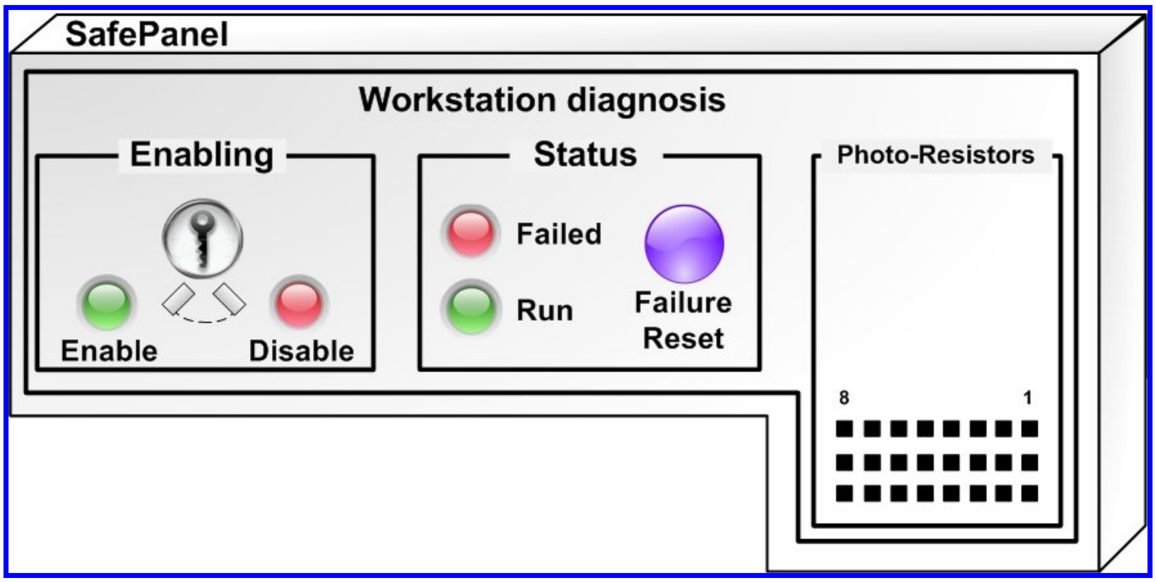



**Figure 3-10 – SafePanel's Layout and Components**

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.

It's the auxiliary hardware component, directly controlled by Safe PLC (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.

<u>In case of IPC fault(s) detected by Safe PLC, the operator realizes anomaly condition by SafePanel indications and moves the other workstation to continue execution of safety monitoring and command functions</u>.

##### *3.5.3.2 SMR Architecture*

SMR CBACS Safe architecture, shown in **Figure 3-8**, is based on dual channel with diagnostic architectural pattern (1oo2D); similar to OCC, then the same components and measures (diversity, fault detection and reaction) are applied to the SMR.

Anyway, some details have to be described:

- Each SMR has a single WS, Safe PLC and Safe Panel, resulting alone 1oo1D architecture;
- Each SMR can monitor and command emergency scenario of adjacent station.

<u>In case of workstation fault(s) detected by Safe PLC, the operator realizes anomaly condition by Safe Panel 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</u>.

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

- Safe PLCs in SMR and OCC have the same hardware implementation (with exception of the programmable module that is present only in OCC);
- Safe Panel in SMR and OCC have the same hardware implementation.

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

For detail of safety protocol of CABS Safe, refer the Technical Specification **ID.03.**

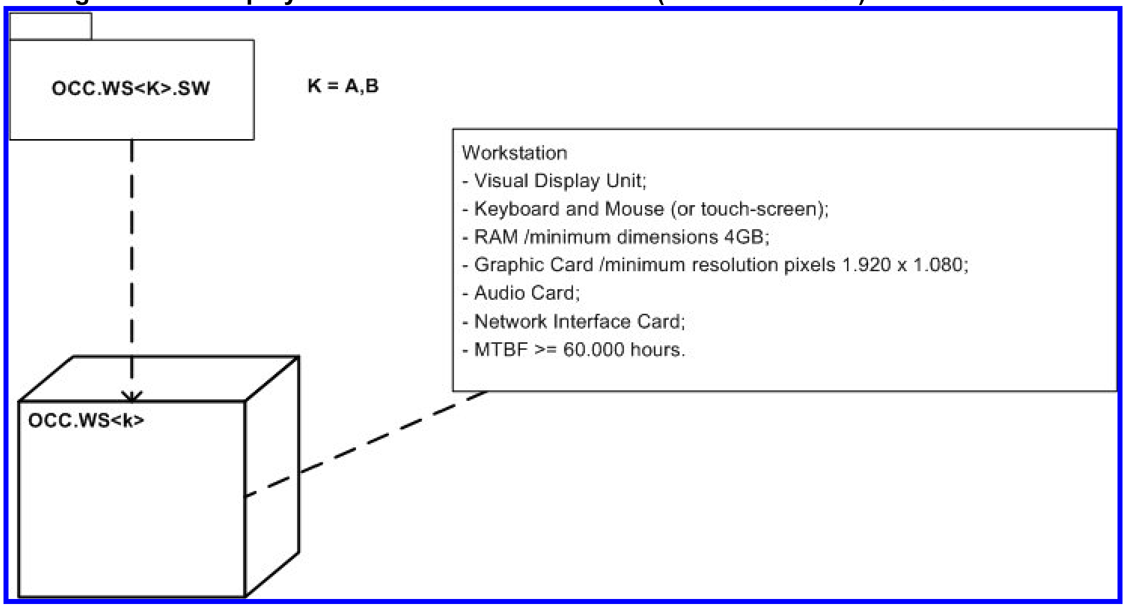
### 3.5.4 CBACS Safe S/W Architecture

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 but the graphics will be identical from the operational point of view. In term of HW reliability parameters, workstations has MTBF >= 60.000 hours.

In **Figure 3-11** 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 3-11 – Deployment of OCC Workstation SW (OCC.WS<k>.SW) on WS Hardware**




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 3-12** shows the main architectural software packages of OCC Workstation<A>.

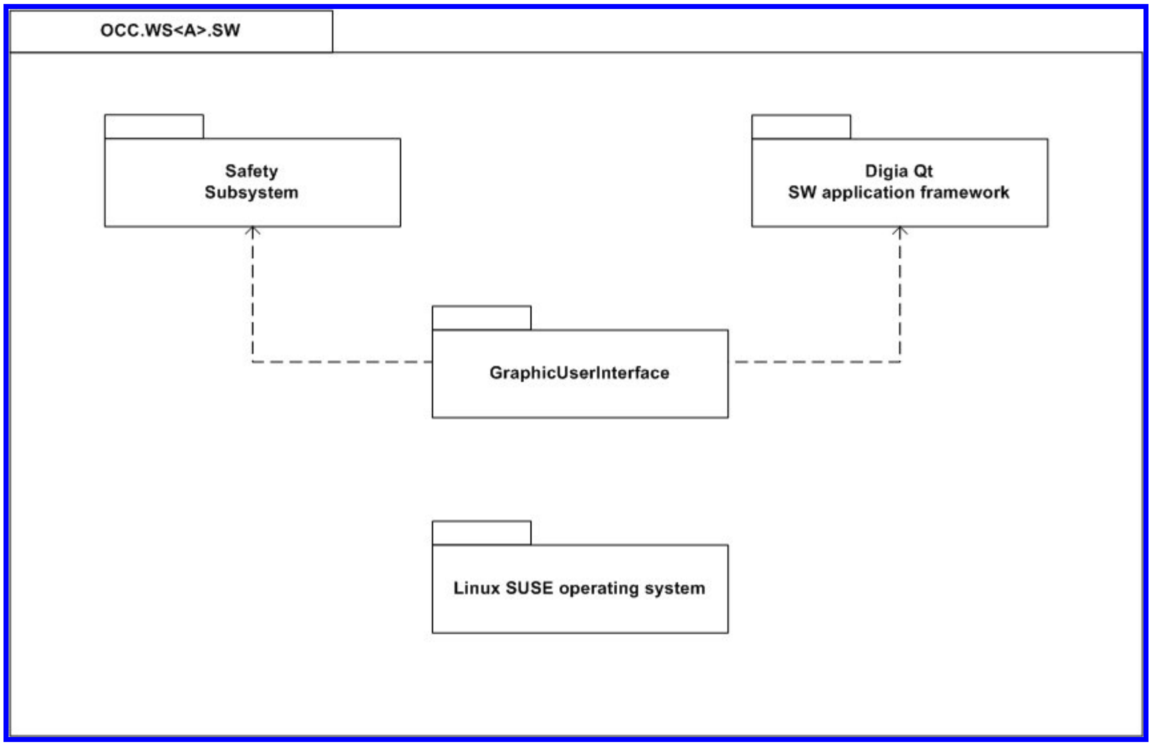



**Figure 3-12 – OCC Workstation<A> SW Packages**

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.

The next **Figure 3-13** shows the main architectural software packages of OCC Workstation<B>.

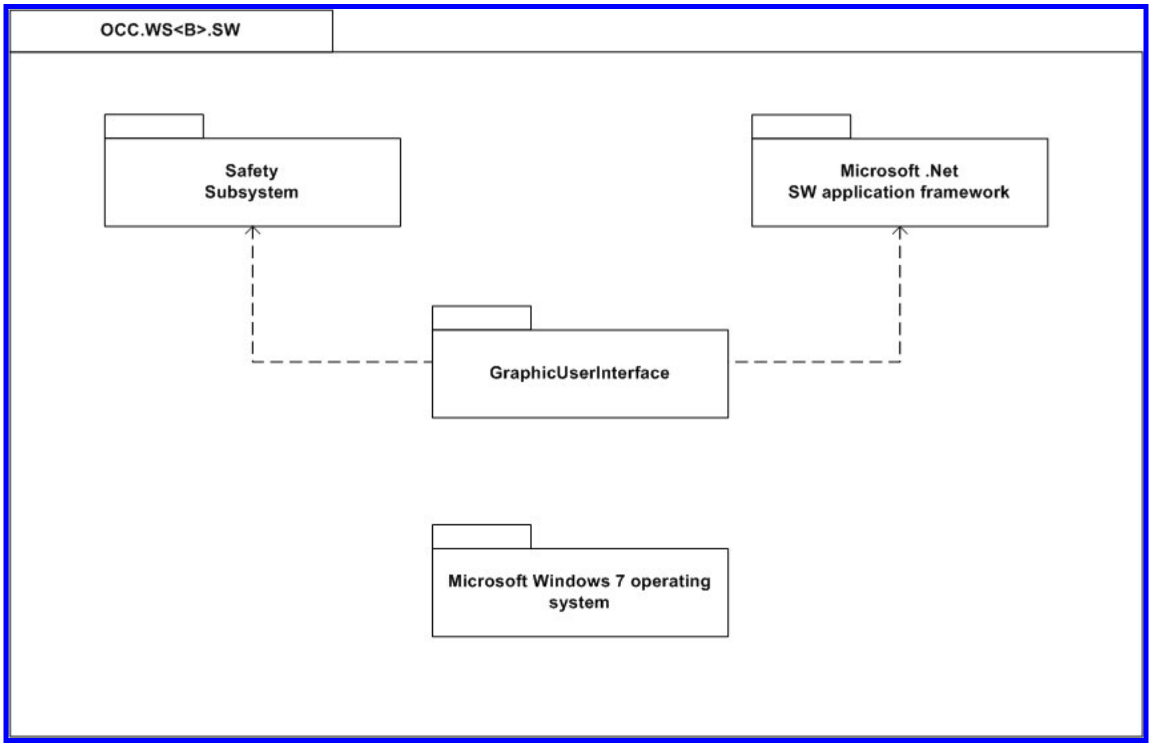



**Figure 3-13 – OCC Workstation<B> SW Packages**

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.

## 3.6 Local BACS H/W Architecture

### 3.6.1 Subsystem's Overview

This paragraph describes, for **Local BACS**, the HW components and relevant operating location.

Local BACS (LBACS) system consists of local substations cabinets equipped with necessary inputs and outputs for monitoring and control of electrical and mechanical CW sub systems

### 3.6.2 Local H/W Architecture

The system is composed by **95** (ninety five) PLC Racks distributed in the **13** (thirteen) stations, tunnel and shafts, at the depot and at the administration building.

The PLCs shall provide through the associated I/O modules the interface to the Tunnel Ventilation and HVAC switchboards as well as to the Station and Tunnel E&M equipment and shall perform local control logic, data manipulation and control of the plant equipment as listed hereafter:

Tunnel Ventilation equipment:

- Blast Shaft fans (BSF), and associated equipment
- Platform Over Track Exhaust fans(OTE) and associated equipment
- Platform Supply Air Fans (SAF) and associated equipment
- Tunnel ventilation Jet fans (JF);
- Shaft Roller Shutter Doors (RSD);
- Motorised Dampers (MOD);
- Fireman box (FB);

HVAC and E&M equipment

- Supply Air Fans for technical area (SAF);
- Exhaust fans (EXF);
- Motorised dampers (MOD);
- Chillers, their pumps and plant;
- Heat Pumps (HP);
- Fan coil units (FCU);
- Uninterruptible Power Supplies (UPS);
- Normal and Emergency Lighting;

- Pumping and drainage systems;
- Hydrants, hose reel systems and deluge valves (DEV);
- Lifts;
- Escalators;

The whole Local BACS for technological systems consists of 13 LBACS installed in Stations; each of them will be composed of 5 fully cabled cabinet containing the PLC unit and relative I/O modules for hardwire interconnection to equipment and Modbus (RS485) Gateway modules (only for HVAC PLC). This unit will be connected to the WAN and consist in the following equipment:

- BSFE (Blast Shaft Fan East side) system;
- BSFW (Blast Shaft Fan West side) system;
- SAF/OTE (Supply Air Fan - Over Track Exhaust) system;
- HVAC (Heating, Ventilation and Air Conditioning) system;
- E/M (Electro-Mechanical) system.

Therefore, each station includes 5 (five) PLC racks, as already described, and each PLC interacts and controls the equipment just mentioned.

In addition to PLCs mentioned before, there are 4 (four) JF PLCs (2 at the start of tunnel and 2 at the end of tunnel), 1 (one) MFD PLC, the Depot PLCs (EM and HVAC) and the 14 (fourteen) PCP PLCs subdivided between 6 (six) stations.

For more details, see **Figure 3-14**

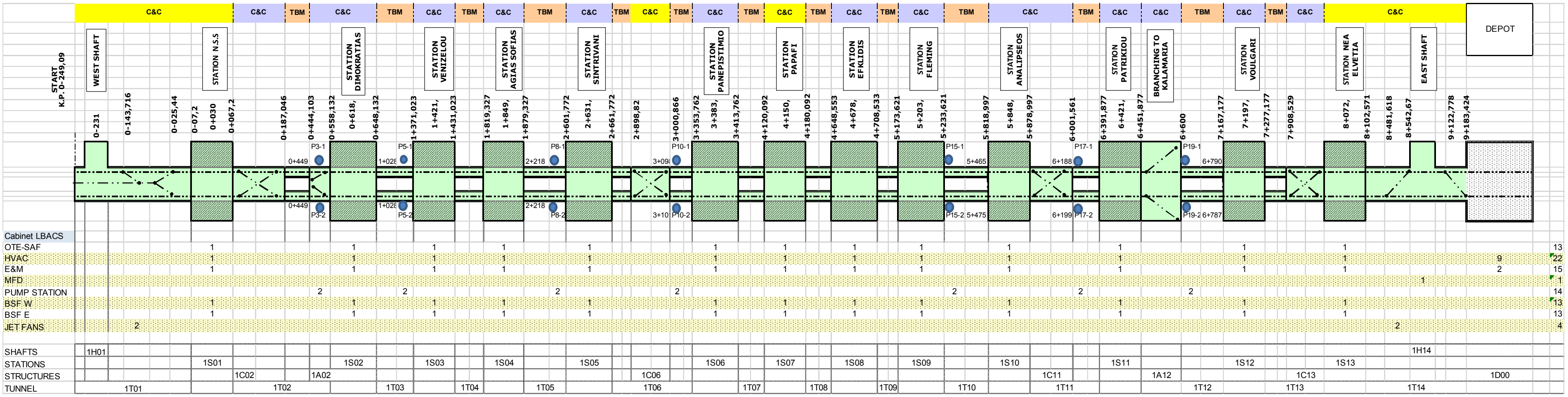



**Figure 3-14 -** Overall of PLC's Station

The PLC's subsystems mentioned before are described below:

- BSF System, is related to Ventilation equipment of the Western and Eastern shaft, and shall comprise of appropriate power feeders, switchgear and automation for the blast shaft fans and relative equipment with that shall interact.
- SAF/OTE System, is related to the Ventilation equipment of the station platform and tunnel, and shall comprise appropriate power feeders, switchgear and automation for the SAF fans that supply air via the SAF ducts at the platform sides and the OTE fans that extract air via the OTE ducts at the area over/above the track and relative equipment with that shall interact.
- HVAC System, is related to HVAC equipment and shall comprise of and shall comprise appropriate power feeders, switchgear and automation for the Ventilation, Air Conditioning and heating of personnel rooms, passenger rooms and technical rooms of the station.
- E/M System shall comprise of electric control panel of the equipment escalator, lifts, pumps, dry stand pipe system, normal and emergency lighting.
- JF System, is related to Ventilation equipment, and shall comprise of appropriate power feeders, switchgear and automation for the jet fans and relative equipment with that shall interact.

Tunnel between forestation and "New Railway" station (S01) includes **2** (two) PLC Racks that monitor and command the relevant **JF** (Jet Fan) subsystem (1T01/JFA, 1T01/JFB). Each JF PLC manageds a group of 4 fans.

Tunnel between "Nea Elvetia" station (S13) and East Shaft includes **2** (two) PLC Racks that monitor and command the relevant **JF** (Jet Fan) subsystem (1A14/JFA, 1A14/JFB). Each JF PLC manageds a group of 6 fans.

The East Shaft includes **1** (one) PLC Racks that monitors and commands the relevant **MFD** (Motorized Fire Damper) subsystem.

The Depot Building & Areas (also named Complex 1) includes **6** (six) PLC Racks that monitor and command the relevant **HVAC** and **E/M** subsystems.

The Administration Building (also named Complex 2) includes **5** (five) PLC Racks that monitor and command the relevant **HVAC** and **E/M** subsystems.

The number and type of PLCs concerning Depot (Complex 1 and 2) could be different by the **Figure 3-15**


**Figure 3-15 – Local BACS – PLC Type**

All PLC Racks house all equipment necessary for monitoring and command; thus:

- Power supply units for electronics devices and hardwired I/Os;
- Protection units against over-voltage, over-current, short-circuit circuits;
- Ethernet switch(es) and electrical-to-optical media converter(s);
- PLC components, which include housing chassis, CPU, communication modules, DI/DO modules.

All the cabinets described earlier will be connect to the WAN through I/O card and network devices.

Quantity and typology of equipment will be different from site to site (and PLC to PLC) in order to keep into account, the relevant I/O signal to manage.
The cabinets will be connected to one UPS power line.

**Implemented Protocols:**

- Modbus over TCP/IP;
- Ethernet/IP;
- Modbus over Serial RS 485;
- SIL 2 Safe protocol (based on time synchronization server master clock).

**Interfaces:**

- Copper RJ45 Ethernet for DTN connection;
- Copper cable for Power supply
- Copper cable for earth connection
- Copper cable for Hard-wired I/O data with field equipment;
- Copper cable for Serial I/O data with field equipment;
- Fiber Optic cable for LAN LBACS.

For more details, see **ID.11**

**Hardwired connection:**

- According to **Figure 4-2**, for each Station.

**ModBus RS485 connection:**

- According to **Figure 4-2**, for each Station in HVAC cabinet.

**TCP/IP using copper connection and DTN facilities:**

- Communication servers at OCC

**Ethernet using copper connection and DTN facilities**:

- PLCs time Synchronization

The **Figure 4-2** below shows system's architectural view, including network connections for Local BACS of Station and Depot. The "cloud" symbol with the equipment inside, represent the networking equipment (DTN) and is out of scope of BACS.

### 3.6.3 Local S/W Architecture

The PLCs software architecture will be based on:

- Real Time Operating System (RTOS) that ensures deterministic engine features;

- Application Software that executes the raw data scaling in engineering units (field interface by means of hardwired or networked signals) and strategy execution.

Development software will provide the standard tools to configure, program, diagnose and maintain programs and devices (PLCs and RIOs).

All software shall be developed using appropriate techniques and measures to ensure that the software and firmware meets the systematic failure requirements of all specific safety functions at least at SIL 2. The application will be implemented using programming languages compliant to IEC 61131.

The software shall comprise a hierarchical structure which using techniques that functionally breaks down the requirement in to a few smaller, more manageable, comprehensible functions having well defined interfaces shall be used.

The PLC Software programming shall use industry standard programming languages like Ladder logic; however functional block or structured text can be used where required to reduce the complexity of the program code or to perform complex mathematical tasks or algorithms.

If more than one programming language is used, it shall be used in a consistent manner and shall be seamlessly integrated into the PLC system to avoid confusion in understanding the application.

The organization of the program data, data tables and program files within the PLC shall be structured and methodical in approach using different files for functions to allow ease of understanding.

Reuse of proven software in equivalent applications is to be encouraged.

All software shall be understandable, analyzable, testable, verifiable and maintainable, and shall be designed and fully documented so that it shall be managed from competent staff.

### 3.6.4 Operation Mode and Control

There are different modes to control the local equipment.

Normally commands can initiate from OCC, Subsystem level (if present), and equipment level (if present) that is the highest priority level in the command execution. As well, a Fireman Box mimic panel that can be used as intermediate level in the command chain. Fireman Box can control only a subset of subsystems, those related to safety in critical conditions.

The choice of the control mode is performed by means of hardware selectors.

The Operators is able to initiate manually the control of all plant and equipment from:

1. OCC operator workstation;
2. SMR operator workstation;
3. Local switchboard via pushbuttons.

In manual mode all automatic control on the selected equipment is disabled.

On deselecting equipment from the Automatic to the Manual mode the equipment state shall remain unchanged. The operator shall perform all control actions after selection to the Manual mode.

Table 1 below summarises the control locations for manual operation of equipment.

| Equipment Designation | Equipment use | Control available | Location |
|---|---|---|---|
| Electrical switchboards | Motor Control Centre (MCC).<br>This is the central motor starter panel for a group of fans and MODs. This panel contains the electrical protection and control gear for the equipment under control and the PLC's in enclosed PLC-panels with associated I/O for the Tunnel Ventilation and HVAC Systems and E&M Systems.<br>Local control can be selected and performed from this location | Remote/Local or Remote/ Local normal/ Local emergency | Blast shaft and station plant rooms |
| FB | Fireman Box<br>This is a pushbutton operated back up panel that is principally used in emergency situations | Remote / Scenario | Station concourse |
| SMR Operator workstation | Computer terminal with graphical interface within the station used by the operator for plant and equipment monitoring and control of the Tunnel Ventilation and HVAC Systems and E&M systems | Auto / Manual | SMR |
| OCC Operator workstation | Computer terminal with graphical interface within the central Operations Control Centre used by the operator for plant and equipment monitoring and control and parameter adjustments of the Tunnel Ventilation and HVAC Systems and E&M systems. | Auto / Manual | OCC |

**Table 3-8 - Equipment Control Source**

Depending on position of selectors different control mode can be performed.

Below is depicted the chain of a command starting from OCC Level to equipment Level. It is depicted the two cases in which Fireman Box is or is not involved.

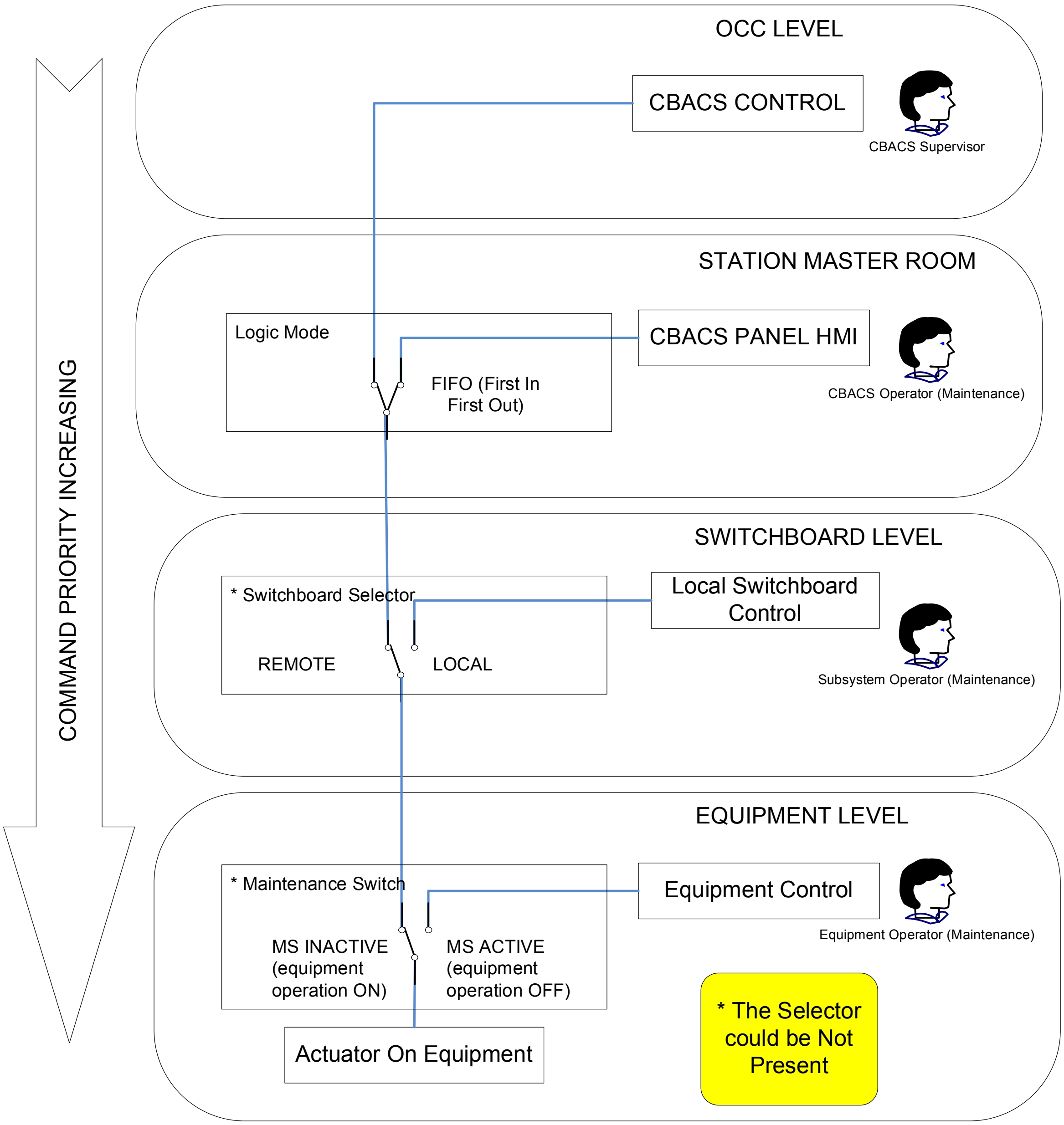



**Figure 3-16 - Typical Flow of command from HMI BACS to equipment; Fireman Box is not involved**

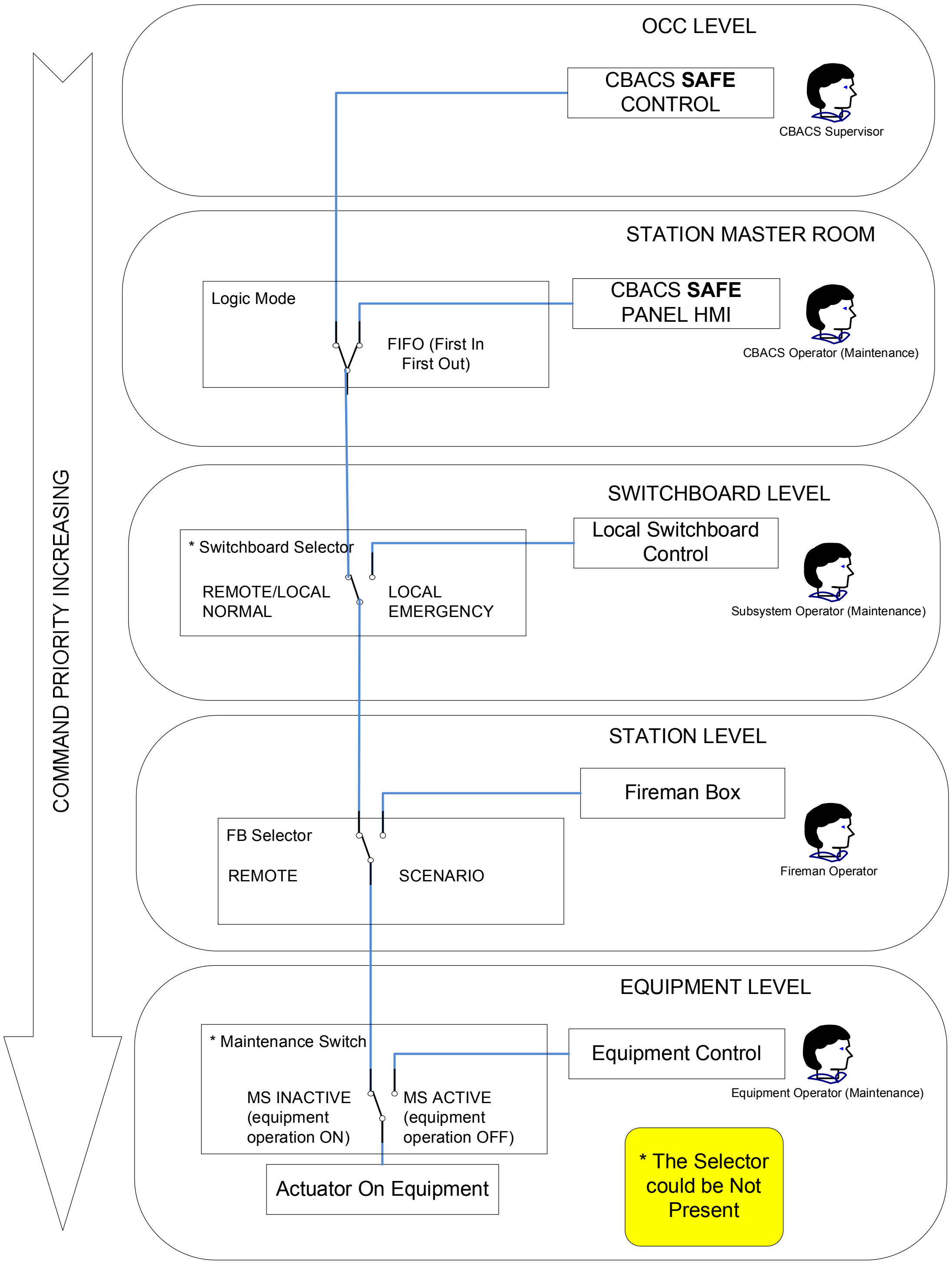



**Figure 3-17 - Typical Flow of command from HMI BACS to equipment; Fireman Box involved**

Starting from the highest command priority level (equipment) we have:

- **Equipment Maintenance Switch** : when activated, setting the hardware equipment selector in this position on the equipment, all other levels can only monitor the 'OFF' state of the equipment. A data point is transmitted to the BACS when the maintenance switch is in position for maintenance.

  This modality affects only the equipment or, in case of partial local, the group of equipment involved. The activity on equipment MUST be carried out by a Equipment Operator.

- **Fireman Box Control Mode (Remote/Scenario)**: when the local hardware selector is on Scenario position on Fireman Box, the control is taken by this last one and both OCC and SMR can only monitor the state of the equipment. In this modality no command or sequences coming from OCC or SMR can be performed if related to equipment controlled by the Fireman Box. The Fire-mans' Box (FB) operation is controlled by a switch (REMOTE - SCENARIOS) on its panel:

  1) In position "remote", no intervention is possible from the FB

  2) In position "scenarios", 4 scenarios can be executed from the FB: 1 - fire on concourse, 2 - fire on platform, 3 - fire on train at platform/track-1, 4 - fire on train at platform/track-2.

  The execution of these 4 scenarios are executed directly from the switchboard at the station level and the PLC OTE/SAF is hard wired notified, and informs the CBACS. Note that from the FB, scenarios can be executed even if the switchboard is in condition LOCAL - EMERGENCY MODE or LOCAL – NORMAL also. This mean that only if the equipment maintenance switch is active mode the FB can't be executed the scenario.

- **Switchboard selector switch** (Switchboard Level in accordance to): two data points are produced by the same selector switch.
  - **Remote Mode.** In this position, the equipment connected to the electric switchboard cannot be locally controlled. All control is handled by the others level.
  - **Local Mode.** Note that when activated, the Central BACS (HMI) can only monitor the state of the subsystem and the control will be available only from the switchboard. To have total control from CBACS the related switchboard must be in remote mode. The activity on subsystem must be carried out by a Switchboard Operator (maintenance).

- **Switchboard selector switch** (Switchboard Level in accordance to): three data points are produced by the same selector switch.
  - **Remote Mode.** In this position, the equipment connected to the electric switchboard cannot be locally controlled. All control is handled by the others level.

- **Local Normal Mode**. In this position the equipment connected to the electric switchboard can be locally controlled, by the corresponding pushbuttons on the switchboard, through the CBACS SAFE software. This position corresponds to the operation with active supervision through CBACS SAFE. In this position the equipment connected can be controlled from the FB or by scenarios from the SMR or OCC (FB has the highest priority). In this position, all equipment protections and damper positions are taken into account. In this position, local control of equipment is accomplished through the BACS functionality. Note that when activated, the Central BACS (HMI) can only monitor the state of the subsystem, to have total control from CBACS the related switchboard must be in remote mode. The activity on subsystem must be carried out by a Switchboard Operator (maintenance)
- **Local Emergency Mode.** In this position, the equipment connected to the electric panel can be locally controlled from the electric panel or from the local FB. All equipment protections (Temperature sensors, vibration sensors, differential pressure sensors) and damper positions are ignored even if this leads to equipment destruction. In this position, local control of equipment is accomplished from the electric panel internal circuitry without the BACS intervention other than monitoring.

- **Central BACS (OCC and SMR):** At the SMR and the OCC, CBACS SAFE can be activated to execute all fire scenarios. These scenarios are executed through the LOCAL BACS PLCs if the switchboards are in condition REMOTE or LOCAL – NORMAL. If a switchboard is in condition LOCAL - EMERGENCY it will not execute, the commanded by the corresponding PLC.

  When all selectors are in Remote position, it will be possible to control the local equipment from the Central BACS.

The full control depends anyway on the selector position at FB, Switchboard and Equipment levels.

The Central BACS System logs the change of state and especially when a change of operational mode is performed.

The activation of the maintenance switch will be treated as a low level Alarm for upper levels.

# 4 Network, BACS Network & Diagnostic Features

Concerning to traffic information between and inside stations, the TLC is opportunely configured to manage the traffic and routing, in high performance (millisecond order), without modify or/and filter the data's package between different LANs of the BACS. But, also the telecommunication infrastructure must warranty the compartmentation of data:

- the real time data must have a different routing from the no real time data (i.e. printer)
- default denied must be applied for routing data from the external systems, so only some IPs address for each external systems must be connected to BACS.

## 4.1 CBACS Connection

The Central BACS is the HMI layer of the whole BACS. The communication between the Central BACS Server PCs at the OCC and Local BACS PLCs of a station "i", is physically supported by WAN infrastructure (DTN).

The couple of CBACS (**Figure 3-5**) servers are connected, by their dual Network Interface Cards (NIC), to the OCC Ethernet TCP/IP LAN, so that, they are able to directly communicate with the OCC Operator Workstations and the External Systems Servers (Time Server, SMS Server and ATS) connected on the same LAN.
The communication between the CBACS servers at the OCC and PLCs of a station "N", is physically supported by WAN infrastructure, independently to SMR server

The WAN supports the peer to peer communication between the PLCs of the station "N" with the PLCs of the adjacent stations "N-1" (previous station) and "N+1" (next station), independently to SMR.
The LAN that are present in each site (OCC LAN, station LANs, depot LAN, Local BACS LAN) are completely interconnected via WAN.

The CBACS workstation in the SMR is connected to the station LAN, so that, it's able to communicate with the PLCs, "independently" to the OCC CBACS; at last it can communicate, through the WAN, with the Time Server.

The independency concept between the OCC and SMR allows the management the faults in the OCC CBACS.

The OCC CBACS servers operate in applicative redundant (hot-backup) configuration, that is, one server only (Master or Primary) performs the main functions, whilst, the second server (Slave or Secondary) is continuously aligned with the first one, by specific redundancy management application task included in the SCADA System Framework.

In event of failure of the Primary server, the redundancy management application activates the Secondary server immediately to perform the main functions, previously provided by the Primary; this operation will be made in a transparent way.

## 4.2 CBACS Safe Connection

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

The communication between the CBACS Safe Boxes at the OCC and the Field PLC LAN of a station <i> is physically supported by WAN infrastructure.

The CBACS Safe Boxes in the SMR is fed by local station power supply and is connected to the station LAN, so that, it's able to communicate with the Field PLC LAN, "independently" to the OCC CBACS Safe; at last it can communicate, through the WAN, with the external systems Time server.

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

The CBACS Safe Boxes in the SMR allows the operator to execute the monitoring and command functions of plant equipment of the two linked adjacent stations.

For more details about communication and protocol, see **ID.12**

Considering **Figure 4-1** (package "WS" mean CBACS Safe Boxes composed of Workstation, Safe Panel and Safe PLC and the package "Field PLC" mean Local BACS PLC and Fiber Optic LAN), we define the scope of the safety system being the CBACS Safe.

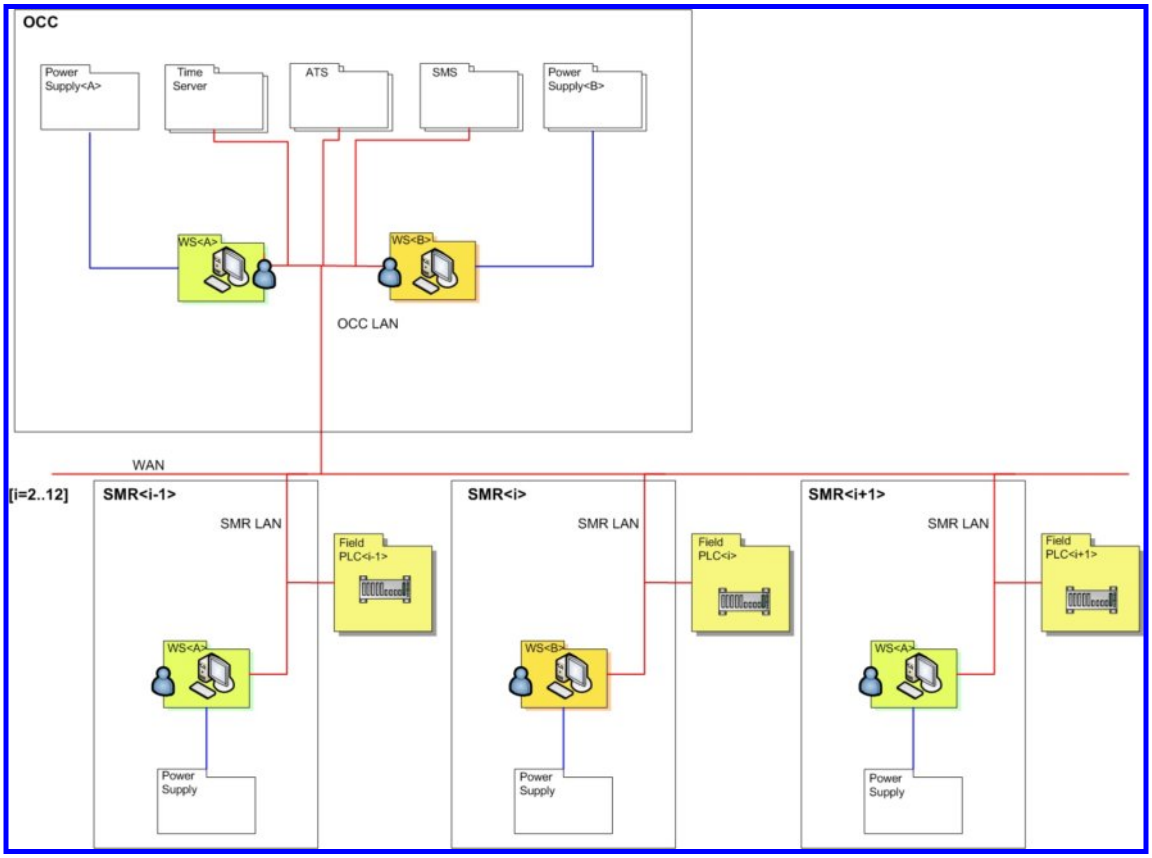



**Figure 4-1 – Local BACS WAN Network**

## 4.3 LBACS Connection

Different segments of network are foreseen to connect Local BACS cabinets to WAN. Below a brief description of each segment:

**WAN segment**: this network connects the LAN's Field PLCs through L3 LAN/WAN Switch in the Telecom Room, to the central server at the OCC via the DTN Network. With this system, the PLCs shall communicate with the servers of near station, with the BACS servers at the OCC and, finally, each PLC shall communicate via peer to peer with the neighbouring station.

**Local Optical Ring:** this network connects the local PLCs. Is the LAN's Field PLCs. Each PLC shall communicate via peer to peer with the PLC in the LAN. To avoid single point of failure on the network, a ring topology protocol is implemented. This protocol is able to manage correctly the network reconfiguration in case of fault of a communicating element on the ring.

The **Figure 4-2** shows system's architectural view of the connection of each Station.

### 4.3.1 Diagnostic Features

The Local BACS Subsystem will provide self-diagnostic information. Diagnostic information is divided by function:

- Power supply, Communication, Acquisition Cards, PLC.

Each functional unit contains diagnostic information deriving from equipment that realizes the specific functionality. A brief explanation is depicted below:

**Power Supply:**

For Power Supply the following Diagnostic information is foreseen:

- **Surge Protection Device failure**:
  In case an internal Surge Protection Device fails, a cumulative alarm at cabinet/RIO level will be generated.
- **24VDC Power supply failure :**
  In case a 24VDC power supply configuration fails, a cumulative alarm at cabinet/RIO level will be generated.

**Communication:**

For Communication unit the following Diagnostic information is foreseen:

- **Network device Failure**
  This signal arises when there is failure on one or more Communication module. It is a cumulative signal.
- **Connection to OCC Failure**
  This alarm arises in case the substation PLC cannot communicate with Central BACS server. It is generated at substation level.
- **Connection to LOCAL BACS PLC Failure**
  This alarm arises in case Central BACS server cannot communicate with PLC. It is generated at Central BACS level.

**Acquisition Cards**

For Acquisition cards the following diagnostic information is foreseen:

- **Card Failure**
  A failure occurrence on a DI, DO, AI card will be transferred as cumulative failure to Local HMI. This alarm does not identify the single channel, but it is a cumulative one related to a single Card. For Central BACS this alarm will be provided as cumulative at cabinet level.

**PLC**

For substation PLCs, the following Diagnostic information is foreseen:

- **PLC Failure**

A non-halting failure occurrence on a PLC will be transferred as cumulative failure to both Local HMI and Central BACS.
The PLC software shall include a ‘watchdog’ timer system to monitor and detect faults and to cause the equipment to enter a recovery state in the case of failure of the operational software.
The case of Halt of PLC will generate a different alarm as already defined in Communication diagnostic (“Connection to CW PLC Failure” and “Connection to Central BACS Failure”).

The following table summarizes the diagnostic information divided by cabinet substations will be provided.

| Function | Diagnostic Alarm | CABINET |
|---|---|---|
| | Surge Protection Device failure | √ |
| | Power supply line | √ |
| | 24VDC Power Supply failure | √ |
| Communication | Network device Failure (cumulative) | √ |
| | Network device Failure (for each communication card) | √ |
| | Connection to Central BACS Failure | √ |
| | Connection to Local BACS PLC Failure | √ |
| Acquisition Cards | Card failure (for each card) | √ |
| | Card failure (cumulative) | √ |
| PLC | PLC Failure (cumulative) | √ |

Table 4-1: Local BACS Diagnostic signals

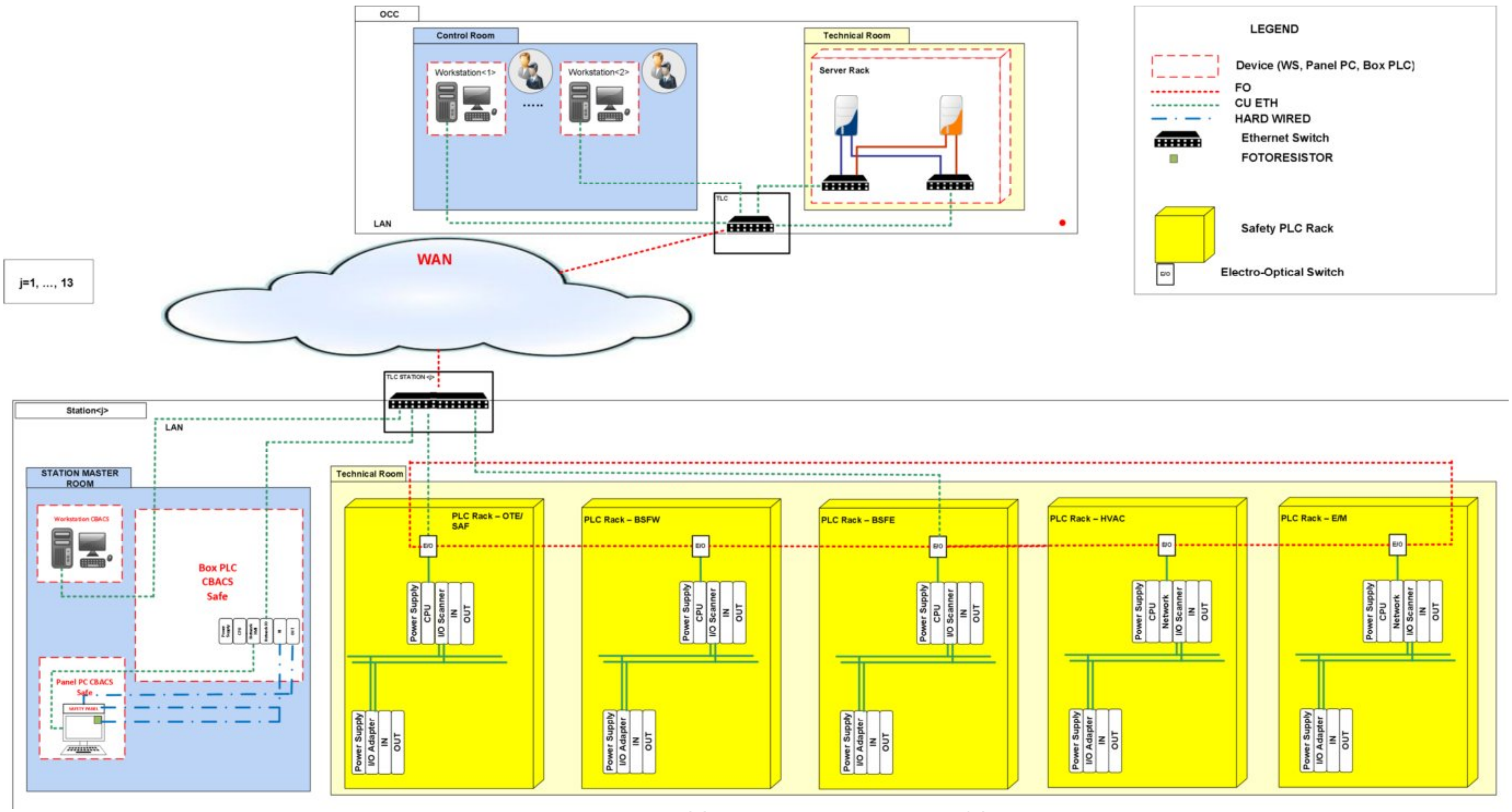



**Figure 4-2 – Local BACS – Details Architectural of Station**