EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
ORGANISATION EUROPÉENNE POUR LA RECHERCHE NUCLÉAIRE

CERN - ST Division

CERN-ST-2001-009
30 January 2001

ACHIEVING A "SIL 1" TCR MONITORING SYSTEM

R. Bartolomé, F. Havart, L. Scibile, S. Grau

Abstract

SIL 1 (Safety Integrity Level 1) refers to the quantification and measurement of the availability, reliability, maintenance and safety of the monitoring system. In the last few years the computer infrastructure used to acquire and to diffuse data to the TCR has evolved very rapidly. A number of measures in hardware, software and management have been introduced to cope with this situation. These include: the Multipurpose Monitoring Device (MMD), a standard data acquisition platform used in the renovation of old front end monitoring equipment, the Smart Equipment Controller (Dsec), a driver that reduces the layers in the data diffusion pyramid, the multiplatform monitoring software to integrate the different SCADA systems, a software configuration tool (RAZOR) for problem tracking and version control, and a complete development environment reproducing a real installation for thorough testing of any changes. To achieve SIL 1 objectives, while mastering the evolution of our systems will be the challenge for the computer team.

Presented at the 4th ST Workshop
Chamonix, France, 30 January - 2 February 2001

1 INTRODUCTION

1.1 Motivation

In the past few years, CERN's technical monitoring infrastructure has evolved very rapidly. New solutions based on complete System Control and Data Acquisition (SCADA) systems have been installed, and some of them are already in operation (i.e.: the Electrical Network Supervisor ENS). Others will be in operation soon (i.e.: the ventilation of LHC's surface buildings, ST/CV's Water 2000 project). At the same time, large changes are foreseen in the computer and network infrastructure to match the LHC requirements and to follow the market tendency.

The Technical Data Server (TDS) is the computer based monitoring system used by the Technical Control Room (TCR) and the Safety Control Room (SCR) to acquire and to diffuse data to their client applications, basically UMMI applications and alarm systems. The TDS uses the technical monitoring infrastructure to provide the service to the TCR and the SCR, so therefore it must be adapted to follow the evolution of this infrastructure. Recently the TDS has been chosen as the redundant path during the installation period for the future CERN Safety Alarm Monitoring (CSAM) system [2] .

The above points strongly recommend having a TDS with a Safety Integrity Level 1 (SIL 1) [4] to assure the standard monitoring mode and the CSAM redundancy. The acceptance of a SIL 1 means that the level of hazard is sufficiently low and that a TDS system with 90% availability is acceptable, as is shown in the following SIL cataloging table.

Table 1
SIL cataloging table

SIL	AVAILABILITY	IMPACT OF THE FAILURE
4	>99.99%	Catastrophic community impact.
3	99.90 - 99.99%	Employee and community protection.
2	99.00 - 99.90%	Major property and production protection. Possible injury to employee.
1	90.00 – 99.00%	Minor property and production protection.

The first step towards the TDS SIL 1 is a complete and in-deep functional safety analysis. This analysis will identify the set of necessary actions to match the required SIL 1.

1.2 Scope of the paper

A complete functional safety analysis of the TDS [1] covers more than what is intended to be included in this paper. On the other hand, the authors wanted to present the procedure that has been followed in the complete analysis. To cope with this situation, the analysis of only one of the TDS main functions (*Data diffusion to UMMI views*, marked as 1 in **Figure 2**) is treated.

This paper is divided using the same structure that is used in the analysis. In chapter 2 External Functional Analysis, describes the TDS, its environment and how these elements are related to offer the final service the TDS must provide. In chapter 3, Internal Functional Analysis, describes the components of the TDS. The recommendations given in chapter 4 refer to the complete system, and are a reduced set (chosen by the authors) of the recommendations listed in [1] .

1.3 Considered architecture

The functional analysis is based on a stable and well-defined physical architecture of the system. The TDS physical architecture considered in this paper is presented in **Figure 1**. The hosts are represented with boxes. Each box contains the host name, the functionality, the main programming language and the operating system.

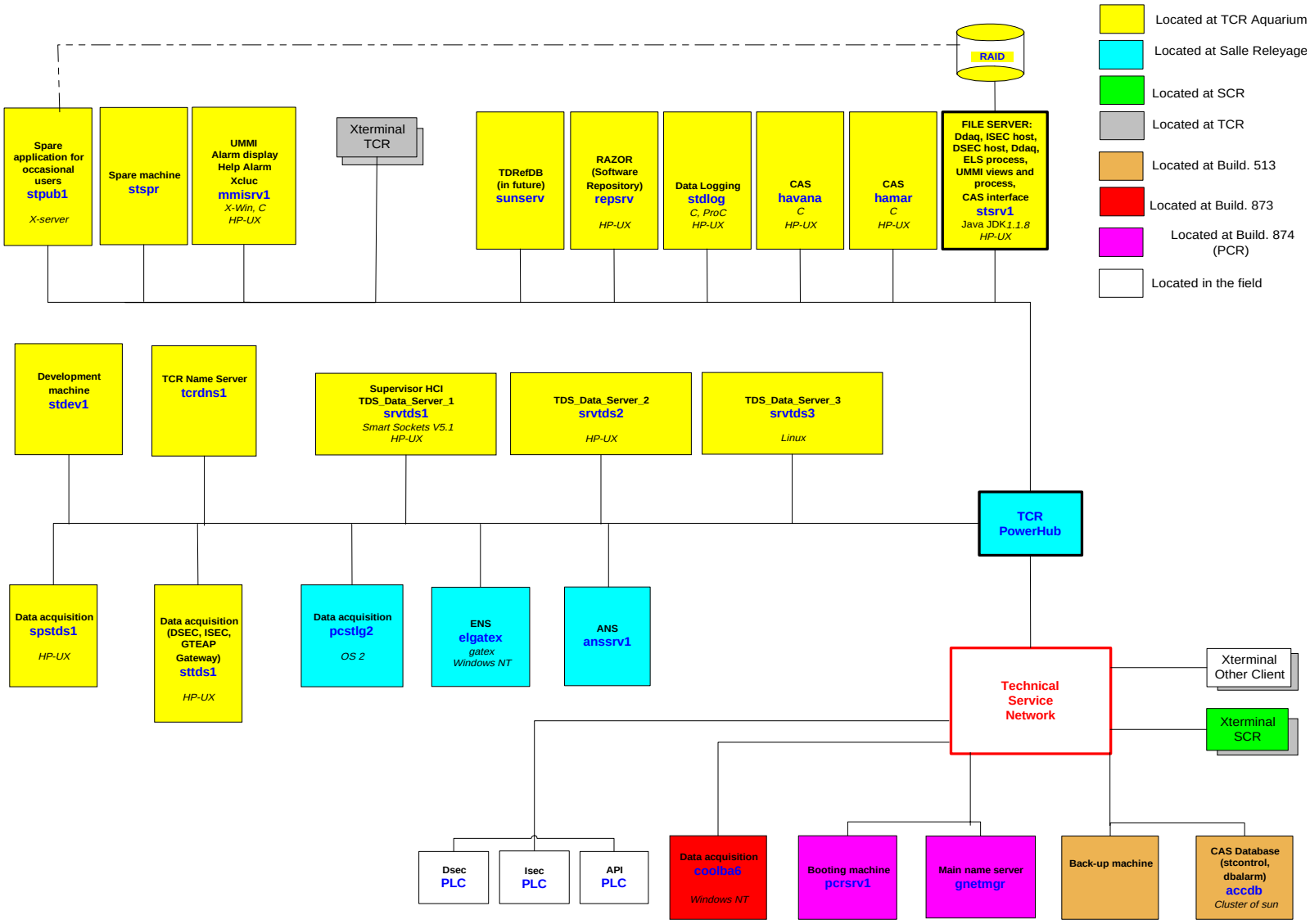

Figure 1 TDS physical architecture

2 EXTERNAL FUNCTIONAL ANALYSIS

2.1 Objectives

The objectives of the External Functional Analysis are to define the system under study (TDS), and its environments, as well as to describe the service the system shall provide to the TCR and SCR.

In order to define the TDS, the MISME (Methode d'Inventaire Systematique des Milieux Environnants) method is used. This method enables to define the system under study, by systematically analyzing the different environments affecting the system and their interactions.

2.2 TDS definition using MISME diagrams

The **Figure 2** contains the MISME diagram of the TDS when function 1 is in operation mode. The diagram shows the TDS (marked as S), and its environment. The external systems are denoted by an 'E' followed by an integer to distinguish between them, and they are described in 2.3.

Represented by lines, two different types of functions can be identified: *main functions* and *constraint functions*. Main functions are represented by numbers, and they show flows of data established between two or tree environments through the system. This is the case of function 1: through the TDS, the data generated in the equipment are transmitted through the communication network and shown at the UMMI synoptic views. Constraint functions are represented by letters, and they show flows of data only established between the system and an environment. Note that constraint functions do not always represent a real flow of data but the influence on the system of a given environment. The environments not joined to the system S (in the figure, E11, E12 and E5) do not have a role in the function under study *Data diffusion to UMMI views*, but they are presented to show the complete MISME diagram.

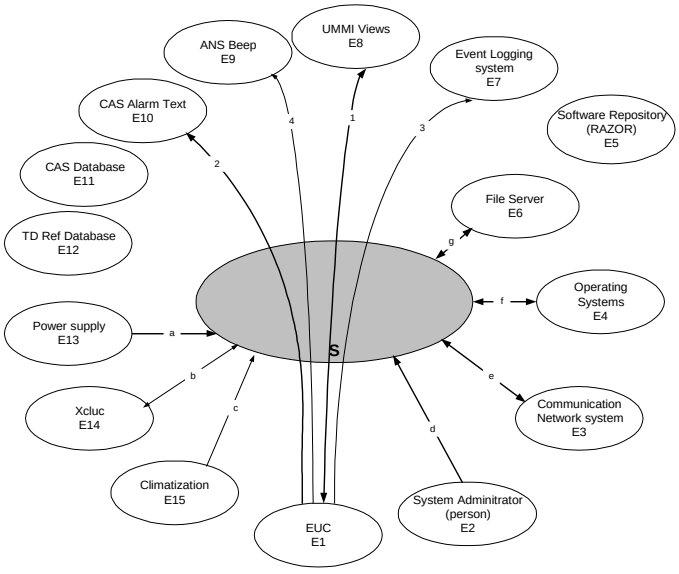

Figure 2 MISME diagram of the TDS

2.3 Description of the external elements

The Table 2 describes the external elements of the TDS related to the function 1.

Table 2
Description of external elements

IDENT.	DESCRIPTION	SPECIFIC DESCRIPTION
S	System under study	The computer based monitoring system used by the Technical Control Room (TCR) and the Safety Control Room (SCR) to acquire and to diffuse data to their client applications, basically UMMI applications and alarm systems.
E1	EUC	Equipment Under Control. Equipment that is connected to the TCR/SCR monitoring infrastructure, but its configuration data are not stored in the TDrefDB
E8	UMMI Views	Synoptic views at the TCR/SCR for monitoring the EUC

2.4 Description of the interfaces

The Table 3 describes the flow of data between the system and the external elements. More detailed information about interface flow is presented in the Internal Functional Analysis.

Table 3
Description of the Interfaces

RELATION SHIP	INTERFACE FLOW	INTERFACE TYPE
S - E1	The data transmitted are technical data, commands and command reports	The protocol is based on TCP/IP. The data format can be data structures, GTEAP messages, ISAP messages, SCADA data structures or SmartSockets data messages, depending on the element.
S – E8	Status, command reports	The data format is SmartSockets data messages.

2.5 Description of the functions

A description of the TDS function under study is given in Table 4. The function is identified by an integer; in this case, it is also split into different sub-functions. After the function identifier, another integer will denote the sub-function.

Table 4
Description of the Function

FUNCTION	RELATIONSHIP BETWEEN ELEMENTS	DESCRIPTION
1.1	E1 → E8	Generate a complete and correct UMMI display at the TCR and SCR for each incoming event, to assure TCR and SCR interventions
1.2	E8 → E1	Send a command from the TCR/SCR to the equipment under control
1.3	E1 → E8	Send a command report from the equipment under control to the TCR/SCR

3 INTERNAL FUNCTIONAL ANALYSIS

The objective of the *Internal Functional Analysis* is to describe how the function defined in the External Functional Analysis is allocated in the physical architecture presented in **Figure 1**. This means, to determine the hardware and software implementing the function.

Data diffusion to UMMI views is represented in **Figure 3**. The information acquired in the equipment under control (EUCs) is formatted depending on the acquisition system and transmitted to the data acquisition servers. These servers diffuse the information to the data dispatching servers. The information, at this moment, is routed to the appropriated data treatment server, before being shown in the UMMI views.

In the component block analysis, four server redundancies are considered: *sttds1-spstds1*, *srvtds1-srvtds2*, *mmisrv1-stspr* and *stsrv1-stspr*.

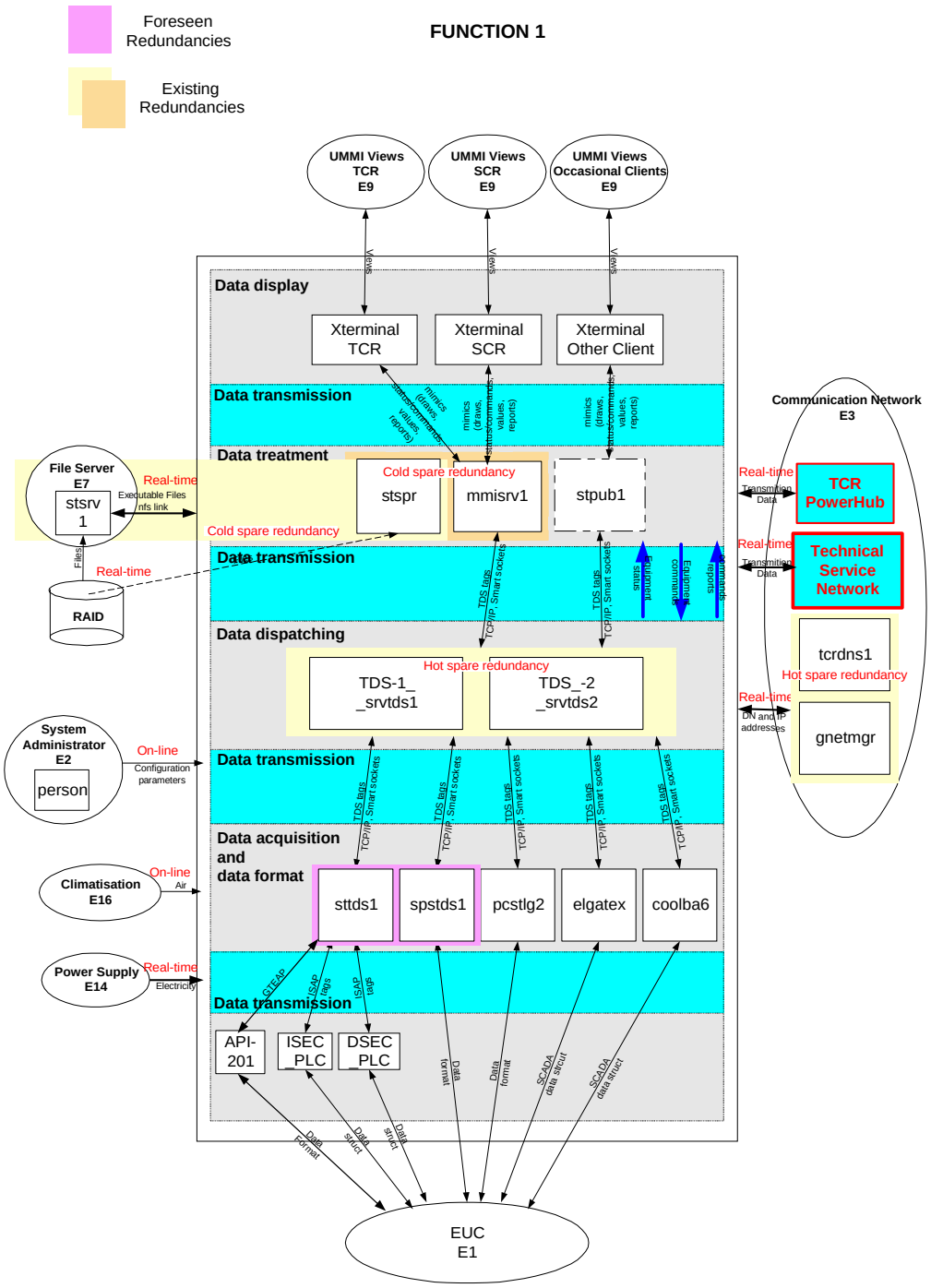

Figure 3 Internal function and component block analysis

4 RECOMMENDATIONS

The following recommendations are drawn from the analysis. The aim of this list is to identify single projects (or action items) that could be distributed among those responsible.

1. The preliminary availability result places the analyzed function into a good availability range, even though to determine the SIL of the system, the same procedure would need to be repeated for all the functions of the system. SIL allows also control of the changes, control in the documentation and software configuration. For these issues, action items have been defined. An impact analysis

of the TDS will be designed in the first two months of 2001. The TDS documentation will be included in the EDMS tool, and the software configuration is already managed using RAZOR.

2. To validate the preliminary availability results it would be very useful to set up the system supervisor to keep the evolution in time of the system components. This supervisor should continuously record measures of availability for each machine/module. An action item result of this recommendation is the implementation of *alive* messages. These messages are periodically sent by the PLC and archived in a supervisor client. Analyzing these logging files, the availability of the complete diffusion chain can be tracked back in time. This action has already been partially done, and it will take one and a half months to be completely finish.

3. To validate the preliminary availability results it would be required to verify if the redundancies effectively exist and are feasible. There are four redundancies to be tested, and each of them has been estimated to take 2 man/days to be verified, including the definition of the procedure to be followed. Task has been scheduled to be done during February 2001.

4. At the moment, all the Equipment Controllers and PLC are unique. As demonstrated by the analysis, the possibility of making these machines redundant increases the final availability (point 3 in this list). However, since not all the machines can be redundant, an analysis of the communication protocol and machine process could lead to an improvement on the final availability. This analysis will start soon, and it is estimated to take 3 man/weeks.

5. The TDS is a large and complex system with centralized configuration processes for the majority of the machines. A good improvement is to homogenize and centralize the configuration procedures for all the functions and machines. If this were not feasible, at least a synchronization of those procedures would increase the availability and reliability of the data shown at the TCR. This centralization of the configuration procedures (and the TCR databases) has started, and it will be finished by the end of the second quarter 2001.

ACRONYMS AND ABBREVIATIONS

Gteap	Generic TDS Equipment Access Protocol
ISAP	Industrial System Access Protocol
SmartSockets	Middleware used to inter-communicate the different TDS modules
TCP/IP	Transmission Control Protocol/Internet Protocol
TDrefDB	Technical Reference Database

REFERENCES

[1] S. Grau, L. Scibile, R. Bartolome, *Technical Data Server to Safety Integrity Level 1. Functional Safety Analysis*, CERN 2001.

[2] CSAM team, *CSAM Functional and Safety requirements document*, CERN 2000.

[3] JRC Ispra, *Starts Studio 2000 v0.9, the art of RAMS analysis*

[4] IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronics (E/E/PE) systems, Part 1, General Requirements*, Geneva: International Electrotechnical Commission.