MELISSA

Contract Number: ESTEC/CONTRACT: 15671/01/NL/ND

Technical Note: 72.5

Future Work on System Engineering

Version: 1

Issue: 0

NTE Document Number:	MEL-3400-RP-041-NTE
Written by:	Jordi Duatis
Revised by:	Joan Mas
Quality Assurance:	Sònia Ferrer
Approved by:	Joan Mas

Document Change Log

Version	Issue	Date	Observations
1	0	28/07/2004	New Document

TABLE OF CONTENTS

1 SCOPE 5

2 APPLICABLE AND REFERENCE DOCUMENTS 5

2.1 Applicable documents 5

2.2 Reference Documents 5

3 INTRODUCTION 6

4 CONSOLIDATION OF RELIABILITY 8

4.1 Redundancy at Master Control Level 8

4.2 Redundant Network 8

4.3 Redundant PLC 9

4.4 Redundant Sensors and Actuators 9

5 EXPANSION 10

5.1 Expansion to the rest of the plant 10

5.2 Complex Analysers and Devices 10

5.3 Alarm Management 11

5.4 Data Management 11

5.5 Access Control 12

5.6 Auditing 12

6 MAINTENANCE 12

7 ADAPTATION FOR SPACE 13

1 SCOPE

Taking into account as the requirements established for the MELISSA loop's Control System Architecture [R1], as well as the results obtained after the test campaign of the Control System Demonstrator with the Plant [R3], this document identifies the advantages and weaknesses of the set-up and evaluated control system.

Limiting factors are discussed and future actions are proposed for the development of the complete MELISSA loop following the requirements of [R1] and the proposed architecture in [R2].

2 APPLICABLE AND REFERENCE DOCUMENTS

2.1 Applicable documents

[A1] **MELISSA. Adaptation for Space, Phase 1. Statement of Work**. TOS-MCT/2000/2977/ln/CL. Issue 5. April 2001.

[A2] **MELISSA. Adaptation for Space-Phase 1. Proposal issued by NTE**. MEL-0000-OF-001-NTE. Issue 2. October 2001.

[A3] **Memorandum of Understanding between the UAB and NTE S.A.** MEL-0000-SP-007-NTE. Version 1. Issue 0. 21 January 2002.

2.2 Reference Documents

[R1] **Definition of the control requirements for the MELISSA Loop**. TN 72.2. Version 1, issue 2. November 2002.

[R2] **MELISSA Control System Architecture and Trade-off**. TN 72.3. Version 1, issue 0. February 2003.

[R3] **Control System Demonstrator Data Package.** TN 72.4, Version 1, issue 1. July 2004.

[R4] **Review of the Melissa Loop and identification of Critical Developments.** TN 72.1. Version 1, issue 0. July 2002.

3 INTRODUCTION

The results of MELISSA Spacialisation Phase 1 project, for what concerns the development of a new Control System for the MELISSA loop can be summarised as follows:

- Establishment of requirements for the MELISSA Control System compiled in[R1]
- Control System Architecture(s) proposal and trade-off, as described in [R2], resulting in the concept presented in Figure 1
- Implementation, connection to the Plant and validation of a Control System Demonstrator used for a practical assessment of the selected architecture, as explained in [R3] and shown in Figure 2

However, the Control System Demonstrator presented some limitations. A first, obvious one was due to the reduced number of operative compartments currently implemented in the MELISSA loop. Thus, the Demonstrator was limited to Compartments III and IVa.

In addition, the Demonstrator covered only partially the functional requirements established in [R1]. Thus, requirements related to the operation of MELISSA for the two mentioned compartments where implemented whereas requirements related to special sensors, bioreactors interconnection etc were not contemplated. Non-functional requirements such as reliability, safety, performance and security were also partially implemented.

Therefore, the work should continue to pursue the validation of the complete Control System Architecture requirements set. Accordingly, the following main lines of future work in system engineering are envisaged:

- Consolidation of the reliability requirements of the software and hardware currently installed
- Expansion of the proposed architecture to the rest of the plant
- Maintenance of the current installation
- Evolution of the MELISSA concept for space utilisation

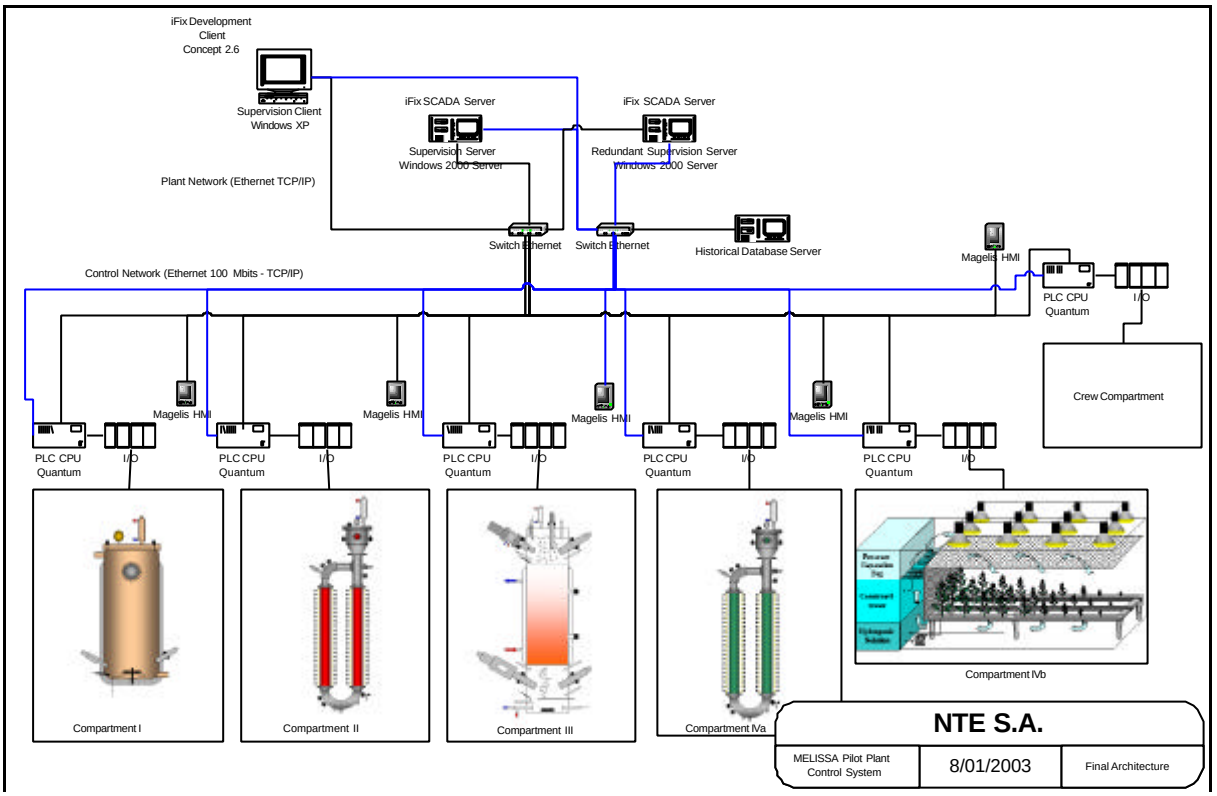

Figure 1: Control System Architecture Proposal ([R2])

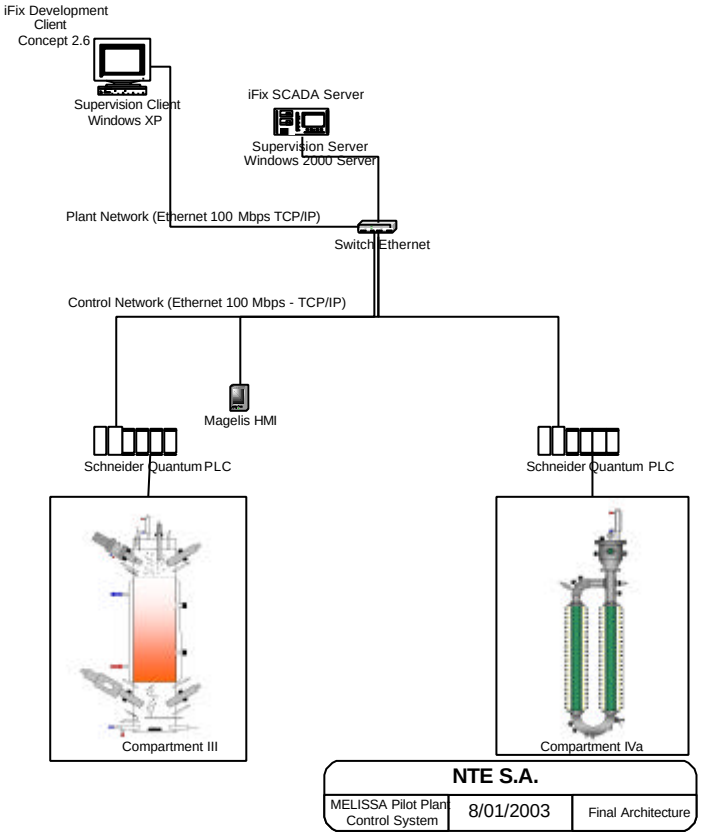

Figure 2: Control System Demonstrator implementation ([R3])

4 CONSOLIDATION OF RELIABILITY

The Control System Architecture defined in [R2] contemplates the implementation of reliability at different levels.

In general, the Control System Demonstrator does not implement redundancy. However, it has been designed and deployed in such manner that it can be expanded to fully meet the proposed reliability requirements. Therefore, the work should continue in this direction, particularly covering the following tasks:

- Implementation and test of redundancy at Master Control level
- Implementation and test of a redundant network
- Implementation and test of a redundant PLC CPU for each compartment
- Implementation and test of redundancy at sensors and actuators level

4.1 Redundancy at Master Control Level

This issue is particularly important since during the set-up and tests it was detected that reboots of the Supervision Server to perform maintenance tasks caused the Master Control to be out of service. Obviously this is not acceptable for long experiments, especially for the ones involving living test subjects.

This situation can be avoided with the installation of the redundant Supervision Server planned in the proposed architecture (see Figure 1). As stated in [R2], the redundant Supervision Server could become active in case the primary one is stopped either for a hardware / software problem or for maintenance tasks.

4.2 Redundant Network

A redundant network will avoid problems due to interruption of the physical connectivity between the PLCs and the Supervision Server. Such a failure would impair the control performed at higher levels (control laws) running in the Master Control since variations of the manipulated variables could not be communicated to the PLC.

To implement a redundant network the following tasks must be carried out:

- Install a redundant network card in the Supervision Servers (Primary and Redundant)
- Install a redundant switch into the Supervision Rack
- Install a redundant network module in each PLC configuration
- Cabling and configuration of the redundant network

The redundant network is depicted in blue in Figure 1.

4.3 Redundant PLC

The installation of a redundant CPU within the PLC will avoid the problems of hardware failures in the primary CPU (with low occurrence probability compared, for example, to sensors/actuators failures, as shown in [R2]) and also maintenance stops. Both CPUs are synchronised through a fibre optic connection and in case of interruption of service in the primary CPU, the redundant one becomes operative with a switching time in the range of milliseconds. This will lead to a fault tolerant PLC system.

In case of the installation of a redundant network, communication modules shall then be duplicated in each CPU to connect to primary and secondary network. PLC redundant configuration is shown in Figure 3

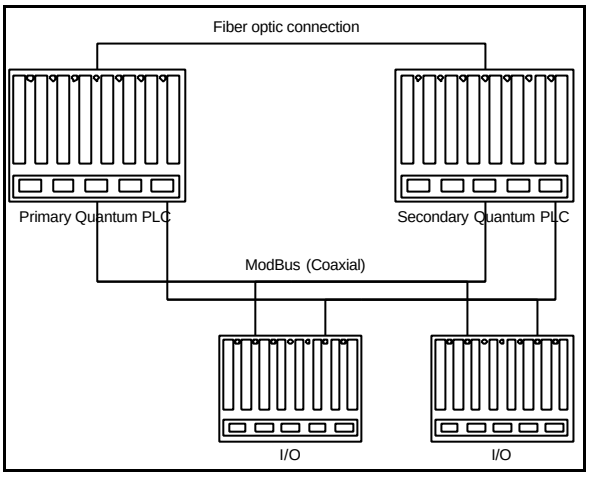

Figure 3: Redundant PLC CPU (from [R2]).

4.4 Redundant Sensors and Actuators

In order to be tolerant to failures of mandatory sensors and actuators redundancy at this level is also needed. This redundancy is also contemplated in the proposed architecture design by duplicating the I/O modules for each CPU. This configuration will thus allow the detection of sensor / actuator malfunctions and the possibility of using alternative hardware to avoid these problems. The control algorithms should then be modified to obtain measures from primary and secondary sensors. The algorithms should be updated to consider the case of a failure in a primary actuator and switch actuation to a secondary one.

To implement redundancy at this level an accurate dependability study to determine which sensors / actuators are mandatory for the process is required.

Finally, additional tests should be performed on the hardware and software in order to verify the proper operation of the redundancy.

5 EXPANSION

Expansion should go in the direction to extend the proposed control system architecture to the rest of the MELISSA loop, developing the required hardware and software. Furthermore, the current installed software and hardware presents some features that have not been fully developed / deployed in the context in which the Demonstrator has been used.

Tasks associated to the expansion of the proposed control system should cover the following aspects:

- Deployment of the control architecture to the rest of the compartments (CI, CII, HP and Crew)
- Integration of the communications of complex analysers and complex devices (such as cameras).
- Deployment of Alarm Management to cover the maximum of non-nominal situations and to use the full features of the Supervision Software.
- Data Management: Installation of a Relational Database System to allow the management of information with a robust industrial software that can handle properly the amount of data generated by MELISSA.
- Access control: Definition of profiles depending on the tasks to be performed in the plant as for example: Administration, Maintenance, Operation, and Supervision. Definition of the permissions associated to each profile.
- Auditing: Deployment of the auditing capabilities of the Supervision Software to log changes performed in the system configuration.

5.1 Expansion to the rest of the plant

Since the proposed architecture is proved to be suitable for the implementation of the MELISSA Control System requirements, this architecture should be expanded to the rest of the compartments. The experience gained during the implementation, installation and verification of compartments III and IVa can be used as a guide to the process of implementing, installing and verifying the software and the hardware of the other compartments in the Pilot Plant.

In addition, the interconnection of compartments will need the installation of additional hardware and software. The installation of this new hardware will need to be designed, implemented, tested and verified as for the compartments, distributing the control of this new sensors and actuators among the PLC belonging to the different compartments.

Other aspect that will need to be covered when compartments will begin to be interconnected is the higher control level, from the supervision displays to the control laws and control loops.

5.2 Complex Analysers and Devices

Complex analysers can be integrated to the system using their capabilities of communicating through complex protocols. This allows the use of the full features that they implement. One of the goals of the proposed architecture was the integration of these devices into the system

with all the capabilities available. The Supervision Server can handle complex protocols and different types of communications. A study should be performed about the different analysers (present and planned) in the Pilot Plant to gain information about the capabilities that are interesting to minimise the human intervention in the maintenance tasks and alarm management (such as auto-scaling, alarm notification, auto-calibration, etc.). Following, the integration of these analysers using the available protocols will imply the implementation of the corresponding software to handle this communications and the installation of the corresponding hardware.

In addition, another complex devices such as image acquisition devices are planned to be present in the plant. The integration of these devices can also be performed through the installation and implementation of the corresponding software into the Supervision Server or through an intermediate computer able of sending analysis results to the server.

5.3 Alarm Management

Expansion of the Alarm Management should include:

- Analysis of the alarm situations and possible detectable failures and designing and implementing proper counter-measures
- Implementing the Alarm Management using all features available in the Supervision Server (Alarm classification, Alarm notification, Alarm logging, etc.)

During the Demonstrator tests and set-up the need for expanding the alarm management was detected. For example, a new alarm-reporting situation was discovered after the interruption of external gas supply.

A detailed analysis of alarm situations and possible counter-measures should be performed in order to verify that the system is able to react to the maximum of non-nominal situations without scientific loss or safety threats. This will also result in a more reliable system.

The Supervision software iFIX allows the classification of alarms per areas. Alarms can also be logged in the Database and notified through several means. For example, a highly critical alarm could be notified through a cellular phone with the installation of additional, appropriate hardware. It follows, thus, the recommendation to define a policy with respect to alarm management.

5.4 Data Management

The Data Management concept implemented in the Demonstrator showed that the Supervision Software is able to manage and store data into a Relational Database System. However, the physical support for the Database is Microsoft ® Access files. This support has been useful for demonstration purposes but it is known that it presents consistency problems when the file size becomes large (around gigabytes). The MELISSA system generates data at very high rates. These data cannot be discarded in a regular basis because could be crucial for the analysis of experiments whose execution could require long time (months of even years).

Therefore, it is highly recommended to define a data management policy and the use of a specialised Relational Database Management System with its specific management (e.g. the Microsoft ® SQL Server). This would allow the availability of common data management features such as easy the exploitation of the data, the implementation of summarising procedures to generate historical data.

In addition, the Supervision software iFIX can be improved to display Database data in the supervision displays to allow the operator to access historical data of previous days.

5.5 Access Control

Access control is a feature available in the Supervision Server that will allow the definition of policies to access to the system. For example, four levels of access control can be defined:
- Administration: Full access rights.
- Maintenance: Limited access rights.
- Operation: Change of parameters and visualisation of Supervision displays.
- Supervision: Visualisation of Supervision Displays only.

For each level a group of access permissions needs to be defined. Users belonging to each group will be identified and authenticated.

The set-up of the Control System Demonstrator showed the criticality of a defined policy for access control. The MELISSA Supervision Server is connected to a WAN to allow its access from remote sites and this exposed the Server to suffer a computer viruses infection, causing a Denegation of Service (DoS) during a test session. Optimally, the server should be protected through a firewall, anti-virus software and with severe access restrictions.

5.6 Auditing

The iFIX Supervision software is able of auditing changes in the configuration of the system, i.e. registering the changes and identifying the author. To implement auditing, feature not currently in use, an access control policy needs to be defined.

6 MAINTENANCE

Several maintenance tasks can be envisaged:

- Support in the integration of changes in the control laws.

It is expected that the control laws for compartment III and IVa will be refined. The process of refining could imply the recompilation of the software modules involved and a regression test at integration level.

- Trade-off, procurement and integration of sensors and actuators

The compartments III and IV will be modified with respect to the number and type of sensors and actuators. The selection of the appropriate sensors/actuators will imply a trade-off, an integration of the new device to the compartment, and finally software modifications in the control loops and in the supervision screens.

- Data management: automatic handling of data in a Database server.

The increase of the amount of data can raise a problem in current data handling process because nowadays is supported by Microsoft Access data files. A relational database management system such as Microsoft SQL Server should be used in order to prevent the corruption of data files, problem that is known in very large Access data files. In addition, automatic processes for summarizing data and create historical files can also be implemented to avoid manual data management.

- Control System Demonstrator's Hardware and Software maintenance

Two types of maintenance over the current software and hardware installed are expected:
- Corrective maintenance, that is, to correct potential problems rising while the system is extensively used
- Improvement maintenance, developing new features or improvements to the current system

7 ADAPTATION FOR SPACE

The use of space qualified hardware and constraints in terms of mass, volume, energy and crew time will likely limit the implementation options of the Control System for a flight version of MELISSA.

It is envisaged, thus, that the Control System's hardware and software that would be used in an operational model of MELISSA in Space will be very different to the solution selected in the architecture trade-off and implemented in the Demonstrator. In fact, this solution is quite different from known space implementations of current Environmental and Life Support Systems. A study from a systems engineering point of view of the ECLSS in use (e.g. in ISS) could be performed to incorporate synergies of the well-tested technologies and solutions that could be applied to MELISSA. Performing, at the same time, a study of the incorporation of the MELISSA concept and on-going technologies to the current ELSS in a obtaining feedback in both directions. This will lead to shorten the distance between the Pilot Plant and a space-qualified version of MELISSA.

Adaptation of the MELISSA Control System for use in space missions
- Adaptation of the hardware to meet the environmental robustness required by the Space mission.
- Adaptation of the software, that should be developed and tested according to the Space Standards.

- Adaptation of the architecture to meet fundamental requirements (safety, reliability etc.) in space environment, including a thorough FMECA-like study.
- Definition of a logistics policy (maintenance, spares etc.)

Tracking the evolution of the state-of-the-art in control systems, particularly those used in biotechnology applications, is also recommended in view of the time span until space missions using MELISSA will be possible. This can be of particular interest to determine whether commercial, on-the-shelf products can be traded-off against customised ones, or viceversa.

Finally, it is noted that some critical technologies and developments for the spacialisation of the MELISSA concept have been addressed in [R4].