ADERSA

MELISSA

Memorandum of Understanding
ECT/FG/MMM/97.012

ESTEC/Contract N° 13292/98/NL
Contract change notice No 02 of 24 October 2000

TECHNICAL NOTE : 62.9

Dependability technical analysis specification

Part I : MELISSA program scope
Part II : Elements for the MELISSA loop control system upgrading

Version : 1
Issue : 1

J.-L. TESTUD

June 2002

10, rue de la Croix Martre
91873 PALAISEAU Cedex
Phone : (33) 1 60 13 53 53
Fax : (33) 1 69 20 05 63
Email : adersa@adersa.com

aderSa

SUMMARY

This document is the property of ADERSA Scop. It can't be used, duplicated, modified or transmitted without his authorisation.

This document is the property of ADERSA Scop. It can't be used, duplicated, modified or transmitted without his authorisation.

1. PRELIMINARIES REMARKS

1.1 Document historical record

Date	Version	Issue	Author	Update object
2001-06-26	1	0	JL Testud	Creation Part II
2001-11-20	1	0	JL Testud	Creation Part I
2002-06-10	1	1	J. Albiol	Updating §6

1.2 Modified pages indexes

All pages from this edition are located at the last document index

Version 1.1 is the result of modification of pages 15 to 23 from Version 1.0

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

1.3 Summary document

Part I :
This part includes:

- Elements required to define the MELISSA program to prepare dependability analysis
- Process proposal and technical specification for dependability analysis

Part II :
This part includes functional specifications of the driving system features. This document includes all updated available information in Adersa with reference to the Melissa driving system :

- Current driving system reminders of the Melissa loop (Life Support System)
- Primary technical requirement specifications and advice for equipment, software and next driving system networks for the ground version Melissa loop that is meant to replace the current system at the Universitat Autònoma de Barcelona (UAB)

This document is unfinished and has still to be validated by the committed people (ESA and Melissa project partners).

As this document intends to be also a working document for further use it may evolve in the future and it will be necessary to update it frequently particularly in cooperation with UAB and NTE.

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

2. OTHER INFORMATIONS

2.1 Adersa contacts

People in charge of:

- Functional topics,
  - ♦ Jean-Louis TESTUD (01.60.13.53.37)
- Technical aspects regarding process
  - ♦ Jacques RICHALET (01.60.13.53.20)
  - ♦ Jean-Joseph LECLERCQ (01.60.13.53.27)
- Technical aspects regarding industrial coding,
  - ♦ Christian VALLEE (01.60.13.53.68)

2.2 Data source

TN 62-9_0 ADERSA .doc

2.3 Reference documents

- ESA Documents:
  - ♦ TN 18-1
  - ♦ TN 37-6
  - ♦ TN 47-5

- UAB Documents:
  - ♦ Anne VERNEREY's thesis
  - ♦ Julio PEREZ's thesis

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

3. REQUIREMENTS

3.1 Requirements definition

3.1.1 Part I

The scope of part I of this technical note is to provide a first reflection on dependability analysis. It is also to define the requirements of the MELISSA mission in terms of safety, availability, reliability, maintenance and logistic support.

All the items will be discussed and completed later.

3.1.2 Part II

The scope of the part II is to provide the relevant information in order to offer technical solutions for the Melissa driving system described herewith.

Requirements are referred to the computer architecture, communication systems and software.

Technical choices will be justified.

This memo provides the main system specifications and the driving system constraints.

The driving system upgrading is performed together with the transformation of the pilot of the current state E1, which matches the pilot version currently operating in UAB.

3.2 MELISSA loop description reminders

3.2.1 Principles

Melissa project (Microbiological Ecological Life Support System Alternative) is developed by the European Space Agency (ESA) for an ecosystem mainly based on the microorganisms. It claims to be a tool for artificial ecosystem understanding and for a next support system of the biological life for long spatial flights (Mergeay and al, 1988).

The Melissa project is based on the edible biomass recovery from wastage, CO_2 and minerals and using the light as energy source for photosynthesis.

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

The process is composed by 5 sub-systems (called compartments) strongly interconnected with liquid, solid or gas links. The first compartment (COMP V) mainly consists of the staff that uses oxygen and biomass and produces waste and CO. Other compartments are made of the necessary elements for the waste reprocessing and the production of nutritive elements and oxygen (bioreactors, separators …)

The diagrams below describe the main loop and links organisation.

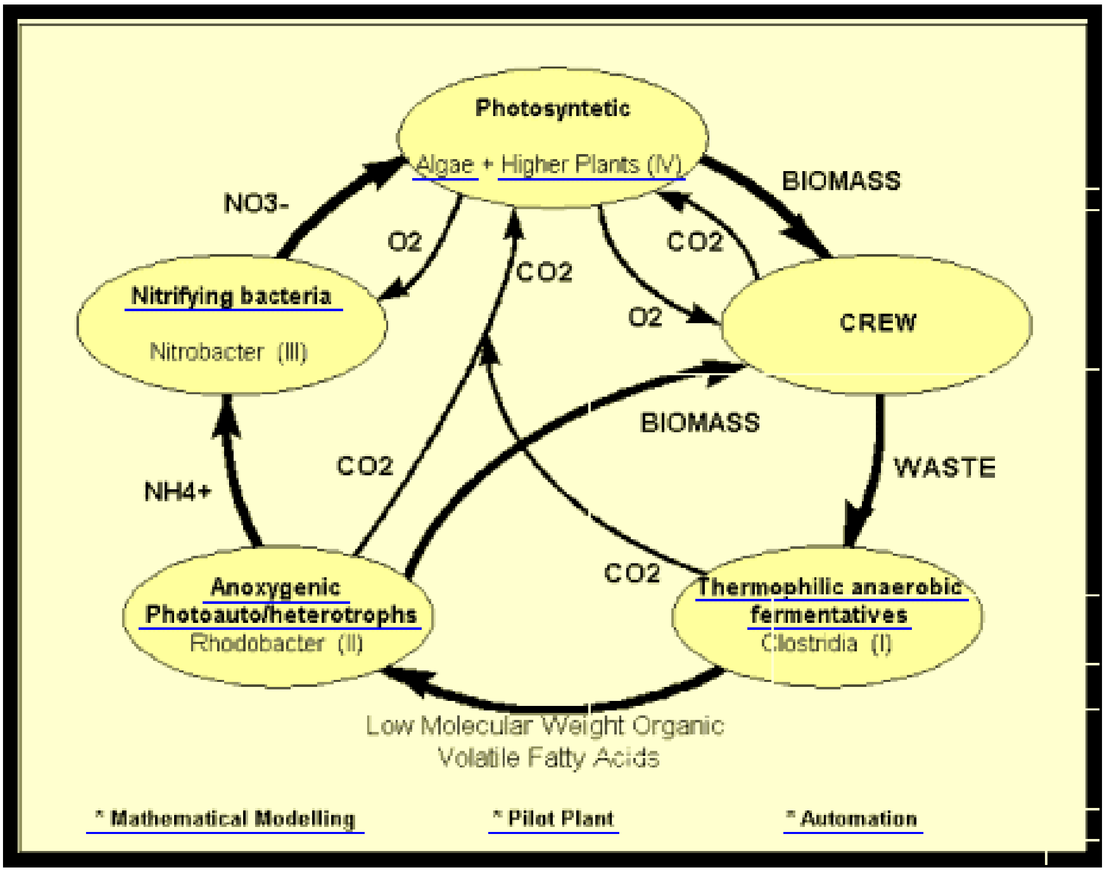
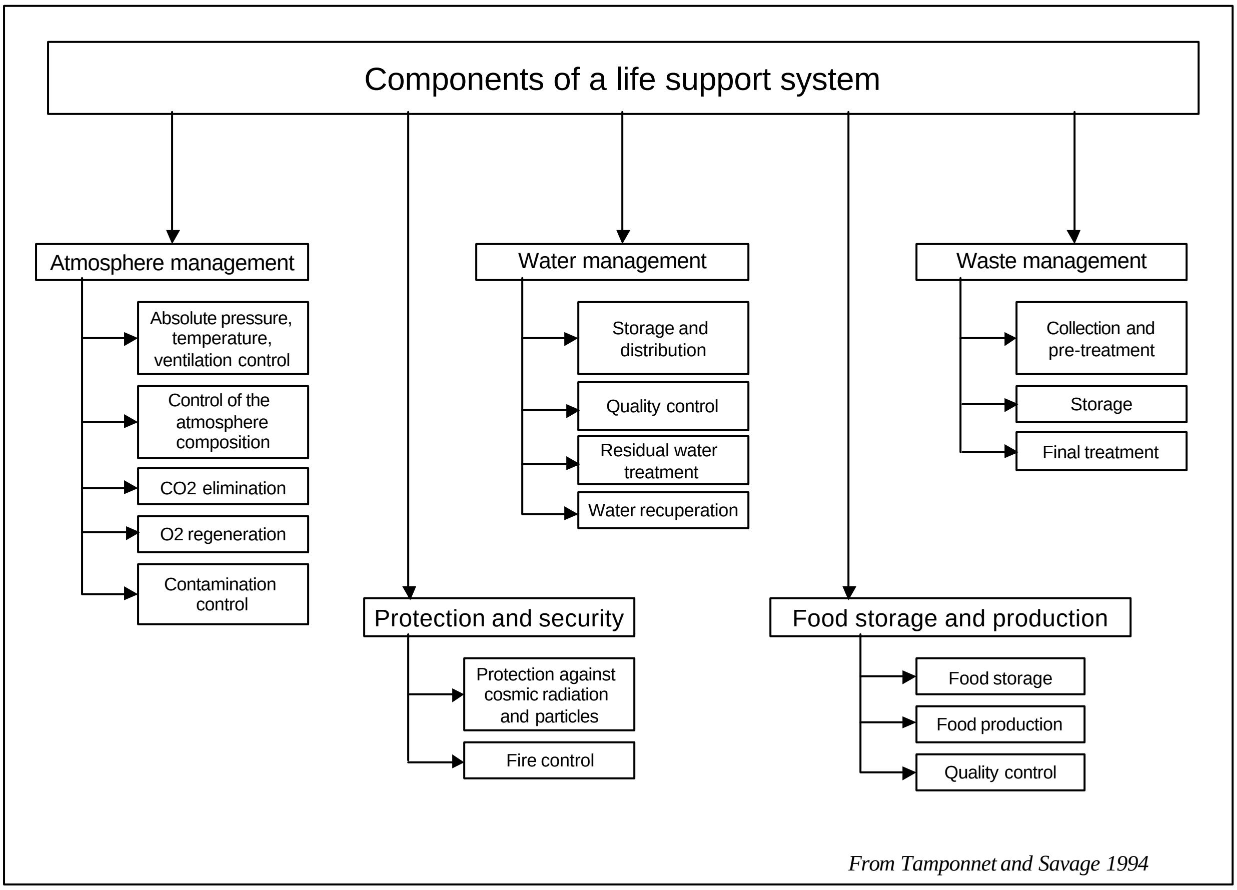


Diagram N ° 1 : Principle plan of the Melissa loop

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

4. SPECIFICATIONS OF MISSION MELISSA (PART I)

4.1 Main components of a life support system



From Tamponnet and Savage 1994

Diagram 3 : Main components of a life support system

4.2 Main objectives of the system

- To put conditions together to insure the life (food, water and atmosphere) of the crew during the whole duration of the mission.
- To waste recycling or destruction
- To avoid contamination

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

- To make sure of good working of all components during the whole duration of the mission

4.3 Main elements of the control system

- Sensors :
  - Different categories of instruments measurement (sensors and analysers)
  - Different function modes (real time measurement or by sampling)
  - Different metrological features

- Actuators :
  - Different categories of actuators
  - Different categories of operation mode
  - Different categories of metrological features

- Data management
  - Filing
  - Process, statistics, outputs, trends, …
  - Display unit

- Process Control
  - Regulations (necessary functions for Melissa loop operation)
  - Level 0 « Basic control »
  - Level 1 « Local control »
  - Level 2 « Global control »

- Support : Technical documentation, technical data basis and eventually hot line with Earth

- Monitoring : Man/Machine Interface

- Main functions :
  - Level 0 functions:
    - Composition check (purity, humidity …)
    - Quality testing (water, air,…)
    - Electrical supply generator check
    - Air conditioning system testing
    - Steam control for bioreactor sterilisation in situ
    - Fluids control (distilled water, N_2, 0_2, H_2, CO_2, He, air, …)
    - Culture preparation check
    - …

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

- Level 1 functions:
  - Positive pressure system control with external sterilised air
  - Level 1 control functions for each reactor
  - …
- Level 2 functions:
  - Safety control : fire, protection against cosmic radiation (glow screen)
  - Fault detection
  - Diagnosis
  - Maintenance
  - Operation Safety
  - Melissa loop Operation Management
  - …

4.4 Mission duration

- Mars connection flight : about 6 months
- Mission on Mars : about 18 months
- Earth connection flight : about 6 months

4.5 Main characteristics of the mission

- Autonomous mission
- Possibility of maintenance operations, realised by the crew, during the mission
- Weight, volume, size and composition of the stock are limited
- No supplying opportunity during the mission

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

5. SAFETY ANALYSIS PLAN (PART I)

5.1 Theoretical safety analysis plan

The main goal of a safety analysis plan is to define the effort and the nature of activity that is required to develop that is necessary to be sure that every risk is under control.

Synchronising the steps is essential for the safety analysis plan and the steps of the project development plan.

A safety analysis plan covers a project from the definition phase to the exploitation phase including conception, development, manufacturing, installation, exploitation and maintenance phases.

A safety analysis plan must be adapted to the characteristics and the constraints of the process.

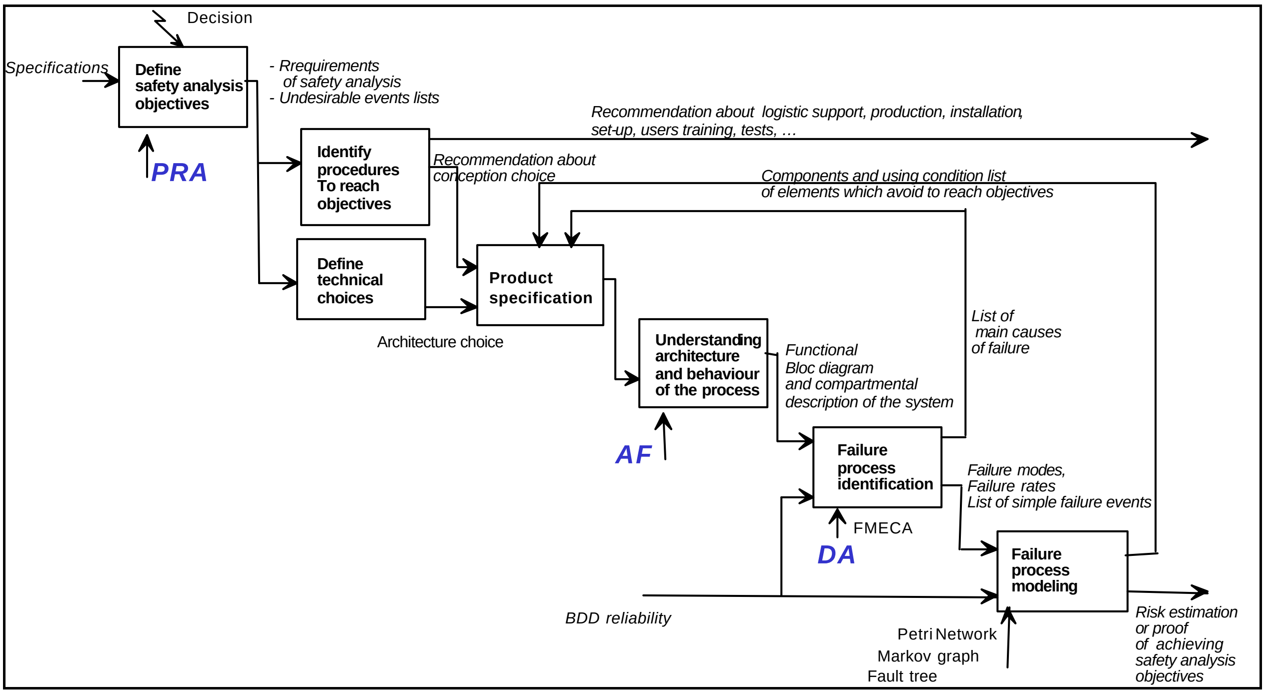

Decision
Specifications
Define safety analysis objectives
PRA
- Rrequirements of safety analysis
- Undesirable events lists
Identify procedures To reach objectives
Define technical choices
Recommendation about logistic support, production, installation, set-up, users training, tests, …
Recommendation about conception choice
Components and using condition list of elements which avoid to reach objectives
Product specification
Architecture choice
Understanding architecture and behaviour of the process
AF
Functional Bloc diagram and compartmental description of the system
List of main causes of failure
Failure process identification
FMECA
DA
Failure modes, Failure rates List of simple failure events
Failure process modeling
BDD reliability
Petri Network
Markov graph
Fault tree
Risk estimation or proof of achieving safety analysis objectives

Diagram 4 : Proposition of safety analysis plan *(from Schneider)*

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

5.2 MELISSA safety analysis plan – proposal

Adaptability of the theoretical plan to the MELISSA context consists in three steps. Preliminary Risk Analysis (PRA) – Functional Analysis (FA) – Dysfunctional analysis (DA)

5.2.1 Step 1 - Preliminary Risk Analysis (PRA)

PRA allows to highlight the risks and to organise them.

For each risk, PRA defines the following items:

- Risk identification
- Risk gravity
- Detection procedure and sensors specific to this kind of risk
- Occurrence probability
- Prevention means

Useful inputs for PRA:

- Specification document
- Interviews reports with experts
- Question files

Outputs produce by PRA:

- List of risks
- Safety analysis objective

5.2.2 Step 2 - Functional Analysis (FA)

Functional analysis is a preliminary and necessary step for all accurate safety analysis. It allows realisation of a complete inventory of the installation. It is a fundamental step in comprehension and synthetic description of the operative modes of the process.

A initial step of functional analysis of MELISSA is related in the TN 62.7 and TN 62.8.

This analyse can result in recommendation about system conception or choice of components.

This analyse requires commitment of all partners of the project. That's why it is essential to be able to use a representation of the process including the following characteristics:

- Easily up dating

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

- Easily handling (text files form)
- Easy to exchange (by web for instance)

At the end of SDF actions 2001 ADERSA proposes an action plan and software tools to support a representation which includes those characteristics (See TN 62.7 and TN 62.8).

Useful inputs for FA:

- Operational context
- Functional requirements
- Question files

Outputs produce by FA:

- Functional and structural description of the system
- Synthesis of recommendations

5.2.3 Step 3 – Dysfunctional Analysis (DA)

Failure modes, effect and criticality analysis (FMECA) are procedures which allow to identify:

- Failure mode possibility for each component defined during functional analysis
- Occurrence causes
- Failure consequences for the system
- Failure criticality

Result of analysis :

- Elements for risk analysis (identification of critical components, estimation of life duration of the system,…)
- Test strategy and diagnosis help

Useful inputs for DA:

- Functional analysis
- Question files

Outputs produce by DA:

- FMECA synthesis
- Synthesis of recommendations and proposition of corrective actions

6. CURRENT DRIVING SYSTEM

6.1 General features

6.1.1 Present status of the MELISSA pilot laboratory

This chapter describes the present status of the Melissa loop located at the UAB. Only headlines are mentioned, documents describing these headings are at Partners' disposal:

TN 18.1 – TN 37.6 – TN 47.3

A. Vernerey and Julio Perez's thesis

6.1.1.1 Present hardware architecture

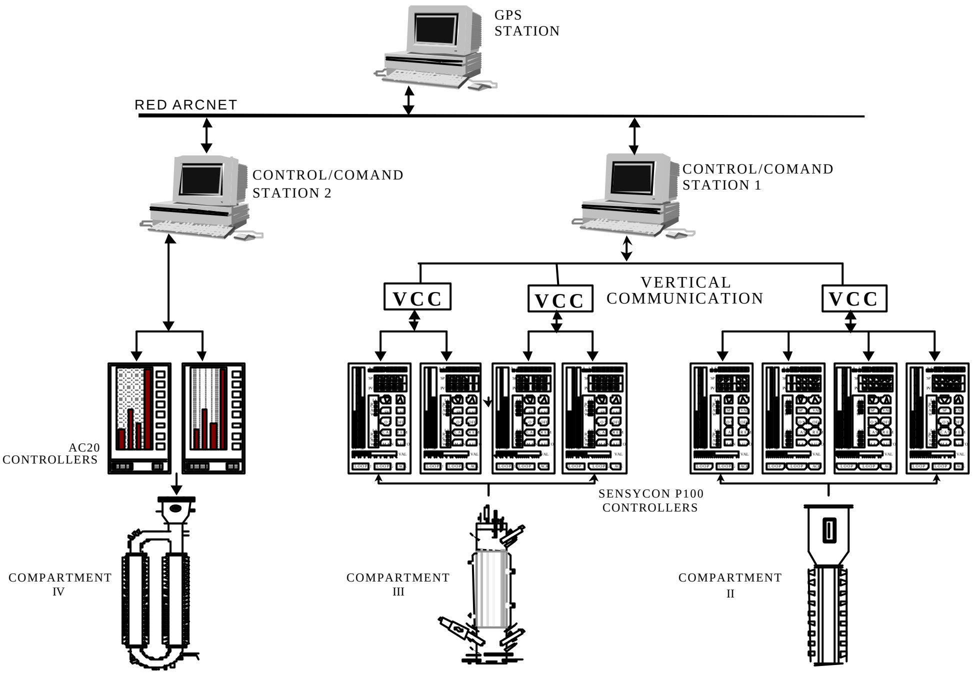


Diagram 5 ; present hardware architecture (Vernerey 2000)

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

6.1.2 Main characteristics of the control command system in UAB

Since its first installation the system has gone through different modifications and upgrades. In the following it will be mainly described the present configuration although some indications of the previous configurations may also be given.

The installed system is composed of a group of personal computer stations which initially were interconnected via ARCNET network. This was later modified to an Ethernet thinwire.

The stations are:

- Station 1 is a PC (COMPAQ 486) with MS-DOS as operating system.
- Stations 2 is a PC (COMPAQ 386) with MS-DOS as operating system.
- GPS Station is a PC (Pentium 200) with Windows95 as operating system

User Stations are PC (COMPAQ 386) having MS-DOS as operating system.

At present time there are 2 control/command stations. The Control/Command station 1 is connected to the process via an interface of communication (VCC) and several Controllers. It consist in a COMPAQ 486 and is interconnected to the VCC and Sensycon MICON P-100 controllers. Each VCC is able to drive two or four MICON P100. Four P-100 controllers receive the measurements from compartment II and another group of 4 P-100 controllers receive the measurements from compartment III (in this case 2 VCC are used, this is required in order to be able to use its 2 extended loops capabilities). The second control command station, a COMPAQ 386s is directly linked to the Ascon AC-20 controllers, via serial RS-485 (MODBUS protocol), and receives the process measurements from compartment IVa.

P100 is a fully autonomous programmable device able to manage 4 regulation loops (However only 2 are used in MELISSA compartment II because it only presents 2 analogic outputs) In compartment III the 4 loops are used however 2 of them are used only for monitoring purposes or acting on digital outputs, due to the lack of analogic outputs.

The ASCON AC-20 are able to manage 4 regulation loops and include 4 analogic outputs together with 8 digital inputs, 8 digital outputs and 8 analogic inputs. Therefore in practical terms one AC-20 is equivalent to 2 MICON P-100.

The MICON P100 and ASCON 20 are connected to the sensors and actuators of the process. Inputs/outputs are configurable for either 0-5V, 4-5V, 0-20 mA, 4-20 mA.

The GPS station is interconnected to compartments II, III and IV via the control/command stations.

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

6.1.2.1 Control /Command station

System management : this function allows the manager to customise the system.

Control/Command : direct link between the station and the controllers in charge of the process. Station1 operates with compartment II and III controllers and station 2 operates with compartment IV

6.1.2.2 User station

This station has only the control / command possibilities with eventually limited access to data. At present time it is not connected to the system.

6.1.2.3 General Purpose Station (GPS)

This station communicates with the Control / Command station connected to the process to read or write data relative to the process. It is a sort of control command programming station.

6.2 Measures acquisition function

Each controller Sensycon MICON P100 drives a process interface with analogue and digital input/output connected to sensors and actuators (Analogue digital conversion 12 bits – Analogue links are all made using current loops 4-20 mA).

Each controller ASCON AC-20 drives a process interface with analogue and digital input/output connected to sensors and actuators (Analogue digital conversion 16 bits – Analogue links are all made using 0-5V 1-5Vcc or current loops 0-20, 4-20 mA using external shunt resistance 250 Ohm).

6.3 Regulation mode

Each P100 controller drives two regulation loops. A regulation loop is a set of 20 lines (40 is possible in the extended loop mode), each line containing one of the 100 internal functions of P100 library.

PID is the common regulation type.

Each ASCON AC-20 drives 4 regulation loops. Programming allows multiple configurations Inputs/ outputs, conversions, P, PI, PID, filter, linearizations, selectors,….

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

6.4 Coding mode

Instructions for coding MICON P-100 are performed by user from GPS, control/command stations, always with its main control programs disconnected or defined during off line system configuration. Programming makes use of a MS-DOS software accessing the controllers via the same installed network and PC (RS485), or can be programmed using a side keyboard.

Instructions for coding ASCON AC-20 are coded using a windows user interface program in a PC linked to each controller via a frontal RS-232 serial link (different from the rear RS-485 (MODBUS/JBUS) for connecting to the Control/command stations).

6.5 Process control function

- Control command laws implemented into P100 and AC-20
- Centralised alarm management via control command station
- Curves display via control command station (also included in GPS)
- Archiving and reports edition via control command station
- Programming interfaces via General Purpose Station
- Communication software using a mailbox to exchange data

6.6 Man machine interface function

6.6.1 Archiving applications

Two data bases with structure and performance limitation in control/command stations and one data base in file format mode, recorded by GPS software. Control/command software suffer of the so called ‘year 2000 effect’ and datafiles and displays present wrong dates.

At present time data from compartments II, III and IV are received, stored and ready to be used with the new implemented control laws. In the MS-DOS version of the GPS careful timing of each control law will have to be managed wen more than one compartment is regulated at the same time due to the non-existing multitasking infrastructure in MS-DOS.

6.6.2 Synoptic

A user interfaces configuration can be used to customize the synoptic on the screen of stations. Upgraded user interface added to the GPS station (lately named MCS station) in the MS-DOS version.

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

There also exists a Windows user interface programmed in Java which interfaces the user with the MS-DOS GPS software. The interface using the MS-DOS GPS software is required due to the impossibility to use the libraries supplied with the copntrol/command software for interfacing with external programs with other compilers than Microsoft C v4.0. Therefore a special version of the MS-DOS GPS is used as a bridge with the control/command stations when the windows user interface is in operation.

A local visualisation of data is available from the front face of the P100 and AC-20. AC-20 have limited graphical curve display of data in the front screen.

6.6.3 Alarm management

Alarm configuration off line

Alarm visualisation all the time in the lower part of the screen of the stations and in a dedicated screen.

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

7. NEW CONTROL SYSTEM SPECIFICATIONS

7.1 General specifications

- To allow implementation of advanced control command solutions
- To allow utilisation of new categories of sensors and actuators with possibility of implementation of intelligent function.

7.2 Main lines of progress

- Innovation cost under control
- Exploitation and maintenance recurrent cost reduction
- Integration of the functions to comply with a minimum of hardware and software connected platforms.
- Promotion of intelligent and communicating solutions.
- Digital is better than analogical and software is better than material.
- Self service is better than made-to-measure.
- To give priority to continuous modes and "without human intervention" : except specific requirement, fully manual graceful degradation to be banished
- To optimise the quantity and space of cupboards or boxes, wires flow an volumetry .
- To standardise Human-Machine Interface (IHM) on graphic colour monitor : indicators, keys, mimic diagrams to be represented with computer objects : Human-Machine Product security units use to have a real physical existence
- To set-up a hot-line that should gather all multimedia documentation
- Systematically implement the "assistance to maintenance diagnosis" mode
- Systematically implement the "metrological standardisation management" mode

7.3 Main improvements required

All functions required by the transition from a laboratory pilot limited version to an industrial version, and especially :

- Management of the control structure and get the proper software
- Organisation the Technical Data Base and get the proper software

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

- Maintenance and help issue definition
- As mathematical models are in constant evolution, it is necessary to easily update and to keep all the versions of the models
- Several global operating modes of the Melissa loop : biomass and/or atmosphere reconditioning
- Safety high level, long flight, far, hostile environment
- Size, weight, space conditions constraints
- User station concept which gives access to the technical data basis in the read-only access. If maintained, this functionality must be described accurately : access and condition modes, transfer speed…
- MCS (Melissa control system) Station concept for which enables to configure command rules. If maintained, this functionality must be described accurately.
- The main target of this Melissa ground pilot version is to test the connection of several compartments of the Melissa loop over a long period. The driving system must make possible the necessary functions to be perform to check this target, and more particularly :
  - ♦ It is compulsory to track and analyse the loop behaviours. technical database importance (archiving, access, readability, "traçabilité"…)
  - ♦ The organisation of the process must be able to accept the process hardware, software and/or methodological evolutions.

7.4 Future control system

7.4.1 Location diagram of the loop (future ground pilot version)

The compartment IVb (or IV HP) corresponds to the higher plant compartment.

The Diagram n° 6 describes the position of the compartments and states the sizes to define and assess the network data and cables required.

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

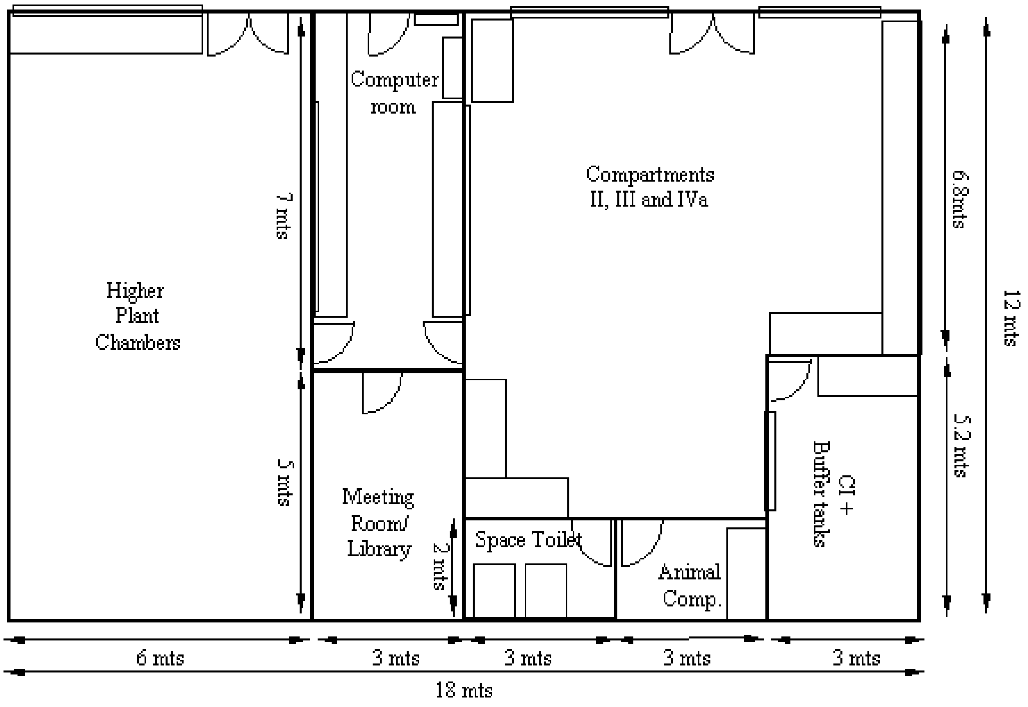


Diagram 6 : General layout of the expanded pilot plant laboratory

7.4.2 I/O of the compartments

The chart here-under gives an indication regarding the quantity of input/output and regulation loop of the different compartments.

Complex analysers are directly connected to computer by RS 232 connection.

E = input, S = output, ana = analogic, num = numerical, tor = everything or nothing, Reg = regulation loop of level 0

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

Inputs outputs needs

	E ana ou num	S ana ou num	E tor	S tor	Reg
Comp 0	6	6	64	32	6
Comp I	10	4	64	32	4
Comp II	10	5	64	32	5
Comp III	9	8	64	32	8
Comp IV	10	7	64	32	7
Comp IV HP	8	7	64	32	7
Tota	53	37	384	192	37
Overestimated amount	***128***	***64***	***512***	***256***	***64***

7.5 Technology strategies

7.5.1 Advanced industrial data-processing platform

This platform defines the work station of several people committed to the industrial process management : manufacturing operator, maintenance man, metrologist …

This platforms receives on one hand the industrial applications and in another hand the supports, protocols and communication services.

This platform is an application of the industrial communications server and moreover It can also be a data server.

7.5.1.1 PC

Except specific case, the platform is composed by current standards computers .

If not absolutely required, industrial computers are not used.

7.5.1.2 OS - Processeur

Windows NT 4.0 from MicroSoft (Service Pack level 3 mini or 6 a maxi) is the Operating System which is recommended, if equipped with its technical resources kit.

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

Unless necessary, Windows NT Embedded, Windows 2000 and Windows XP are excluded. Except imperative necessity to guarantee for some particular tasks an execution time below 10 milliseconds, every « real time », OS Windows CE included and every «real time extension for NT » are banished.

Intel processor is the recommended one (at least for the Pentium range) with a minimal RAM OF 128 M0.

7.5.1.3 Hard disks

SCSI OR IDE able to store OS, applications and data.

OS, applications and data are stored on disk units on different logical partitions, using NTFS format (NT File system).
Swap file size is RAM x 2

7.5.1.4 Other peripherals

Monitors are colour graphics, according European standards for energy savings, interference waves reduction, reprocessing of its not-contaminating components.

Standards keys for the key-board : a trackball if possible integrated to the keyboard substitutes the usual mouse.

JAZ, CDROM, DON, DLT Backup or archiving peripherals are SCSI or IDE and have a capacity suitable for the hard disk(s).

7.5.2 Communication technologies

7.5.2.1 Communication services : layers 7, 6, 5 of the OSI model

The target selected for user interface with the « application » layers for industrial communications between components of the same « application », from one application to another application, fom application to equipment, from equipment to equipment, are the following by decreasing preference order :

- OPC customers-servers services (OLE 2.0 for Process Control) with « OPC Automation » and «OPC Custom » at the last update interfaces published by OPC Foundation, i.e. in « Data Access 2.0 » and « Alarms and Events 1.0 » versions used within the DNA distributed architecture (Distributed internet Application) by application exchanges and by TCP/IP Ethernet networks. Except absolute necessity, any « real-time extension for OPC », such DCX will be banished.
- The generic software is recommended among « OPC server » software on the market, i.e. free-standing from any API or SNCC supplier and holding all protocols and numeric

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

networks. However, OPC server and UNI-TE from Schneider-Electric are accepted to connect standard API (TSX family from Télémécanique) on industrial network ETHWAY .

- DDL (Device Description Language) services used by industrial networks like FOUNDATION FIELDBUS, PROFIBUS-PA, HART.
- DDLM (Direct Data Link Module) services used by industrial network PROFIBUS-DP.
- Basic services of industrial network **ASI**, are also accepted in the case of binary (TOR) sensors and actuators connection.

7.5.2.2 Communication services : layers 4 and 3 of the OSI model

Respect the stack of TCP/IP protocol is a good recommendation for all communication between lower and upper layers of the OSI model.

The main protocols TCP/IP are :

- IP, ARP et ICMP for the network layer
- TCP, UDP for the transport layer

The main utilities working with the TCP/IP layers are ARP and RARP, NETSTAT, PING, FTP and TFTP, RCP, RSH,REXEC,…

Among numerical network family, a lot of industrial networks accept intermediate layers TCP/IP.

7.5.2.3 Communication services : layers 2 and 1 of the OSI model

Layers 2 and 1 concern the traffic mode (synchronous or asynchronous) of MAC :

- Method of access to the media:
  - ♦ Deterministic : Producer – Consumer or master - slave
  - ♦ Stochastic : multimasters
- Type of transmission synchronous series media:
  - ♦ Wire : copper, optical,…
  - ♦ Wireless : laser, infrared, radio waves, …
- Type of junctions :
  - ♦ RS 485, IEEE 803.3, BC 20mA, …

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

- Type of topology :
  - ♦ Bus, Star, Ring, …

The lower layers of following numerical network are recommended, in decreasing order :

- Ethernet LAN
- Industrial networks FOUNDATION FIELDBUS, HSE and H1
- Industrial networks PROFIBUS, DP and PA
- ASI is accepted with Foundation Fieldbus H1 and Profibus PA, but it can connect only binary input output.

7.5.2.4 Network architecture

Exchanges between levels 2 and 3 of the « CIM pyramid » (Computer Integrated Manufacturing) are performed by our private network TCP/IP.

Industrial networks mainly match the communication requirements of the 0, 1 and 2 levels of the pyramid.

From now, this pyramid has been replaced by a MES cube (Manufacturing Execution System) crossed by several channels which allow the circulation of the information and its vertical and transversal access.

This MES concept makes the identification of 11 functions that frame the information system of execution of the production (i.e. the data process referring to controllers, automates, regulators, carried out I/O , sensors and monitors).

Industrial computer platforms require to be connected either to industrial networks and private network : as communication bridges, the platforms must imperatively be equipped with several network cards.
On the private network side, the connection card must be an Ethernet card 10/100 Mbps for bus PCI 2.1 with driver NDIS/NT 4.0 and double interface (RJ45copper connector and ST optical connector).

7.5.3 Availability technologies

7.5.3.1 "Symmetric MultiProcessing" (SMP)

NT versions traded by Microsoft deal with two processors maximum for NT workstation, 4 for NT Server Enterprise (NT Server option).
This technology choice can be useful and has to be justified

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

7.5.3.2 "Redundant Arrays of Independent Disks" (RAID)

- RAID Software

Only NT Server implements, for faulty hardware tolerance, software RAID : RAID1 or « mirrors set » (requiring 2 physical disks), RAID 5 (requiring at least 3 physical disks)

- RAID Hardware

As a complement to NT WorkStation or as an alternative to RAID software from NT Server, RAID Hardware makes possible to insure the redundancy with a RAID control card FOR SCSI or IDE disks.

RAID Hardware is preferred : RAID1 for OS redundancy ; RAID5, if the requirement is justified for redundancy.

7.5.3.3 "Cluster" or "Virtual Machine"

Only available under NT Server Enterprise, « Cluster » technology enables at least two NT Server platforms, working together in the same logical machine, to help in a dynamic way when one of them is faulty.

These technologies choice must be justified**.**

7.5.3.4 High availability

Given the conditions of the next mission, reliability obligations mean « high availability »:

- « 3 new » for a direct operation of 99,9%, which corresponds to a yearly immobilisation maximal time , planned and non planned, of 9 hours approximately (i.e. 525,6 minutes in relation with 8760 yearly hours)
- « 4 new » for a 99,99% availability, i.e. a yearly stop-break time less than 1 hour
- « 5 new » for a 99,999% availability, i.e. a yearly stop-break time of 5 minutes approximately.

Consequently, “high availability” technologies are preferentially examined, as “hot swapping” (insertion or extraction under tension of the electronic card, fan, feeding, disk, ..) “2N redundancy” (every critical resource is doubled) or “N+1 redundancy” (some resources have in line one change element at their disposal). Hot standby (Schneider) … etc.

The MTBF (Mean Time Between Failures), the MTTR (Mean Time To Repair) and estimated duration are to be provided systematically for every proposed solution.

If happen issues on hardware with NTFS format, a tool like Easy Recovery 5.0 from Ontrack can make easier the lost information recovery .

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

7.5.4 Security technologies

Only the technologies from NT 4.0 are recommended , which are configured at least for C2 classifications of TCSEC American standards (Trusted Computer System Evaluation Criteria) and E3/F-C2 of European standards (Information Technology Security Evaluation Criteria).

SNT4.0 securisation is to set up mainly for :

- NT boot process of NT : boot, repair, MBR (Master Boot Record) diskettes
- Opening NT session process on a field or a computer : user accounts (rules for password, activation option, session restrictions from computers), group accounts (local, global) : user profiles, user opening session scripts, system strategies (domain or computer, user, group)
- SAM basis (Security Account Manager)
- Register
- NTFS resources (NT File System)
- ACLSs (Access Control List) on local resources and shared NTFS, licenses on printing resources)
- Rights (at the SAM basis level)
- Security audit strategies (on field or computer, on NTFS, on printing resources)
- Saving and restoration strategies

Antivirus software, according current standards, is to be installed systematically, in the specified version, on data processing platforms

7.5.5 Storage technologies and data management

Except for temporary or intermediate data, all coding data requiring to be stored or recorded (process data and management data) are to be located in permanent process database.

ODBC standards are recommended for Database management systems (SGBDR), asking by SQL.
Oracle for Unix, Access for NT workstation are the current SGBDR for Company servers.
Access and SWL server have been selected for our industrial platform.

If not strictly proved, real time data have not to be distinguished from management data process : all of them have to be stored and managed with namely SGBDR .

If possible, all data are to be managed (or handled) with designation and storage unicity : they have to be located in a disk unit different from those of the application or operating system.

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

The whole information « on line » on industrial platforms have data structures at disposal that can be easily reused with standard tools of office automation (Microsoft) or Drawing (Autocad 2000) and that can be published at the HTML format.

7.6 Management strategies

Management, piloting, control are considered as having the same meaning.

Process management is defined to be the capacity to handle and interfere in a dynamic way on the process with IHM handling views and synoptic, trend curves, alarms and events, … all the process evolution being pay and display and recorded on disk.

Process management is performed, on an industrial platform, by a software package series which has an OPC internal structure (all major components of the series communicate with Data Access 2.0 and Alarms & Events 1.0) and only one ODBC database (all variables of the process has a the same and unique name and address for all the major components of the series).

« NT services » is carrying out background tasks among the major components of the series.

The series must offer in a toolbox standard optional components, OPC to development tools (Visual Basic ; C or C++), SQL question and data presentation tools, predictive control tools (automates and regulation) etc …

7.7 Control strategies

The two main types of available control technology are exposed.

Conventional control type like PID (Proportional – Integrated – Derivative) appear in two type :

- Classical PID : series PID – Parallel PID
- Augmented PID : Mixed PID – Feed forward PID – Ratio PID – Split range PID – Override PID)

Conventional control reaches his limits when a stable process has got a time delay upper than his dynamic or when the process is non linear, unstable or constrained.

In that cases, Advanced Control techniques are more suitable than PID

This advanced techniques are different if the process could be approached by a physical or comportment model, based on algebraic equations, or by an empirical model based on logical rules.

In the first case, comportment approach, the main techniques are:

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

- MBPC - Model Predictive Based Control
- Linear quadratic control
- Model control
- Time delay compensation

In the other case, heuristic or cognitive approach, the main techniques are :

- Expert system control
- Fuzzy control
- Neuronal control

Classic or advanced, every control engineering can be wisely used and without useless sophistication (if required it is a must).

Classic and advanced approaches turn out to be more complementary than competitive.

Implementation numerical targets of the control can be either our industrial platform which is handling the automatism and/or regulation, either an API or a regulation rack on numerical network.

A workshop of conception and prototyping of the control law has to be systematically proposed. It allows to realise correctly the main steps of the design of control laws:

- ♦ Conception
- ♦ Coding
- ♦ Focusing
- ♦ Test in simulation or via the IHM with the operative part of the process
- ♦ And eventually downloading of the control law into the API

In addition to those functionality, this workshop has to match the following requirements :

- To act as a control tool-box, classic and advanced, able to cooperate with every global solution component within a broadcast architecture which suits the OPC specifications and numerical networks
- To remain independent of any API or SNCC provider
    - ♦ Suit IEC6-1131-3 and IEC848 standards which are a control program label for all 5 standard languages the 3 graphic languages (« Ladder » also named « contact language » or relay language, from electricians ; « Block Diagram Function » or « Functions block language » from electricians ; « Sequential Function Chart », which is like Grafcet as described in IEC848 standard)

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

- ♦ both textual languages (« Structured Text » from Pascal language : « Instruction list » which is like Assembler language
- To be compatible with a lot of targets by generating a C control software

7.8 « Products-Offers » strategies

In principle, there is no exclusion, except any contradiction with the progress and strategies thrust described in the previous paragraphs or any special requirements.

Being material or software or mixt, "products-offers" solutions which are proposed must be, if possible, natively "interoperable" : the interoperability between two products is defined as the capacity to communicate towards OSI model layers.

Interchangeable solutions are to be identified : the "interchangeability" between two products is defined as the capacity for both products to be used one at the place of the other and reciprocally.

"Open" solutions does not mean "heterogeneous" solutions : for a specific kind of products (as management, control software …) the offer must be limited to two, or three at the most.

Global solution strategies must absolutely match the whole functions required in the Specifications with the right process and respect the main thrust of progress and strategy described in the previous paragraphs, except negotiated derogation.

This solution is limiting the « owner » solutions, in particular the « customized » developments.

If a specific software turns out to be necessary to complement one of the software of the global solutions, it must be engineered with the available standard development tool for the appropriate software.

For any specific software, it is absolutely necessary to have a strict partition between test environment and exploitation environment : programs (source, binary, executable) and execution procedures must have a location on disk, a version, a name, different if they are being up-dated or if they are operational.

Like the global solution software, software package and specific developments are to be set up with « NT services » and can be used towards native security NT technologies.

Required architecture documents must demonstrate the perfect integration of the whole software components (specific software and software package) together with the material and network components that participate to the global solution.

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

7.9 Specifications detailed by function

7.9.1 Data elaboration function

A Technical Data Base (TDB) is updated. TDB contains all information about each component of the process:

- Builder information
- Performance information
- Maintenance characteristics

A Real Time Data Base (RTDB) is updated. RTDB allows real time accessibility of all variables and parameters.

7.9.2 Supervision Function

This part describes the main functionality of the man-machine interface :

- synoptic
- cycle start-up
- automatic control
- semi-automatic control
- remote control
- various

In general, the system will allow a multi-windows and multitasks mode

7.9.2.1 Synoptic

It will be possible to display several synoptic simultaneously, in the multi-windows mode.

7.9.2.2 Cycle start-up

Before the effective beginning of a cycle of each compartment, an auto-diagnosis module allows to control the whole installation. It checks associated sensors and materials.

If the machines are not working properly, all these check-ups produce alarm and are recorded. Some of these check-ups can obstruct a cycle start-up (red light).

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

The operator will have to validate the results of the auto-diagnosis to be able to launch the effective cycle.

7.9.2.3 Automatic management

The main mode (normal one) of the loop used is the automatic mode.

The operator can display the whole parameters of the MELISSA loop on charts, curves, messages and graphics.

A software module allows to process the specific alarm with record, examples : cut sensor, wrong empty level, bad working of one machine …

The operator will have the possibility to interference with the system to modify the input (invalidation of the sensor …) or the outputs (heat level …).

In every case, the system maintain a track of these actions and keep on data logging tasks.

7.9.2.4 Semi automatic management

It must be possible to work with one or more compartments in manual mode and the others in automatic mode.

7.9.2.5 Remote surveillance

It will be useful to make possible a real time data transmission between Mars and Earth in case of special maintenance mode adapted to the special and very long transmission timing (more of 20 minutes).

7.9.2.6 Various

All the alarms are double dated (absolute calendar dating – AA/DD/JJ/MM/SS 100ms- and relative dating related to the beginning of the current batch) and recorded. They will be printed upon request. Some can set off a sound alarm.

A minimum level of automatism will be kept out from the supervision for mainly the machine security and the extremes limits of the current process.

7.9.3 Maintenance function

7.9.3.1 Help to predictive maintenance diagnosis for the general means

The main purpose of a predictive maintenance tool is to make possible the feed-back of the auto-diagnosis from group equipment towards supervision PC ; a bi-directional

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

communication makes also possible the configuration and set-up of parameters of the equipment from this PC.

The purpose is to watch permanently over the ground equipment, without having to move physically in order to prevent any potential damage of the process function or the quality product and make intervene, if necessary, the maintenance technicians (part of the crew).

The equipment proposed, like transducers and valves, even the pumps, device, speed variators, power electronic, are classically connected on analogical links 4-20mA, or numerically connected on ground networks.

Pre-required : to have « intelligent » equipment with auto-diagnosis functionality, a computer with maintenance predictive maintenance software and a numerical communication between equipment and computer are required.

Regarding the OPC customer-server model between the computer and the equipments, 1.0 version of « Alarms and Events » printed by OPC Foundation state that OPC server sends back to the OPC customers the wrong conditions (alarms) and the events (state modification) found.

Predictive maintenance software on the computer will allow to display on a screen the ground equipment supervised, to control the state of the diagnosis variable, the technical documentation of the equipment and the industrial log.

7.9.3.2 Metrology standardisation management

7.9.4 Acquisition function

Acquisition and coding of data are centralised.

Sensors and actuators are standardized for all the compartments.

Required performances are specified.

7.9.5 Regulation function

Software solutions for regulation function are better than hardware solutions.

Solutions have to be checked, tuned and receipted in the platform that contains a simulation of operative part of the process.

Each kind of regulation must be homogeneous from one compartment to the others.

Predictive solutions have to be preferred.

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

7.9.6 Automatism function

Many solutions:

7.9.6.1 Solution 1 – Classical way

API controller platform is connected to a software monitoring on a separated PC platform.

7.9.6.2 Solution 2 – PC controller

Solution 2 connects « PC controller» and monitoring package on a PC platform.

PC controller means a controller card on PC with its software driver (or « driver ») or a controller software on PC (also named « Soft Logic ») controller.

This kind of solution :

- standardises the hardware and software platform (only one machine instead of two in order to interconnect, one is the owner API , only one designation for the variables -check the database standardisation- and consequently variables up-to-dating label for the whole controller-monitor group
- makes easier the connections between supervisors and monitors if the controller-supervisor group matches the OPC specifications (Data Access 2.0, Alarms & Events 1.0) and makes possible the synthesis information feed-back towards upper management coats (office data processing applications, Intranet electronic messaging, ERP …)
- allows to release the owner solutions provided we take care of holding « control workshop » on PC that should be in addition :
  - independent, i.e. not connected with a specific API, not integrated to a supervision package
  - in accordance to the IEC6-1131-3 and IEC 848 standards that enable to program with all the 5 standard language of Automatic control, i.e. the 3 graphic languages (« Ladder » also named « contact language » or « relay language » from electricians < ; « Block Diagram Function » also called « language par blocs de functions » from electricians. « Sequential Function Chart » which is like Grafcet as described in the IEC848 standard) and the 2 textual languages (« Structured Text » from Pascal ; « Instruction List » which is like an Assembler language)
  - able to generate either intermediate code (in C language for example) which can be performed on the OS-Processor platform or compiled code working on a Windows-Intel platform targeted like NT one

For example : WizPLC Version 2.1 of e-Mation Compay (ex PC Soft International) and Virgo2000 Version 2.0 form Altersys company (which incorporates Isa GRAF Pro form CJ

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

International and IHM FrontVue of ARC Informatique Company) state they comply with these recommendations.

Some software (automatism toobox) working on PC, for example, WinAc from Siemens propose even a soft path for the API solutions to be converted in «PC controller » by generating the code by selection, either for a control PC card or for a PC (« Soft Logic »).

Possible functionality for « control workshops » software on PC can be provided beyond the simple control program checking-out (debugger, record of the program process with break points, input/output data capture) statement by integrating more or less sophisticated simulators of E/S control.

Close to « control workshop » software, there is also a simulation and control toolbox software that in addition make possible the reproduction of the operational part of a controlled industrial facility (i.e the process) on a virtual reality way on PC : the breadboard put in situation (but without production flow) maintenance technicians and manufacturing operators that can train and validate the facility (either for operational or security purposes)

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.

8. CONCLUSIONS

The works related in this technical note concern two parts.

8.1 Part I - Dependability analysis

Part I of TN 62.9 contains process proposal and technical specification for dependability analysis. All these propositions have to be fitted into the context of MELISSA project.

Schematically the project MELISSA can be cut in three main periods:

- Period I: Design and independent tests of each compartment of MELISSA loop
- Period II: Ground version of the pilot plant in UAB that check the connection of all compartments. The main goal of the pilot plant is to check the ability of each compartment to work with each others and is to be sure of hitting the target of the mission without space constraints for hardware and software.
- Period III: Space version of the pilot plant. This version maintains the organisation and the functionalities of the ground version but revises components and hardware solutions to adapt them to the space conditions.

The project is actually at the beginning of the period II and the dependability aspects can seem a little untimely.

But the concept of system reliability, which includes in particular the studies in reliability, availability and fault tolerance, is a very vast subject, both on the theoretical and industrial levels.

TN 62.9 reports some modest recommendation concerning dependability analysis organisation.

For a as complex and ambitious system as MELISSA, the component reliability is essential. The whole equipment is expected to operate in an autonomous way over a long period of time with minimum local maintenance.

This kind of study must be carried out following a Systemic Approach, while taking into account, in a global way, the hardware, the functional and control aspects as well as the human interaction.

For historical reasons, in the majority of real industrial cases, reliability studies are carried out a posteriori, the unit being already in service. The reason is the separation of the tasks and responsibilities for the various actors in the design of the different components.

This document is the property of ESA. It can’t be used, duplicated, modified or transmitted without his authorisation.

The most effective way is to take into account the reliability requirements as a part of the preliminary draft, and to carry out a true operation of Integrated Design .

It is not too early: the fundamental operation principles are defined and the principal technical options are taken or under study. Modelling and simulation are now accessible.

It is not too late*:* if the study results in objecting any characteristics of some components, it is not to late to modify their specifications.

8.2 Part II – Functional specification on the driving system features

Part II of TN 62.9 reports general recommendation on technical choices concerning hardware and software aspects of driving system of MELISSA loop.

This work, after iteration and validation by the partners, can be used to build detailed technical specification for the driving system of the ground version of the pilot plant in UAB.

This document is the property of ESA. It can't be used, duplicated, modified or transmitted without his authorisation.