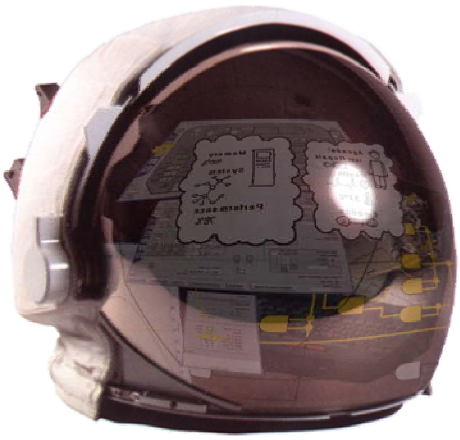
# ETECA

## Expert Tool to Support Crew Autonomous Operations in Complex Human Spacecraft



| | |
|---|---|
| **Title:** | ETECA Executive Summary |
| **Reference:** | ETECA-RP2 |
| **Issue:** | 1.1 |
| **Date:** | 2009-10-09 |
| **Author:** | Christian Knorr |
| **Contract No.:** | esa 21585/08/NL/HE |

**ESA STUDY CONTRACT REPORT**

| **ESA Contract No** | **SUBJECT** | | **CONTRACTOR** |
|---|---|---|---|
| 21585/08/NL/HE | Expert Tool to Support Crew Autonomous Operations in Complex Human Spacecraft | | Astrium GmbH, Space Transportation |
| *** ESA CR ( ) No** | *** STAR CODE** | **No of volumes** 2<br>**This is Volume No** 1 | **CONTRACTOR'S REFERENCE**<br>ETECA-RP2 |

**ABSTRACT:**

The main objectives of the study were to describe and assess a concept for autonomous crew operations onboard complex spacecrafts supported by analysis and diagnostics functions and the definition of the required decision support tool capabilities. Furthermore the potential advantages and risks of tool-supported decisions and the autonomous operations approach should be assessed.

The study also comprised the definition of a tailored process for cost effective development of necessary support tools and the development of a proof-of-concept demonstrator along with the definition of relevant scenarios and the according requirements and specification for an interactive tool.



**Name of authors:** Christian Knorr

| **NAME OF ESA STUDY MANAGER** | **ESA BUDGET HEADING** |
|---|---|
| Mikael Wolff<br><br>**DIV:** Software and Systems<br>**DIRECTORATE:** Technical and Quality Management | G1/100060/6005100/GPA/RD100/08I64 |

* Sections to be completed by ESA

# ETECA Executive Summary Report

This report summarizes the work carried out, the results and the findings of the study

"Expert Tool to Support Crew Autonomous Operations in Complex Human Spacecraft"

performed under ESA/ESTEC contract 21585/08/NL/HE. The study has been performed by an industrial consortium lead by EADS Astrium Space Transportation, Bremen, consisting of the following companies:

- EADS Astrium Space Transportation, Bremen, Germany
- Space Applications Services, Zaventem, Belgium
- Science & Technology, Delft, The Netherlands
- TNO Defence, Security and Safety, Soesterberg, The Netherlands

The main objectives of the study are to describe and assess a concept for autonomous crew operations onboard complex spacecrafts supported by analysis and diagnostics functions and the definition of the required decision support tool capabilities. Furthermore the potential advantages and risks of tool-supported decisions and the autonomous operations approach shall be assessed.

The study also comprises the definition of a tailored process for cost effective development of necessary support tools and the development of a proof-of-concept demonstrator along with the definition of relevant scenarios and the according requirements and specification for an interactive tool.

## Research

An initial phase assembled the current state-of-the-art in research and available tools regarding decision support topics and technologies. A synthesis of the studied literature revealed the following relevant topics and technologies:

- **data fusion**: integrating disparate data from different and distributed sources.
- **health determination**: developing tools for fault detection and diagnostics of crew, systems and tools *themselves.*
- **procedure automation**: transforming current (spacecraft) procedures into structured, i.e., machine understandable, information that machines can reason with and about.
- **situational awareness**: providing the relevant information for understanding the current and predicting the future system state (e.g., impact and risk assessment).
- **adaptive tools**: developing tools that use experience to adapt their behaviour by, e.g., user or tool feedback (truth maintenance).
- **development processes**: how to develop, test (making use of existing infrastructure), verify & validate, and certify (decision support) tools.

Beside the very valuable input for the ETECA study itself this research also identified further reasons for fostering more crew autonomy in future human space flight missions:

- Crew motivation
- Communications delays
- Communications bandwidth

## Process Definition

An essential activity of this study was the definition of a general process for cost effective development of decision support tools in support of onboard crew autonomous operations of complex space vehicles. The adaptation of the situated Cognitive Engineering (sCE) methodology proofed to be an appropriate approach and the positive feedback from the evaluators of the ETECA demonstrator regarding the ETECA concept supports this.

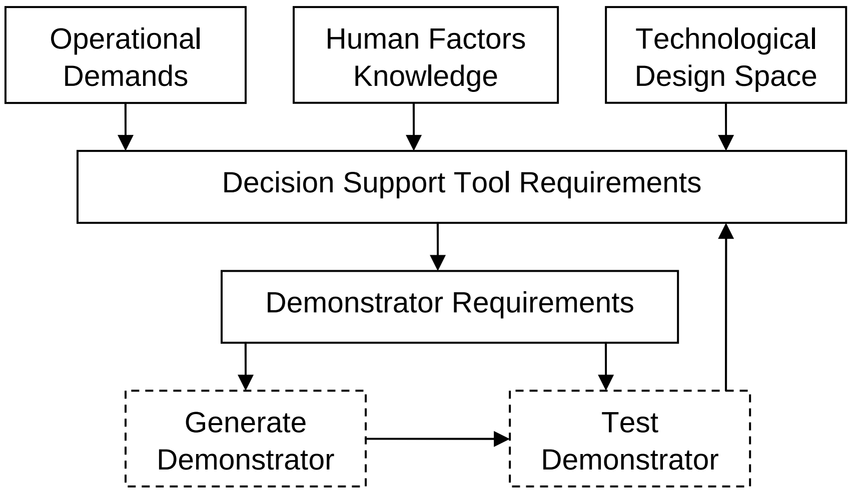



**Figure 1: sCE approach**

Despite the definition of the incremental iterative development process the matter of knowledge transfer between equipment providers and decision support tool developers has been elaborated. This takes – on the process level – into account that space projects usually involve numerous stakeholders who all need to be activated to create a suitable knowledge base for expert tools.

## Supporting Scenarios

As part of the study, Columbus-like failure scenarios have been selected and described which served two main purposes:

- to be the basis for astronaut interviews to gather end user requirements
- for validating the developed concept using a proof-of-concept demonstrator

The scenarios which have been developed are the following:

**Water Pump Assembly (WPA) Switchover from WPA1 to WPA2 by automatic FDIR**

This scenario addresses an error in equipment software which is triggered by an operational monitoring activity itself. The important fact is that no mechanical damage occurs but the equipment software identifies an internal dead-lock which is not directly visible on the system level. Solving the problem requires a good understanding of the current operational state including the history of relevant events (Situational Awareness, SA) and good knowledge about the subsystem and equipment architecture.

**Nominal Data Management System (DMS) Data Distribution Break Down**

A very common problem of complex systems lies in the interface boxes between different equipment. Together with the general electronics problem of radiation this scenario covers the aspects of similarity of errors, applying past experience and the need for dedicated functions to analyze system functions through the different integration layers (i.e. system, subsystem, assembly, equipment).

**Missing Broadcast Ancillary Data (BAD) Packages**

With growing complexity of a system problems are often caused by side-effects of changes in very different areas. This scenario requires again means for analyzing system functions through the different integration layers (i.e. system, subsystem, assembly, equipment). But equally important is a good understanding of low-level data flows and data structures. In addition configuration changes need to be well reported and understood to identify the cause and effect relationship of such changes. For working around the problem a good understanding of computer software and common software problems is essential.

**Nominal Command and Monitoring Unit 1 (CMU1) Temperature Increase**

This last scenario describes not a real failure case but rather a potential equipment failure in the future. To address this scenario a system would need to provide early indication of off-nominal behaviour in parallel to the currently implemented static threshold monitoring. Additional monitoring functions should allow the observation of a dedicated parameter over long time periods and preventive actions need to planned and performed to avoid a real failure of equipment.

## Operational Concept and Core Functions

With the inputs of the initial research, astronaut interviews, usability analysis and general domain analysis and following the defined process an operational concept has been developed supported by the described scenarios. This helped to identify necessary core functions which finally were described and refined by a specification for a general decision support tool.

The common paradigm of the operational concept is about increasing crew's autonomy in performing a wide range of tasks. Although the main context is future space flights, e.g. flights to Mars where increased crew autonomy is of paramount importance, current ISS context is also considered, where the ETECA operational concept could (i) be tested and evaluated in a well-known and well-defined operational background, and (ii) actually support and improve current ISS crew operations.

Two high level operational modes have been identified for ETECA:

1. Support for troubleshooting, in its wider meaning, i.e. ranging from failure detection (or even anticipation) to systems full recovery (nominal).
2. Support for day to day operations: supporting monitoring and control of devices and payloads/sciences operations. ETECA may e.g. alleviate crew members from the most repetitive (and time consuming) tasks.

For realizing the operational concept the following 7 core functions (CF) have been identified:

- CF1: Make the decision maker aware of the need to make a decision (i.e. triggering “alarms”, notification)
- CF2: Identify relevant procedure(s) in the current context and present them to the decision maker
- CF3: CoA generation and value estimation, “what-if” simulation modes, results and justification display
- CF4: Provide guidance to implement the selected course of action, e.g. by training the decision implementer
- CF5: Support the implementation of the steps in the course of action: indeed this could be done either only by the decision maker, or by an interleaved course of actions of both the decision maker and the ETECA system (under supervision of the decision maker)
- CF6: Provide guidance to verify the implementation, e.g. by monitoring certain sensors
- CF7: On-request background / reference documentation consultation

These core functions have been detailed in use cases which describe individual situations and the expected sequence of steps which need to be supported by the core functions. The use cases also comprise so-called testable claims which are expected results that can be tested to verify a function.

## Requirements Baseline and Specification

Based on all inputs and the analysis work performed a requirements baseline has been developed for a general decision support tool. The requirements have been organised in the following requirements categories or groups:

- General Requirements
- Functional Requirements
- Operations and Usability Requirements
- Maintenance and Maintainability Requirements

Finally a technical specification has been generated which classifies the requirements according to their importance and relevance and which discusses the classification more in detail.

## Proof-of-Concept Demonstrator

A subset of the defined requirements – focusing on situation awareness by means of diagnostics functions, integrated context specific documentation and relevant possible actions (utilizing existing operational procedures) – has then been implemented in an interactive proof-of-concept demonstrator. The main components which have been developed as part of the study work are a diagnostics server process, a diagnostics user interface and as a support component a data simulator.

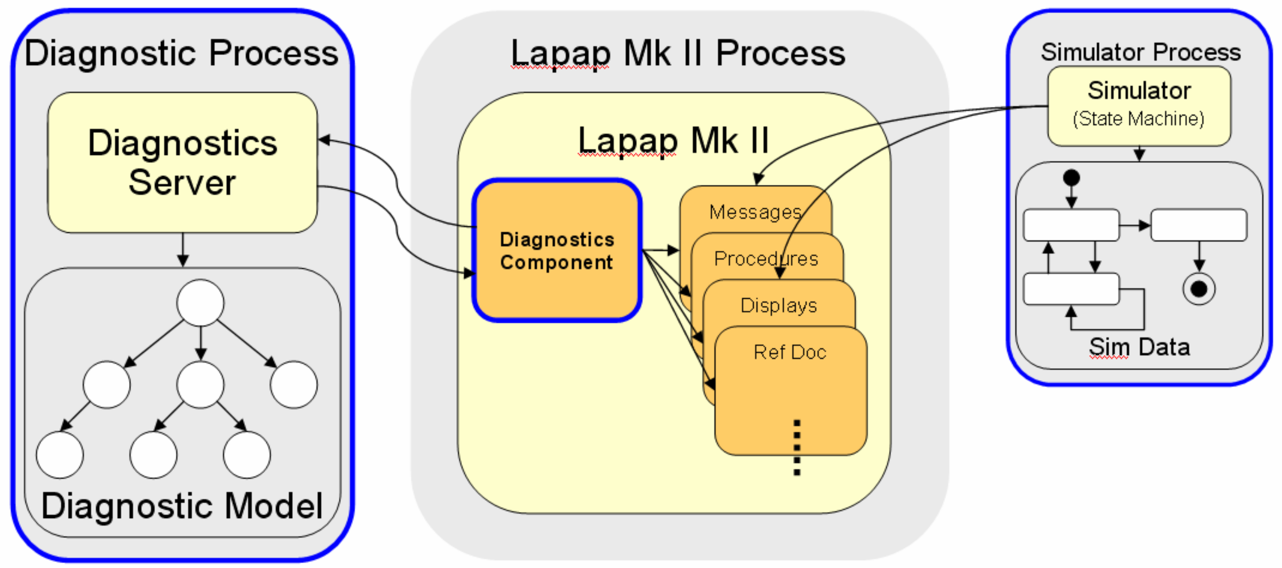



**Figure 2: ETECA Demonstrator Architecture, the blue borders mark components which have been developed as part of the ETECA study work**

The diagnostics server is built on an existing diagnostics engine which follows the model based diagnostics (MBD) method. It performs stateless diagnoses based on a model of the monitored system and system observations. For ETECA the diagnostics server has been wrapped by a web service to make it available as external process using a standard protocol.

The demonstrator is based on the existing Columbus crew interface Lapap Mk II which resulted in a look-and-feel which is close to a real operational environment making use of existing functions and data products.

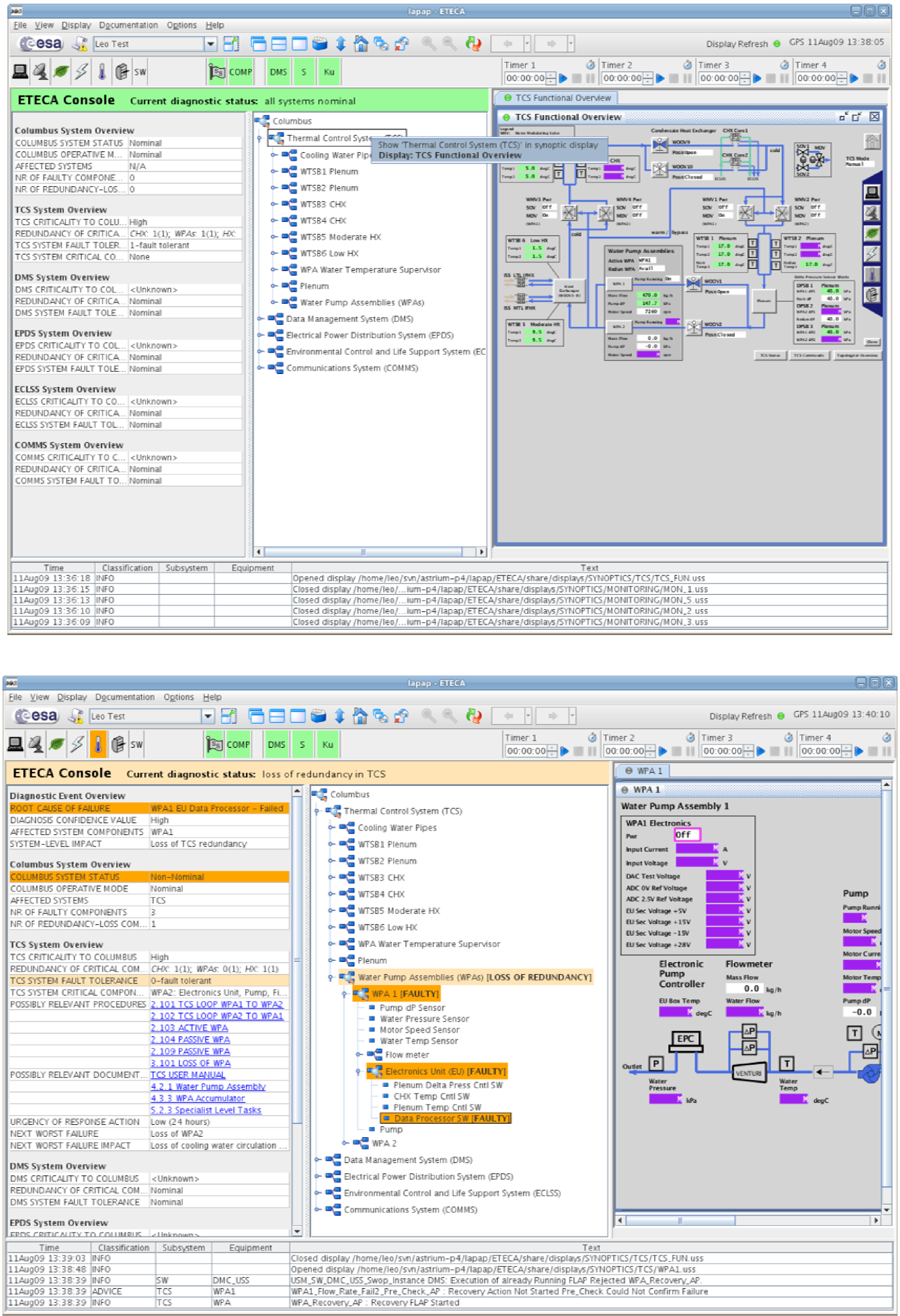



**Figure 3: The ETECA user interface; nominal (above) and off-nominal (below)**

# Evaluation

The final evaluation of the proof-of-concept demonstrator by an astronaut, Columbus flight controllers, instructors and expert staff attested “an efficient and effective support to the understanding of the situation”.

The system has been evaluated by end-user reviews as well as an expert assessment. The end-user reviews built upon a realistic failure scenario which was inspired by a real Columbus failure during in-orbit operations. An astronaut, an astronaut instructor and two flight controllers used the interactive demonstrator to analyse the simulated failure. The system was considered easy to use and to be an effective support to handle failure situations which are similar to the evaluation scenario.

The evaluation of the system in more complex failure scenarios was requested and some of the functions that are defined by the general specification of a decision support tool which have not been implemented in the demonstrator have been considered relevant for the concept.

The expert assessment was held with a small group of evaluators concentrating on the usability aspects of the demonstrator and discussing any identified issue. It strongly supported the general applicability of the ETECA concept and positively evaluated the diagnostics function and the according user interface being the main function of the ETECA concept which is implemented in the demonstrator.

Several very detailed suggestions have been formulated by the experts to improve the demonstrator for a new development and evaluation iteration.

# Conclusion

The ETECA project was the first step of an incremental iterative development approach, demonstrating the opportunities for effective decision support tools with the corresponding requirements. Individual aspects have the potential to add benefit to already currently existing systems in-orbit as well as on ground while follow-on activities would be useful to elaborate on areas which have not been addressed in detail in the scope of this study.

A follow-on activity could concentrate on evaluating the concept in more complex failure scenarios or it could implement missing functionality like support for manual root cause analysis (e.g. supported by case-based reasoning), solution implementation support (e.g. by automated crew procedures) and solving of problems which have not been anticipated and prepared by procedures (e.g. planning of activities based on documentation and past experience rather than predefined procedures). Either way an incremental approach is proposed to elaborate the concept and the demonstrator following the described process.

## List of Study Deliverables

The following documents have been produced as part of the study and the final report and the technical notes provide further details on the subject:

| | |
|---|---|
| ETECA-RP1 | ETECA Final Report, Issue 1.1, 09.10.2009 |
| ETECA-RP2 | ETECA Executive Summary, Issue 1.1, 09.10.2009 |
| ETECA-TN1 | Survey on Decision-Support Research and Tools, Issue 1.2, 09.10.2009 |
| ETECA-TN2 | Decision Support Tools Development Process Definition, Issue 2.1, 09.10.2009 |
| ETECA-TN3 | Requirements Baseline and Technical Specification for a Crew Decision Support Tool, Issue 1.2, 09.10.2009 |
| ETECA-TN4 Part 1 of 2 | Design of a Proof-of-Concept Demonstrator, Issue 1.1, 09.10.2009 |
| ETECA-TN4 Part 2 of 2 | Assessment of a Proof-of-Concept Demonstrator, Issue 1.2, 09.10.2009 |