Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2000-533

The development of the diagnosis procedures for the European Robotic Arm

J.F.T. Bos and M.J.A. Oort

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2000-533

The development of the diagnosis procedures for the European Robotic Arm

J.F.T. Bos and M.J.A. Oort*

* *Fokker Space B.V.*

This report is based on a presentation held at the International Conference on Safety and Reliability ESREL 2000, Edinburgh, Scotland on June 2000.

Division:	Information and Communication Technology
Issued:	October 2000
Classification of title:	Unclassified

Summary

Currently Fokker Space B.V. is developing the European Robotic Arm (ERA) under contract to the European Space Agency (ESA). ERA will help assemble and maintain the Russian Segment of the International Space Station. The purpose of this paper is to describe the approach followed in deriving the procedures for quick failure diagnosis during a mission with ERA, and to describe the verification approach of the derived procedures.

Contents

1 Introduction 4

2 Approach 5
2.1 Recovery 5
2.2 Purpose and Task allocation 5
2.3 Diagnosis: how to do it 7

3 ODF format 9

4 Verification approach 10

5 Conclusions 12

(14 pages in total)

1 Introduction

Currently Fokker Space B.V. is developing the European Robotic Arm (ERA) under contract to the European Space Agency (ESA). ERA will help assemble and maintain the Russian Segment of the International Space Station (Kampen et al. 1995). In late 1998, the first two modules of the International Space Station (ISS), the Zarya and the first node Unity, have been launched and coupled successfully.
ERA is a symmetric seven degree of freedom manipulator of about 11 meters length which can relocate to various positions (basepoints) on the Russian Segment (Fig. 1). It can transport large objects (such as solar arrays) during the Russian Segment Assembly Phase, and exchange Orbit Replaceable Units (ORU's) as well as inspect the Russian Segment during the Operational Phase of the station. The ERA can be controlled directly by Extra Vehicular Activities (EVA) crew members, or remotely from a laptop-type work station by the crew members in the modules of the Russian Segment, i.e. by Intra Vehicular Activities (IVA) crew members (Fig. 2). It is scheduled to be launched end 2001 or 2002.
The ERA program has November 1999 past successfully the Critical Design Review. First test results on the Engineering Qualification Model(s) are available (Hofkamp et. al 1998).
In (Beerthuizen et al. 1998) the general safety strategy is described. In (Bos & Oort 1997) the concept of the Failure Detection Isolation and Recovery (FDIR) system is described, containing a description of the data available for the diagnosis. The purpose of this paper is to describe the approach followed in deriving the procedures for quick failure diagnosis during the mission (what is done with the data), and to describe the verification approach of the derived procedures.

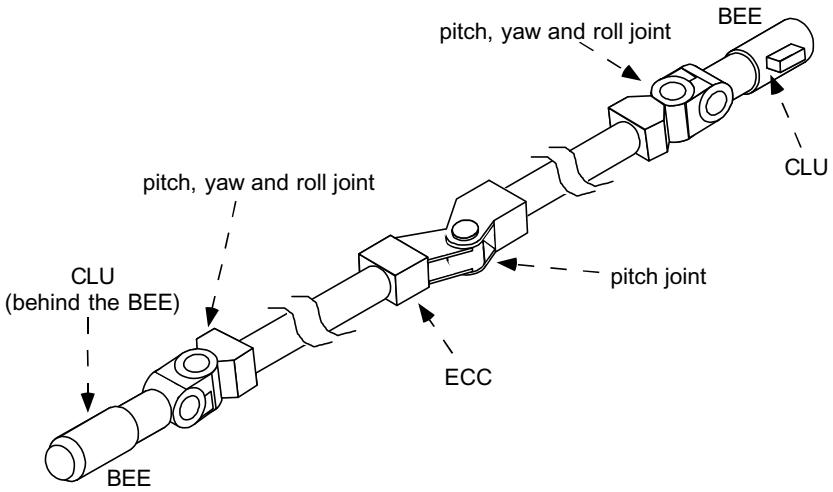

Fig. 1 The ERA manipulator with 7 joints, two Basic End-Effectors (BEE), Camera Lighting Units (CLU) and the ERA Control Computer (ECC)

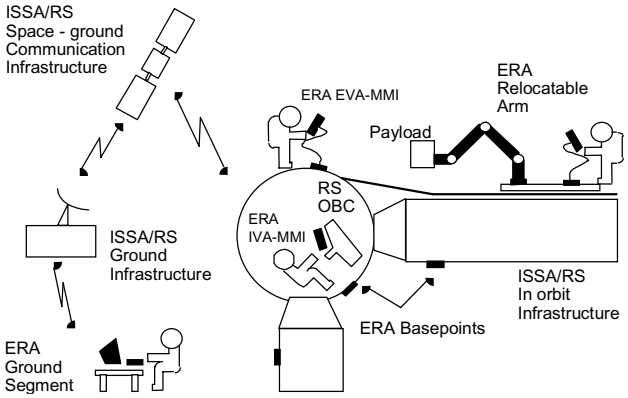

Fig. 2. Elements of the ERA system

2 Approach

Diagnosis starts if a failure is detected either by the automatic Exception Handling system or by the operator. The purpose of the diagnosis is to find the cause of the problem to that level that an appropriate recovery action can be taken to continue the ERA mission in a successful manner. Therefore, the possible recovery actions will be described before addressing the diagnosis approach.

2.1 Recovery

In principle, there are only five possible recovery scenarios (Bos & Oort 1997):

- Resort to the redundant databus for a particular S/S
- Resort to the redundant power-bus, to which the redundant units of all ERA sub-systems are connected
- Ignore the error and disable the associated check(s), or wait until the conditions become nominal by themselves (e.g. over-temperature)
- Change the S/W in the Control computer or sub-system (e.g. degraded motor torque)
- Replace the failing sub-system by a spare available in the station (e.g. a new Wrist assembly).

The driving requirements for diagnosis state that it shall be possible to trace each detected failure to replacement unit level or to the level of redundant paths.

2.2 Purpose and Task allocation

ERA is not an autonomous system, but it is controlled by an operator, either using supervisory control or manual control. This means that operators can and will play a role in the failure diagnosis process to meet the restrictions due to the limited processing power on-board.

Although the party most capable of properly diagnosing a failure and defining a recovery action is the Mission Control Centre, in some cases the space operators are able to handle the failures themselves, and the diagnosis and recovery can be allocated to the crew. Effectively, the following basic rules have been applied with respect to the task allocations between cosmonauts and Ground:

1 In case of an anomaly the IVA operator gets in charge, irrespectively whether an EVA cosmonaut is controlling ERA.
The reason is that the IVA operator must always be present and monitor the mission (ISS rule), and he is far better equipped to assess the situation than the EVA operator. The major limitation for the EVA operator is imposed by the limited display and control possibilities of the EVA-MMI.

2 Where possible the IVA operator performs the diagnosis and recovery, but on-line Ground support needs to be involved when:
data from dedicated memory dumps need to be examined. This can be done in the Russian Mission Control Centre.
a special Auto Sequence, i.e. a command file to be executed by the computer, needs to be made for diagnosis or recovery purposes. This needs to be done with Mission Preparation and Training Equipment (MPTE) (Pronk et. al 1999).
external failures originating from Space Station level operations needs to be considered (including Russian Central Post Computer related operations)
history trends of data have to be considered. This can be done on-line with data from missions in the past.
deciding on mission abortion (for instance, if the diagnosis/recovery would take so long that the oxygen of the EVA cosmonaut will be insufficient to complete the mission)

3 When an EVA cosmonaut is already present (i.e. outside the ISS), EVA is *preferred* to be involved when:
external failures originating from the environment needs to be considered (damaged grapple/latch interface etc.)

In principle the diagnosis can be performed at two levels:

1 to find the cause of the problem to that level that an appropriate recovery action can be taken to continue the ERA mission in a successful manner. Since the recovery possibilities are limited, and on a relatively “high level” (total power switch, ERA Replaceable Unit exchange, etc.) no detailed diagnosis finding the cause to component level is needed.

2 to find the cause to the lowest possible level (which can be even at component level): to understand why the error occurred, and optionally to prevent the error from happening again when spares are considered.

For ERA the diagnosis in the operational context needs to be done to the level of redundant paths or replaceable unit level. Therefore, the first relatively high level of diagnosis, is appropriate.

So, we have to map the error symptoms (checks which triggered plus accompagning data) to the recovery possibilities as illustrated in Figure 3. Basically the symptoms will be the danger events raised.

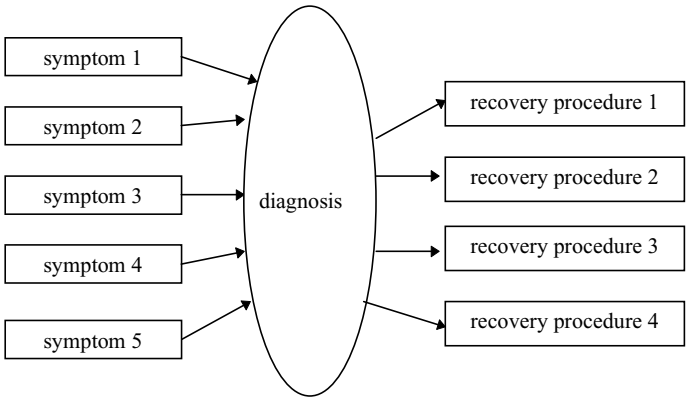

Fig. 3. Diagnosis is to map symptoms to the right recovery procedures

Performing diagnosis is to be considered in the operational context. An important question is whether the mission has to be aborted or can be continued. The answer to this question depends on several factors like:

- Is the time margin left enough to perform diagnosis and/or the identified recovery action? This is largely driven by the question whether the EVA cosmonaut has enough oxygen left.
- Are the physical resources available to perform the identified recovery action during the present mission? For instance, in case of a necessary replacement of a piece of hardware the present mission has to be aborted.
- Is the cause of the problem sufficiently understood?

2.3 Diagnosis: how to do it

In creating methods and tools for the diagnosis often knowledge is used which is represented in Failure Mode and Effect Analysis, Fault Tree Analysis, or using expert (design) knowledge. In manned space applications like the Shuttle, so-called malfunction procedures are developed to allow the crew a structured and unambiguous way to deal with the situation. The development of these malfunction (diagnosis) procedures is subject of this paper. As the diagnosis in space needs to be done to such a level that the appropriate recovery action can be selected, an effort was made to structure the diagnosis flow in a consistent way over all procedures handling the symptoms. Figure 4 presents at a high-level all elements that are involved in an ERA operation.

To perform diagnosis in a structured way, first a class of main error sources is defined based on Figure 4, each requiring its own recovery approach:

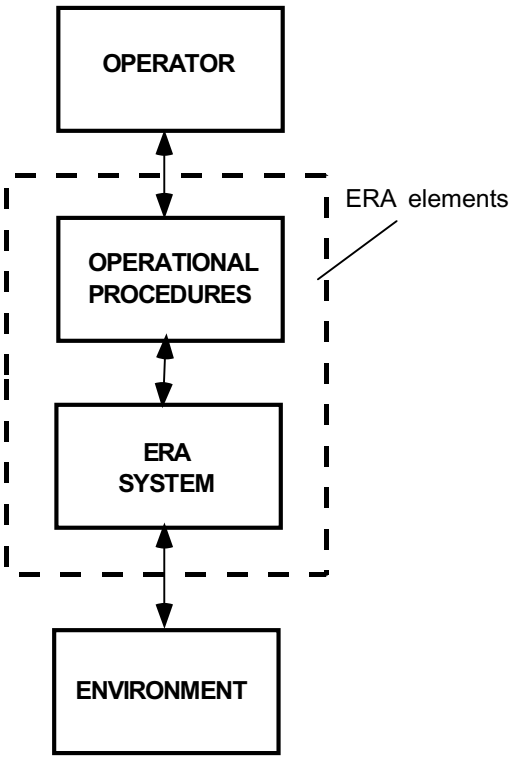

Fig. 4 ERA Operations on a high functional level

The following fault categories can be distinguished:

1 *operator errors*
Using the MMI the operator can give erroneous commands, i.e. commanding a motion in a wrong direction, setting a wrong payload class etc.

2 *operational (procedures/planning) errors*
For instance, a wrong payload class is selected (in the Auto Sequence, which contains the command for automatic execution of a mission), or the payload was not present where it was assumed to be.

3 *environment(induced) errors*
For instance, the grapple interface is damaged, the thermal environment is out of specification, or there were disturbances caused by the ISS Attitude Orbit Control System (AOCS).

4 *system errors*
H/W and/or S/W error of the ERA S/S. In case of a *system error*, the following error classes, which point directly to a recovery action, can be distinguished:
* mechanical error
* electrical power error
* databus error
* S/W error
* thermal error

5 *False alarms*
It can happen that a failure is detected which did not really occur.

Considering the fault sources, the possible safing actions, and the basic diagnosis/recovery approach, the basic FDIR flow for ERA can be detailed and yields Figure 5. The fault diagnosis blocks in Figure 5 are basically fault elimination steps, where the possible faults belonging to a symptom are derived from the FMEA's and expert knowledge. In these fault elimination steps visual inspection, operational history, commandable check-outs etc. are used. For instance, to determine whether the CCD of the camera is still functioning correctly a special check-out can be commanded. A specific LED is exploited, that provides a reference illumination pattern on the detector. This illumination pattern is used to verify both the quality of video images and the correct detection of saturated pixels.

3 ODF format

The malfunction (diagnosis) procedures have to be written in accordance with an ISS-wide applicable standard, the Operations Data Format (ODF). This allows the ISS crew to be able to quickly understand and run through any procedure on the ISS, using any equipment. An example where the operator needs to switch off ERA is given in Figure 6.
The malfunction procedures need to cover all possible paths, and are written in the style of a flow-diagram [if… then…else…]. These procedures are meant to be used by the IVA crew member, because the procedures tend to become too complex to allow summarizing the steps on cuff sheets for an EVA crew member. Note that these procedures need only cover the steps which can be taken on board. For the diagnosis and recovery steps on the ground, the more standard documentation is used.

- 'MENU' (the display area)
- sel 'menu' (the button)
- sel 'CPC Commands' (another pull-down menu)
- 'COMMANDS' (the display area in which the CPC commands are displayed upon activating the pull down menu)
- **cmd** 'ERA OFF' **Execute** (the required entry in the pull down menu; the Execute is required, because the command to switch off ERA needs to be confirmed)
- 'STATUS' (display area)
- ✔Power - ERA OFF (verify that ERA is indeed switched off)

Fig. 6 Example of procedure steps in ODF, where comments for this paper are between brackets

4 Verification approach

Due to the interaction of the ERA system with a crew member, the verification approach to the procedures is somewhat more extensive than for autonomous systems, and concentrates on different aspects. In the verification approach it is assumed that the autonomous part of the system has already been verified, i.e. that all functions are working properly. The objective of the verification is not to uncover errors in the autonomous system, but to verify that the human element has correctly been taken into account. Not only the correctness of the procedures themselves need to be verified, but also whether the information presented to a crew member is sufficient (but not too much) to allow the correct decisions. So, there is a close link with training aspects.

As shown in section 2.2, the ensemble of possible failures is very large, while the number of symptoms is much less, and even more so the number of recovery paths. It is therefore essential not to fall into the trap of approaching the verification from the inside out, i.e. as designers of a system one tends to over-verify because the designers knowledge of the system exceeds that of the crew. For a complete, but not over-complete, verification the basis of the tests should be the item which first triggers the attention of an operator. In the ERA case this is the Event message, like "Path deviation exceeds limits", which points directly to a unique procedure (see section 2). The verification philosophy is to find per test a failure which will generate a particular Event

message (Fig. 7). The same Event can have multiple corresponding recovery actions. Multiple failures must be considered which cover the paths to the recovery actions. The combined tests should cover all events, at all levels of severity.
Because the tests are end-to-end and involve feedback from the operator, it is also necessary to design a verification environment which allows successful execution of the recovery from the failure (the failure must disappear when the correct recovery action is taken).
Note that it is a practical impossibility to verify that the operational procedures will give the correct recovery action to each and any failure in the system. There might even be a failure, for which the diagnosis procedures does not yield the correct recovery. In such inconclusive situations ground has to be contacted. However, given the limited number of recovery actions, one can allow that in actual operations, aimed at a short term solution, Ground decides that "If recovery action A fails to solve matters then resort to recovery action B".
The verification of the procedures cannot be automated, because the verification does not only cover the correctness of the procedure themselves, but also how they are perceived and used by the crew member. Thus, these types of verification are very time-consuming and labor-intensive. These tests must be carried out when the rest of the system verification is complete, i.e. when the autonomous part of the system is known to be correct and the design is stable.
The verification of the procedures will primarily be done using the simulator in the MPTE (Couwenberg et a. 1998). Where procedures involve the need for interaction with the actual flight Hardware, tests will also be done on the flight arm in a dedicated flat-floor test facility (where movements are limited to 2-D) at Fokker Space. As the verification of the procedures do not include mission preparation, input to the tests are already validated missions. The duration of a typical mission is several hours.
Because actual astronaut time is very valuable, they will be involved as test subjects only at the latest stage. Most of the tests will be done by engineers which have sufficient background knowledge on the operation of ERA, but not so much that they will execute operations without following the procedures.

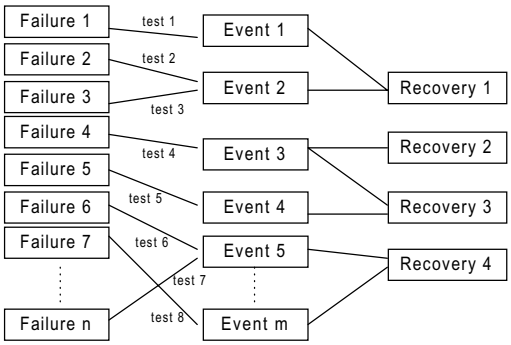

Fig. 7a Verification philosophy: incorrect approach

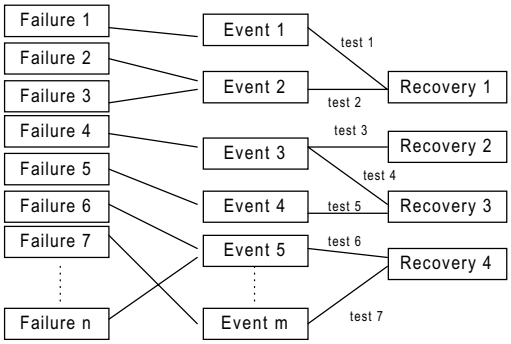

Fig. 7b Verification philosophy: correct approach

5 Conclusions

Due to the limitations in space, the aim of the ERA Operational Malfunction Procedures is to home in on the correct recovery action after the occurrence of a failure, not to diagnose the origin of the failure in detail. It is indispensable to be able to achieve a safe situation or even to allow continuing of an operation, the "why" of the failure is of secondary importance, and can be determined off line (by the ground segment). The procedures concentrate on the immediate tell-tales (symptoms) visible to the on-board operator. Verification of the procedures follow the same approach. From a view-point of the possible failure cases of ERA, verification can never be complete because of the sheer number. Verification is aimed at testing all possible messages to the operator, and their recovery actions. Because of the human element, verification is labor intensive.

References

Beerthuizen P.G. et. al 1998, ERA safety strategy, proc. DASIA '98 Conf. on Data Systems in Aerospace, Athens, Greece, 25-28 May 1998, (SP-422), pp. 321-326

Bos J.F.T. &. Oort M.J.A 1997, Failure Detection Isolation and Recovery concept for the European Robotic Arm, Proc. Int. Conf. on Safety and Reliability ESREL '97, June 17-20, 1997, Lisbon, Portugal, NLR TP-97155

Couwenberg M.J.H. et al. 1998, The ERA Simulation Facility for the European Robotic Arm programme, *Proc. Simulation technology: science and art. 10th Eur. simulation symp. and exhibition ESS'98*, pp.676-678

Hofkamp et. al 1998, ERA test results, *5th ESA workshop on Advanced Space Technologies for Robotics and Automation, ASTRA'98*, ESTEC, Noordwijk, Netherlands, 1-3 December

Kampen et. al 1995, The European Robotic Arm and its role as part of the Russian segment of the International Space Station Alpha, *paper IAF-95-T.3.03*

Pronk Z., Schoonmade M. & Baig W. 1999, Mission preparation and training facility for the European Robotic Arm (ERA), *Proc. 5th int. symp. on AI, robotics and automation in space*, 1-3 june, 1999, (ESA SP-440), pp. 501-506, NLR TP-99248

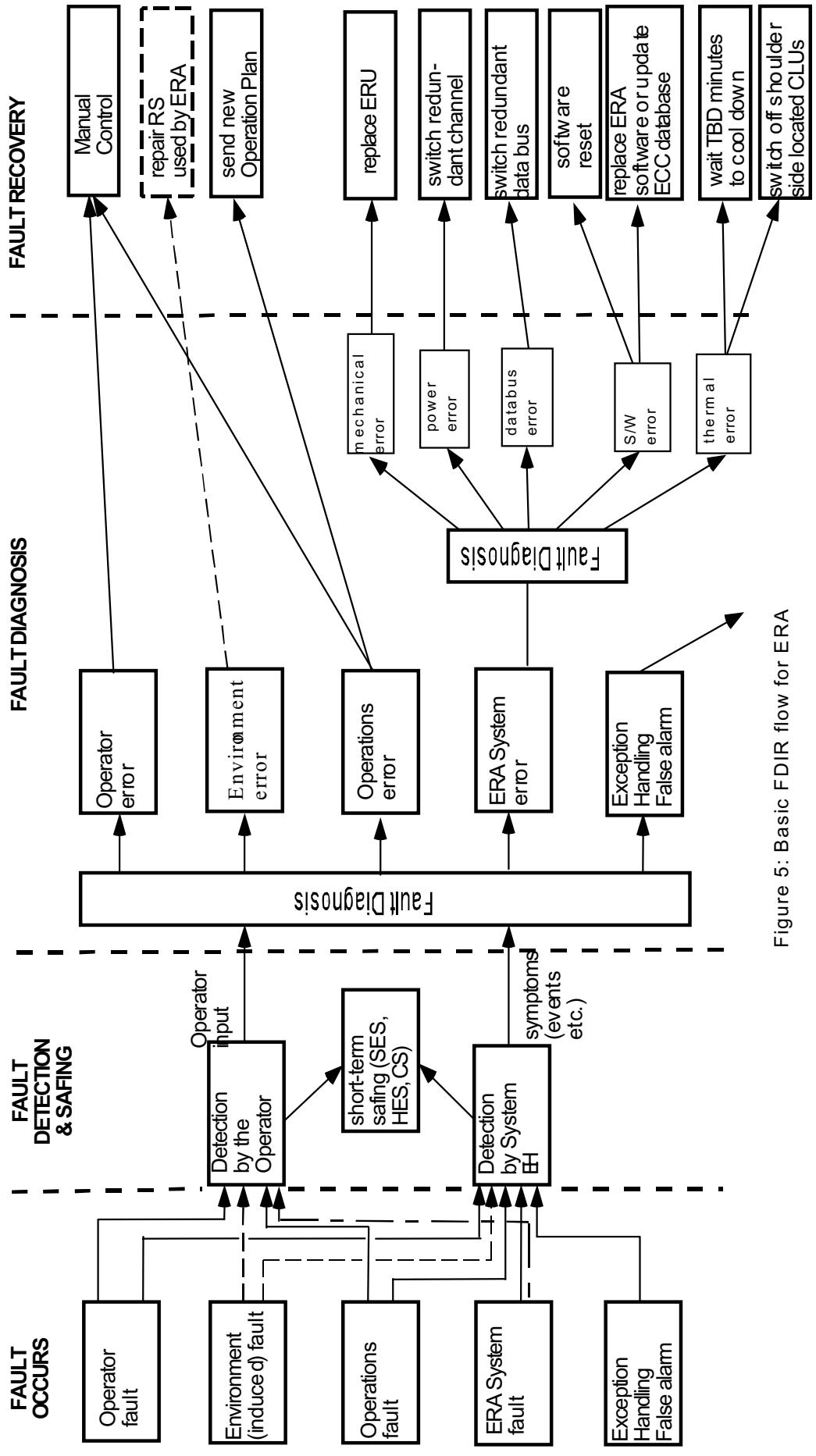

Figure 5: Basic FDIR flow for ERA