Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR TP 97155

Failure detection, isolation and recovery system concept for the European robotic arm

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

DOCUMENT CONTROL SHEET

	ORIGINATOR'S REF. **NLR TP 97155 U**		SECURITY CLASS. **Unclassified**

ORIGINATOR
National Aerospace Laboratory NLR, Amsterdam, The Netherlands

TITLE
Failure detection, isolation and recovery system concept for the European robotic arm

PRESENTED AT
the International Conference on Safety and Reliability ESREL'97, Lisbon, Portugal, June 17-20, 1997

AUTHORS **J.F.T. Bos and M.J.A. Oort**	DATE **970317**	pp **11**	ref **9**

DESCRIPTORS
Automatic control
Autonomy
Design analysis
Diagnosis
European space programs
Fault detection
Man machine systems
Real time operation
Recovery
Robot arms
Space stations

ABSTRACT
Currently Fokker Space B.V. is developing the European Robotic Arm (ERA) under contract of the European Space Angency (ESA). ERA's main mission is the assembly and servicing of the Russian Segment of the International Space Station Alpha. The purpose of this paper is to describe how the safety requirements, given the specific possibilities and limitations of a space robotic system, has resulted in the design of the Failure Detection, Isolation and Recovery (FDIR) system of ERA. One example is used throughout the paper to illustrate the concept.

Failure Detection, Isolation and Recovery system concept for the European Robotic Arm

J.F.T. Bos[1], M.J.A. Oort[2]

[1]National Aerospace Laboratory NLR,
P.O. Box 90502, 1006 BM Amsterdam, The Netherlands,
E-mail: jftbos@nlr.nl
[2]Fokker Space B.V.,
P.O. Box 32070, 2303 DB Leiden, The Netherlands,
E-mail: M.Oort@fokkerspace.nl

ABSTRACT

Currently Fokker Space B.V. is developing the European Robotic Arm (ERA) under contract of the European Space Agency (ESA). ERA's main mission is the assembly and servicing of the Russian Segment of the International Space Station Alpha. The purpose of this paper is to describe how the safety requirements, given the specific possibilities and limitations of a space robotic system, has resulted in the design of the Failure Detection, Isolation and Recovery (FDIR) system of ERA. One example is used throughout the paper to illustrate the concept.

KEYWORDS: space, robot, failure, detection, diagnosis, recovery

INTRODUCTION

Currently Fokker Space B.V. is developing the European Robotic Arm (ERA) under contract of the European Space Agency (ESA). ERA's main mission is the assembly and servicing of the Russian Segment of the International Space Station Alpha. 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 [Kampen *et al* (1996)]. It can transport large objects (such as solar arrays) to a maximum of 8000 kg during the Russian Segment Assembly Phase, and exchange Orbit Replaceable Units (ORUs) as well as inspect the Russian Segment during the Operational Phase of the station. The ERA system, which has a flight segment and a ground segment, will be controllable 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. It is scheduled to be launched in February 1999.

ERA consists of several sub-systems (S/S), as is illustrated in Fig. 1. ERA consists of limbs, joints, camera's, end-effectors and a (main) computer, the ERA Control Computer (ECC).

Part of ERA is the Failure Detection Isolation and Recovery (FDIR) system. Under contract of Fokker Space B.V. the National Aerospace Laboratory NLR provides a major contribution to the design of the FDIR system.

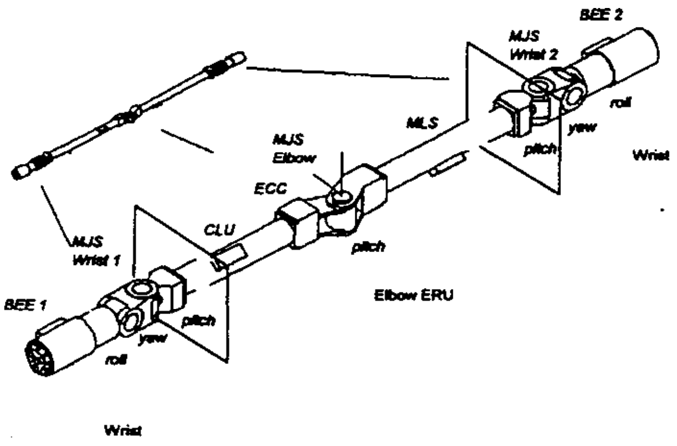

Figure 1 (The ERA manipulator)

The purpose of this paper is to describe how the safety requirements, given the specific possibilities and limitations of a space robotic system, has resulted in the design of the Failure Detection, Isolation and Recovery (FDIR) system of ERA.

The outline of the paper is as follows. Firstly the general design approach is stated, and then the elements of the FDIR system are described in more detail. One example is used throughout the paper, and the example is marked by a border surrounding it.

DESIGN APPROACH

The space environment imposes stringent requirements for the design of ERA with respect to safety (2 fail-safe, fail-operational), robustness (use proven technology), and flexibility (override autonomous functions).

ERA is required to retain all of its functions after a single failure (one fail-operational), and to remain safe after two failures. For every critical hardware or software failure, there are at least two automatic, independent detection mechanism that would stop the arm.

A failure can easily lead to a threat to human life. Without safety precautions, the arm may hit a cosmonaut during Extra Vehicular Activities (EVA), or the failure may cause such damage that the cosmonauts life is indirectly in danger. The stringent safety requirements lead to the design principle to safe the ERA after each detected failure, without autonomous verification of the justifiability of the alarm. False alarms also lead to safing. This is a valid approach, because ERA is not an autonomous system, so operation can easily be resumed. In addition, protecting human life is more important than operational interrupts. (Of course the false alarm rate must be kept as low as possible.)

A second design principle is a distributed detection and safing responsibility, shared between the ERA Control Computer (ECC) and the ERA Sub-Systems (S/S). If the S/S detects a failure, the S/S performs local safing (de-activates itself), and the failure is reported to the ECC. The latter takes care of the system level safing.

Another design principle to keep the design simple (increased robustness) is that the responsibility for diagnosis and recovery lies with the space/ground operators. Apart from robustness issues, the space environment puts severe limitations on the computing power, which puts clear constraints on the allowed complexity and frequencies of the FDIR system.

For robustness, preferably proven technology should be used. Since ERA is a completely new product, a lot of new technology is introduced for ERA as a whole. With respect to the FDIR system use was made of some proven concepts which were applied to ISO [Beerthuizen, Oort (1994)].

Flexibility requires that autonomous functions must be overridable by the operator. Therefore, in principle, each check and safing action can be disabled/enabled.

In Fig. 2 the global FDIR concept which is part of the ECC is shown.

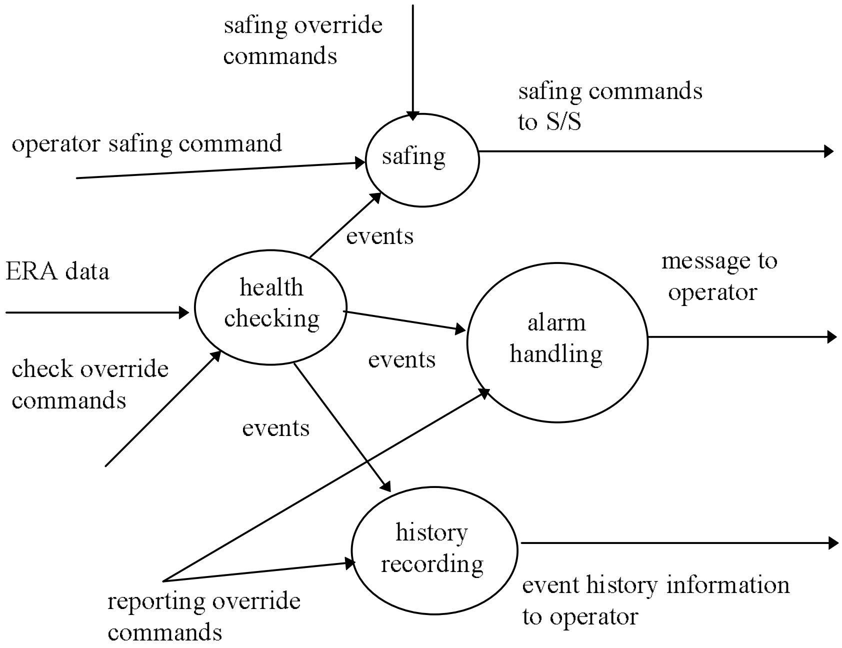

Figure 2 (Global FDIR concept which is part of the ECC)

The thermal aspects, weightless and vacuum conditions in space are quite challenging, and cosmic radiation is a complicating factor. Although, these space environmental factors had a major impact on the ERA design as a whole, the FDIR design was influenced only to a small extent. The most significant impact was that the EVA operator could have no role in the diagnosis, since the EVA operator has to wear a space suit and the EVA Man-Machine Interface (MMI) needed to be “space-proof”. Both limited the display and control possibilities on the MMI.
In addition, the possibilities for repair are very limited in space. This had an impact on the recovery possibilities (redundant chains etc.).

DETECTION

In general the detection means, i.e. the checks, are required to have two detection levels: caution and danger. In case of a caution situation the operator is informed that there might be an incipient failure, but no further automatic action is taken. In case of exceeding a danger level, immediate automatic safing is initiated.

One of the main hazards is uncontrolled motion, for instance caused by a fault in the elbow joint. The detection means are distributed over the joint and the ECC. In the joint a very fast detection (300 Hz) is based on the motor current sensing. Its role is to detect fast evolving failures. In addition, it limits the maximum accelerations possible after a failure. Slower (20 Hz), but more sensitive detection means in the joint are the velocity tracking error check and the joint angle tracking error check. These checks have to be simple because of the limited computing power in the joint. The checks are of the limit checking type. The detection thresholds are adjustable, and their values depend on the payload attached to the ERA.

In the ECC the so called Path Deviation check determines whether the Point-Of-Resolution, i.e. mostly the tip of the End-Effector, follows the prescribed *Cartesian* path (both position and orientation) within certain accuracy bounds. When the arm is operating near structures, which is the most safety critical situation with respect to tracking errors, the Cartesian errors use the positioning measurements generated using the camera image, which is independent of the joint angle measurements. The control mode where camera information is used to correct the ERA movements is called proximity control.
The Path Deviation check is the most sensitive check, and it runs on a low frequency (2 Hz). As for the checks located in the joints, the parameters are adjustable. Their values depend on the type of motion (open-loop control, proximity control etc.), and of the payload mass.
Note that the minimum detection times (and maximum) depend on both the frequency with which a check is executed and the accuracy of the information it uses. The assessment is that all four detection means (current, velocity, joint angle, and Path Deviation check) are necessary to obtain a two fail-safe system for all failure cases.

As an example consider the failure case where the velocity sensor of a joint is stuck. Given the joint control structure, a stuck velocity sensor will cause an increasing joint velocity tracking error, resulting in increasing joint accelerations, and thus a joint runaway. If the accelerations become too large (in a short time) the current check will trigger. Also the joint velocity tracking error check will trigger.
The ERA movement at Cartesian level can be such that an almost constant joint velocity is required. Then the failure will propagate slowly. Despite the fact that the Path deviation check runs on the lowest frequency it will trigger first, because at Cartesian level the allowed deviations are most strict.

SAFING

ERA is in a *safe status* when its status does not constitute a potential hazard to Space Station, his crew and operations. Depending on the failure, the ECC must initiate a safing action. Two safing action to be initiated by the ECC exist:

1. the Soft Emergency Stop (SES)
2. the Controlled Stop.

Basically, the SES makes that ERA is put into a safe status, as defined above. It applies the brakes on the joints, and disables the power to all units which make motion or other potential dangerous things possible.
If the SES is not completed in time (determined by the SES check) a Hard Emergency Stop (HES) request is send to both the Russian Central Post Computer (CPC) and the MMI, resulting in cutting the ERA power. By sending the request to the MMI, the operator will see that he has to press the Hard Emergency Stop (HES) button. If the CPC receives a HES request, the CPC cuts the power.

A Controlled Stop is intended for those kinds of failures that allow a nice smooth stop of ERA, to prevent all kinds of re-initialisation that are necessary after/during a SES. The ERA is not commanded in a safe state as defined in the previous section. The controlled stop is always followed by a transition to Controlled Hold. Operation can be restarted in an easy way.
In principle a Controlled Stop may only be used to cover failures with have at most Major consequences.
The Controlled Stop is performed to prevent deleterious effects due to singularities. A SES is not appropriate in this case, because just because of the uncontrolled movement due to the SES, a singularity may occur.

It must be noted that applying a SES does not mean automatically that ERA will be in a safe status. For instance, after a SES the arm might block an airlock, prohibiting that a cosmonaut can be brought into safety. For these kind of situations manual override of the joints exists.

Assume a fault in the elbow joint, which is detected by the joint angle tracking error check in the joint itself (see previous section). Local (in the joint itself) safing is performed automatically, by cutting the motor power and applying the brakes. The joint reports the failure to the ECC, which in its turn initiates a SES. The result is that all joint movements are stopped as fast as possible by cutting the motor power and applying the brakes.

In the example described in the previous section the failure detection could be done by a check located in the joint itself, or at system level, i.e. by a check located in the ECC. In the first case, the joint de-activates itself by cutting the motor power and applying the brakes. The failure is reported to the ECC, and the ECC commands a SES, which de-activates all other joints to stop the ERA motion.
In the second case the ECC directly initiates a SES.

REPORTING

Error reporting is also driven by considerations particular to the limitations induced by the space environment. As indicated above, the ERA Exception Handling Design is such that there is an autonomous response to a failure detection, without the need for intervention by an operator. In view of the operator's limited capabilities for diagnosis and recovery (especially while conducting EVA), error reporting has been designed to follow these rules:

- The operator should be informed of a detected failure only in high-level terms, i.e. the severity of the failure, and an indication of the check which detected the failure.
- Information on the severity of the failure must be distinguishable even in the most adverse conditions, i.e. while the operator is in a space suit, without the capability to constantly look at the screen of the MMI. Thus, both visual and audible signals must be given. Also, a failure detection report must remain visible/audible until the problem has been solved, or the operator has disabled the checks.
- Complete information on the reason for triggering of the check (including the input data which lead to the triggering) must be retained (time-tagged) inside the control computer for downloading and analysis by the Control Center. In ERA this has been implemented by storing all events and event related data in a dedicated circular buffer which can contain at least 100 events. This buffer can be read by means of a dedicated memory dump of the Control Computer

As in many other non-space FDIR systems, the ERA design distinguishes between two levels of severity of a detected anomaly. A Caution condition is used for several purposes. The first is as a warning to the Operator of the detection of an anomaly which may or may not be an indication of an impending failure. An example is a single communication failure, autonomously corrected by a successful retry. The second usage is the warning of the operator of an imminent nominal condition which may be harmful to the operator if not realized, like an imminent laser switch-on. The Operator has the freedom to continue in the spite of the message or to stop and investigate.
The Danger condition signals a failure which could endanger the system if no action is taken immediately. Examples of this are total communications failures or imminent collisions.

The first two bullets already indicate that an operator can be informed of the presence of one exception at a time (the last most critical one). It is therefore necessary to enforce a number of rules on real-time event reporting which allows the operator to be informed of the most critical occurrences. Two of these rules are:

- Danger events have a higher priority than Caution events
  This means that while a "danger" condition is still in force, the reported event remains the last occurred Danger event, even though a Caution event may have occurred after the Danger event.
- communication failures (danger) have priority over all other events.
  If the communication is not reliable the operator must know this, because it may be the cause for the occurrence of a lot of other caution/danger events.

In the example above in the case the ECC detects the failure, the Path Deviation Check has a Caution limit of XXX mm and a Danger Limit of YYY mm. The values XXX and YYY depend on the actual control mode. If the Caution limit is exceeded the Operator is merely warned by means of a Caution message "Path Deviation Check out of range [Caution]". If the Operator continues and Danger limit is exceeded, a Danger message "Path Deviation Check out of range [Danger]" is displayed on the MMI, and the ECC takes autonomous action. Caution and Danger events have different colors on the MMI display and/or are accompanied by a flashing signal.

DIAGNOSIS AND RECOVERY

Diagnosis and recovery are coupled, because diagnosis needs to be done to that level that the appropriate recovery action can be selected.

The ERA design is based on the premises that the only party capable of properly diagnosing a failure and defining a recovery action is the Mission Control Center. The Operator in space can, by means of manual overrides, temporarily implement a work-around solution to complete a critical operation (e.g. use a backup MMI if the main MMI fails), but even there he is severely limited.

Because not all contingencies can (naturally) be foreseen, the bulk of standard telemetry data consists of raw data from sub-systems, which are not used during nominal operations, but allow performance analysis on ground in the event of a failure. It also allows trend analysis to detect degradation before it becomes dangerous. This information, together with the events generated at the detection of an error, has in past space projects been shown to be sufficient for diagnosis of all but the most subtle failures [Beerthuizen, Oort (1994)].

Recovery in ERA is, again, limited. There are only five possible scenarios:

- 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)
- Resort to the redundant databus for a particular S/S
- Resort to the redundant power-bus, to which the redundant unit of all ERA sub-systems are connected
- Replace the failing sub-system by a spare available in the station (e.g. a new Wrist assembly).

The ERA Flight Operations Manual will contain the procedures to home in on the underlying failure which triggered health checks, and will give the recommended recovery action. The ground segment in the end is responsible for defining the procedures to implement the proposed recovery action, and to define the actions necessary to restart operations. The operators role in all this is relatively passive.

In the example above the first action would be to dump the Event buffer. In the case where the joint has not reported an error itself, the origin of the failure must first be determined down to sub-system level. The possible culprits are the ECC and the joint. By replaying the critical part of the mission on ground and comparing the actual output of the sensors in the ERA telemetry with the expected ones, the failing sub-system can be identified. Examination of the sub-system FMECA database will lead to isolation of the error to the velocity sensor. By using a database for the FMECA, it can be used fro top-down failure identification. The recovery in this case would be to resort to the redundant power bus, to which the on-line redundant unit is connected. If the failure propagates within the sub-system, the joint assembly can be replaced as a whole.

CONCLUSIONS AND FUTURE WORK

The FDIR concept is mainly based on analysis to assess its performance. Currently, the ERA design is in a stage where models become available which allow a more accurate “as-designed” assessment of the performance. During the design of the ERA system, also the FDIR concept evolves due to changing S/S design, new insights, and compromises have to be made due to new restrictions.

The decision not to centralize failure detection, but give the sub-systems themselves a certain amount of responsibility for detecting failures has the inherent danger that certain failures will have too many barriers, and some too few (because each party thinks the other has implemented a protection). A strict shadowing by the Prime Contractor is essential to minimize these dangers.

An advantage of decentralized failure detection over having “one” overall check which covers the complete functional path from operator command to ERA response, is that more detailed diagnosis is possible.

The ERA exception handling design is special, because the role of the space located operators (cosmonauts) has been reduced significally. The ERA itself brings the arm into a safe state, and the ground segment diagnoses and corrects the error. Given the special conditions imposed by the space environment, this is the only logical choice. However, it limits the autonomy of the cosmonaut.

The safety requirements currently imposed by ESA are independent on the probability of a failure. For instance, it is stated that “No single ERA failure shall lead to Catastrophic, Serious or Major consequences” [Bentall *et al* (1995)]. The current safety requirements account only for the consequences of a failure. Although a failure having Major consequences can be very unlikely, either preventive or reactive measures need to be taken, which can be very costly. One should consider a safety approach based on risk assessment. Risk is defined as the product of the probability that a failure occurs and the consequences of that failure. If a failure is very unlikely why spent a lot of money to cover this failure if its consequences are not “too bad”. In fact, the risk based approach is already in favor of some ESA departments [Preyssl (1996)], where it is claimed that “the classical approach is expensive and rather inefficient in improving the system in a balanced way with respect to safety, reliability, performance and cost. A risk based safety approach is not perfect, for instance it will be difficult to obtain realistic failure probabilities, but worthwhile considering for having a successful project faster, with less cost.

A topic for future FDIR work is “predictive maintenance” [Breeman (1996); Tutar, Breeman (1996)]. Whereas the FDIR system in space focuses on the safety aspects of failures, Ground needs to detect more subtle degradations, find the cause of the degradations to determine *what* maintenance may solve the degradations, and assess *when* performance will degrade to such an extent that maintenance is necessary. In the present design of the Ground system the operator support for predictive maintenance will be very limited, but updates are envisaged [Boumans *et al* (1996)]

REFERENCES

1. Beerthuizen P.G., Oort M.J.A. (1994). Fault tolerance techniques applied in ISO-AOCS, Proc. 2nd ESA Int. Conf. on GNC, ESTEC, Noordwijk, 12-15 April, ESA WPP-071, pp. 269-275
2. Bentall R.H. et al (1995). ERA System Requirements Document, ESA document HS-RQ-ER-0001-ESA
3. Bos, J.F.T. (1996). ERA FDIR Analysis report, NLR report CR95459 L
4. Bosman R.A. (1996). System Hazard Analysis, report HS-AS-ER-004-FSS
5. Boumans R. et al. (1996). ERA: Baseline capabilities and future perspectives, Proc. 4th ESA workshop “ASTRA 96”, 6-7 nov., ESTEC, ESA WPP-122
6. Breeman J.H. (1996), FDIR on the basis of observer schemes, NLR report, to appear
7. Kampen S. 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
8. Preyssl C. (1996). European Space Agency program for risk assessment & management, Proc. Int. Conf. on probabilistic safety assessment and management, Crete, Greece, June 24-28, pp. 2030-2035
9. Tutar L., Breeman J.H. (1996), FDIR on the basis of parameter identification using subspace methods, NLR report, to appear