Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-98168

Control of the joint runaway hazard for the European Robotic Arm

J.F.T. Bos and R.A. Bosman

Nationaal Lucht- en Ruimtevaartlaboratorium

National Aerospace Laboratory NLR

NLR-TP-98168

Control of the joint runaway hazard for the European Robotic Arm

J.F.T. Bos and R.A. Bosman*

* *Fokker Space*

This report is based on a presentation to be held on the International Conference on Safety and Reliability ESREL ’98, Trondheim, Norway, June 16 - 19, 1998.

Division: Informatics
Issued: March 1998
Classification of title: unclassified

Control of the joint runaway hazard for the European Robotic Arm

R.A. Bosman
Fokker Space B.V., Leiden, the Netherlands; P.O. Box 32070, 2303 DB Leiden, the Netherlands, E-mail r.bosman@fokkerspace.nl

J.F.T. Bos
National Aerospace Laboratory NLR, Amsterdam, the Netherlands; P.O. Box 90502, 1006 BM Amsterdam, the Netherlands, E-mail jftbos@nlr.nl

ABSTRACT: Currently Fokker Space is developing the European Robotic Arm under contract of the European Space Agency. Its main mission is the assembly and servicing of the Russian segment of the international space station Alpha. One of the main hazards of ERA is that after a failure the arm could start to move in an uncontrolled way. An unintended motion of ERA could lead to damage of the space station, or loss of a cosmonaut who is operating the ERA.

The purpose of this paper is to describe how the safety requirements, given the specific possibilities and limitations of a space robotic system, have resulted in design and operational constraints to control the joint runaway hazard. Simulation results are presented to illustrate the safety efficiency.

1 INTRODUCTION

Fokker Space 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. ERA will be launched in the year 2000. 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 (Fig 1), 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 from a portable console by extra vehicular activities (EVA) crew members, or remotely from a laptop type work station by the crew members inside the modules of the russian segment.

ERA consists of several sub-systems (S/S), as is illustrated in Figure 2. ERA consists of limbs, joints, camera's, basic end-effectors (BEE) and the (main) computer, the ERA control computer (ECC).

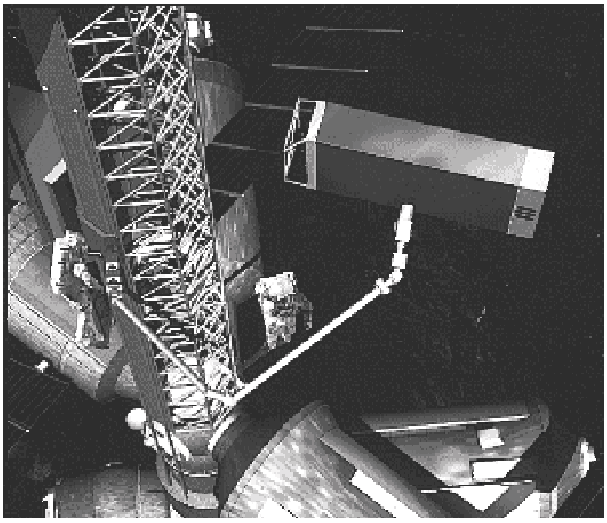

Figure 1. Two cosmonauts on the international space station Alpha use ERA to transport a folded solar array package.

Part of ERA is the failure detection, isolation and recovery (FDIR) system (Bos & Oort 1997). Under contract of Fokker Space the National Aerospace Laboratory NLR provides a major contribution to the design of the FDIR system.

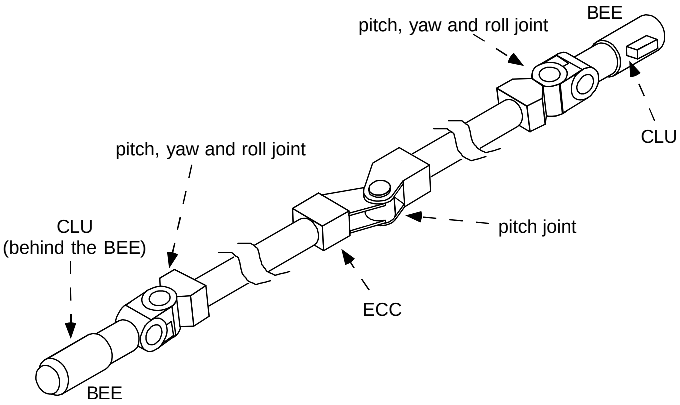

Figure 2. The ERA manipulator

The purpose of this paper is to describe how the safety requirements, given the specific possibilities and limitations of a space robotic system, have resulted in a design, controlling one of ERA's main hazards, the joint runaway hazard. A joint runaway might lead to catastrophic consequences, such as loss of life when ERA would hit the cosmonaut, or damage of the space station.

The outline of the paper is as follows. At first the driving safety requirements are provided, and various aspects of the hazard discussed. This is followed by a description of the design- and operational safety controls. Finally the achieved level of safety is discussed, illustrated by simulation results.

2 DESIGN DRIVING REQUIREMENTS

The following requirements (Bentall et al. 1995) from the customer are driving the design:

- No single failure shall lead to loss of life or serious damage;
- No second ERA failure independent from the first shall lead to loss of life or serious damage.

The requirement to be safe after a second failure is implemented as follows: after failure of one check, at least one other check shall be active to ensure timely and adequate prevention of a catastrophic consequence.

3 JOINT UNCONTROLLED MOTION

When ERA is moving, the ECC generates position setpoints for all active joints at a rate of 20 Hz. The setpoints are calculated from the mission plan (which contains the motion trajectories), or from the direct motion commands given by the operator. The setpoints are sent to the joints via the redundant 1553B databus.

The joint position control on the Joint I/O microprocessor receives the 20 Hz setpoints from the ECC and extrapolates each last received value to generate setpoints for the joint velocity control loop. The joint velocity control runs on the joint control microprocessor with a frequency of 300 Hz (Fig. 3).

Uncontrolled motion is the event when a failure or otherwise initiates the ERA to deviate from the planned trajectory, for instance one joint stops while the others continue. When acceleration occurs due to a failure this is called *joint runaway*, which is the subject of this paper.

The most critical situation for joint runaway is when the ERA approaches an ERA standard grapple fixture (SGF) to grapple an ORU, or an ERA basepoint (BP). During *proximity motion* (closed loop control via the camera) and *compliant* (contact) *motion* the arm moves close to the space station in the order of centimeters, or is in contact with the SGF / BP respectively. In these situations a collision after a joint runaway cannot be averted. When ERA moves in free space this is called *free motion*.

The hazard is characterized by two parameters: the maximum kinetic and potential energy after failure, and the stopping distance after failure. The *stopping distance* is defined as the maximum travel of the arm tip, measured from the moment of failure occurrence to the moment of stationary standstill.

3.1 *Examples of the joint runaway initiators*

- The ECC could make errors in the calculation of the joint position setpoints from the mission plan.
- The joint control electronics (JCE), using position- and velocity sensor data, calculates the required motor torque. A failure in the sensors, the control hardware, or the control software may send wrong torque settings to the motor drive electronics resulting in path deviation, excessive torque or excessive acceleration of ERA.
- A single event upset (SEU) in the ECC or one of the joints.

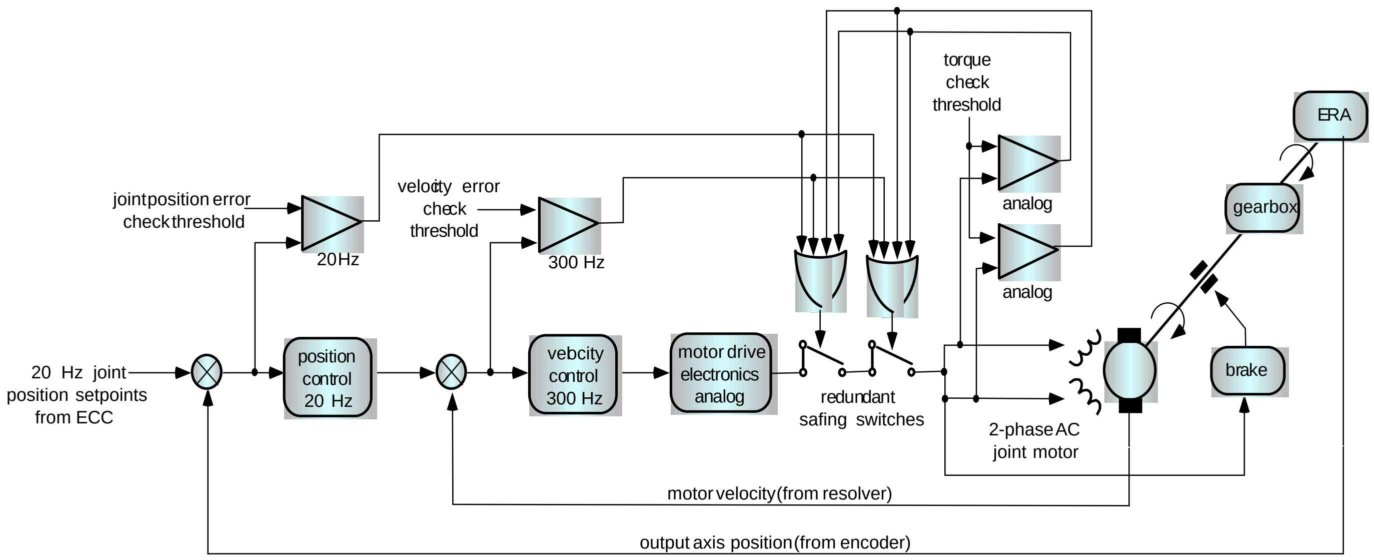

Figure 3. Joint control, safety checks and joint safing.

In order to ensure that the hazard is controlled to an acceptable level, an iterative approach has been followed of alternating analysis and design improvements. Among the analyses which were carried out are: failure mode effects and criticality analysis (FMECA), system hazard analysis, common mode / common cause analysis, human error analysis, fault tree analysis, failure detection-, isolation and recovery analysis, and warning time analysis.

4 SAFETY DESIGN APPROACH

The joint runaway hazard cannot be eliminated from the design, because the hardware and software functions that have to convert the mission plan trajectories to joint motion can not be removed, and hence for any selected design will be sensitive to failures. When hazard elimination is not possible, the hazard must be controlled.

4.1 *ECC checks*

In the ECC the path deviation check determines whether the tip of the arm follows the prescribed Cartesian path within the accuracy bounds (position and orientation). The accuracy bounds are adjustable. The arm tip position and orientation is calculated applying forward kinematic algorithms to the joint position sensor data.

During proximity motion the Cartesian errors are computed from the processed camera image of an optical target. In this way higher position accuracy is obtained because the calculation is independent of the misalignments, (thermal) deformations and bending in the robot arm.

The path deviation check is the most sensitive check for low-acceleration failures, and runs on a low frequency (2 Hz).

In case of compliant motion the torque-force levels measured by the torque-force sensor in the BEE are monitored as well.

4.2 *Joint Fail-Safe Design and Checks*

The motor drive hardware design is unsensitive to motor runaway: the two-phase AC motor is driven by a FET-bridge. An electrical short or open circuit in the motor drive electronics would bring the bridge in unbalance upon which the motor stops.

This appears to be safe but it is not: the other moving joints have to be stopped, because the ERA will leave the planned trajectory. Stopping of the other joints is both ensured by a watchdog protocol, and by the subsystem that reports detected failures to the ECC. However since acceleration is not present this is a slow effect and is not of primary concern.

The joint checks have to be simple because of the limited computing power in the joint. All joint detection thresholds are adjustable.

To control the hazard, in each joint there is a torque check (Fig. 3), one on each phase of the AC motor. Its role is to detect failures which result in a high (650 Nm at maximum) motor torque. These are the most hazardous. The torque check redundantly measures the motor current and via a comparator, without intervention of software, it switches off the motor current upon exceedence of the torque check threshold. The current switchoff is performed by circuit breakers. The brakes engage autonomously upon loss of current.

The torque check is entirely independent of software and control failures, but it does not detect failures like wrong position or velocity. It is the primary safety barrier against the common mode failure of joint velocity control and velocity tracking error check, which may inject high motor torques in the joint. It is hot redundant in order to provide two-failure tolerance.

The velocity tracking error check is the fastest check in the joint software, both for its frequency (300 Hz) and since the monitored velocity originates from the motor side of the gearbox.

Failure of the joint velocity control microprocessor (for instance the clock freezes or the software gets stuck in an infinite loop) could both lead to joint runaway and disable the joint velocity tracking error check. For this failure an internal watchdog ensures that the joint is brought to safe status.

The joint position tracking error check runs at 20 Hz. It is the slowest joint check because of the hysteresis effects and flexibility in the gearbox. However, it is the primary barrier to protect against an inadvertent position step in the ECC position setpoints. Also it is the only joint check which will notice a static velocity error or position drift.

Loss of the joint position control microprocessor also disables the position tracking error check, but again the joint internal watchdog will ensure all motion is stopped.

4.3 *Operational measures*

Depending on the operational situation different safety constraints exist. During free motion, ERA moves relatively far away from the space station, with relatively high speed. To limit possible collision impact energy, the maximum allowed coasting speed depends on presence and inertia of a carried ORU. The maximum speed is calculated to restrict the possible kinetic energy to less than 4.0 Joule after two ERA failures. In addition, the stopping distance after two failures shall be smaller than 40 cm.

Also the cosmonauts shall keep a safety distance of more than 80 cm to all ERA moving parts.

ERA approaches the space station in proximity motion, where the cameras image is used for more accurate closed loop control. Grappling payloads is performed under compliant motion, where the Torque/Force sensor is used to prevent force build-up.

To constrain possible impact and build-up of potential energy due to motor runaway in proximity- and compliant move, the maximum speed is calculated to limit the maximum kinetic energy to 0.5 Joule maximum after two ERA failures. The stopping distance after two failures shall be smaller than 15 cm.

5 JOINT RUNAWAY STOPPING DISTANCE

The joint runaway stopping distance consists of six phases (Fig. 4): a) before the runaway the ERA tip is moving nominally; b) when the motor runaway occurs the joint starts to accelerate; c) the runaway is detected, but the acceleration continues until joint safing is executed; d) first the failed joint cuts the motor current and the acceleration ceases while the other ERA joints continue to move; e) after mechanical latency the brake engages and the runaway joint decellerates; f) The ECC has received the signal that the joint is unhealthy and brings the other joints to an emergency stop; g) the ERA comes to stationary stand-still.

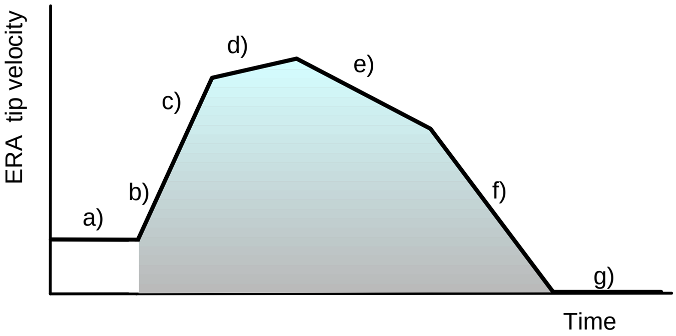

Figure 4. Phases in Joint Runaway Safing. The shaded surface represents the stopping distance.

From Figure 4 it becomes visible that an important safety risk of the joint runaway is vested in the acceleration part. Large stopping distances would result when a high acceleration is detected and safed too late. For this reason and to be independent of software, the torque check was implemented entirely in hardware. Also to prevent safing latency it was decided that the joint safing should be as much as possible independent of the ECC, and therefore located inside the joints.

The various phases can be modelled to calculate the stopping distance. To allow a first assessment the phases were implemented in a spreadsheet. In Figures 5, 6 the stopping distance is calculated for each of the joint and ECC checks, for the no payload and 3000 kg payload cases respectively. These calculations are excluding the joint gearbox and limb flexibility.

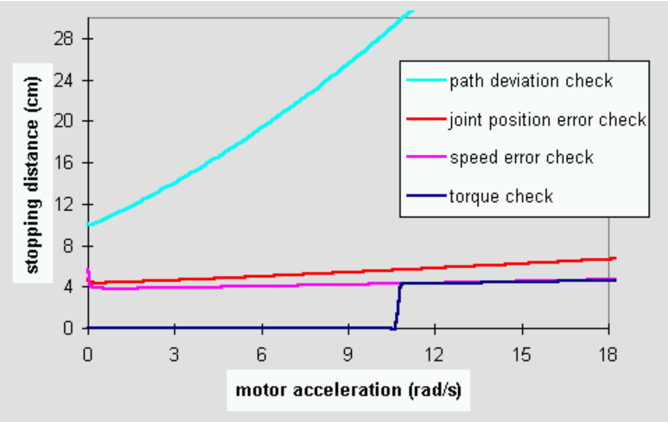

Figure 5: stopping distance per check versus the acceleration caused by the failure while ERA carries no payload and moves with an initial arm tip velocity of 10 cm/s**.**

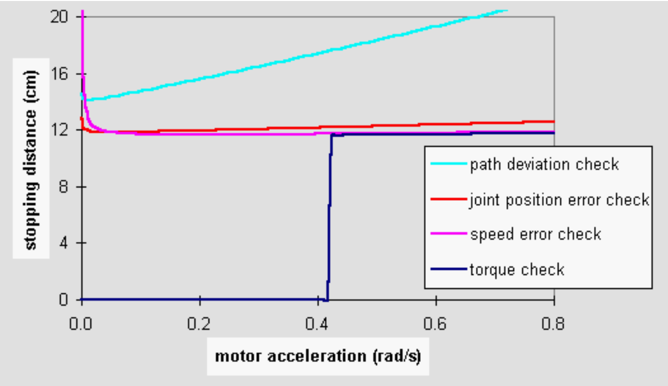

Figure 6: stopping distance per check versus the acceleration caused by the failure while ERA carries a payload of 3000 kg, at initial arm tip velocity of 4 cm/s**.**

6 SIMULATION RESULTS

Below some preliminary simulation data obtained with the ERA Simulation Facility (ESF) are presented. ESF contains detailed dynamic models of ERA and is being used for the ERA flight qualification of threedimensional motion.

For the simulations the following cases were selected: for the shoulder pitch joint and with stretched arm motor runaway could result in high arm tip acceleration because of the approximately 10-meter arm length. An important hazard is the maximum acceleration of the motor. Another important case is a runaway torque just below the torque check threshold: here only the velocity error check and the joint position error check are fast enough to bring the ERA to a safe stop.

Further the effect of transporting a large payload (3000 kg) on the joint runaway stopping distance is simulated, to investigate the larger oscillation amplitude due to higher inertia. As a last case, the stopping distance of a joint runaway on the “hand” side of ERA is simulated to investigate possible acceleration effects of the lower inertia.

All the above simulations were performed at maximum free motion speed and including mechanical and structural flexibility.

To investigate the influence of higher velocities, the shoulder pitch runaway was also simulated for double coasting velocity.

6.1 *Shoulder pitch joint runaway*

From Figure 7 it can be observed that the stopping distance is in the same order of magnitude as in Figure 5, when taking into account the increased stopping distance due to the flexibility.

Figure 8 shows that the stopping distance is a factor of approximately 5 worse than calculated in Figure 5. This is because the gearbox, in response to the acceleration of the input axel from the motor, due to its flexibility first winds up and then accelerates. The position sensor, measuring at the joint output axis, is delayed in its detection due to the wind-up. The torque check and speed error check do not degrade from this effect because they directly measure the current and the motor axis velocity respectively.

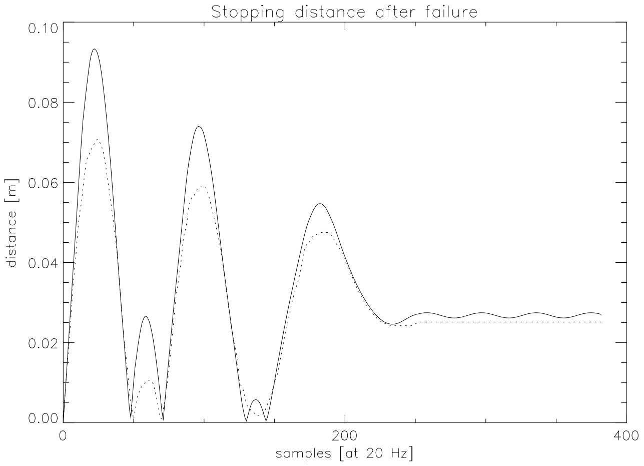

Figure 7: simulated stopping distance of a shoulder pitch joint runaway with maximum failure torque, detected by the torque check. Dotted line: without limb flexibility. Straight line: with limb flexibility.

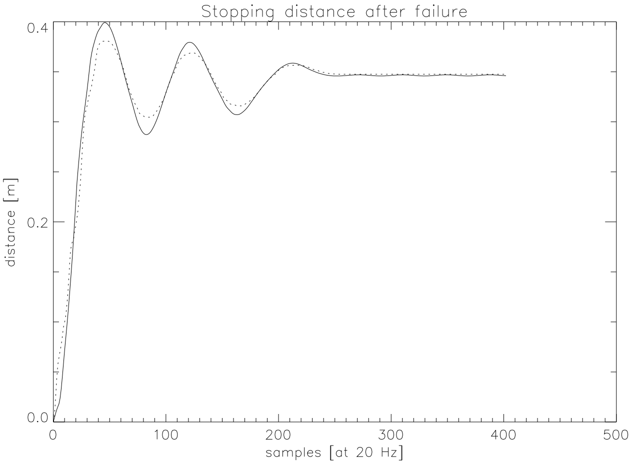

Figure 8: simulated stopping distance of a shoulder pitch joint runaway with maximum failure torque, detected by the joint position error check. Dotted line: without limb flexibility. Straight line: with limb flexibility.

The thus built up potential energy (in all three pitch joint gearboxes) causes oscillations in the ERA tip acceleration, and overshoot after engagement of the brakes. It is expected that this effect is less for other ERA poses because of their lower inertia.

6.*2 Path deviation check*

The gearbox wind-up is expected to be also present in the path deviation check (PDC), which was not simulated yet. From Figures 5 and 6 it appears that the stopping distance of the PDC could grow unacceptably high, caused by the low frequency of the check and the wind-up effect.

In this respect it should be noted that most failures would not lead to acceleration, but to a transient or steady state error where the stopping distance due to joint runaway is not relevant. For these failures the PDC is more sensitive than the joint checks, because the joint can not be adjusted inside the range which is used for nominal control, and because the PDC software is independent from failures inside the joint. The joint checks function as safeguard against joint runaway, the PDC against more subtle steady-state errors.

6.3 *Influence of 3000 kg payload*

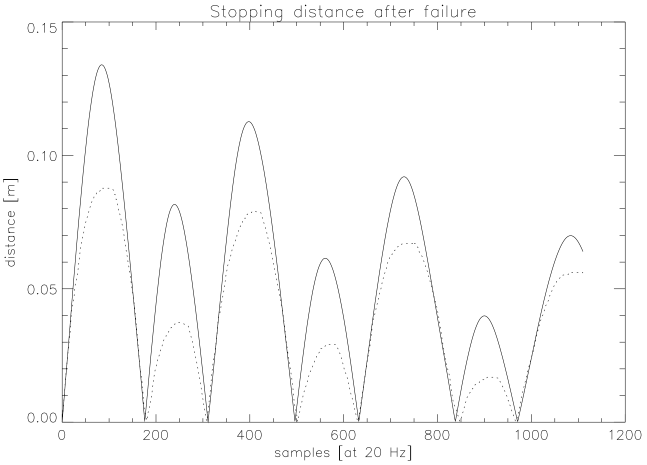

Figure 9: simulated stopping distance of a shoulder pitch joint runaway during transport of a 3000 kg ORU, detected by the torque check. Dotted line: without limb flexibility. Straight line: with limb flexibility.

For the calculated stopping distance in Figure 6, it appears that the presence of 3000 kg on the tip of ERA results in a shorter stopping distance than without a payload. However, Figure 9 shows that the gearbox and limb flexibility wind-up effect increases the stopping distance due to the higher inertia.

6.4 *Hand pitch joint runaway*

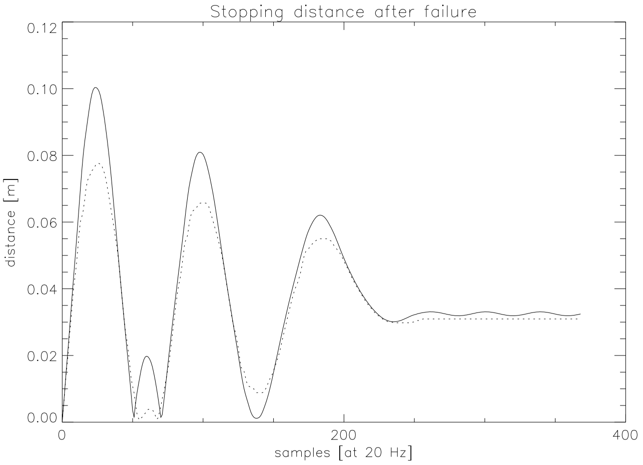

Figure 10: stopping distance simulation of a hand pitch joint runaway, detected by the torque check. Dotted line: without limb flexibility. Straight line: with limb flexibility.

Figure 10 shows that for the hand pitch joint the stopping distance basically is identical to the shoulder pitch joint stopping distance, with the exception of the joint position error check. This is caused by the decreased wind-up effect.

6.5 *Higher coasting speed*

To shorten the mission duration, higher speed could be allowed during free motion. In that case the minimum safe distance of ERA to its surrounding objects has to be adjusted in coherence with the maximum possible stopping distance. Also the cosmonauts minimum safe distance to ERA should be adjusted when necessary.

6.6 *Stopping distances*

From the simulation results the following stopping distances were derived (Table 1). Of the given stopping distances the ones printed in bold indicate the fulfillment of the two-failure tolerance requirement. All rows except the last were performed when ERA was moving at maximum coasting speed of the arm tip.

Table 1: stopping distances for the different joint checks

stopping distance (cm) torque check / speed error check / joint position error check	runaway with max torque	runaway torque is just below torque check threshold (300 Nm)
shoulder pitch no payload tip velocity 10 cm/s	10 / **9** / 40	-- / 8 / **38**
shoulder pitch no payload tip velocity 20 cm/s	17 / **18** / 65	
shoulder pitch payload 3000 kg tip velocity 4 cm/s	14 / **11** / 18	-- / 13 / **40**
hand pitch no payload tip velocity 10 cm/s	10 / **7** / 10	

7 CONCLUSIONS AND FUTURE WORK

From the first simulation results a tentative conclusion can be drawn that the ERA complies with its safety requirements for the joint runaway hazard.

The torque check and velocity error check are effective means to nearly eliminate the acceleration phase effect.

The design results in the initial velocity being the driving parameter for the stopping distance, not motor torque of the joint runaway.

The checks that directly monitor the motor motion or its current detect a joint runaway faster than the checks that monitor the joint output axis, because of flexibility inside the gearbox.

Higher velocity can be allowed for free motion, when the minimum safe distance of ERA to objects and cosmonauts is adjusted as necessary.

When payloads are carried by ERA, the related maximum coasting speed ensures that the stopping distance remains similar as for the unloaded ERA.

A joint runaway in a hand joint instead of a shoulder joint gives a similar stopping distance for the torque check and speed error check, but decreases for the joint position error check and the path deviation check.

The path deviation check in the ECC is a necessary check to detect steady state and transient errors, and because of its independence from the joint.

Further verification and validation will be performed by simulation of joint runaway for other joints and ERA poses, and by testing of single joints and on the ERA zero-G simulation facility.

For ERA, extensions of its capabilities by means of tools are under investigation, as well as application of ERA on target platforms other than the Russian segment of the international space station (Boumans 1996). The platform-independent design of ERA makes it suitable for a scala of applications, like servicing of a panel with scientific instruments that are mounted external to the space station. And so the new millenium could be the beginning of a new ERA.

8 REFERENCES

Bentall R.H. et al. (1995). ERA System Requirements Document, *ESA document HS-RQ-ER-0001-ESA*

Bos, J.F.T. (1996). ERA FDIR Analysis report, *NLR report CR95459 L*

Bos, J.F.T, Oort, M.J.A. (1997). Failure Detection, Isolation and Recovery system concept for the European Robotic Arm, *Proc. Int. Conf. on Safety and Reliability ESREL '97*, Lisbon, Portugal, June

17-20, pp. 2285 - 2292

Bosman R.A. (1996). System Hazard Analysis, *Fokker Space report HS-AS-ER-004-FSS*

Boumans R. et al. (1996). ERA: Baseline capabilities and future perspectives, *Proc. 4th ESA workshop on Advanced Space Technologies for Robotic Applications ASTRA"*, 6-7 Nov 1996, ESTEC, Noordwijk, the Netherlands.

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*

The Control of the Joint Runaway Hazard for the European Robotic Arm on the International Space Station Alpha

R.A. Bosman[1], J.F.T. Bos[2]

[1] Fokker Space B.V.
P.O. Box 32070, 2303 DB Leiden, the Netherlands,
E-mail: r.bosman@fokkerspace.nl
[2] National Aerospace Laboratory NLR
P.O. Box 90502, 1006 BM Amsterdam, the Netherlands,
E-mail: jftbos@nlr.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. One of the main hazards of ERA is that after a failure the arm could start to move in an uncontrolled way, thus threatening the life of the cosmonauts who are operating the ERA. An unintended motion of ERA could lead to damage of the Space Station, or loss of a cosmonaut.

The purpose of this paper is to describe how the safety requirements, given the specific possibilities and limitations of a space robotic system, have resulted in design and operational constraints to control this hazard. Simulation results are presented to illustrate the safety efficiency.

KEYWORDS:
Space, robot, failure, safety, detection, hazard.

Paper to be presented at the International Conference on Safety and Reliability ESREL '98,
16 - 19 June 1998, Trondheim, Norway.