SAFETY APPROACH OF JAPANESE EXPERIMENT MODULE REMOTE MANIPULATOR SYSTEM

Matsueda Tatsuo, Naoki Satoh, Takahisa Satoh, Yasushi Hisadome, Shinobu Doi* / NASDA
Fumihiro Kuwao+ / Toshiba

* National Space Development Agency of Japan, JEM Project Team,
Tsukuba Space Center, 2-1-1 Sengen, Tsukuba-City, Ibaraki, 305-8505JAPAN
Phone: +81-298-54-3934, Fax: +81-298-50-1480, E-mail: doi.shinobu@nasda.go.jp

\+ Toshiba Corporation, Komukai Works
1, Komukai-Toshiba, Saiwai-ku, Kawasaki-City, Kanagawa, 210-8581 JAPAN
Phone: +81-44-548-5125, Fax: +81-44-541-1211

ABSTRACT

The Japanese Experiment Module (JEM) Remote Manipulator System (JEMRMS) is a JEM element and will be used for exchange of Payloads (P/L) and Orbital Replacement Units (ORU).
In general a malfunction of a robotics system or improper operation by Intravehicular Activity (IVA) crew might cause catastrophic hazards for crew members or ISS itself. Very strict H/W and S/W safety design is required to prevent these hazards. Therefore, JEMRMS has many safety-related functions.
This paper summarizes the safety-related design of JEMRMS and the Manipulator Flight Demonstration (MFD) which was conducted as a flight demonstration of JEMRMS prior to JEM launch.

1. INTRODUCTION

JEM is the major Japanese contribution to the International Space Station (ISS) and consists of the Pressurized Module (PM), Experiment Logistics Module - Exposed Section (ELM-PS), Exposed Facility (EF), Experiment Logistics Module–Exposed Section (ELM-ES) and JEMRMS. The EF provides an external experiment environment that is attractive to researchers. The primary mission of JEMRMS is to replace P/Ls and exchange of ORUs on EF and ELM-ES. These tasks are performed by the Main Arm (MA) and the Small Fine Arm (SFA).
A malfunction or improper operation of the robotics system might cause a collision against JEM structures such as PM, or inadvertent release of a P/L or ORU. These hazards are identified as catastrophic hazards because they might result in loss of crew members or ISS. Very strict safety requirements are imposed on the H/W and S/W design to prevent them. The first part of this paper summarizes how these requirements are implemented and verified in JEMRMS design.

In the current concept of JEMRMS design, on-board crew will still be needed to ensure JEMRMS safe operation by monitoring telemetry data and arm movement or sending commands. In the near future, however, the operation from a ground site is expected to reduce crew load and to conserve IVA resources. NASDA has conducted the preliminary Ground Commanding (GC) experiment, a sort of robotics operation from the ground, as a part of the MFD mission aboard the Space Shuttle. The latter part of this paper summarizes the safety concept of MFD mission and introduces unique safety implementation of GC experiment.

2. OVERVIEW OF JEMRMS

JEMRMS consists of the Main Arm (MA), Small Fine Arm (SFA) and RMS Console.
The MA has six degree of freedom and is approximately 10m long. It has an End Effector (EE) and two vision systems, one is installed on the wrist joint and the other on the elbow. The primary mission of the MA, whose base mechanism is fixed on the PM end cone, is to replace large P/Ls (1.85*1*0.8m) and handle JEM elements such as the EF to back up the Space Station RMS. The MA overview is shown in Figure2-1.

The SFA has six degrees of freedom and is approximately 1.5m long. It has the Tool as an End Effector, force torque sensor and a TV camera on the tool. The Tool has three fingers to grapple an ORU by opening fingers and a torque

Proc. Fifth International Symposium on Artificial Intelligence, Robotics and Automation in Space, 1-3 June 1999 (ESA SP-440)

drive mechanism to screw or unscrew bolts. The SFA mission, which is attached to the tip of MA, is to perform dexterous tasks such as ORU replacement. The SFA overview is shown in Figure2-2

The performance of the MA and SFA is shown in Table 2-1.

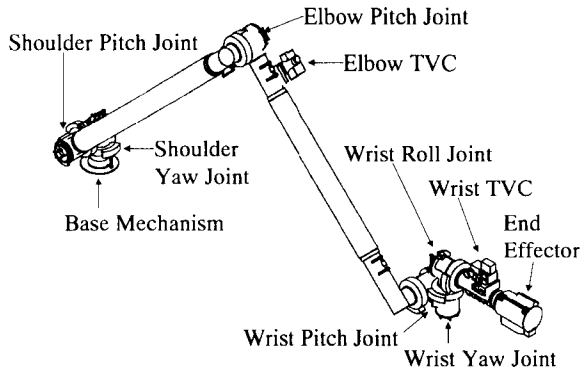

Figure 2-1. Main Arm overview

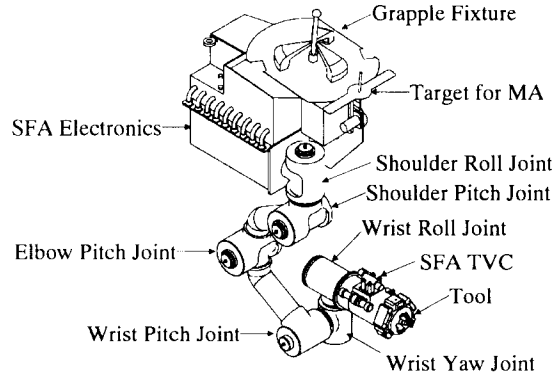

Figure2-2. Small Fine Arm overview

The arms are controlled by two computers in the RMS console. These computers communicate with six Joint Electronics Units (JEU) for MA and SFAE (SFA electronics). One of the computers is the JEMRMS main computer and is called Management Data Processor (MDP). The other computer is the Arm Control Unit (ACU) which controls arm movement while communicating with the JEU and SFAE. These computers have almost the same performance as shown in Table2-2. MDP sends an arm tip position command to the ACU. In manual mode, the ACU generates the Frame of Resolution velocity command in proportion to the voltage input from the Hand Controller by a crewmember. The ACU processes it by resolving inverse kinematics and generates each joint angle and angle rate. The ACU sends the angle commands to the JEU and then six JEUs control the servo of each joint. The ACU sends angle rate commands to SFAE and then SFAE controls the servo of six joints.

Table2-1. Payload Handling Performance of JEMRMS

	MA	SFA
Maximum payload weigh	7000kg	300kg
Maximum payload inertia	20000kgm2	30kgm2
Maximum payload size	4.5m*6m Dia.	0.8m*0.6m Dia.
Maximum c.g.offset	2m	0.3m
Max. Translation Speed	60mm/sec	50mm/sec
Max. Rotation Speed	2.5deg/sec	7.5deg/sec
Position Error	<±50mm	<±10mm
Attitude Error	<±1.0deg	<±1.0deg

Table2-2. Computer performance of JEMRMS

	MDP/ACU
CPU	2CPU(MQ80386)
FPU	2FPU (MQ80387)
Clock	25MHz
Throughput	3.8 MIPS
System ROM	128KB
Main memory	4MB
EDAC	1bit detection/correction per every 8bits

3. JEMRMS SAFETY APPROACH

To ensure safe design, the following steps are taken:

(1) Identify potential hazards in JEMRMS

(2) Identify the control and verification method for each hazard

(3) Verify each control by analysis or test

Figure 3-1 shows the safety-related schematics of JEMRMS to help readers understand the following descriptions.

3.1. HAZARDS

Typical manipulator hazards are the accidental release of objects and collision against other structures.

JEMRMS has the same potential hazards and identifies the following hazards as catastrophic, Severity Ⅰ.

(1) Inadvertent release of objects such as P/L during berthing or unberthing.

(2) Collision against EVA crew or the structures such as the PM.

Collision against EVA crew members is not covered in detail in this section because safety is assured by established procedures such that power is never supplied to arm motors during co-operation with EVA crew members. In addition, collisions against structures are identified as catastrophic only when a structural failure could result in a floating object in space, space debris.

3.2. REQUIREMENTS

The JEMRMS must adopt a two fault tolerance (2FT) design for catastrophic hazards. Therefore, JEMRMS must remain safe after two mis-operations by crew, two failures of system, or one mis-operation and one system failure. In addition, three independent inhibit are required where inadvertent operations could result in catastrophic hazards, and at least two of the three inhibits status must be monitored by a crewmember.

The safety requirement for inadvertent release requires confirmation of three independent grapple statuses.

3.3. JEMRMS SAFETY DESIGN

The JEMRMS operation sequence is roughly divided into three phases. First is the maneuver phase in which the JEMRMS maneuvers in the Non-proximity area far enough from the EF or other structures to stop safely. Second is the approaching phase in which the JEMRMS approaches from the pause position to the final target position. Third is the berthing phase, an example is the cooperation with the Equipment Exchange Unit on EF (EEU-EF) to transfer a P/L grappled by EE to EEU. The following paragraphs describe how safety is achieved in each phase.

3.3.1. Maneuver phase in Non-Proximity Region

In this phase, collision hazards might occurred due to electrical or electromechanical failure affecting arm control, improper operation by IVA crew, mechanical failure such as galling, joint brake failure, or failure in the control path. However, at least one of the functions below works for any two combinations of failures. Basically 2FT design is assured by JEU or SFAE, ACU and MDP.

(1) Detection by JEU/SFAE

When JEU detects its own failure, it issues the brake on and servo off commands to itself. When SFAE detects one joint failure, SFAE will issue the brake on and servo off commands to all joints. JEU and SFAE report the error detection to ACU.

◆Check of Sensor data and Command

Each MA joint has two joint angle sensors (encoders) and a joint motor axis angle sensor (resolver). Each JEU Firm Ware (F/W) checks the followings using these sensor:

-Cross checks joint motor axis angle sensor and primary joint angle sensor.

-Cross checks primary and redundancy joint angle sensor.

-Checks continuity of joint angle command from ACU.

-Cross checks joint angle command from ACU and joint motor axis angle sensor.

-Cross checks joint angle command from ACU and primary joint angle sensor.

-Checks limit of joint angle by F/W and the limit switch

-Checks motor current limit.

Each SFA joint has two joint motor axis sensors. The primary sensor is an incremental encoder, and the redundant sensor is a hall device. SFAE F/W checks the followings using these sensors.

-Checks continuity of motor axis angle rate command and joint angle.

-Cross checks primary and redundant joint angle sensors

-Checks limit joint angle, angle rate and a force torque sensor

◆Watch Dog Timer

All checks above are performed by F/W running on SIOP and the Motor Control Processor. WDT is provided to detect anomalies of processor and F/W.

(2) Detection by ACU

If the ACU detects at least one malfunction in the following safety-related functions or detects the error status from JEU or SFAE, the ACU will issue the Emergency stop (E-stop) command to the Power Distribution Box (PDB) to cut-off the power to motors. In addition, the JEMRMS adopts the negative-actuated brake mechanism for fail safe design. The ACU reports the error detection to the MDP.

◆Region check

Region check area can be set with a maximum 10 by 10 mesh to cover the whole surface of the PM end-cone and EF including P/Ls and ORUs. ACU Software (S/W) detects the invasion of the arm tip or other reference points into the region check area by calculating the motor axis sensor data from the JEU and SFAE. The example of region check area is shown in Figure3-2.

In manual mode, an additional region check area about 80mm outside of the above area will be set. If the ACU S/W detects the invasion of the arm tip or other reference points into this region, the ACU S/W restricts commands from the Hand Controller driving the arm in the direction of invasion but allows commands in the opposite direction. In this case, ACU will not send E-stop command. This additional region check function is allocated to only the ACU.

◆Check of sensor data and command

The ACU S/W cross-checks the command and the status of the arm tip position and attitude, and checks limit of the arm tip velocity and limit of the arm tip trajectory error.

In addition, the ACU S/W checks the following using sensor data from the JEU during MA operation:

-Checks limit of the expected motor axis angle data.

-Checks limit of joint angle by S/W and limit sensor.

-Cross checks motor axis angle command and motor axis angle data.

-Check limit of motor axis angle command compared with motor axis angle rate.

-Cross checks primary and redundant joint angle data.

-Cross checks of primary joint angle data and motor axis angle data.

The ACU S/W checks following using sensor data from SFAE during SFA operation:

-Checks limit of expected motor axis angle data.

-Checks limit of joint angle by S/W and limit sensor.

-Cross check motor axis angle command and motor axis angle data

-Checks limit of motor axis angle command compared with motor axis angle rates

-Cross checks of primary and redundant joint angle data.

◆Communication error check

The ACU communicates with the JEU and SFAE via the Arm bus using a MIL-STD-1553B Bus interface. The Arm bus is a redundant bus. When the ACU, Bus Controller, detects a communication error, the ACU sends E-stop command. Crewmember will be able to re-start arm operation after manually switching the bus.

◆WDT

All checks above are performed by S/W running on two CPUs. WDT is provided to detect CPU or S/W anomalies.

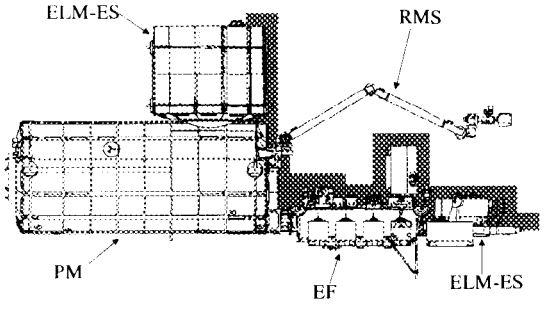

Figure3-2. Example of region check area

(3) Detection by MDP

If the MDP detects at least one malfunction in the following safety-related functions or detects the error status from ACU, the MDP will issue the E-stop command to the PDB to cut-off the power to motors.

(i) Region check

The region check area independent of ACU can be set in the same manner as ACU. MDP S/W detects the invasion of arm tip or other reference points into region check area by calculating the joint sensor data from ACU.

(ii) Check of sensor data and command

During MA operation, MDP S/W checks the following:

-Cross-checks between joint motor axis angle sensor and redundant joint angle sensor

-Checks limit of joint angle

During SFA operation, MDP checks the following:

-Cross checks between primary and redundant motor axis angle data

(iii) Communication error check

MDP communicates with the ACU via the Console Bus using a MIL-STD-1553B Bus interface. Console bus is redundant bus. When MDP, Bus Controller, detects communication error, MDP switch the bus automatically. When the communication does not recover even after switching the bus, MDP sends Emergency stop command.

(iv) WDT

This function is same as ACU.

(4) Detection by IVA crew

IVA crewmember will monitor the arm data on the RLT (RMS Laptop terminal: Thinkpad 760XD) and actual arm motion on TV Monitors to ensure safe arm operation. IVA crewmember can send brake command manually from the Remote Interface Panel (RIP) when he or she detects an anomaly. Basically, however, the JEU, ACU and MDP can control all hazards described in this section before IVA crewmember acts. Therefore anomaly detection by IVA crewmember is not identified as the control path for hazards but just as a redundant path.

3.3.2. Approach phase in Proximity region

When approaching the berthing mechanism in the proximity region, JEMRMS could collide against the berthing mechanism because there is not enough distance to stop safely even if the JEU, ACU or MDP detects the failure, which results in uncommanded motion and sends E-stop commands. The delay time for detecting an anomaly and initiating safing determines the impact energy. The worst-case impact energy is calculated based on the maximum velocity for the worst case delay time when two failures occur simultaneously. Therefore, to achieve two-fault tolerant design, the following method are adopted:

(1) Calculate the maximum impact velocity and the impact load by worst-case (two fault case) analysis.

(2) Confirm that the maximum impact load is within the structural allowable level and that structures will never fail.

3.3.3. Berthing phase

When MA berths a P/L to an EEU on the EF or ELM-ES,

or when SFA hands an ORU to attachment mount on EF, ELM-ES or Airlock Table, a payload may be inadvertently released by:

- False indication of grapple mechanism,
- Inadvertent actuation of release mechanism, or
- Mechanical failure of grapple or release mechanism

The JEMRMS, thus provides three independent grapple statuses and two inhibit switches on the power supply line to meet the requirements. This requirement also applies to co-operating mechanisms such as the EFU and ORU attachment mount. Example of typical MA and SFA operational cases are given.

(1) EE grapple status

Before releasing a P/L from EEU, IVA crew member must confirm the following three grapple statuses.

-EE micro switch status: Confirm the capture status on the RLT using signal from EE micro switches which indicate capture, snare-closed and rigidization.

-Side view on TVM: Confirm there are no gaps between the EE and the surface of the Grapple Fixture (GF) in the TVM images captured by one or two exposed cameras. 80%of the EE edge ring should be monitored.

-Target view: Confirms the criteria given by the overlay displayed on the images of the GF target from wrist TVC.

(2) TOOL grapple status

An ORU is fixed on the attachment mount with two bolts. Before unscrewing the second bolt, a crewmember must confirm following three grapple statuses.

-Micro switch status of Tool Latch Mechanism: Confirm the finger open status and the latch status on RLT. The finger open status is generated when three micro switches indicate "open" and two micro switches indicate "not closed".

-Two Side views on TVM: Confirm that two out of the three visual cues on Tool indicate latch completion on TVM and that there is no gap between Tool and the surface of Tool Fixture.

(3) Release command

The release command to EE and Tool adopts the same safety concept. Therefore, the following three independent actions based on two independent information sources are taken to meet the two fault tolerant requirement. Before releasing a P/L, crewmember must confirm three captured statuses from the cooperating mechanism. Crewmember, then, sets two power enable switches from the Remote Interface Panel (RIP) and monitors each status on the RLT. Crewmember, then sends the release command from the Rotational Hand Controller (RHC) after confirming that the RHC status is "HOT" on the RLT. This active status is generated from the two power enable statuses. The release command is sent to each motor driver after the prerequisite check in the MDP S/W.

3.4. VERIFICATION OF HAZARD CONTROL

All hazard control methods are verified by analysis or PFM testing during the JEMRMS development. However the safety design in the berthing phase will be demonstrated in the JEM overall system test.

4. MFD SAFETY APPROCH

The MFD took a different safety approach from the JEMRMS to achieve two-fault tolerant design. This section gives the basic concept of the MFD safety design and then introduces the unique safety approach in GC experiments that NASDA and NASA took.

4.1. Mission overview of MFD

The mission of MFD project was to demonstrate the prototype SFA (MFD robot arm) functions and performance including the man-machine interface system in a micro-gravity environment, and to feed the results back to the SFA PFM development.

The MFD system consisted of the Shuttle onboard system (MFD payload) and the ground segment. The MFD payload was launched on board STS-85 / Discovery from NASA's John F. Kennedy Space Center on August 7, 1997. The MFD payload consisted of the Payload Bay (PLB) element (Fig.4-1) consisting of the MFD robot arm and other electronics components and the Aft Flight Deck (AFD) element consisting of two 3 degrees of freedom hand-controllers and workstation.

Following the crew-tended demonstrations, file transfer-based Ground Commanding (GC) experiments were conducted as planned using the computer network in JSC (Fig.4-2.) to obtain useful basic data for future space robot arm operations.

All the planned tests and experiments in the MFD mission including GC experiment were accomplished successfully in 12 days. Discovery landed on KSC on August 19, 1997.

4.2. GC Experiment Overview

GC was an advanced technological experiment as well as a preliminary step toward the ground control of a future space robotics system. It showed potential in assisting future Space Station crewmembers so that they could focus their time on the other more important tasks.

The GC experiments were initiated by electronic arm-trajectory file transfers from the ground facility to the Space

Shuttle. These remote control experiments were the first of their kind conducted on board a manned spacecraft with hardware exposed to the space environment. One of the experiments was to repeat a crew-operated robot arm motion on orbit by recreating the crew-operated trajectory in a digital format on the ground. From the arm motion telemetry resulting from prior crew control, an arm-trajectory file was developed on the ground. Since one digital file size was limited to 10 Kbytes due to the system design, an interpolation method was adopted to reduce and adjust the number of pathway points. The trajectory file was then up-linked and executed.

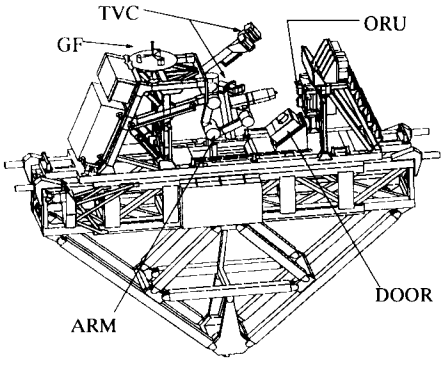

Figure 4-1. MFD PLB element

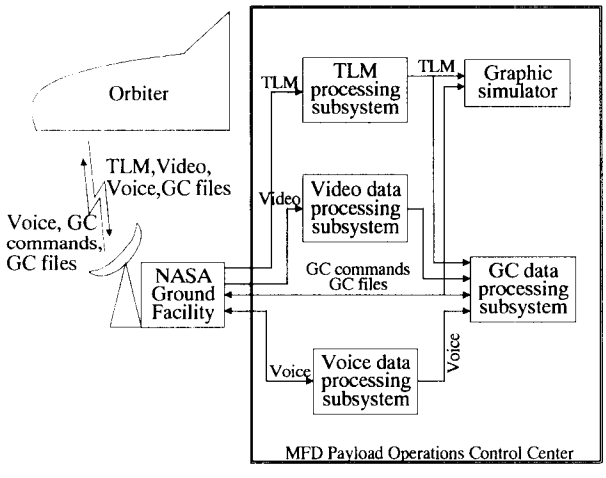

Fig.4-2. MFD GC system

4.3. MFD Mission Safety Concept

The MFD robot arm had the same potential hazards as the JEMRMS. MFD, however, took a different approach than JEMRMS because of its zero-fault-tolerant computer-system. Therefore MFD achieved two-fault tolerant design by assuring safe return of the Orbiter not collision.

(1) To control unplanned contact hazards, the robot arm reachable envelop was restricted by software and mechanical joint stoppers.

(2) A collision tolerant design was adopted for the robot arm and the structures.

(3) Extra-Vehicular Activity (EVA) compatible design was adopted and flight operation scenarios were developed to stow the robot arm in a safe configuration if it lost the functions due to the collision.

4.4. Unique Approach of GC Experiment

In the GC experiment, the Arm Control Computer (ACC) drove the MFD robot arm based on the arm tip trajectory file. This file was up-linked from the MFD Payload Operations Control Center (POCC) in NASA JSC through NASA data network system. In addition to the major safety-related features above, a step-by-step verification approach was adopted in the GC experiment operations to prevent an arm collision.

(1) To verify the proper command (trajectory) generation, the commands were demonstrated and confirmed one by one by the ground segment prior to up-link.

(2) To detect communication error, the up-linked command was sent back to the ground for validation.

(3) The received and memorized command in ACC was checked using syntax check by ACC prior to arm movement.

In addition, only free-in-motion of an unloaded robot arm without ORU was permitted for safety.

5. CONCLUSION

This paper has presented JEMRMS design and the MFD design concept focusing on safety design.

The MFD mission has completed successfully and has been feed-backed many useful techniques and experiences to JEMRMS including safety design. But in the GC experiment, however, crewmember still must monitor the operation to ensure safety. This suggested to us the theme to study how crewmember should be involved with unmanned robotics operation on a manned space facility.

The JEMRMS safety related design, that is the identification of potential hazards and the hazard control, has been approved by the ISS safety panel. JEMRMS was now completed in the design phase and is undergoing the Proto-Flight Model manufacturing, assembly and testing. The identified control will be verified in the series of PFM test. The verification results will also be reviewed and approved at the ISS safety panel in the JEM PQR phase.

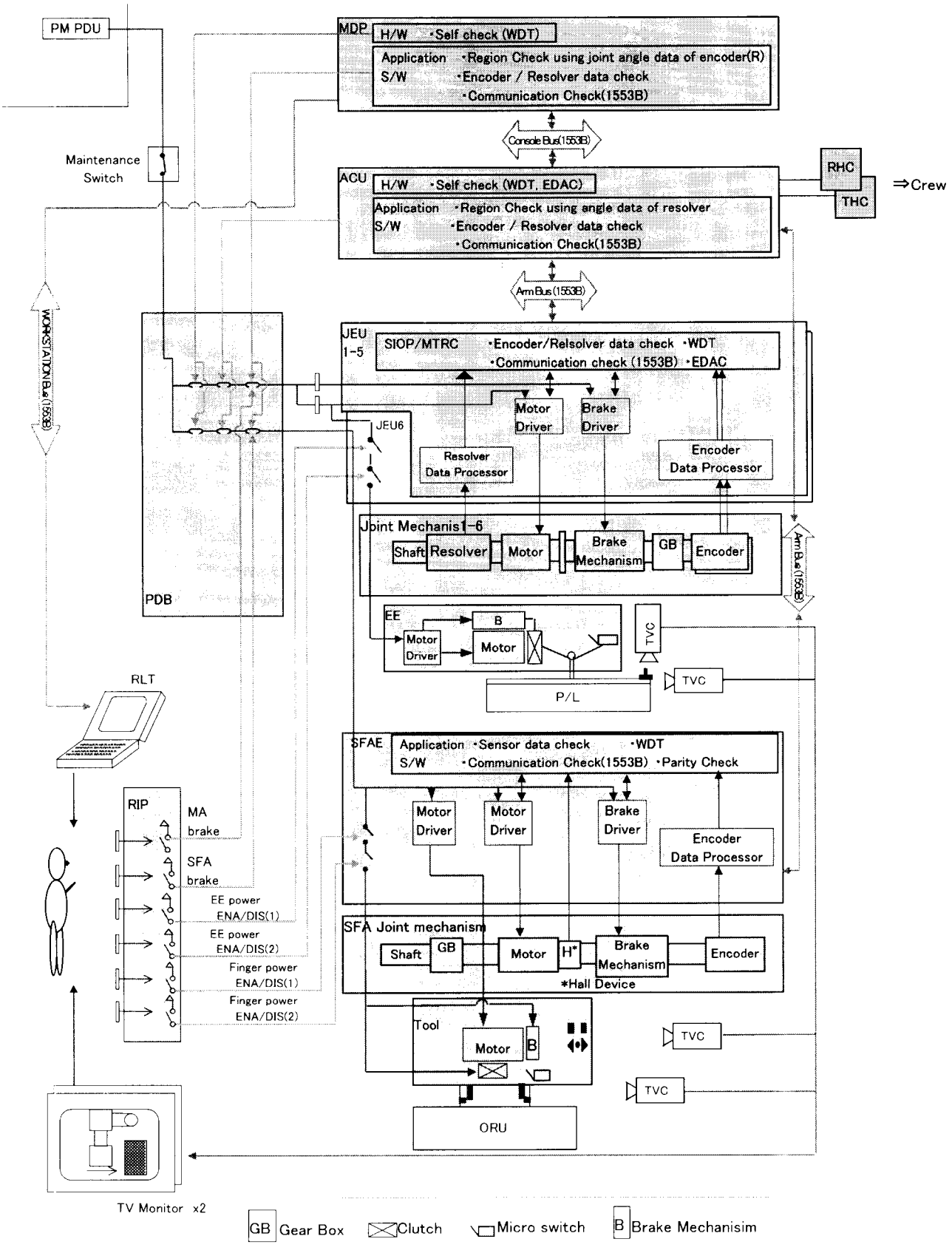

Figure 3-1. Safety-related schematics of JEMRMS