ESA's Data Management System for the Russian Segment of the International Space Station

J. Graf, C. Reimers & A. Errington
ESA Directorate of Manned Spaceflight and Microgravity, ESTEC, Noordwijk, The Netherlands

In October 1997, two flight units of the Data Management System (DMS-R) for the Service Module of the Russian Segment of the International Space Station were handed over by ESA to the Russian Space Agency (RKA) for use by RSC Energia, the prime contractor for the Service Module and the entire Russian Segment. The Data Management System was developed and manufactured in Europe by an industrial team led by Daimler-Benz Aerospace (DASA) in Bremen, Germany, under a contract placed by ESA's Directorate of Manned Spaceflight and Microgravity in Noordwijk, The Netherlands. The project is governed by a cooperative agreement between ESA and RKA.

This is the first delivery of ESA flight hardware within the International Space Station Programme to another International Partner. It will be launched with the station's third assembly flight, in December 1998.

Role of the Data Management System

The first modules of the International Space Station (ISS) will be the Functional Cargo Block (FGB, built by Russia and financed by NASA), NASA's Node 1 and the Russian Service Module. As the Service Module has to be autonomous from the beginning of its orbital life, it carries its own Data Management System (DMS-R).

Ultimately, the Data Management System will not only control the module itself, but also perform overall control, mission and failure management of the entire Russian Segment, such as:

- system and subsystem control, especially guidance, navigation and control
- mission management and supervisory control by ground and crew
- management of onboard tasks and failure recovery
- time distribution, time tagging and synchronisation
- data acquisition and control for onboard systems and experiments
- exchange of data and commands with the other parts of the station

It will also provide overall guidance and navigation for the entire station.

Overall DMS-R Configuration

The Data Management System architecture of the Russian Segment and its interfaces with the overall International Space Station is shown in Figure 1. Ten MIL-STD buses provide the interconnectivity between the various elements and equipment. The ESA-provided Service Module onboard units are:

- Two Fault Tolerant Computers (Figure 2): a Control Computer and a Terminal Computer.
- Two Control Posts (Figures 3 and 4) for command and control by the crew via the DMS-R, and for commanding experiments and the European Robotic Arm (ERA), which is also being developed by ESA under a cooperative arrangement.

A more detailed block diagram of the Service Module Data Management System is shown in Figure 5. The Control Computer and Terminal Computer have built-in redundancy to provide the required failure tolerance. The Control Posts can be configured to execute different, dedicated tasks or to operate in redundancy mode.

The application software for the onboard computers is being developed by the Russian Service Module contractor, RSC Energia, using an ESA-provided Ground System, which provides the hardware and software environment to support software design, development, simulation, test and validation. It is also being used to integrate hardware and software into the Service Module Flight Model.

Principles and implementation of failure tolerance

The Control Computer and the Terminal Computer feature a fault-masking architecture and are single-failure tolerant.

Fault masking is achieved by majority voting following parallel execution of the application programs in three identical computer units. These units are called Fault Containment Regions. For this voting process, the Fault Containment Regions must receive identical, synchronised input values in order to be able to deliver identical output values.

Because of potential errors in data distribution, some distribution rules have to be considered. These are defined by the 'Byzantine Theory', which specifies the required number of Fault Containment Regions, individual data links and data distribution rounds, depending on the number of failures to be recovered.

As a result, a Byzantine Fault Tolerant Computer system consists of multiple Fault Containment Regions cross-strapped by multiple high-speed point-to-point data links.

In order to survive F simultaneous faults, the system must meet the following requirements (according to Lamport, Shostak and Pease, 'The Byzantine General's Problem'):

- the system must consist of 3F+1 Fault Containment Regions
- the Fault Containment Regions must be interconnected through 2F+1 individual paths
- the inputs must be exchanged F+1 times between the Fault Containment Regions
- the Fault Containment Regions must be synchronised.

For data distribution, electrically-isolated full duplex serial data links are used to avoid error propagation between the Fault Containment Regions. The realisation of an individual data path must be a point-to-point connection. Keeping in mind the data throughput, which is reduced by the required data distribution rounds, these data links must have very high transmission rates.

This DMS-R development is the first time that the Byzantine Theory on failure tolerance has been realised for a space application.

One of the most critical problems in the design of synchronised computer systems is the elimination of deadlock situations, where one software task is waiting for an event or data coming from another software task, which itself is waiting for events or data from the first. In order to avoid such situations, all communication paths in the software have been modelled by an abstraction method in order to reflect all related vectors and variables. The integrity of the design and the absence of any deadlock situation have been verified through many millions of simulation runs. The simulations and design analysis were performed by an independent team at the University of Bremen, Germany.

For the Russian Service Module, the required configuration for the Fault Tolerant Computer consists of three Fault Containment Regions, which provide masking of one deterministic fault.

Associated ground system

The DMS-R onboard equipment is complemented by a set of ground hardware and software for the application software development and verification process, as well as for system integration and check-out. The Ground System is based on the Columbus Ground Software, developed by DASA for ESA's Columbus Orbital Facility, one of Europe's main contributions to the International Space Station. The Columbus Ground Software is a consistent set of software products that forms the basis for a comprehensive set of integrated ground facilities. It is also in use at NASA for the Space Station Mission Build Facility and the System Verification Facility.

The Ground Segment consists of three main facilities:

1. The Software Design and Development Facility
2. The Software Integration and Test Environment
3. The Test Facility with the necessary Electrical Ground Support Equipment and onboard DMS engineering models for system-level software integration. This facility is also connected to the Functional Cargo Block (FGB) ground facility, provided by NASA to support integrated Service Module/FGB/Node/Shuttle interface verification testing.

ESA and Russia: the cooperative experience

A challenging aspect of DMS-R development was working within two contrasting engineering cultures. A number of important differences in approach became evident early on, while some were not fully appreciated at the time.

The old 'Soviet' approach to spacecraft development, like other activities of key importance to the former Soviet Union, was to assign abundant resources within the prime contractor and its various subcontractors, all under the overall responsibility of the General Designer, who had almost absolute power to accomplish the required task.

The development itself was driven mainly by design ideas rather than by detailed functional and interface requirements. It required very close cooperation between individual designers, plus repeated iterations and intermediate breadboarding of individual design elements until the desired overall performance was achieved. This approach meant that functional and interface requirements of the individual design elements could change significantly during the design process, but it offered performance improvements and optimisation during development. Documentation was limited to essential high-level requirements, as all detailed information was open to change anyway.

Although this approach is changing with Russia's political and economic evolution, the old philosophy still very much influences the attitudes not only of individual engineers but also of corporate entities.

In contrast, the Western European approach to development is for the customer to generate a set of System Requirements. These are then used by a prime contractor to elaborate lower-level specifications and interface requirements for subcontractors and, ultimately, to conclude a fixed-price contract. In this scenario, technical changes usually lead to considerable schedule and cost impacts, and are therefore avoided whenever possible.

It is obvious that combining these approaches in a cooperative programme carries the potential for conflicts, so it was no surprise that the DMS-R programme had to surmount such problems. The situation was complicated by the constraint that the requirements for the DMS-R computers were developed with a view to their reuse in ESA's own Columbus Orbital Facility and Automated Transfer Vehicle projects. These requirements were defined in a System Requirements Document (SRD), which established the technical basis for the fixed-price contract with Industry, and in parallel Joint Systems Requirements (JSR), which defined the technical basis of the agreement with the Russian Space Agency.

In practice, the difficulties manifested themselves in the limited emphasis of the Russian partners in following up and reacting to the early DMS-R design and definition activities, including the related reviews. Their interest and involvement started to increase after the Preliminary Design Review, with the consequence that the first requests for changed or new requirements were raised at that time. This continued throughout the implementation and even the verification phases, almost up to the Qualification Review. Similarly, great reluctance was met in freezing the Interface Control Document at a sufficiently early stage.

Considerable analysis and persuasion therefore went into discussing and constraining the Russian changes to items essential for creating a properly functioning integrated system, while limiting schedule and cost impacts to acceptable levels. Eventually, however, it became evident that the most effective approach was to encourage active Russian involvement in matters of common concern long before they would have become interested under the old system. This triggered an early understanding of design characteristics and implications, highlighting unavoidable changes as early as possible.

History of European/Russian Cooperation on DMS

The project goes back to 1992, when discussions were initiated between Russia and Europe on potential ESA contributions to the planned Mir-2 station. One candidate was the Data Management System. However, the political climate evolved very rapidly and the International Space Station, built and operated under multi-national cooperation, replaced the separate Freedom and Mir-2 programmes. The European/Russian DMS was also confirmed for the new Space Station scenario and fully endorsed by NASA.

DMS development was formalised in an ESA/RKA Arrangement, signed on 1 March 1996, which defined ESA's DMS obligations and RKA's obligations, in exchange, to design and deliver to ESA the Russian Docking System for ESA's Automated Transfer Vehicle (ATV). The ATV, launched by Ariane-5, will support ISS resupply.

On 10 May 1995, the ESA Council approved the final DMS-R declaration, with a programme participation of approximately 74% from Germany, 13% from France, 8% from Belgium and 5% from The Netherlands. The industrial contract with DASA-RI as prime contractor, and Matra Marconi Space, Alcatel Bell Telecom and RST as direct subcontractors, was signed on 14 December 1995.

Key Milestones during the DMS project implementation phase were:

- System Requirements Review (SRR) December 1994
- Preliminary Design Review (PDR) June1995
- Critical Design Review (CDR) June 1996
- Qualification Review (QR) September 1997
- Flight Acceptance Review (FAR) October/ November 1997

Figure 1. Data Management System architecture of the station's Russian Segment

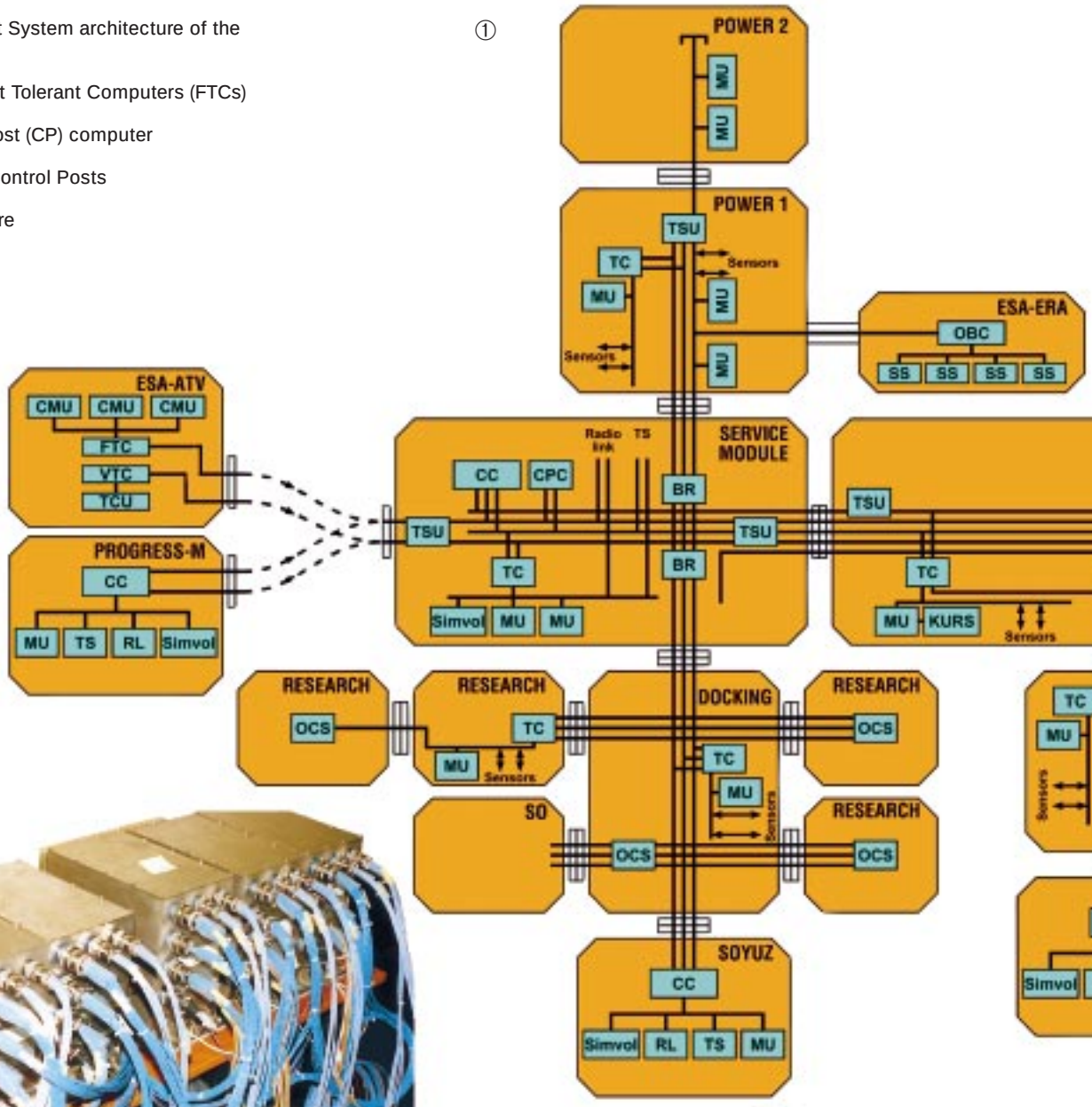
Figure 2. DMS-R's two Fault Tolerant Computers (FTCs)

Figure 3. DMS-R Control Post (CP) computer

Figure 4. The two DMS-R Control Posts

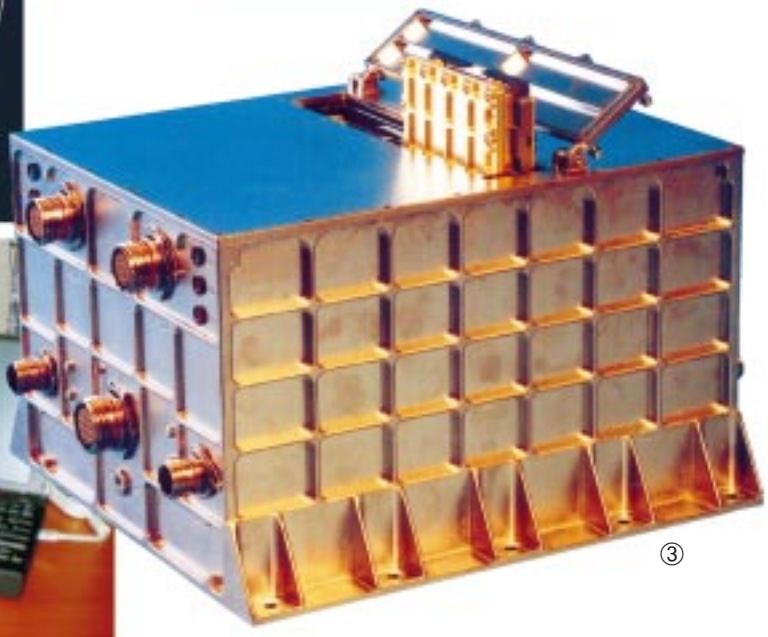
Figure 5. DMS-R architecture

①

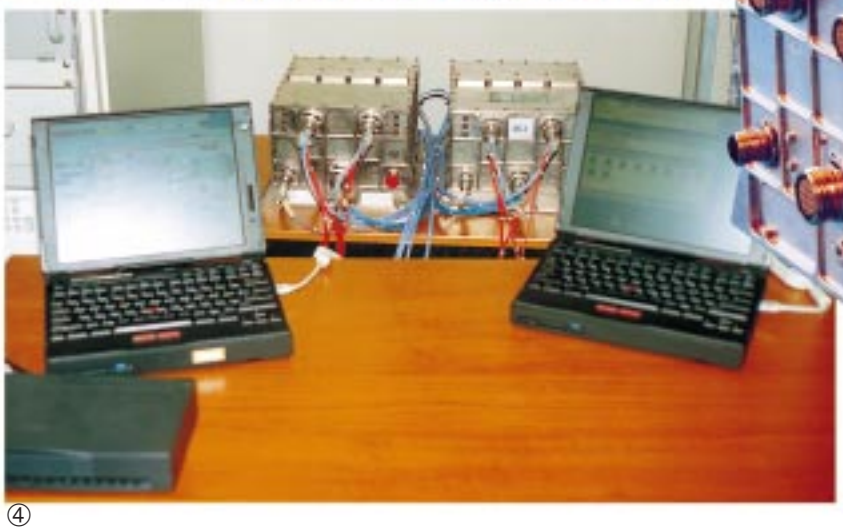


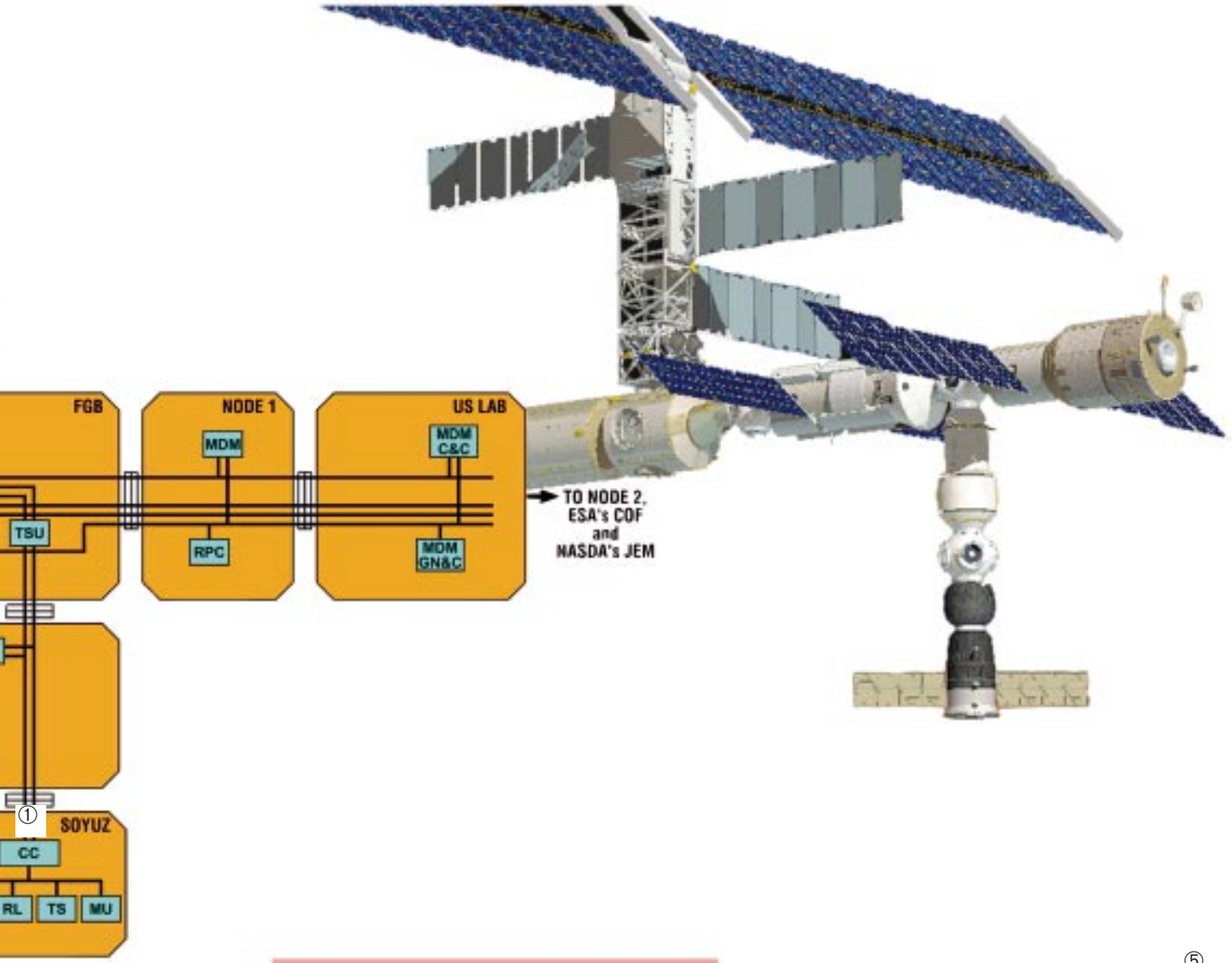
②

③

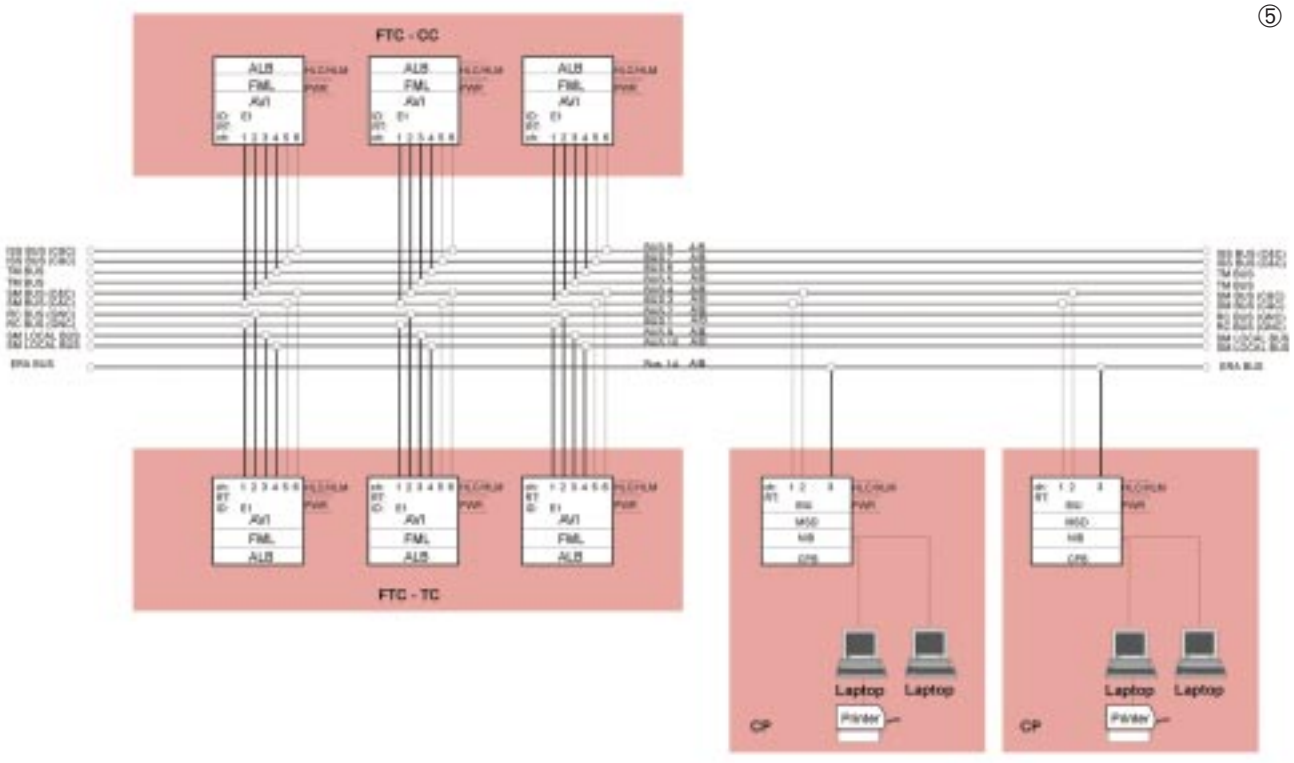


④





⑤



Courtesy: DASA

ESA's Data Management System, as part of Russia's Service Module (left, in main artwork), will provide critical control, guidance and navigation functions for the International Space Station. Inset is one of the two DMS Fault Tolerant Computers.