DOI: 10.13009/EUCASS2019-996

A RE-USABLE HIGH RELIABILITY COMPUTER FOR AUTONOMOUS MISSIONS

Mr Steven De Cuyper
QinetiQ Space nv, Belgium, steven.decuyper@qinetiq.be
Mr Ruben Willems
QinetiQ Space nv, Belgium, ruben.willems@qinetiq.be

Abstract

In this paper we present the selected QinetiQ Space On-Board Computer for the Re-Entry Module part of the Space Rider mission. Next to a general introduction of the features and its performance, we also clarify how our design meets the key mission and system challenges. We further focus on its reliability and the used calculation method. The results demonstrate the reliability of our solution and how this evolves throughout the lifetime of Space Rider over the various launches/mission profile.

1. Introduction

QinetiQ Space's developed On-Board Computer, ADPMS [1][2], was selected for many applications such as small satellite missions (like the Proba missions). PROBA stands for "Project for On-Board Autonomy" and is thus especially developed to enable a high level of autonomy. Next to the small satellite missions, the ADPMS computer was also selected for the European re-entry from LEO, Intermediate eXperimental Vehicle (IXV) [3], again an application that requires a high reliability computing solution. Based on our extensive ADPMS heritage and knowledge, QinetiQ Space developed the next evolution On-Board Computer suited for a wide range of possible applications. Next to the upcoming small satellite missions, the computer is also selected as a cornerstone equipment of the IBDM (International Berthing and Docking Mechanism) [4][5]. IBDM is the European androgynous low impact docking mechanism that is capable of docking and berthing large and small spacecraft. Here again a high reliability computer is the basis for successful and safe docking and berthing.

A re-usable high reliability On-Board Computer (OBC) for autonomous missions such as the ESA Space Rider mission [6] need to fulfil a wide range of key mission requirements. The Space Rider programme is the successor of the Intermediate eXperimental Vehicle (IXV) programme: the first European unmanned spaceplane that does not feature any wings but uses an aerodynamic shape supported by flaps and thrusters to autonomously steer it back to Earth. The spaceplane was successfully launched and recovered on February 11th 2015. While IXV was intended to showcase the latest technologies and critical systems in a demonstration flight, the Space Rider mission builds further on this experience to build an operational space transportation system for routine access and return from low orbit. Therefore the Re-entry Module (as part of Space Rider) will integrate a MPCB (Multi-Purpose Cargo Bay).

The selected On-Board Computer was especially developed to tackle the following Space Rider key mission and system challenges:

- Maximization of Payload Mass & Volume and Payload Mass/EUR ratio (miniaturization of OBC)
- Minimization of Cost (development and operational including refurbishment)
- Maximization of Reusability (developed for multiple flights)
- Minimization of Risk (developed taking into account reuse and lesson learned analysis)
- Maximization of Reliability (developed for surviving multiple launches and operating multi-years and in space environment)

To maximise competitiveness of each mission, challenging system requirements need to be met. A critical one is the maximization of payload mass & volume and payload mass/EUR ratio. This overall requirement results in the miniaturisation of all on board units both in volume and mass: this enables to reserve an as large as possible volume

DOI: 10.13009/EUCASS2019-996

for potential payloads. This also affects the On-Board Computer requirements: the OBC should be as small as possible with an increase in performance capability. Another important system requirement is to maximise re-usability which results in equipment that are developed for multiple flights with a minimal refurbishment cost. Also, the risk should be minimised by re-using equipment with flight heritage and taking into account the lesson learned. Finally, the reliability needs to be maximised to survive multi-years in space environment (combined with multiple launches over the complete mission).

2. System Architecture

2.1 Introduction

Before going in detail about reliability, first a general introduction is given about the OBC design for Space Rider. The design of the Space Rider OBC is based on the IXV OBC but taking into account the mission key requirements of miniaturisation, increased processing performance capability ability to fully recover after one single failure, modularity and system expansion options (minimisation of cost).

2.2 Redundancy concept

In order to increase the reliability of a system, it is mandatory to implement redundancy. Briefly explained, redundancy can be implemented by doubling parts in a system to achieve a SPF free system. However, at the end of the (doubled) chain, there is only one output. According to the criticality of the system, as well as the required speed of the switch-over sequence, the way of implementing the redundancy might change. This means that the position of the switch-over mechanism in the chain will be different. The closer to the output the switch-over takes place, the hotter the redundancy gets. We have defined 4 possibilities of redundancy:

- Cold redundant
- Cool redundant
- Warm redundant
- Hot redundant

The drawing in Figure below illustrates these 4 definitions.

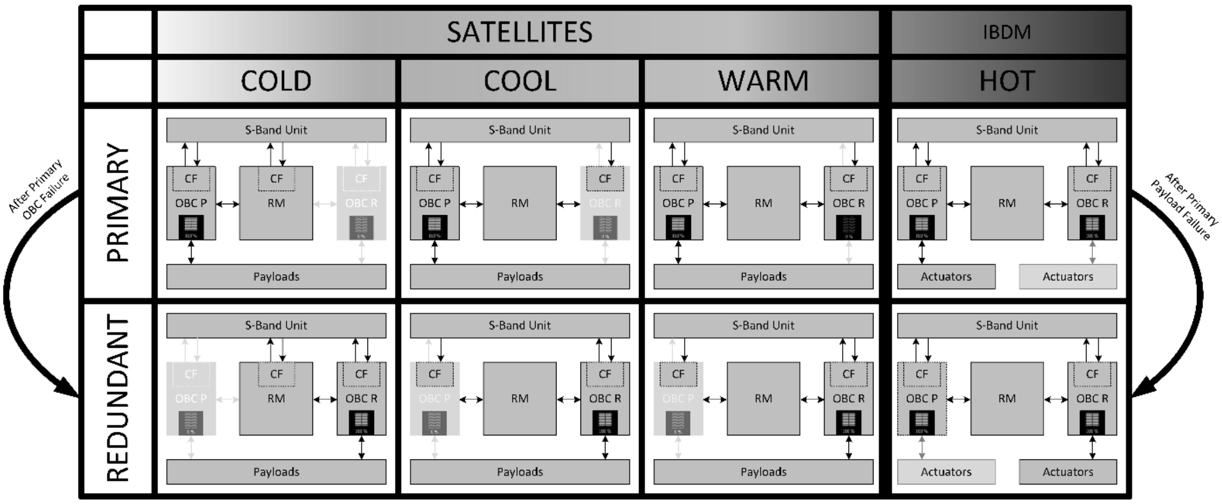

Figure 1: Redundancy definitions

A typical space computer exist of a primary and redundant OBC, a Reconfiguration module (RM), a PCDU and S-band RF unit. The output of the system are actuators for hot redundancy and payloads for cold, cool and warm redundancy. The definition of each redundancy is given in the next paragraphs.

In a **cold redundant system** only one OBC is powered at any time, and therefore, only one OBC is able to communicate with the S-band RF unit. In case of a switch-over, the primary OBC power will be switched-off, followed by a switch ON of the redundant OBC power. After a switch-over, the redundant OBC will start up and will start loading its

DOI: 10.13009/EUCASS2019-996

software. This implies that, to make the system more robust, the RM will also have some critical functions aboard with an additional TM/TC interface.

In a **cool redundant system** the Critical Functions (CF) are always active (HOT) on both OBCs. This means that both OBCs are powered in this configuration. However the non-active OBC will be configured as such that only the critical functions are active, while the remaining functions are in standby and no software is running on the non-active OBC. Where possible, devices which can be powered OFF will be powered OFF in order to reduce the power consumption of the non-active lane to a strict minimum. In case of a switch-over from primary to redundant OBC, the primary OBC will only keep the critical functions active while the SW on the redundant OBC will boot and takes over the control.

In a **warm redundant system**, both OBCs are powered. The only difference between the active and the non-active lane is that the OBSW is not running on the non-active lane. As such, only the active lane will have control over the S/C.

In a **hot redundant system** both OBCs are powered permanently and the OBSW is running on both lanes while performing the same tasks simultaneously. The RM shall be responsible of directing which payload or actuator will be given the authority to take control. This redundancy will reduce the duration of the loss of control of the system to the absolute minimum.

The Space Rider consortium has chosen for a cool redundant system. The (same) Processor Module (PM) is able to support all four redundancy concepts showing the high flexibility of our modular approach. The only board that differs between the different redundancy systems is the Reconfiguration Module (RM).

2.3 Key features

The proposed On-Board Computer is built around a multicore GR712 LEON processor to be able to provide up to 170 MIPS (typical value on dual-core). The double core feature enables the increase of processing power that can be initiated upon demand at any stage of the development process. It also paves the path towards a very high autonomous mission. Such a highly integrated processor solution further enables the miniaturisation of the overall OBC since it contains a wide range of interfaces. A large scale companion FPGA that controls additional peripheral functions and handles OBC communication interfaces. In the standard configuration of the OBC, memory blocks used for OBSW storage, boot memory, and safeguard memory will be connected to the FPGA while memory blocks used for working memory and BIOS are connected to the platform controller. Furthermore, the OBC contains UART (RS422), CCSDS TM/TC, SpaceWire, CAN, Ethernet, MIL1553, analogue and digital IO interfaces.

For the analogue inputs required, an ADC with SPI interface is included in the OBC architecture as a companion to the FPGA.

As such a two-board solution, consisting of a Processor Module (PM) and an Extension Module (ExM), can be presented for the main functionality. As for Space Rider, where a cool redundant configuration is selected, the two OBCs are both connected to a Reconfiguration Module (RM) that contains the switch-over functionality.

To cover the additional Space Rider specific interfaces (32 High Priority Commands), which are not part of the standard configuration, an additional board has been added to this OBC: the High Priority Command Module (HPCM). Also existing in a nominal and a redundant board. As such, the high reliable OBC consists of in total seven Printed Circuit Boards in total.

Additionally, the QinetiQ Space OBC could be extended with an in-house built MMU with configurable storage capacity (160GiB to 480GiB) including error correction capabilities. Thanks to its modular mechanical design, this could be integrated into one single housing.

This OBC is also selected as the cornerstone for our small satellite missions and integrated into our IBDM – International Docking and Berthing Mechanism.

3. Reliability

3.1 Introduction

Reliability is the probability that a device or a system will function as expected without failure for a given duration in an environment. For electronic systems, the failure rate over time shows a “bathtub curve” [7]. A product’s life can be divided into three phases: Early life, Useful life and Wear Out.

DOI: 10.13009/EUCASS2019-996

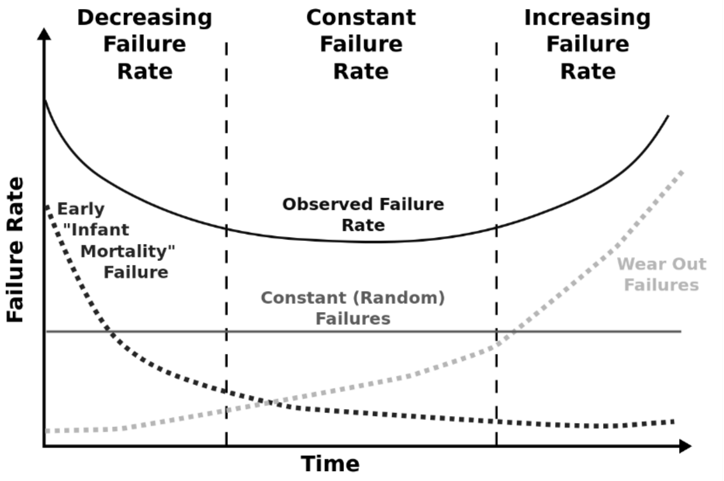

Figure 2: The 'bathtub curve"

Early life is typically characterized by a higher than "normal" failure rate. These failures are referred to as "Infant Mortality" and can be accelerated and exposed by a process called "Burn-in". Space quality assurance requirements for Design, Procurement, Manufacturing and Testing allow resolving Early Life issues and the system is trusted for normal operation.
During Useful life phase, failures are considered to be "random chance failures" which typically yields a constant failure rate. Failure rate (λ lambda) is expressed in FIT (Failure In Time). 1 FIT = 1 failure in 10^9 hours.
The Wear Out phase begins when the system's failure rate starts to rise above the "norm". Most electronic components last a lot longer than what is needed for a mission.
For a constant failure rate (λ), the reliability function over time (t) is:

$$\boldsymbol{R(t) = \exp(-\lambda \times t)} \qquad \textbf{(1)}$$

An incremental computation model was chosen for this study. As the goal is to insure a given reliability, the part count mode has been considered first. Part count mode evaluates the reliability of each component, assuming any failure will lead to mission failure. So the probability of mission failure is the sum of the failure probability of components. Further refinements, by using the part stress mode, and furthermore using function criticality and failure tree are possible if required to obtain more detailed estimate of system reliability.

The global failure rate of the electronic product (usually equipment) is obtained by summating all failure rates for each of its component elements.
Formula for product failure rate: $\lambda_{\text{product}} = \Sigma\lambda_{\text{component}} + \Sigma\lambda_{\text{PCB}} + \Sigma\lambda_{\text{COTSboards}} + \Sigma\lambda_{\text{other}}$
In our application, 'COTS boards' and 'other' are not considered and thus $\Sigma\lambda_{\text{COTSboards}} + \Sigma\lambda_{\text{other}} = 0$. The formula for component failure rate is $\lambda_{\text{component}} = \lambda_{\text{physical}}$ x Π_{PM} x Π_{Process} x Π_{E}

Where:
• $\lambda_{\text{physical}}$ is the failure rate that depends on the function of the component (i.e. capacitor, resistor …), on the technology used (i.e. ceramic for capacitors) and the applied stress (ground benign environment in this calculation).
$\lambda_{\text{physical}} = \lambda_0 * \Pi_{\text{acceleration}} * \Pi_{\text{Pinduced}}$

- λ_0 is the intrinsic failure rate that depends on the function of the component (i.e. capacitor, resistor …), and on the technology used (i.e. ceramic for capacitors).
- $\Pi_{\text{acceleration}} = \Pi_{\text{Thermal}} + \Pi_{\text{Electrical}} + \Pi_{\text{TCy}} + \Pi_{\text{Mechanical}} + \Pi_{\text{RH}} + \Pi_{\text{Chemical}}$
  All these factors are defined per component family.
- $\Pi_{\text{Pinduced}} = 1$, mission phase dependent stresses are included via the environment factor from MIL-HDBK-217F.

• Π factors are modifiers used to take context stress into account:

- Π_{PM} is a multiplying factor that takes into account the quality of the manufacturer, the quality of the component (such as Mil-grade, screened or not), the experience with the supplier. It represents the item quality while the factor varies from 0.5 (supplier better than the state of the art) to 2 (the worst case).

DOI: 10.13009/EUCASS2019-996

- $\Pi_{Process}$ is a multiplying factor that depends on the process of the component such as soldering, PCB, X-Ray verification. This factor can be calculated from a process audit. For the first calculation, the factor is assumed to be “1”. This represents a perfect process, for which all audit questions are answered satisfactorily.
- Π_E is a multiplying factor that depends on the environment of the phase in the mission. This factor is from the MIL-HDBK-217F Notice2 [8].

3.2 Space Rider Mission Phases

The mission phases taken into account for the calculation of the Space Rider Re-entry Module On-Board Computer is summarised in the table below. For the calculation of the ground storage between two missions, a launch every 6 months [9] is taken into account subtracted with the actual intended mission duration of 2 months.

Table 1: Mission Phases for Space Rider Re-entry Module

	MIL-HDBK-2017F environment factor
Ground pre-flight phase	GF – Ground Fixed
Launch/Ascent	ML – Missile Launch
Coasting	SF – Space Flight
Preparing for de-Orbiting	SF – Space Flight
De-Orbiting	SF – Space Flight
RM Coasting	SF – Space Flight
RM Re-entry	MF –Missile Flight
RM Descent & Landing	MF –Missile Flight
Ground post-flight phase	GB – Ground Benign
Ground storage[1]	GD - Ground Dormant

For the last mission (6th flight mission), the final ground storage is no longer taken into account as the mission ends after the landing and (final) on-ground data recovery after the 6th mission.

3.3 Reconfiguration Module

The Reconfiguration Module contains Triple Modular Redundancy (TMR). The reliability of m-out-of-n redundant subsystems:
In case of purely active redundancy (i.e. all components are active from the start) of identical components with constant failure rate and without repair, the Reliability can be evaluated by the Binomial distribution as:

$$\boldsymbol{Rs(t)} = \sum_{\boldsymbol{k=m}}^{\boldsymbol{n}} \binom{\boldsymbol{n}}{\boldsymbol{k}} \boldsymbol{Rc(t)^k} \times (\boldsymbol{1} - \boldsymbol{Rc(t)})^{\boldsymbol{n-k}} \qquad \textbf{(2)}$$

With

$$\binom{\boldsymbol{n}}{\boldsymbol{k}} = \frac{\boldsymbol{n}!}{\boldsymbol{k}! \times (\boldsymbol{n-k})!} \qquad \textbf{(3)}$$

For TMR (= 2 out of 3), n=3 and m=2:

DOI: 10.13009/EUCASS2019-996

$$\boldsymbol{RTMR(t) = RM(t)^3 + 3 \times RM(t)^2 \times (1 - RM(t))} \quad \textbf{(4)}$$

In words: Reliability of TMR system with perfect voter, is reliability of all three modules successful plus three times two modules successful and one module failed.

For RM (3 x same circuitry M on RM), assume failure rate for M = (FIT of RM)/3.
Reliability of circuitry m is

$$\boldsymbol{RM(t) = exp(-\left(\frac{\lambda}{3}\right) \times t)} \qquad \textbf{(5)}$$

Reliability of Module RM is calculated using formula (4)

3.4 System Reliability

Calculating the system reliability of the On-Board Computer redundant system for the Space Rider mission (as described in 2.3 and graphically represented in below figure) leads to the following formula.

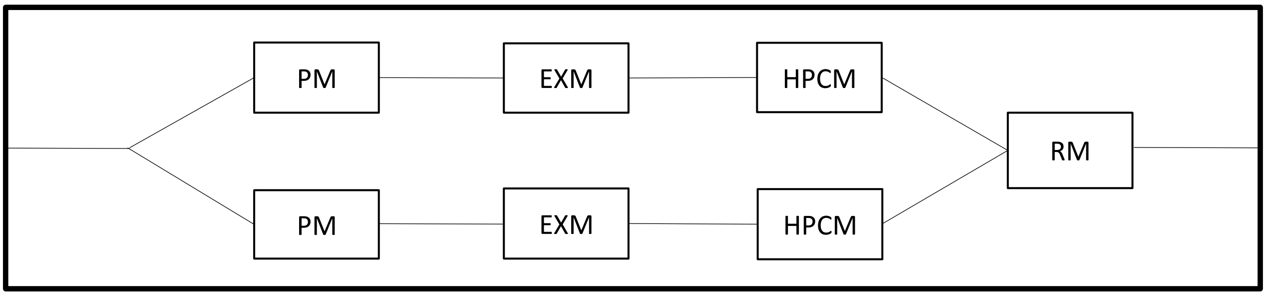

Figure 3: OBC Redundant system

$$\mathbf{R}\boldsymbol{system} = \mathbf{R(RM)\ x\ R(//PM, EXM, HPCM)} \qquad \textbf{(6)}$$

Where R(//PM,EXM,HPCM) = 1 - F(PM,EXM,HPCM) x F(PM,EXM,HPCM)
And F(PM,EXM,HPCM) = 1 - R(PM) x R(EXM) x R(HPCM)

$$\mathbf{R}\boldsymbol{system} = \mathbf{R(RM)\ x\ [1 - \left(1 - R(PM) x\ R(EXM) x\ R(HPCM)\right)^2]} \qquad \textbf{(7)}$$

3.5 Reliability Summary

Without taking the mission profile into account (neither mission phase duration, nor mission phase environmental factors are considered) the computed FIT[1] for the OBC used in IXV (single lane) was 3,919061. As a comparison, the computed FIT[1] for the OBC in Space Rider (single lane, without HPCM for comparison reasons) is 1,340459. All based on the parts count method calculation.

This shows already a large improvement for meeting the reliability requirements for a re-usable high reliability computer.

Taking into account the mission profile of the ESA Space Rider mission (see Table 1), the mission reliability for the On-Board Computer calculated with the parts count method is shown in the table below. The table gives the results based on the configuration as described in Figure 3.

[1] Failure in Time in millions of hours

DOI: 10.13009/EUCASS2019-996

Table 2: Space Rider Re-entry Module OBC Mission Reliability

	OBC Mission Reliability
After mission 1	0,999984
After mission 2	0,999935
After mission 3	0,999853
After mission 4	0,999740
After mission 5	0,999596
After mission 6[1]	0,999430

[1] The 6th mission does not take the ground storage into account

After the 6 missions (including 6 launches and 12 months continuous operation in space), the OBC still has a reliability of 99,943%. As a comparison, the reliability of the (single lane) OBC flown on the ESA IXV mission (108 minutes in total), showed a reliability figure of 99,9943%.

A graphical overview of the mission reliability, as calculated in the parts count method, can be seen in the figure below.

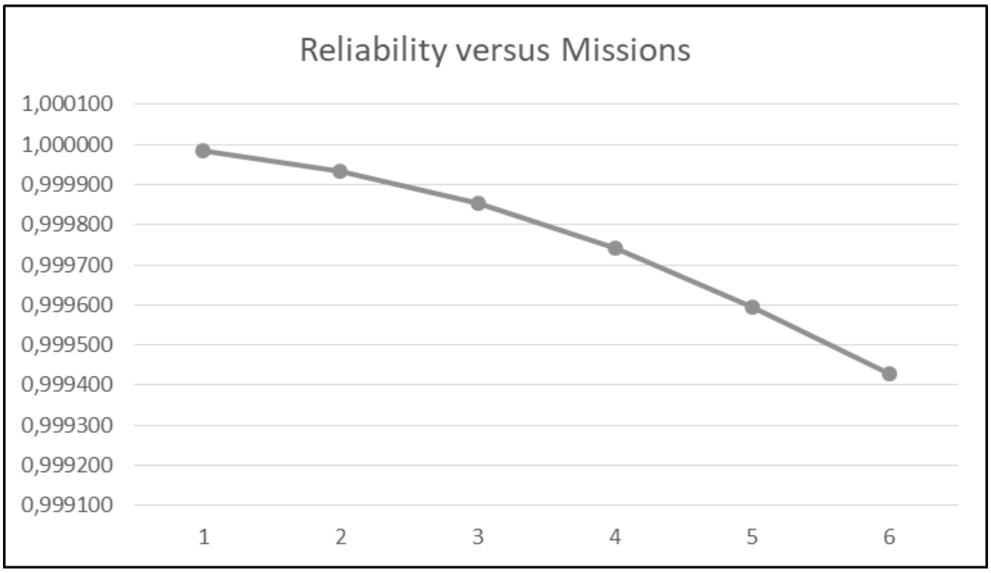

Figure 4: Space Rider OBC mission reliability

4. Conclusion

The powerful computer supplies the spacecraft with the intelligence necessary for a (multiple) safe return flight, calculating the optimum angle for re-entering the atmosphere and making a controlled landing possible. The computer is derived from the successful ADPMS On-Board Computer for high reliable autonomous satellites. The design and qualification approach takes into account the six subsequent launches enabling the Space Rider and future missions. It is also selected as the cornerstone for the QinetiQ Space small satellite platform and is being designed in for various mission applications (such as IBDM) due to its high flexibility (can be used in various redundancy schemes). Thanks to its modular design it can easily be extended with additional functionality, such as additional interfaces (HPC) or additional functionality (MMM).

DOI: 10.13009/EUCASS2019-996

The paper shows that the QinetiQ Space On-Board Computer solution provides a high reliability, even for a multi-launch application (re-usability). With a dual lane reliability of 99,943% after 6 consecutive Space Rider missions, the QinetiQ Space On-Board Computer is ready to be integrated onto many other spacecraft.

References

[1] K. Puimège, E. Jansen, S. Landstroem, D. Hardy, "The ADPMS Experience - An advanced Data & Power management system for small satellites," Proceedings of the 4S Symposium: `Small Satellite Systems and Services,' Chia Laguna Sardinia, Italy, Sept. 25-29, 2006, ESA SP-618

[2] K. Puimège, J. Bermyn, "The ADPMS Ready for Flight: An Advanced Data & Power Management System for Small Satellites and Missions," Proceedings of the 23nd Annual AIAA/USU Conference on Small Satellites, Logan, UT, USA, Aug. 10-13, 2009, SSC09-V-4

[3] F. Preud'homme, S. Dussy, N. Fleurinck, S. De Cuyper, "A high reliability computer for autonomous missions, demonstrated on the ESA IXV flight," Proceedings of the 66th International Astronautical Congress (IAC 2015), Jerusalem, Israel, Oct.12-16, 2015, paper: IAC-15-D2.6.5

[4] M. Caporicci, P. Urmston, O. Gracia, "IBDM: The International Berthing Docking Mechanism for Human Missions to low Earth Orbit and Exploration" Proceedings of the 61st International Astronautical Congress (IAC 2010), Prague, Czech Republic, Sept.27-Oct.1, 2010, paper: IAC-10-C2.7.9

[5] D. Claessens, F. Preud'homme, B. Paijmans, "Development of the International Berthing Docking Mechanism compatible with the International Docking System Standard" Proceedings of the 63rd International Astronautical Congress (IAC 2012), Naples, Italy, Oct.1-5, 2012, paper: IAC-12-B3.7.9

[6] European Space Agency. 2019. Space Transportation (https://www.esa.int/Our_Activities/Space_Transportation/Space_Rider)

[7] J. Lienig, H. Bruemmer. 2017. Fundamentals of Electronic Systems Design. Springer International Publishing. p. 54

[8] Various. 1991. Reliability Prediction of Electronic Equipment, MIL-HDBK-217F + Notice 2

[9] European Space Agency. 2019. Space Rider Fact Sheet (https://esamultimedia.esa.int/docs/space_transportation/Space_Rider_factsheet_HiRes_ok.pdf)