# Very high-speed space communication networks for building the next generation of advanced exploration and military spacecraft*

Prof. Dr. V. David Sánchez A., Ph.D.
Brilliant Brains, Palo Alto, California
November 2023

## Abstract

For well-known reasons, the use of standards for the design and development of computing systems is highly beneficial, in particular the use of standards to link system components and assemble high-performance component networks when building mission-critical next gen space exploration and military spacecraft. The SpaceFibre standard [1] is an up to 6.25 Gbps per lane, on-board network technology for spaceflight applications, successor of and compatible at the packet level to the previously established SpaceWire standard [2], which incorporates quality of service (QoS) using virtual channels and integrates fault detection, isolation and recovery (FDIR) support. Moreover, low latency broadcast messages are provided in SpaceFibre which enable the rapid event signaling, error reporting, and system time information distribution. The low protocol overhead is independent of the unrestricted packet size. Data re-transmission for recovery is point-to-point with an extreme fast reaction time of less than 1us. SpaceFibre networks can be assembled using SpaceFibre routers, ASICs, and IP cores for their implementation into space-qualified SoCs/FPGAs, cf., e.g. [3, 4].

A good example of spacecraft using SpaceWire interfaces is the one being flown in the BepiColombo joint mission [5] of the European Space Agency (ESA) and the Japan Aerospace Exploration Agency (JAXA) to the planet Mercury. It is made of three spacecraft: the Mercury Polar Orbiter (MPO) to study the planet's surface and internal composition, the Mercury Magnetospheric Orbiter (MMO) to study Mercury's magnetosphere, and the Mercury Transfer Module (MTM) to carry both, the MPO and MMO spacecraft to the planet Mercury. The MMO and the MPO will separate from the MTM when it reaches Mercury. Figure 1 shows on the left side, first on top the BepiColombo spacecraft separating from its final rocket stage after its launch from Earth to Mercury, in the middle the launch configuration to be stacked atop the Ariane V launch vehicle, and at the bottom of the left side from top to bottom: the JAXA's Mercury Magnetospheric Orbiter (MMO), the spacecraft's sunshield, which covers the MMO during the interplanetary cruise, ESA's Mercury Planetary Orbiter (MPO), and finally the ESA's Mercury Transfer Module (MTM). Figure 1 shows on the right side the cruise from planet Earth to Mercury and its distinct orbits. The mission was launched on October 20, 2018. The planned MMO and MPO insertion date is December 5, 2025 for both orbiters after a few gravity assist flybys around the Earth, Venus, and Mercury.

Using SpaceWire interfaces, the spacecraft on-board computer has access to the SpaceWire routers and payload instruments for the purpose of configuration and control. Figure 2 shows on the left and right the SpaceWire-based data-handling architectures of the BepiColombo MMO and MPO spacecraft respectiviely. In the case of JAXA's MMO, the mission data processor consists of two data processing units, each of which contains a central processing unit (CPU) and a SpaceWire router.

*This abstract has been granted permission for public release. The author has been designing and building advanced scalable mission-critical concurrent computer systems and custom-chip-interconnects for parallel computers and networks [6] as well as using multiple System-on-Chip (SoC) [7, 8] and neuro-chips [9] for NASA and DoD classified programs.

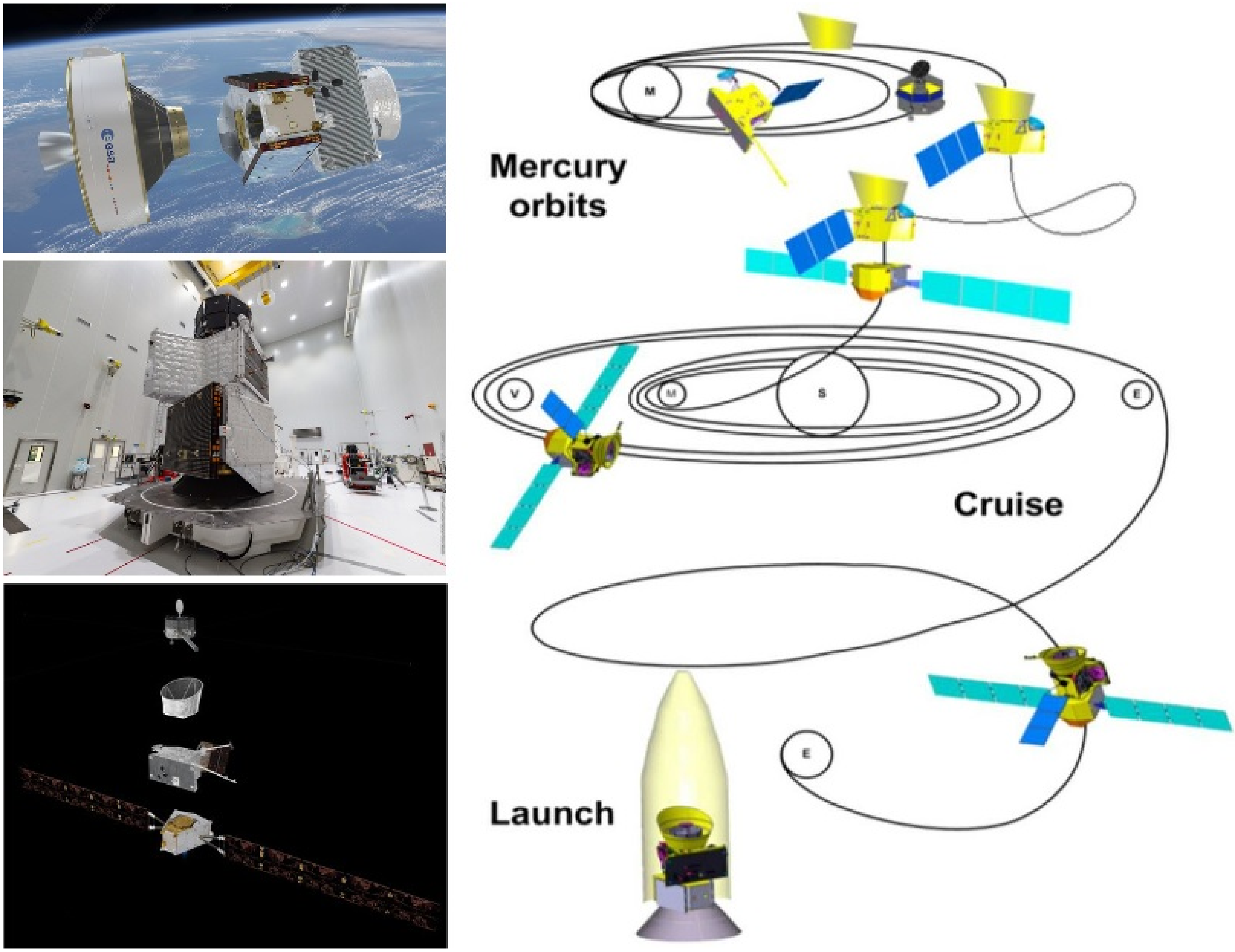



Figure 1: BepiColombo Spacecraft Stack and Cruise Orbits from planet Earth to Mercury [ESA/JAXA]

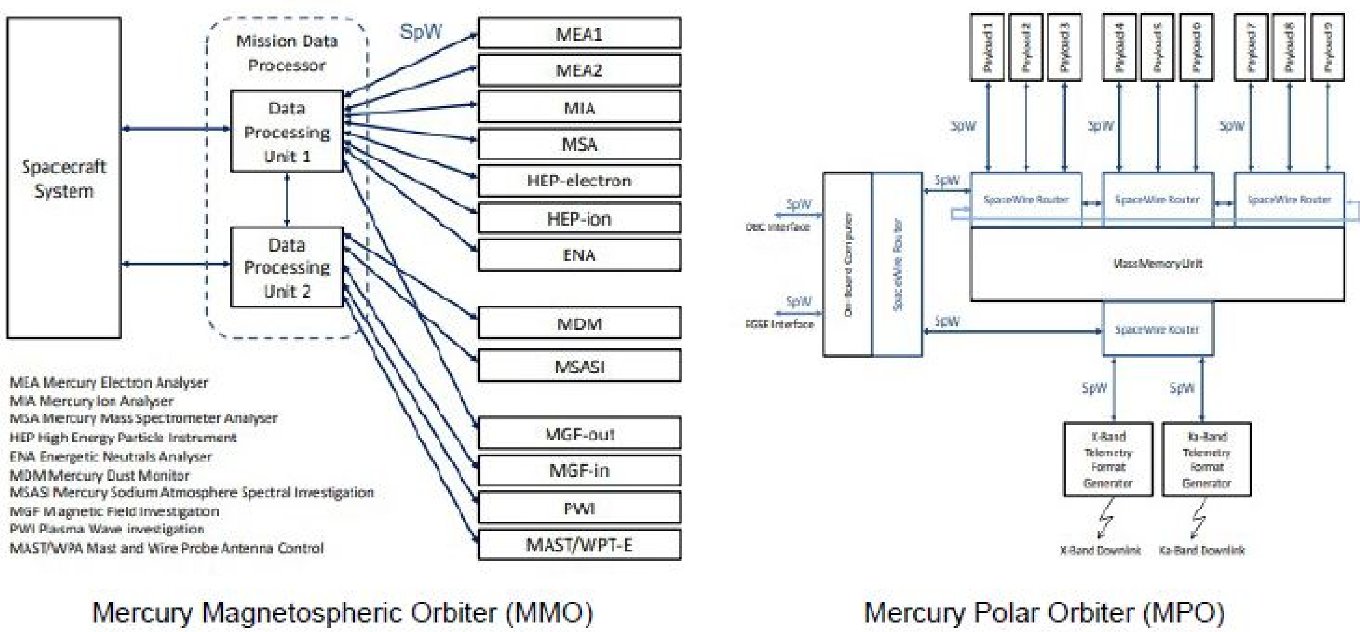
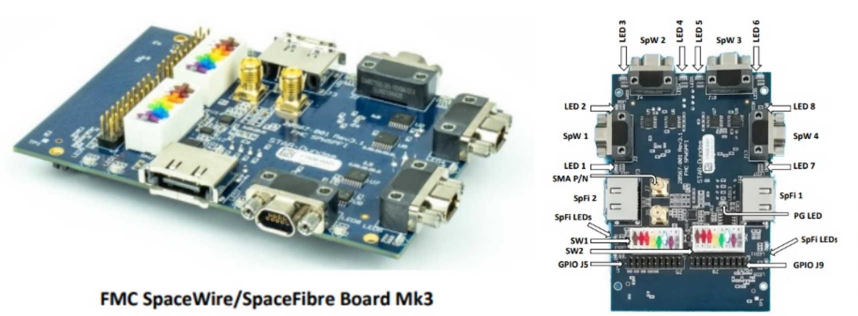



Figure 2: SpaceWire-based data-handling architectures of the BepiColombo MMO and MPO spacecraft [10]


Figure 3: SpaceWire and SpaceFibre router ASICs [STAR-Dundee, Atmel]




| IP Core | Virtex-5QV XQR5VFX130 | Spartan-6 XC6SLX150T | Kintex-7 XC7K325T | Ultrascale KU060 | RTG4 RT4G150 | RT-PolarFire RTPF500T |
|---|---|---|---|---|---|---|
| Single-Lane Interface (1) | 3.1%<br>3.3% | 3.4%<br>1.4% | 1.1%<br>0.7% | 0.6%<br>0.4% | 2.5%<br>1.8% | 0.7%<br>0.6% |
| Multi-Lane Interface (2) | 9.6%<br>11.7% | 8.8%<br>5.1% | 3.3%<br>2.2% | 2.0%<br>1.4% | 9.0%<br>6.8% | 2.8% (4)<br>2.1% |
| Single-Lane Router (3) | 40.5%<br>40.3% | 38.4%<br>16.8% | 14.5%<br>8.0% | 8.6%<br>4.9% | 31.7%<br>21.2% | 9.2% (4)<br>7.4% |

% LUTs
% FFs

- Triple-mode redundancy (TMR) is not included
- Specific IP core configurations:
  (1) 2 virtual channels
  (2) 4 lanes and 2 virtual channels
  (3) Router with 8 SpFi ports (2 virtual channels each) and internal RMAP configuration port
  (4) Estimated values

Figure 4: SpaceWire and SpaceFibre connectors (left and center), FPGA utilization of SpaceFibre IP Cores (right) [STAR-Dundee]

Each MMO's instrument is connected to the mission data processor over a point-to-point link. Due to the low power and mass requirements, a special version, a 2 Mbps SpaceWire was implemented. In the case of ESA's MPO, the SpaceWire routers are daisy-chained, its nine science payloads are connected to three of these routers integrated to the mass memory unit. The routers are also connected over SpaceWire to the on-board computer. Another router connects the mass memory unit to the X- and Ka-band downlink telemetry. Further SpaceWire links connect the on-board computer to the electronic ground support equipment (EGSE).

SpaceWire is an space engineering standard (ECSS-E-ST-50-12C) that provides a unified high speed data-handling infrastructure for connecting together sensors, processing elements, mass-memory units, downlink telemetry subsystems and EGSE equipment [2]. The Standard specifies the physical interconnection media and data communication protocols to enable the reliable sending of data at high-speed, between 2 Mbps and 400 Mbps, from one unit to another. SpaceWire links are full-duplex, point-to-point, serial data communication links. SpaceFibre is an ESA standard (ECSS-E-ST-50-11C) for very high-speed serial communication links [1]. It is compatible with SpaceWire at the packet level, but the data-link and physical layers are completely re-defined in order to have advanced Quality-of-Service (QoS) and Fault Detection, Isolation and Recovery (FDIR) features. SpaceFibre is the successor of, and is compatible with the very popular SpaceWire protocol but allows 15 times higher data rates per lane, up to 6.25 Gbps and beyond. It has fault detection and recovery as well as deterministic communication mechanisms built into the hardware and can operate via copper and optical fibre. Figure 3 shows examples of SpaceWire and SpaceFibre router ASICs. That 8-port SpaceWire router chip, the Atmel AT7910E SpW-10X router [11], is being flown with the BepiColombo mission to Mercury. Figure 4 shows on the left and center an FMC SpaceWire/SpaceFibre board displaying the difference in the connectors for both interface port types and on the right the FPGA usage of some relevant SpaceFibre IP Cores.

Now let us turn briefly to military spacecraft. World-wide, weapons are being developed by current friends and adversaries that could disrupt or deny civil and military space services. Those services

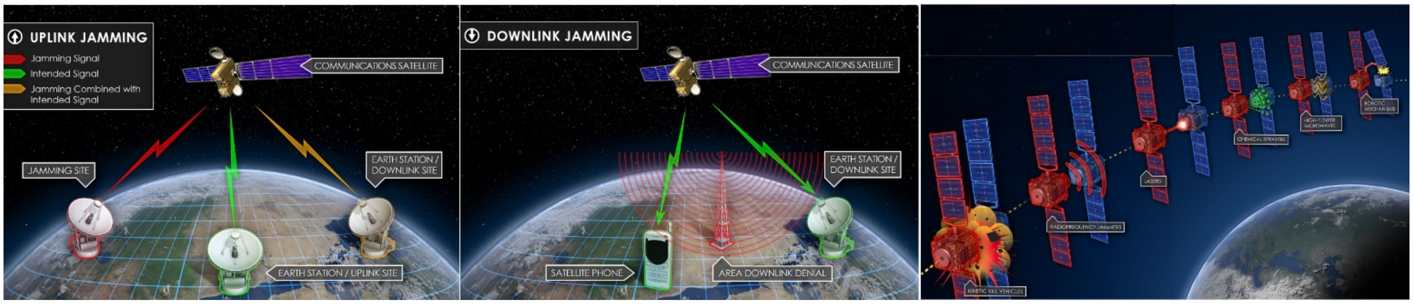



Figure 5: Some threats and weapons against space-based assets [12]

could be damaged or destroyed either temporarily or permanently depending on the weapon used. Attacks could include jamming global navigation and communications satellites used for command and control. The dual-capability of some on-orbit technologies and space systems is worth mentioning, for satellite servicing and debris removal on the one end, and satellite damage on the other, thus advancing counterspace capabilities. Physical and cyber attacks against ground sites and infrastructure that support space operations can also threaten those space-based services. Figure 5 shows some threats and weapons against space-based assets [12]. Space weaponry includes space-based anti-satellite systems that deliver a spectrum of reversible and non-reversible counterspace effects, from simple interceptors to complex space robotic systems. For example, kinetic kill vehicles, radiofrequency jammers, lasers, chemical sprayers, high-power microwaves, and robotic mechanisms can be deployed.

A comprehensive strategy for the U.S. Space Force (USSF) is detailed in [13] highlighting objectives, providing funding and architecture plans to achieve the objectives, identifying needed units and resources, and identifying personnel end-strength requirements for the USSF. In particular, to satisfy the requirements of the Joint Force and the Armed Forces, space capabilities need to be deployed. And for that purpose, the Force Design Architect for Space Systems of the Armed Forces is the Chief of Space Operations (CSO) designated by the Secretary of Defense. A recent review of the space policy and the description of the U.S. DoD's approach to protecting and defending space systems and protecting the Joint Force from adversary hostile use of space is provided in [14]. To assure critical space-based missions; strengthen our ability to detect and attribute hostile acts in, from, and to space; and, to protect the U.S. Joint Force from adversary hostile uses of space, the DoD FY 2024 budget requests the largest space budget ever of $33.3 billion, reflecting an approximate 13 percent increase in space funding over the FY 2023 budget request. In particular, the USSF is to boost its National Security Space Launch (NSSL) program by almost doubling the number of launches from 12 in fiscal year 2023 to 21 in 2024 via the United Launch Alliance (ULA, 11) and SpaceX (10) [15]. Missions included are for the Space Development Agency (SDA), the Space Systems Command (SSC), the National Reconnaissance Office (NRO), the Defense Advanced Research Projects Agency (DARPA), the Global Positioning System (GPS) modernization, missile warning and space research and reconnaissance as well as undisclosed USSF missions. In this report, the methodology together with concrete examples how to design and verify advanced next gen spacecraft for universe exploration and military space applications based on very high-speed communication links and networks are discussed in detail.

## References

[1] European Cooperation for Space Standardization. *Space engineering – SpaceFibre – Very high-speed serial link*, ECSS-E-ST-50-11C, 15 May 2019.

[2] European Cooperation for Space Standardization. *Space engineering – SpaceWire - Links, nodes, routers and networks*, ECSS-E-ST-50-12C, 31 July 2008.

[3] S. Parkes et al. *SpaceWire and SpaceFibre on the Microsemi RTG4 FPGA*, Proc. of the 2016 IEEE Aerospace Conference, Big Sky, Montana, 5–12 March 2016.

[4] A. Gonzalez et al. *A Complete Set of SpaceFibre IP Cores in the New Generation of FPGAs for Space*, Proc. Data Systems in Aerospace (DASIA) 2023 Conference, Sitges, Spain, 6–8 June 2023.

[5] European Space Agency. *bepicolombo – Investigating Mercury's Mysteries*, BR-335, May 2017.

[6] V.D. Sánchez. *A Parallel Distributed Architecture for Vision and Telerobotics (in German)*, in M. Baumann and R. Grebe (Eds.), Parallele Datenverarbeitung mit dem Transputer, Berlin, Springer-Verlag, Reihe Informatik aktuell, 295-303, 1993.

[7] V.D. Sánchez. *Colonization of the Red Planet*. November 2022.
https://profdrvdsaphd.lima-city.de/documents/MarsColonization.pdf.

[8] V.D. Sánchez. *Hochentwickelte Hyperschalltechnologien für Raumfahrt- und terrestrische Anwendungen*. August 2023.
https://profdrvdsaphd.lima-city.de/documents/AdvancedHypersonic.pdf

[9] V.D. Sánchez et al. *The Design of a Real-Time Neurocomputer Based on RBF Networks*. Neurocomputing, 20, 111-114, 1998.

[10] STAR-Dundee Ltd. *SpaceWire User's Guide*, 2012.

[11] Atmel Corp. *SpW-10X SpaceWire Router AT7910E*, 2008.

[12] National Air & Space Intelligence Center. *Competing in Space*, December 2018.

[13] Department of the Air Force. *Comprehensive Strategy for the Space Force*, August 2023.

[14] Department of Defense. *Space Policy Review and Strategy on Protection of Satellites*, September 2023.

[15] U.L. Harpley. *Space Force Plans 21 National Security Launches in 2024*, Air & Space Forces Magazine, November 02, 2023.