HIGH-PERFORMANCE PAYLOAD DATA HANDLING AND SPACE SECURITY SYSTEM

Boris Penné[1)], Carsten Tobehn[1)] , Rainer Rathje[1)], Harald Michalik[2)]

[1)]OHB-System AG, Universitätsallee 27-29, D-28359 Bremen, Germany
[2)] IDA TU-Braunschweig, Hans-Sommer-Str. 66, D-38106 Braunschweig, Germany
Contact: penne@ohb-system.de

1 ABSTRACT

Future Earth observation missions with increasing spatial and spectral resolutions (0,5m to 5m using 8 to 200 channels) set increasing requirements for on-board payload data management in terms of high data rates and large data volumes. The downlink capacity on the other hand is a limiting factor which can only be overcome by recently new technologies within the transmitter technology on one side and the data pre-processing on-board on the other side.

A further domain aspect by transmitting Earth observation data to earth is the confidentiality of the data (e.g. commercial or GMES missions).

This paper presents an advanced and innovative architecture for spaceborne high speed payload data management subsystem designed in a modular approach in order to scope with different requirements in terms of data volumes/rates and redundancy approaches under different security levels. The entire data management chain beginning from the output of the imaging sensor until the downlink will be presented. The chain introduces the advantages of the IEEE 1355 space wire standard to provide scaleable redundancy and performance.

The modules of the chain like on-board data processing (LEON processor) feature data compression, data evaluation and truncation of data to the area of interest as well as data storage, data formatting (CCSDS), data encryption and downlink. The performance of the chain reaches more than 10Gbit/s input rate and an output rate of 740Mbit/s using dual polaristation techniques at X-Band at considerable low resources of about 50W and 40kg in a redundant configuration.

2 INTRODUCTION

Future missions for high resolution (spatial, spectral and radiometric) earth observation will have significant increased performance requirements for onboard data processing.

High performance of data storage and downlink is already required for typical missions today. The following presents a modular system architecture as being used for Kompsat II, SAR-Lupe, and MSRS but also other project running at OHB-System.

Major technology driver are:
1) high speed data processing
2) modular & scaleable design
3) cost effectiveness

Data rates can easily reach 70 up to 1.800 Mbit/s per spectral channel for a ground resolution of about 5 to 1 meter at 10 bit spectral resolution.

Assuming 5 meter ground resolution and a scene size of 50x700km, one would have to store already 84 Gbit per spectral channel on-board the satellite. For 12 channel that aims into a storage capacity of 1.008Gbit, which is demanding in terms of power issues. Assuming further a down-link capacity of 600-700 Mbit/s (actual technology) one would need 1 hour for the downlink. This short example shows, that high speed data processing on-board the spacecraft is necessary to reduce the data amount to the really needed information part. One example for this pre-processing is data compression, other examples are data evaluation and truncation to the area of interest.

A modular design is desired to provide maximum flexibility in order to insert other processing elements into the processing chain. For example there might be the need to truncate data in front of the compression or the data storage is not required as the mission wishes online downlink only (GEO applications). Further, programmatic aspects can lead to a separation of the processing chain into different manufactures.

A scaleable design is desired to easily adapt the processing chain to different numbers of spectral channels or missions requiring high redundant design.

But it leads to a cost effective design. However, for very dedicated missions one can still combine elements of the processing chain like compression, storage and channel coding. This combination would give an optimised mass & power budget. The system architecture for a modular scalable high speed processing chain is given in Figure 1.

The Camera Unit itself is not part of the processing chain and shown for overview purposes. The Camera Unit contains the detectors and provides finally the A/D converted digital signal stream as input for the processing chain.

The processing chain consist of:
1) Data Pre-processing Unit (Compression)
2) Data Storage Unit
3) Channel Coding Unit

A Space Wire standard can be integrated to facilitate the construction as the backbone of the payload data system to which all kind of different blocks can be connected. The Space Wire standard specifies the physical interconnection media and data communication protocols to enable the reliable sending of data at high-speed (between 2 Mbit/s and 400 Mbit/s) from one unit to another. It promote compatibility between the data handling equipment and subsystems. Space Wire links are full-duplexed, point-to-point, serial data communication links. The Space Wire is able to support many different processing architectures using the point-to-point links and Space Wire routing switches. An architecture can be tuned to the different mission requirements and specifications.

The EGSE dedicated to the processing chain has also to provide a modular & scaleable design under cost effectiveness. The EGSE is designed to support a wide range of test on unit level as well as on chain level. Furthermore it is used to verify the data output of the X-Band transmitter.

Moreover the Space Security System offers all the functionality and performance required for reliable and secure missions of today and tomorrow. The system performs all the tasks from key management, authentication, real-time encryption and decryption. These tasks provide protection of all satellite and ground links up to level SECRET. Secured links are from the On-board Computer TMTC function (incl. Inter-Satellite-Links) and from the payload data handling to ground.

3 HIGH-PERFORMANCE PAYLOAD DATA HANDLING SYSTEM

3.1 Data Pre-Processing & Compression

Applications for data pre-processing are for example autonomous object/event detection using a wide field sensor. After on-line detection of events, the selected area will be investigated in more detail using a high resolution sensor steered automatically to the area of the event by the spacecraft itself. This technology is used for example for an autonomous fire detection system studied by OHB-System. The information regarding the location of the fire is provided within 5 minutes in order to enable fire fighting in the early stage.

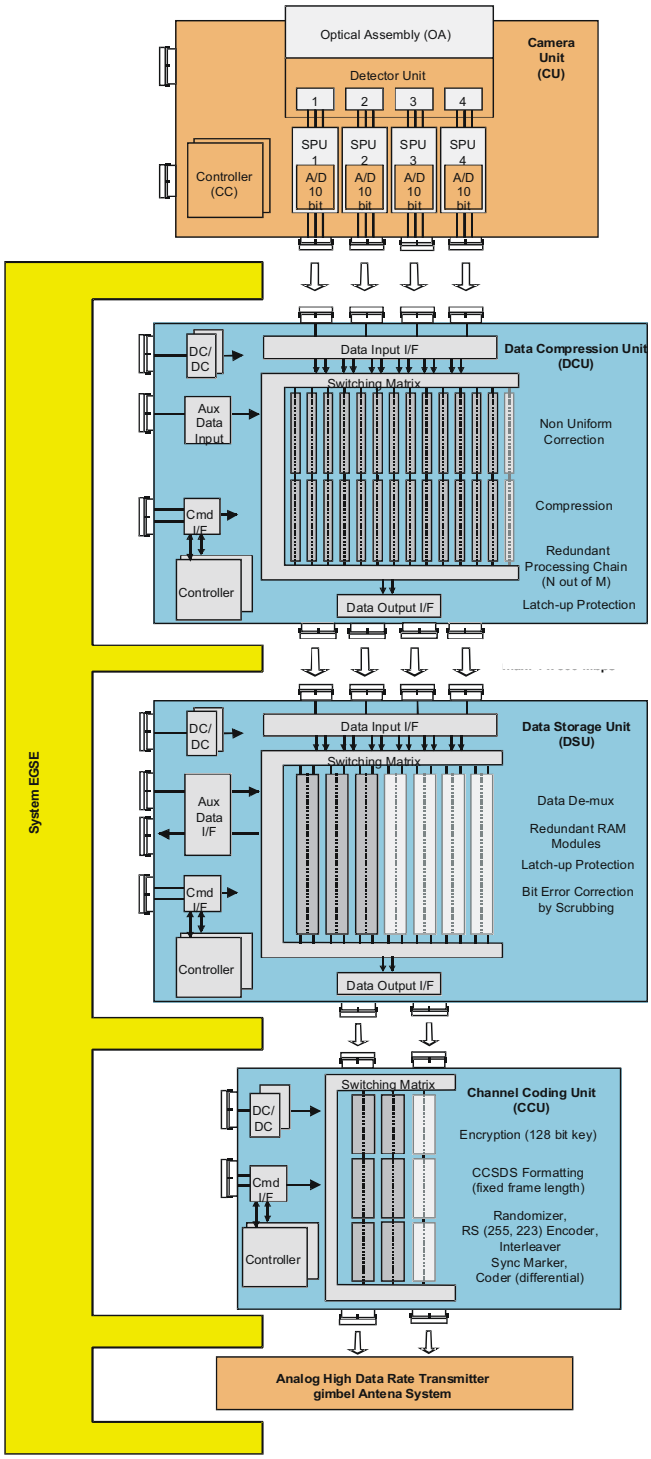

Figure 1: System Architecture

Another example is the online detection of clouds and the resulting selection of cloud-free scenes, e.g. by re-pointing of the spacecraft or instrument mirror. This processing must be performed in real time to close the high precision control loop.
The technology for this pre-processing unit is derived from the VSOP design by OHB-System as described hereafter. Data pre-processing is mainly performed in order to decrease the data volume for downlink issues.

For maximum data reduction one can follow a two step approach:

1) truncate the data to the area of interest
2) compress the (remaining) data

An example for such kind of pre-processing is given in Figure 2.

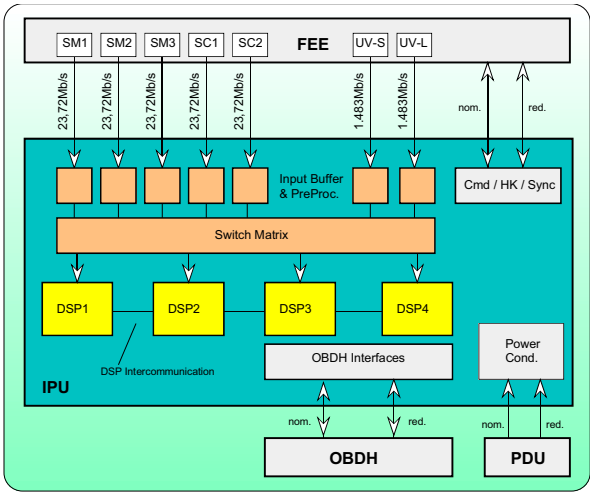

Figure 2: Real-time Pre-Processing with 4 DSPs

The Data Compression Unit uses the JPEG 2000 Wavelet algorithms. For most optical instruments one has to perform data calibration before loss compression. The "Non-uniform correction" algorithm as presented in front of the compression is such calibration task.
The known non-uniformity of the detector pixels is eliminated by a linear transformation. Thereafter the compression starts.
Each spectral channel is compressed independently. This allows the introduction of one or more redundant compression lines and also the adaptation to sensors with more spectral channels without major change.
The "Switching Matrix" is provided to allow redundancy switching but also to enable compression by-pass. The mission operator can decide whether to receive a compressed image or the original.
An example of the core technology used for pre-processing is the VSOP board. This DSP single board computer (160 mm x 233.35 mm) uses the latest high density package technology (CQFP, CERPACK) usable in space.

Figure 3 shows the DSP-Board equipped with commercial components and Figure 4 the VSOP Block diagram.

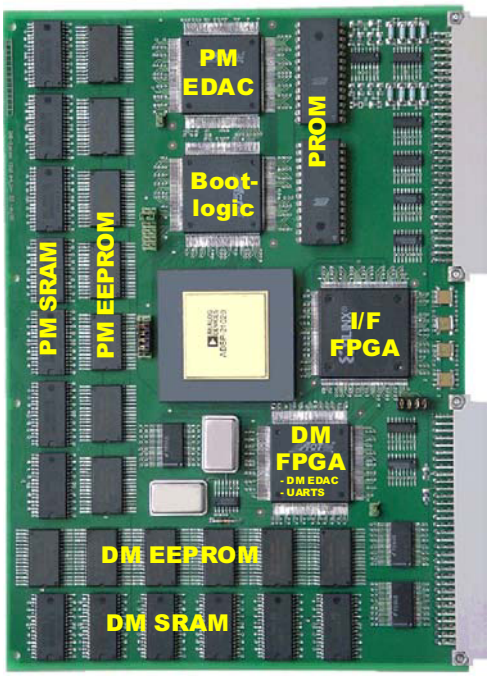

Figure 3: VSOP Board Layout with Commercial Components

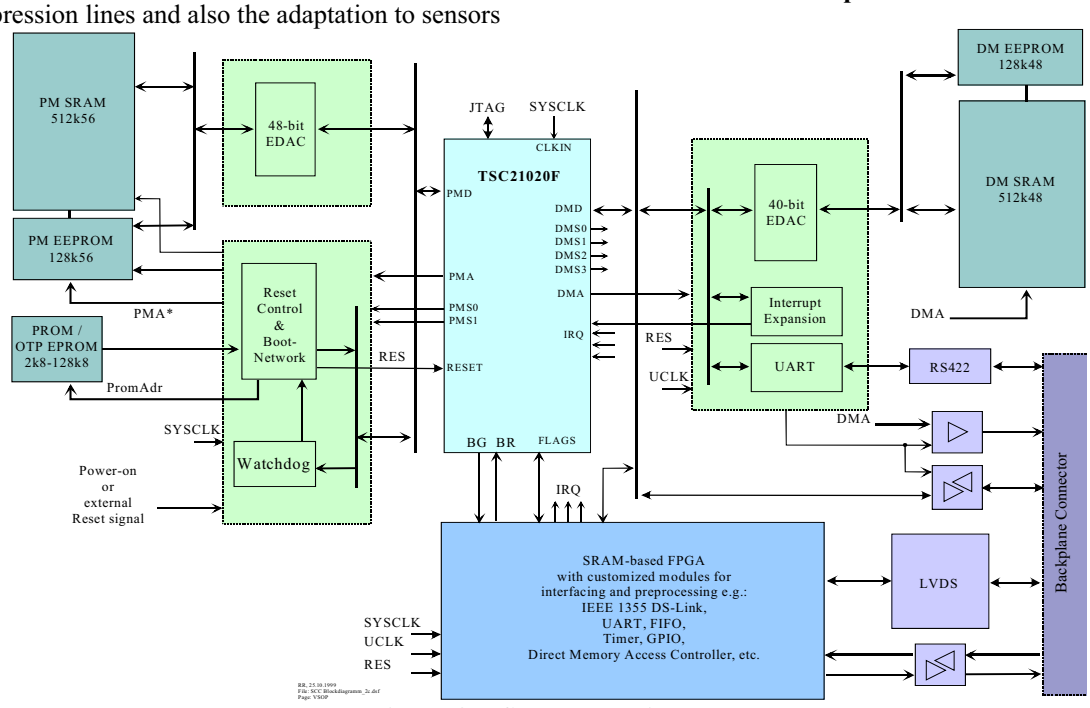

Figure 4: VSOP Block diagram

The program and data memory areas are populated with both volatile (SRAM) and non-volatile (EEPROM) memory chips.
The executable code is stored in EEPROM and is copied into PM SRAM during the initial boot phase. The total SRAM memory net capacity is 3 MByte programme memory (PM) plus 2.5 MByte data memory (DM).
The SRAM, and optional the EEPROM, is protected via two dedicated error detection and correction (EDAC) circuitry's to be immune against sporadic bit-flips by single event upsets (SEU).
Interface components (RS422 and LVDS) are already available on-board. The interface logic itself will be implemented in a SRAM based FPGA, that is available in a space qualified version.
This FPGA can be programmed in VHDL, schematic entry or using already developed IP cores.
This programming can be updated frequently and even during the operation of the board. Because of the final radiation environment a totally radiation tolerant design for the Computer was targeted and achieved. All components are selected for proven radiation tolerance and for latch-up immunity.
The VSOP provides 30 MFLOPS sustained and 45 MFLOPS peak performance. A set of VSOP boards can easily be interconnected to form a multiprocessor architecture for dedicated applications.

3.2 Data Storage Unit

The design of the Data Storage Unit (DSU) follows the rules defined for modularity and scalability. The design is based on space proven technology.

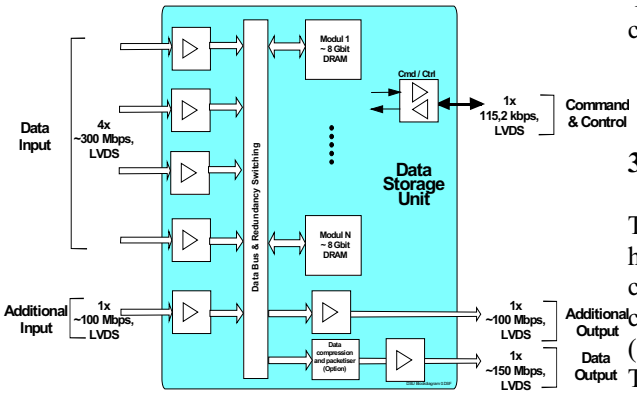

Figure 5: DSU Block diagram

The DSU (Figure 5) handles the image data coming from the Pre-processing Unit. The input data is supplied multiplexed like for the Pre-processing Unit itself. The design of the input circuitry was used twice for cost saving reasons but also allows, that the DSU can be connected directly to the Camera Unit output.
The DSU provides an auxiliary input/output interface. It is used for off-line data pre-processing. These are attitude and position data collected during imaging to be used for data geo-correction on ground. Figure 6 shows the Memory Module PCB of the DSU. A modular design was developed to gain highest reliability. Each Memory Module can be equipped with up to 256 GBit. One redundant Module is introduced to allow the complete loss of one Module.

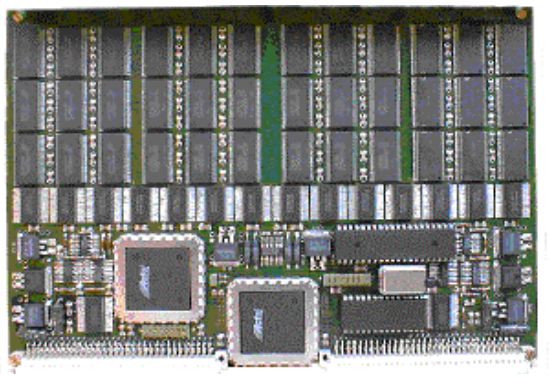

Figure 6: DSU module PCB Layout (Commercial Layout)

Standard measures against radiation effects are implemented. Check symbols are generated during data recording for each word group. These check symbols allows the correction of the corrupted data.
The DSU performs automatically memory scrubbing evaluating the check symbols and corrects possible bit errors in pre-defined intervals.
If a word group is detected to be permanent faulty, only this word group is unmasked. Only a very low memory part is lost in this case.
Further, latch-up protection is implemented to avoid DRAM damage. The switching matrix allows the redundancy switching but also a data bypass.
If for example the compression is enabled, the DSU can be bypassed for on-line down-link.

3.3 Channel Coding Unit

The Channel Coding Unit performs encryption of a high speed data stream together with telemetry channel coding according to recommendations of the consultative Committee for Space Data Systems (CCSDS).
The Channel Coding Unit is a high speed data processing unit that operates on two independent input data streams. The maximum input data rate per pipeline channel equals 2x216 Mbit/s, the output data rate is 2x250 Mbit/s constant.

Figure 7: Channel Coding Unit Core Layout

For the data on both data streams the CCU features:

Encryption: The Data will be encrypted (on demand) in the IDEA standard with 128 bit key length in real-time. IDEA is a world-wide available symmetric encryption standard and has not been cracked up-to-now. T-Des, AES or costumer specific encryption can be used if desired. The encryption itself is performed by dedicated hardware (data encryption module, DEM).

Reed-Solomon encoding: Behind the encryption the data stream will be Reed-Solomon (RS) en-coded. From code blocks of 223 bytes 32 check symbols are generated to provide error detection and correction capability for up to 16 Byte errors. Five of theses RS-encoders are available in parallel for every data stream and are operated in a byte-by-byte time multiplexed manner (interleaving). By this burst errors equal to 80 symbol (640 bit) duration can be corrected.

Header generation: The data is subdivided into packets of equal length, each packet owns a header information. Most of the header information is provided to the CCU via an external interface and the CCU collects and inserts this information into the data stream in real time.

ASM insertion: Each packet is provided with an asynchronous synchronisation marker, a fixed identifier that leads every packet.

Randomiser: All data except for the ASM are randomised in order to provide sufficient 1-0 transitions for transmission.

The CCU is controlled via a redundant bi-directional serial interface for command and control. The interface standard is RS422. It can be mounted together to form a combined case. Since no electrical interconnection exists between the cases, there is no single point of failure for the combined unit.

The CCU provides fast, CCSDS compatible and redundant 128bit Reed-Solomon coding with real-time IDEA encryption for 2x250 Mbit/s output data rate.

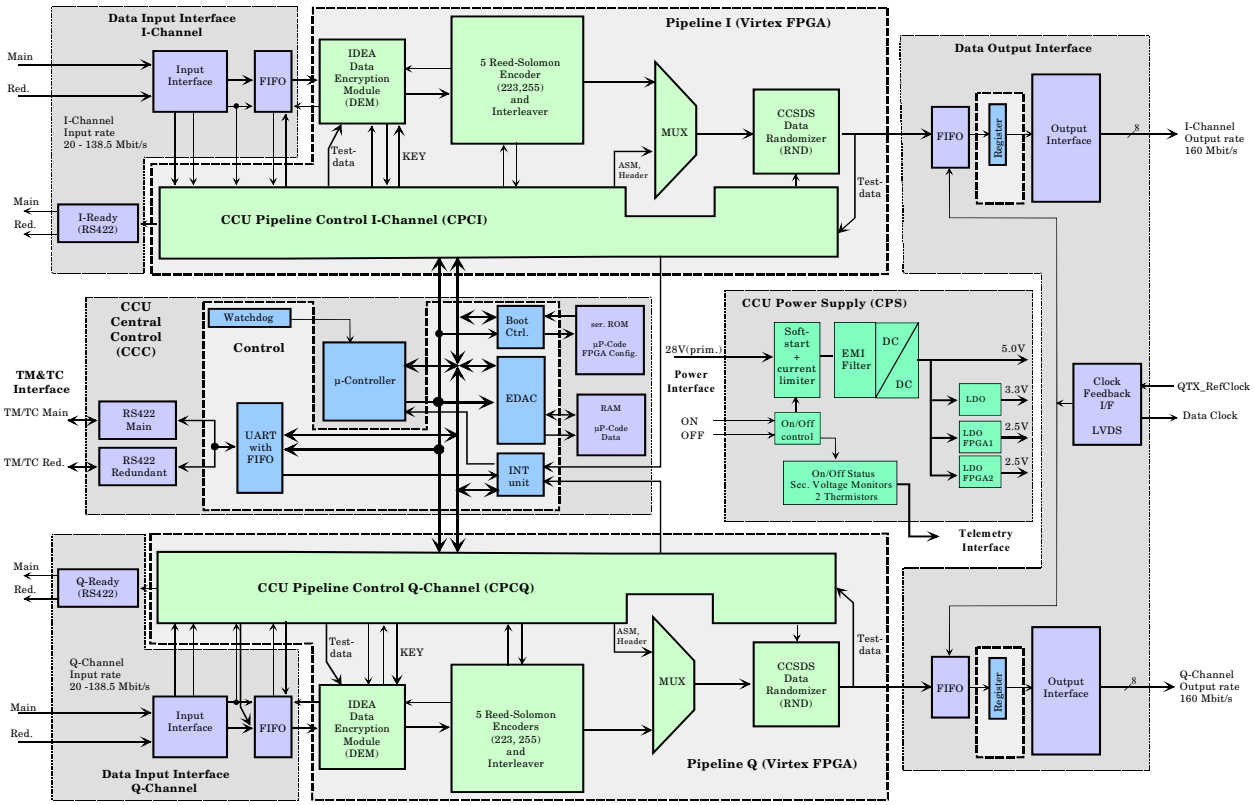

Figure 8: Block diagram of Channel Coding Unit Core

3.4 Transmitter

For the payload data downlink of standard X-band transmitter with a total data rate of up to 622 Mbit/s for 8-PSK and 740 Mbit/s with dual polarisation were considered (as will be used on Orbview 5). Due to the ITU bandwidth limitations of 325 MHz, we propose a concept based on up to 370 Mbit/s transmitters, one in horizontal and one in vertical polarization. A third transmitter is used for redundancy of one of the other two.

3.5 EGSE

The EGSE is a high-speed data test system for advanced high-speed data processing chains including downlink subsystems onboard of earth observation satellites. The EGSE is designed to support the tests demanded by the various test and integration levels:
Single Unit tests: the EGSE acts as unit tester for the processing chain elements like Pre-processing Unit, Data Storage Unit and Channel Coding Unit but also the analogue X-Band Transmitter.

1. Sub-system test: the EGSE allows the test of the entire processing chain.
2. System tests: the EGSE provides interfaces to the spacecraft system EGSE in order to support the complete spacecraft test after integration of all assemblies.

Figure 9 shows a version of the complete integrated test system where all components are located in three 19'' racks.

Figure 9: EGSE Assembly

The EGSE provides stimulus serial data interfaces and accepts 8 bit parallel data at rates of up to 2x250 Mbit/s for testing the digital Channel Coding Unit.
Furthermore the EGSE generates stimulus 8 bit telemetry data streams synchronously to a input clock provides by a high data rate QPSK X-Band Transmitter at rates of up to 2x160 Mbit/s. A integrated X-Band Receiver provides at its output serial data and clocks, separate for I- and Q-Channel, to the Channel Decoding Unit (CDU).
The data can be written to a PC for evaluation purposes or send to a Bit Error Tester. The EGSE provides a complete Bit Error Test-Set, which is selectable via the Selector-Unit of the CDU. The EGSE is completed with measurement equipment to evaluate signal parameters and qualities for high speed digital signals as well as RF signals up to 18 GHz. The functional block diagram of the test set-up is presented in Figure 12. The Bit Error Test is one of the most important tests to verify the performance of the processing chain in combination with the transmitter.
All operations and modes are commanded and controlled by a man machine interface which is connected to the CDU via a built-in LAN interface. This LAN interface provides a complete access of a higher priority test system to the EGSE working as a front-end test system to the spacecraft payload. The CDU of the EGSE is a high-speed data ingest system.
The CDU system consists of a high performance PC and a high performance SCSI controller with a associated hard disk. The high-rate Telemetry Simulator (TSB) and two High-Speed Interface Boards (HSIB) are PC PCI slot card and are installed in the CDU PC system.

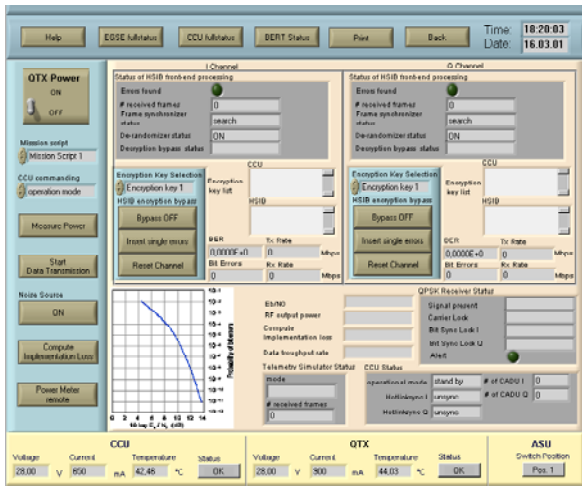

Figure 10: Bit Error Test Setup – MMI Mask

The HSI Board accepts serial data and clock inputs at rates up to 2x160 Mbit/s and performs frame synchronisation, de randomising, error correction and deciphering of two simultaneous data streams.
The CDU archives selectable frame data or row bits with optional quality annotation to a SCSI hard disk array. Error corrected frame data or row bits are available for further processing immediately following a recording session. The HSIB provides real-time data quality statistics for link performance monitoring.

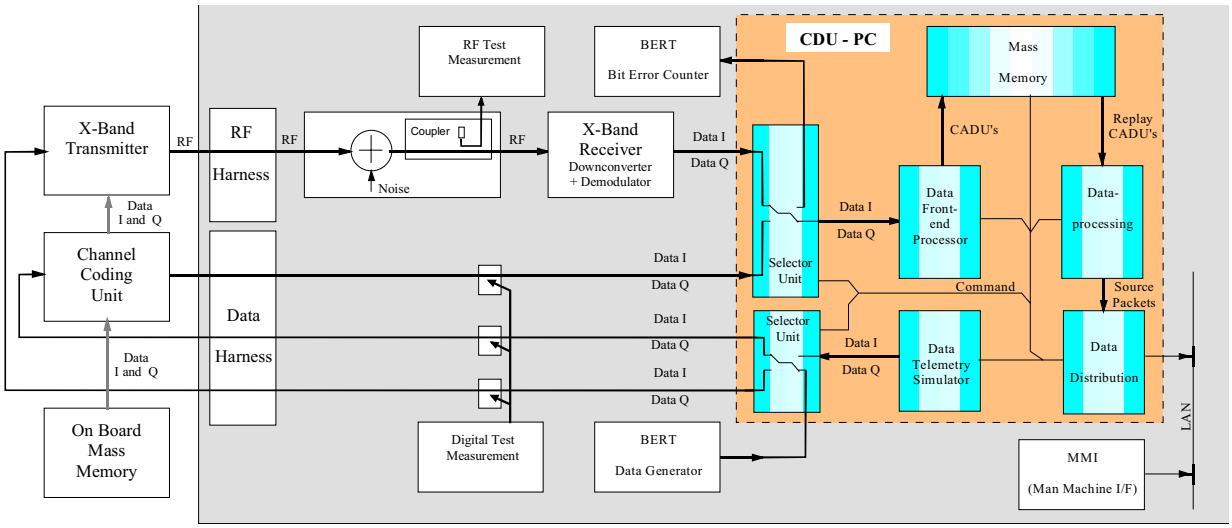

Figure 11: Functional Block diagram of the EGSE and Interfaces to the Units and Test

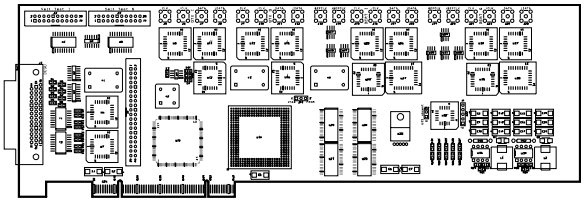

Figure 12: Telemetry Simulator Board Design

The Telemetry Simulator Board (TSB), as shown in Figure 12, provides test data for several interfaces in order to test the Channel Coding Unit and the Transmitter under various conditions. For self test features the HSI Board is provided with data test pattern.

4 SPACE SECURITY SYSTEM

4.1 General overview

The OHB-System crypto concept hardware and software has been fully qualified by the German Department for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI) for space applications with a secrecy level up to SECRET. The cryptographic hardware is designed for the easy exchange of algorithms, thereby providing the option of selecting mission specific algorithms.

Seven units of importance to the cryptographic processes are the

- TMTC External Authentication Unit,
- Satellite Management Unit Crypto Board (SCB),
- TMTC Segment Authentication Server
- Ground Crypto Unit (GCU),
- µProcessor based SmartCards,
- Channel Coding Unit (CCU), and the
- Channel Decoding Unit (CDU).

The key exchange and S-band channel are encrypted and authenticated from the TMTC External Authentication Unit and the SCB in the satellite and vice versa from the TMTC Segment Authentication Server, the GCU and Smartcards on the ground. For the X-band channel, the CCU and CDU pair provide the encryption/decryption services for the payload data.

The security system is expandable to include more satellite units. In this case it is important that the satellites are able to communicate with each other. This is provided by the Inter-Satellite Link (ISL). The link is used to transmit ground data received by one satellite to the other satellites. There is no extra encryption at the link, since the data is already secured through the ground segment encryption and authentication.

Central components of the security relevant system components are

- The Mission Support and Services, which has to insert new image orders into the overall flow plan of the system,
- the Satellite Control for commanding and decoding of the received telemetry,
- the Ground Crypto Unit GCU (also referred to as Crypto Unit), that is the central cryptographic component on ground and contains the dedicated GCB (Ground Crypto Board) and two Smartcards. On the GCB all crypto relevant processes are concentrated, i.e. it provides the symmetric cryptographic algorithm in hardware as well as it controls the data flow from and between the two smart cards. The GCU only works, if both Smartcards have authenticated each other and remain in the system. Only then the GCB can perform the authentication and key negotiation process between GCU and satellite. The Smartcards also serve as secure, redundant key storages.
- The Channel Decoding Unit with its High Speed Interface Boards (HSIB) inside, that synchronize, correct, deformat and decrypt the payload data in real-time and an

- archive, where the payload data and auxiliary data are stored for later image processing.

On satellite side the

- Board Computer (Satellite Management Unit, SMU) receives the encrypted command packets and provides these to the
- SMU Crypto Board SCB, a stand-alone processor based on-board crypto unit that contains the above mentioned encryption/decryption module in hardware. This same SCB contains dedicated H/W modules to support the EC-GDSA authentication and the key negotiation via EC-DH. The SCB is the counterpart to the GCU.
- Channel Coding Unit CCU, that receives the X-band keys from the SMU and provides these according to a provided order list into the formatting/encryption hardware.

4.2 Key management and flow

The security system uses a variety of keys for each of the implemented cryptographic functions.

The data flow of the key management is as shown in Figure 13 and proceeds as follow:

1. Using the long-term keys stored in the Smartcard (SC) and SCB, EC-DSA and EC-DH algorithms generate a short-term S-band key for symmetric encryption.
2. The X-band symmetric keys are generated by the random number generator in SC.
3. Using the S-band channel the X-band keys are encrypted and signed and sent to the satellite. There they are decrypted and authenticated.
4. The X-band keys are loaded into the CCU and CDU.
5. The payload data is downloaded using the X-band channel and encrypted using the keys supplied.

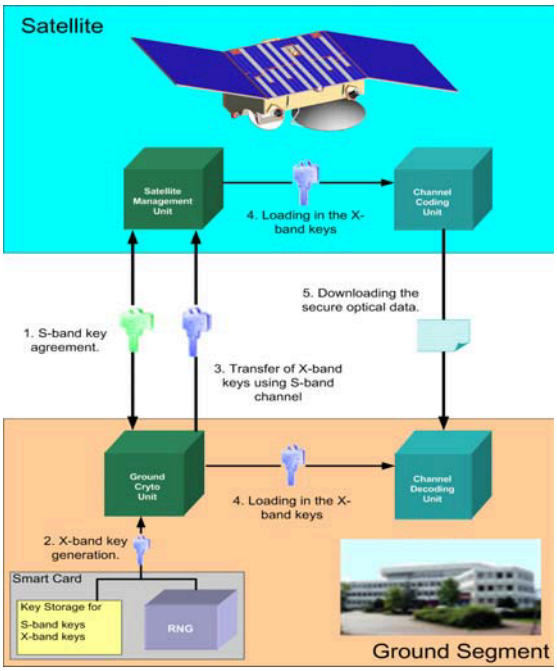

Figure 13: Key flow in security system

4.3 Security Layer Architecture

All commands have to be signed on segment layer and are passed to the first cryptographic barrier, the Packet Telecommand Decoder PTD.

At this stage Hardware Decodable Command for low level S/C functions (Unit ON/OFF, H/W Reset, Solar Cell String ON/OFF) are authenticated before execution. All other commands are authenticated and passed to the OBDH S/W for execution.

The OBDH S/W is able to decode and execute application layer commands. In nominal operation phase these commands are encrypted and signed with keys that have been negotiated during establishment of the connection. Telemetry is encrypted and signed with a different set of keys.

4.4 Satellite Security Elements

4.4.1 TMTC: Segment authentication

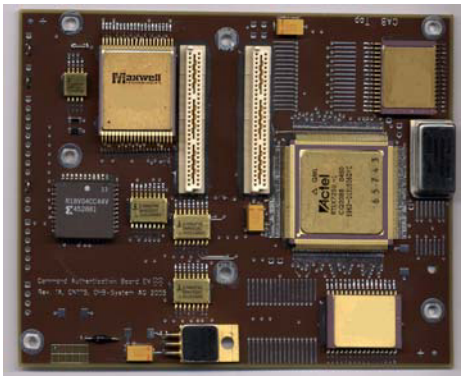

Figure 14: TMTC External Authentication Unit

Low-level command authentication for hardware decodable commands is provided on the satellite by the packet telecommand decoder (PTD) hardware, which contains a dedicated authentication unit (AU) and has a counterpart (HR 160 Authentication Server) in the ground segment.

The AU enables the spacecraft to authenticate the received data. It follows the “plain text with appended signature approach” as described within ESA PSS-04-151.

The embedded authentication of the PTD (“hard knapsack”) is not used in favour to the stronger HMAC-RIPEMD160 algorithm. This algorithm is introduced by dedicated hardware, that is in-system adaptable to also to other algorithms.

4.4.2 TMTC: Packet layer cryptography (Satellite Crypto Board)

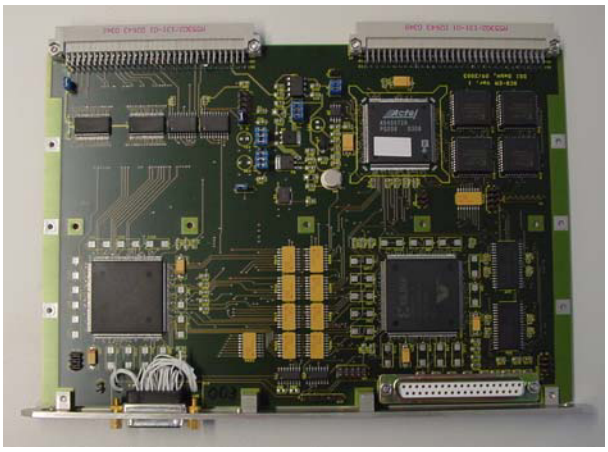

Figure 15: Physical view of an SCB (EM)

The transmission of high-level telecommands (application layer), which are interpreted and executed by the OBDH/SMU, is always encrypted and authenticated. This is provided by crypto functions that are integrated within a satellite based central crypto-board (SCB). Figure 15 shows the physical view of an EM SCB.

More than 10 space-flight versions of the SCB are already qualified for use. For future programs the same hardware can be used, since the software and cryptographic firmware is in-system reprogrammable.

4.5 Security Elements in ground station and EGSE

4.5.1 TMTC: Segment signature (HR 160 authentication server)

Figure 16: HR 160 Authentication Server unit

The security system contains an external authentication unit (shown in Figure 16), which is able to generate and verify signatures, for example, by use of the HMAC-RIPEMD-160 Algorithm .

4.5.2 TMTC: Packet layer cryptography (Ground Crypto Unit)

The counter part to the SCB is the Ground Crypto Unit, shown in Figure 17. The GCU is contained in a 19” industry PC and hold the GCB and the two Smartcards inside, the Session Key Smartcard extract-able from the case.

Figure 17: GCU case with Session Key Smartcard slot

4.5.2 µProcessor based SmartCards

The µProcessor based SmartCards are in charge of the mutual authentication and perform secure key storage for the TMTC server and GCU (key backup).

Figure 18: Master and Session Key Smartcards

4.6 System Aspects of Security

Time to connect

For low earth orbit (LEO) systems the contact time with the ground station is in the order of minutes. It is therefore essential that the time needed for connection and the associated authentication and key negotiation is limited to a small fraction of the typical contact time. If e.g. a connection has to be completely established within 10 seconds, then this task cannot be done in software alone. For this reason the EC-GDSA and EC-DH are hardware modules. Estimations for a “soft-ware only” solution had shown connection times of more than 90 seconds, which is un-acceptable for short contacts. But also in the case of longer contact times (e.g. GEO satellites), a hardware solution is advisable, because of a shorter reaction time in case of problems or while being in transfer orbit.

CCSDS compatibility

The communication on S-Band is completely compatible to the CCSDS standard for TMTC. This results in compatibility to numerous ground stations that can be used for sup-port, while in LEOP or in emergency situations. The X-Band data transmission is done in CCSDS Packets of equal length, allowing the receiving hardware to easier synchronize with the data stream. The header and FEC code overhead has been minimized (about 15%) while still being within standard.

LEOP/emergency phase

The two layer security of TMTC communication of the security system (see section 4.3) allows for a two step commissioning of the satellites after launch. The segment layer authentication is active at all. Unauthorized access to the satellite is prohibited, but no encryption is active. Classified data on the satellite is either deleted or encapsulated and by no means accessible in this phase.

Nominal phase

In Nominal Phase (nominal operation of S/C with image generation and download) the second security layer (packet layer security, see section 4.3) becomes active too and with it encryption and authentication on CCSDS packet layer. Classified data can be transferred from and to the satellite over a secure TMTC channel. If the phase is changed back to LEOP/emergency phase, then all classified data that are not already encapsulated are deleted.

5 CONCLUSION

OHB System provides an advanced on-board data handling chain include a Security System as an adequate solution for future Earth Observation applications and services.
The Payload Data Handling System features high performance in data compression, data evaluation und truncation as well as data storage, data formatting (CCSDS), data encryption and downlink.
The Units of the processing chain are:

- DSP Board (VSOP) for high performance controlling and pre-processing / compression.
- Data Storage Unit (DSU) for high speed and capacity storage.
- Channel-Coding Unit (CCU) for high speed image data processing and formatting.
- EGSE & SCOE for high-speed sub-units check-out and system tests.

On the other hand the security System provide all the tasks from key management, authentication, real-time encryption and decryption to provide protection of all satellite and ground links up to level Secret. The Secured links are from on-board Computer TMTC function and from the payload data handling to ground.

This seven units are important for security:

- TMTC External Authentication Unit for integrity protection on segment layer.
- Satellite Management Unit Crypto Board (SCB) for key negotiation with EC-DH for two sets of encryption and authentication keys.
- TMTC Segment Authentication Server to generate and verify signatures.
- Ground Crypto Unit (GCU) for established authenticated connection with SCB and real-time symmetric encryption and decryption.
- µProcessor based SmartCards for secure key storage and mutual authentication.
- Channel Coding Unit (CCU) as a part of the Payload Data Handling System for high speed image data processing and formatting.
- Channel Decoding Unit (CDU) for real-time decryption and CCSDS type decoder.