SECURITY CONCEPTS FOR SATELLITE CONTROL AND PAYLOAD DATA

C. Tobehn[(1)], B. Penné[(1)], R. Rathje[(1)], A. Weigl[(1)], Ch. Gorecki[(1)], H. 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
Email: tobehn@ohb-system.de

Abstract

The high costs to develop, launch and maintain a satellite network makes protecting the assets imperative. Attacks may be passive such as eavesdropping on the payload data. More serious threat are active attacks that try to gain control of the satellite, which may lead to the total lost of the satellite asset. To counter these threats, new satellite and ground systems are using cryptographic technologies to provide a range of services: confidentiality, entity & message authentication, and data integrity. Additionally, key management cryptographic services are required to support these services.

The key points of current satellite control and operations are authentication of the access to the satellite TMTC link and encryption of security relevant TM/TC data. For payload data management the key points are multi-user ground station access and high data rates both requiring frequent updates and uploads of keys with the corresponding key management methods.

This paper describes the key features relevant for security, as there are key management & communication security methods and role based access control. The implementations of security units on-board the satellite, corresponding ground station units and EGSE as well as operational aspects of security are presented.

The presented concepts are based on our experience and heritage of the security systems for all German MOD satellite projects (SATCOMBw2, SAR-Lupe multi-satellite system and German-French SAR-Lupe-Helios-II systems inter-operability) as well as for further international (KOMPSAT-II Payload data link system) and ESA activities (TMTC security and GMES concepts).

1. GENERAL APPROACH

Cryptography is an essential element in any communication system that transmits across an open channel. This is especially true for satellite systems. The high costs to develop, launch and maintain a satellite network makes protecting the assets imperative. Advances in technology have reduced the costs of satellite communication devices. This has increased the threat of third parties attacking the system. These attacks may be passive such as eavesdropping on the telemetry (TM) and telecommand data (TC) or it may include users gaining unauthorized access to the payload data. More serious threat are active attacks that try to gain control of the satellite or the whole satellite network, which may lead to the total lost of the satellite asset.

To counter these threats, new satellite systems are designed with cryptographic functions to provide a range of services, including:

- Authentication
- Data Integrity
- Data Confidentiality
- Non-Repudiation
- Access Control.

Additionally, key management cryptographic services are required to support these services.

Authentication services are used to verify the identities of entities, or data origins.

Data confidentiality and data integrity services are used to protect the confidentiality and integrity of data in transmission. A traffic flow confidentiality service can be used to prevent traffic analysis attacks. Connection integrity services are provided with or without recovery.

Non-repudiation methods ensure that the transferred data has been sent and received by the parties claiming to have sent and received the message.

Finally, there are access control services to prevent entities from accessing and using resources in an unauthorized way.

Security can affect several links and interfaces (Figure 1):

- inside the satellite,
- inter-satellite links,
- between space-ground (S-Band and X-Band)
- between and inside ground facilities.

This has to be considered in the design of all relevant elements and operations depending on the security level starting from the definition phase.

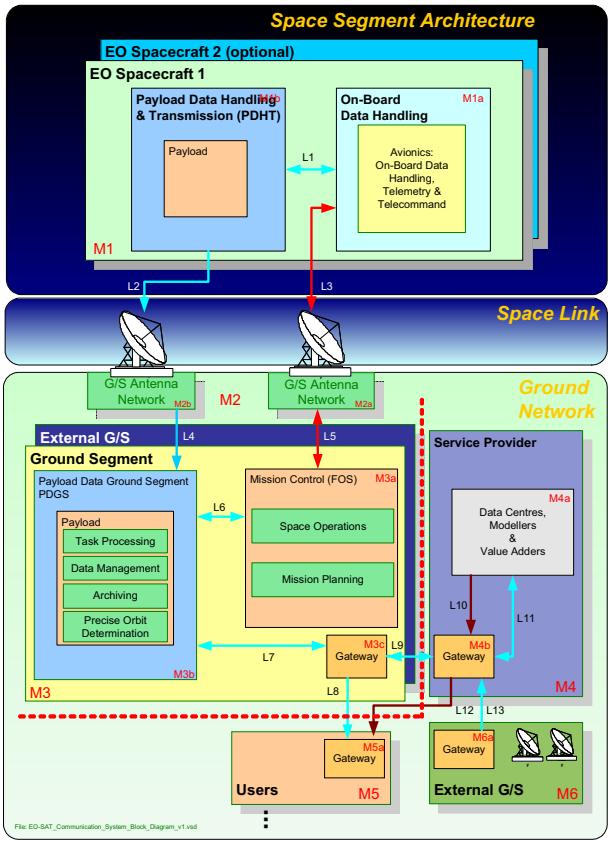

Figure 1: Communication and Data links in overall EO system (satellite and ground segment)

2. SYSTEM ASPECTS OF SECURITY

2.1. 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. Therefore a connection should 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 “software only” solution had shown connection times of more than 90 seconds, which is unacceptable 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.

2.2. AIT Aspects

In the AIT phase of a project, either on subsystem or system level the effort is concentrated on testing of functionality and error conditions rather than security. Typically security is seen as a contra productive issue that poses a problem for test activities. If already full security (i.e. usage of classified parameters and keys) is in the cryptographic units, then also the complete working environment could be raised to classified environment. Complex control issues (need-to-know principle) then will pose a measurable overhead to the AIT activities.

In order to reduce this overhead the AIT should better be done with non-classified keys and parameters leaving also the working environment non-classified. For this reason all crypto-graphic units have in-system program and configuration capabilities, i.e. the change between open (non-classified) and classified status can be achieved by reprogramming in-system. This is even possible for units already installed in the satellite. For flight the units have to be finally validated and the respective interface being sealed and/or tamper protected.

2.3. Formal Evaluation

The final configuration has to be evaluated by an independent, national or international authority that checks for

- correct implementation of algorithms & modes,
- no algorithmic trap- or backdoors
- performance
- electromagnetic emission

The evaluation is a lengthy process and should not be embedded into the standard project flow, especially not the AIT phase. Due to the independency of the evaluating authority this will have impact to the project schedule. Therefore an evaluation model should be introduced into the project. This model can be reduced to the cryptographic units plus EGSE components. In the OHB security system the feature of in-circuit configurability allows to develop the EM and flight units in parallel. If the evaluation results into change request for units that are already built then the chance is high that these changes can be introduced with firmware or software changes (schedule impact: weeks) rather than changing EM of flight hardware (schedule impact: months). By having an evaluation model and in-system configurable units the schedule risk is reduced significantly.

2.4. Ground Segment Security

The ground segment security aspects are defined in the overall IT security concept, that is specific for each project. At first an analysis of threats and risks is performed in order to tailor the security measures for the project. The tailoring process is based on the security or classification level of the project. In most cases at least the following is necessary:

measures on the infrastructure of the G/S

- Access control
- Measures against compromising electromagnetic emission

organizational and personal measures

- accreditation of personnel
- definition of access control (need-to-know principle)

The access to archives and databases is also defined the security concept and cannot be generalized. For a OHB Security system the level of security defines the measures and can be between virtual private networks (VPN) for medium security or dedicated, approved crypto hardware (e.g. SINA-Box protected for German applications).

3. PROTECTION METHODS USING CRYPTOGRAPHY

To provide the previously listed security services mathematical functions are used that allow fast computation when given the algorithm and secret key but are very difficult to compute without the secret key.

3.1. Authentication

Cryptographic authentication verifies that data is from an authorized user or sender. Often before any message is processed the message is authenticated as being a valid message. One method of authentication is achieved by creating a signature from a secret, known by both the sender and the receiver, and the message. The receiver can verify the sender by recalculating the signature with the known secret and the received message.

- Examples: EC-DSA, HMAC RIPEMD 160

3.2. Data Integrity

Integrity services are similar to authentication and often use the same functions. Using the received message and signature plus the known secret, the integrity of the message can be checked. An alteration in the message results in a new signature value and the comparison of the signatures results in a failure.

- Examples: HMAC-RIPEMD-160

3.3. Data Confidentiality

Data confidentiality services hinder the attacker or threat source from viewing the protected original data. Two cryptographic algorithm families that provide confidentiality are symmetric and asymmetric ciphers.

Symmetric Ciphers:

- Symmetric ciphers are mathematical functions that convert a plain text input into an unreadable sequence with random characteristics. The encryption and decryption functions use the same key. There exist very fast and secure symmetric ciphers for a wide range of implementation scenarios (ASIC, FPGA, or software).
- Examples: AES (Rijndael), MARS, TWOFISH, RC6 , IDEA and DES
- Asymmetric Ciphers:
- Asymmetric ciphers, like their symmetric siblings, are mathematical functions that convert plain text inputs into unreadable sequences. However, for asymmetric ciphers there exist two keys, the private and public keys. For secure asymmetric algorithms, given the public key, it is computationally infeasible to calculate the private

key. Asymmetric ciphers generally have slower implementations than symmetric ciphers.

- Examples: RSA and EC-ElGamal

3.4. Anti-Replay Mechanisms

A replay attack uses previously sent data to control the satellite. An attacker can observe the results of a command and resend the same TC at a later time. Using a group of authenticate commands, an attacker can by-pass all the cryptographic security features. Anti-replay mechanisms are inserted into the protocol to prevent this from occurring. The mechanism has to be protected from tampering by implementing it with either authentication or encryption services. The anti-replay mechanism operates by comparing a concurrent running counter or timer on the satellite and ground segment. If the counters do not match, the TC is rejected and deleted.

- Examples: Time stamp, counter

3.5. Access Control

Access to system components must be protected, since sensitive data is often viewable in the system. Access control restricts users and operators from areas (physically and in the system net-work) they do not have clearance. Two common methods for access control are smart cards with pin numbers and accounts with passwords.

Both these two methods provide an identification of the system user and a verification that the person has the rights (password or pin check) to access this information.

- Examples: Smart card ID, user account with password.

4. KEY MANAGEMENT AND FLOW

In order for cryptographic algorithms to properly secure information, they require an unknown. This is provided by cryptographic keys. The problem for security systems that use secret keys is how to generate, distribute and manage these keys. Methods must be found to securely transfer the keys between the parties without it being intercepted by unauthorised third parties. This section provides an overview into key generation, distribution and key types.

4.1. Key Generation

Before a key can be distributed it must first be generated, which is done using a random number generator (RNG). Not all RNGs are appropriate for cryptographic key generation. The main properties of a good cryptographic RNG are:

1) Independent output: bits from an RNG must not be influenced by the previous output. The probability of a “1” in a binary cryptographic generator is always 50%.
2) Uniform distribution: when examining an RNG in the frequency spectrum it should show an approximately equal occurrence of all possible values.
3) Large period: each realized random number generator has a set period. This period should be as large as possible to prevent the sequence from repeating.
4) Unpredictable: an attacker has access to the output and the algorithm of an RNG. Without knowing the initial seed a good cryptographic generator is not predictable even while knowing the algorithm and last output.

- Example random number generators: Blum-Blum-Shub, EC-DSA, rDSA [1].

4.2. Key Distribution

The importance of keeping the cryptographic keys secret presents a challenge in their distribution. Both sides of the communication channel (e.g. satellite and ground station) must be equipped with the same or matching keys. This section will discuss possible ways of providing secure distribution of keys for two different satellite system life phases: pre-launch and during operation. The method for updating keys on a satellite is different for each phase. During the pre-launch phase, the operators have physical access to the satellite and keys can be manually loaded; however, once it has been launched the only effective key distribution methods are by applying cryptographic key distribution protocols.

Some missions use mission lifetime keys and key distribution can be adequately covered by the key fill

interface before launch; however, there are also missions that require the keys to be renewed during the operational lifetime of the system. This is especially prevalent in high security missions. The problem with key renewal of an operational satellite is the transfer of the keys over an open and insecure channel (ground-to-satellite space link). This section presents a method for key renewal that uses both symmetric and asymmetric cryptographic algorithms. The steps listed below are mirrored on Figure 2:

1) Using the long-term keys stored in the smartcard and on-board the satellite, a short-term key for encryption of the S-band channel is negotiated.
2) The X-band symmetric keys are generated by the random number generator in smartcard.
3) X-band keys are sent to the satellite via encrypted
S-band channel.
4) The X-band keys are loaded into the on-board and the ground Channel (De-)Coding Units.
5) The payload data is encrypted using the X-band keys and downloaded.

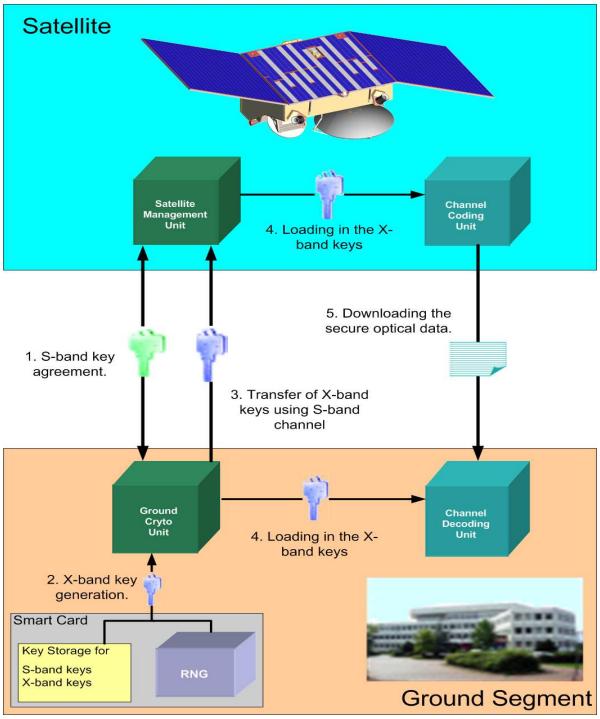

Figure 2: A process for key distribution

The method proposed here assumes two types of secrets used to create a secure channel: long and short term secrets. The initial EC-DH and EC-DSA parameters are long term secrets, while the AES (symmetric keys) are short term secrets. The short term keys may be replaced before each transmission or held for longer periods.

4.3. Key Types

Depending on the cryptographic concept for the satellite mission there can be different types of secret keys available. Some of the more common keys are presented in the following:

Nominal keys:
Cryptographic keys used for normal operation of the satellite. They can be for the cryptographic functions on the TMTC or payload data.

Emergency keys:
Emergency keys are used when the satellite has problems with the nominal key. The emergency keys allows the satellite operator to re-establish secure communication with the satellite. Normally, these keys are used as little as possible to prevent attackers from gaining any information about these keys.

Key Encryption Keys (KEK):
Key encryption keys are used on satellite systems to decrypt the encrypted nominal encryption keys. It allows nominal keys to be transmitted from the ground station securely to the crypto unit. Usually, only the crypto unit is provided with a KEK, where the encrypted keys are finally decrypted.

5. ROLE BASED ACCESS CONTROL (RBAC)

A method to ensure security is maintained inside the satellite system is to restrict users and operators to only the sections where they require access. Permissions and access are tailored for the particular user or operator. This can be achieved by two methods, either directly configuring a user's or operator's permissions and access control or by defining a operational role and defining the access and permissions to that role. A user or operator is assigned the minimum number of roles to cover their required access. A user or operator can be assigned many different roles. Figure 3 is a graphical representation of the role based concept. Users are defined a user name with an associated role or roles. The roles themselves are assigned the permissions which gets transferred to the user. Permissions in this case refers to authorisation, access rights, and privileges.

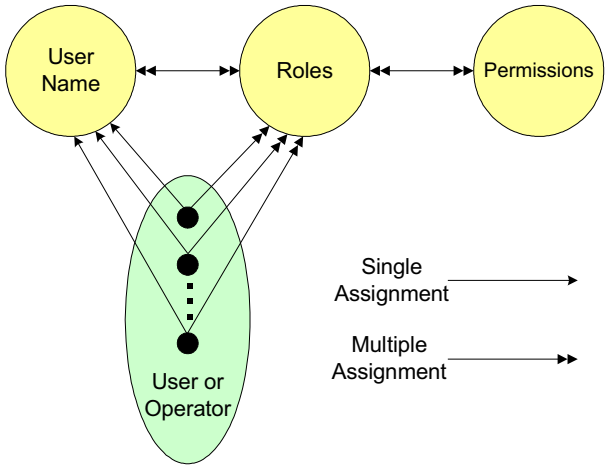

Figure 3: Logic flow of role based access control.[2]

RBACs are used extensively in Windows or Linux based networks, where the operations are built into operating systems. The benefit of RBAC is the ability to add permissions and access control to a user or operator while having little technical skill. A user or operator is defined a role and can be given the permissions for that role by adding them to that grouping. The use of RBAC concept supports three security principles:

1) Minimum required privilege:
   Only the privileges that are required to complete the tasks are assigned to the user or operator.
2) Division of responsibilities:
   Certain roles are responsible for particular system aspects. It may be required that two separate roles are needed to complete a sensitive task (i.e. key management or software updates).
3) Data abstraction:
   Details of the permissions and access rights to particular data are hidden by the role level. The role assignment is only defined once and a user or operator is provided with required role or roles.

6. EXPERIENCE IN SECURITY SYSTEMS

OHB has developed and implemented cryptographic solutions and crypto components for space and ground segments. The crypto hardware and software designs are based on the KOMPSAT-II Payload data link system, the military satellite projects SAR-Lupe and SAT-COMBw2 and the Europeanization of the SAR-Lupe and Helios-II systems due to inter-operability.

SAR-Lupe is a radar-based reconnaissance system consisting of five satellites as well as a ground segment for receiving and evaluating image data. OHB is the prime contractor for the development, construction, and launch of the satellites. This includes also the responsibility for the 10-year operating period, as well as developed and qualified the security elements on-board the satellite and on ground.

For the SATCOMBw Stufe 2 Program (German Military Communication satellite system, geostationary, 2 satellites, 15 year lifetime) OHB has developed the cryptographic system and is manufacturing, qualifying and delivering all cryptographic units (on board and on ground).

OHB was responsible for the integration and test of the overall Data Link System (DLS) for MSC. MSC is the primary payload of the KOMPSAT II Mission, a Korean Earth Observation Satellite. Core of the DLS is the Channel Coding Unit (CCU) developed by OHB.

The E-SGA project goal is the enhancement of the national SAR-Lupe reconnaissance system to a multinational system (E-SGA) and establishment of a system union together with the French satellite reconnaissance system HELIOS II. OHB is Prime contractor and performs design, and manufacturing of the E-SGA and French SAR-Lupe Ground Segment (FSLGS).

The FSLGS project allows French Defence to have access to the radar data capabilities of the German SAR-Lupe system. The users will have independent and confidential access to the SAR Lupe system according to the specified requirements and the user rules agreed between Germany and France.

The SAR-Lupe 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. This crypto concept is not limited to space applications. It can also be used for other applications that require secure communication (submarine, planes, ships). Included in this task are the complete key management (generation, storing, implementation, destroying, etc. of keys, parameters, files containing classified information, etc.). OHB defined and provides the complete infrastructure for handling secret information from integration, during testing, until launch and beyond.

The cryptographic hardware and software is designed for the easy exchange of algorithms, thereby providing the option of selecting mission specific algorithms. The satellite security Elements and features are

- S-Band Satellite TMTC Authentication Unit
- S-Band Satellite Unit Crypto Board
- X-Band Channel Coding and Encryption Unit (CCU)

Ground Security Elements are:

- S-Band TMTC Authentication Server
- S-Band Ground Crypto Unit (GCU)
- µProcessor based SmartCards
- X-Band Channel Decoding Unit (CDU)
- High Speed Data Ground Test Equipment

7. SECURITY ELEMENTS FOR THE SATELLITE

7.1. S-Band TMTC 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.

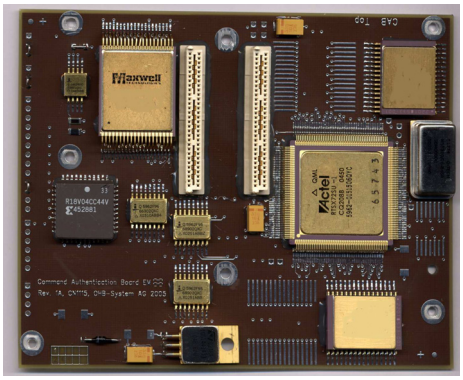

Figure 4: TMTC External Authentication Unit

7.2. Satellite Management Unit Crypto Board

During transmission high-level telecommands, which are interpreted and executed by the OBDH/SMU, are always encrypted and authenticated. This is provided by crypto functions that are integrated within a Satellite Crypto Board (SCB). Figure 5 shows the physical view of an EM SCB.

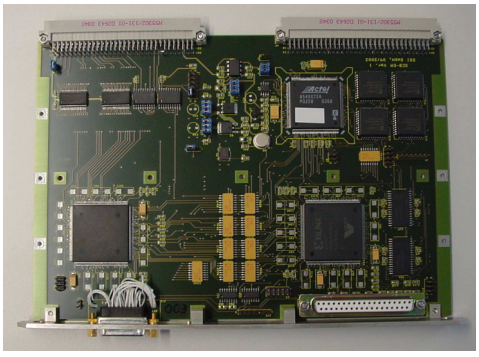

Figure 5: Satellite Crypto Board (EM)

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.

7.3. Payload Data : Channel Coding and Encryption 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.

For the data on both data streams the CCU features:

- Encryption
- Reed-Solomon encoding
- Header generation
- ASM insertion
- Randomiser

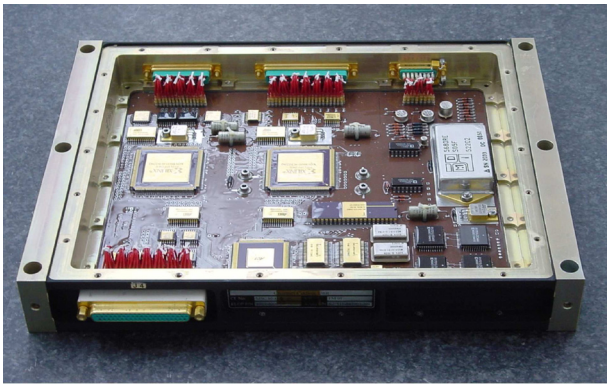

Figure 6: Channel Coding Unit Core Layout

8. SECURITY ELEMENTS FOR THE GROUND STATION AND EGSE

8.1. TMTC Segment Authentication Server

The security system contains an external authentication unit (shown in Figure 7), which is able to generate and verify signatures, for example, by use of the HMAC-RIPEMD-160 Algorithm .

Figure 7: HR 160 Authentication Server unit

8.2. Ground Crypto Unit

The counter part to the SCB is the Ground Crypto Unit, shown in Figure 8. The GCU is contained in a 19” industry PC and hold the GCB and the two Smartcards inside. The Session Key Smartcard are extractable from the case.

Figure 8: Ground Crypto Unit

8.3. µProcessor based SmartCards

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

Figure 9: Master and Session Key Smartcards

8.4. Payload Data: Channel Decoding Unit and Decryption

The Channel Decoding Unit (CDU) on ground is the counterpart of the Channel Coding Unit (CCU) on the satellite. The CDU performs the synchronization, de-formatting, decrypting and storing of the data stream in real-time. The CDU is a PC-based system that is part of the Data Link System EGSE and the Ground Station hardware. The system takes advantage of an already large heritage of the whole chain of high-speed data processing including error detection/correction and buffering of the processed data in real-time as well as hard disk storage and backup systems.

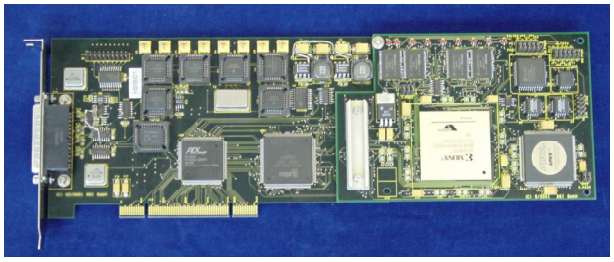

Figure 10: Channel Decoding Unit

8.5. High Speed Data Ground Test Equipment

The electrical ground test equipment (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:

1) 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.
2) Sub-system test: the EGSE allows the test of the entire processing chain.
3) 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 11 shows a version of the complete integrated test system where all components are located in three 19'' racks.

Figure 11: High Speed Data Ground Test Equipment

The EGSE provides a complete Bit Error Test-Set. 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 con-trolled 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.

9. CONCLUSION

In future more satellite system will use advanced security methods and systems. Therefore a standardisation especially on protocol level and also on ground segment level mainly operated by space agencies is required to achieve a harmonised and cost effective infrastructure for the next generation of secured satellites.

One example are currently developed Sentinel-1, 2 and 3 satellites under the EC/ESA GMES programme. Here a common definition of security rules and implementation standards shall be defined by the European Space Agency to enable effective security to protect significant investments and highly operational services as well as on-demand services like disaster management.

OHB-System security solutions provide modular system performing all necessary functions from key management, authentication, real-time encryption and decryption to provide protection of all satellite and ground links up to level Secret.

Satellite Security Elements & Features are

TMTC Authentication Unit :

- Integrity protection on segment layer
- Uses modern Hash algorithm

Satellite Unit Crypto Board (SCB) :

- Full security on application layer
- Establishes authenticated connection
- Key negotiation with EC-DH for sets of keys
- Real-time symmetric encryption and decryption

Channel Coding and Encryption Unit (CCU) :

- up to 2x 216 Mbps
- CCSDS formatting
- 128/256 bit key data encryption (e.g. IDEA, AES, 3-DES or proprietary algorithms)
- Reed Solomon / Turbo coding
- Synchronisation marker insertion
- Data randomiser

Ground Security Elements are:

TMTC Authentication Server :

- Sign segments with HMAC-RIMED160
- Counterpart to TMTC External Authentication Unit

Ground Crypto Unit (GCU) :

- Full security on application layer
- Establishes authenticated connection with SCB
- Key negotiation with SCB
- Real-time symmetric encryption and decryption
- ISL file creation
- Secure key storage

Channel Decoding Unit (CDU) :

- 2x 216 Mbps real-time decryption and CCSDS type decoder
- Real-time storing of data
- Expandable
- Use in Ground station and for EGSE

In summary, OHB's Security System feature:

Modular system performing any or all of the functions:

- Multilayer security for TMTC satellite links
- Authenticated connections to satellite transceiver, on-board computer and payload data downlink
- Key Management for Satellite Constellations and distributed Ground Segments
- Real-time & High speed encryption and decryption

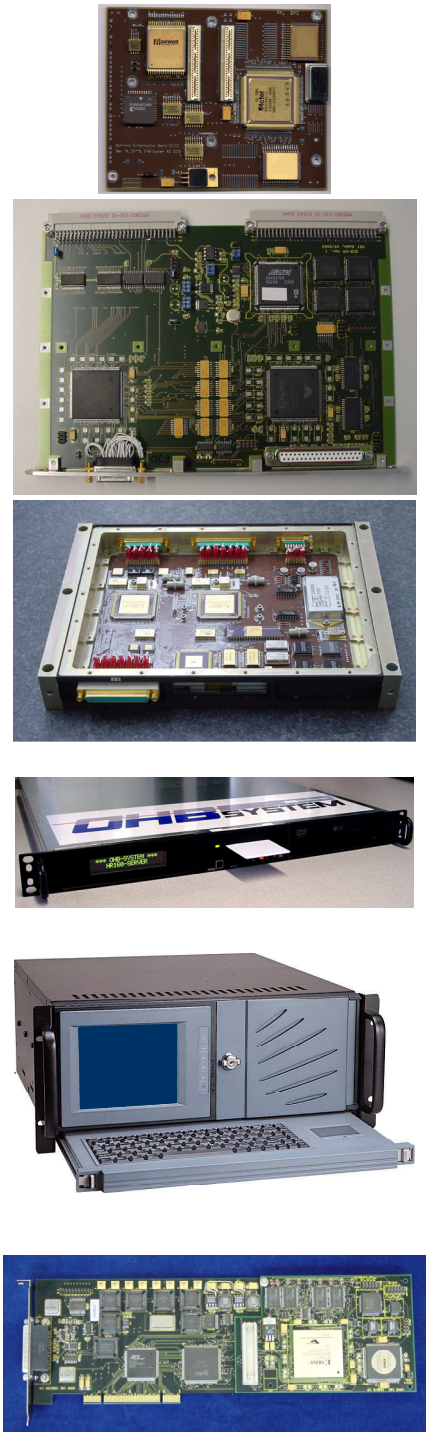

Figure 12: OHB Security Elements

10. REFERENCES

[1] NIST, FIPS 140-2: Security Requirements for Cryptographic Modules

[2] Courtois, N. et al., Cryptanalysis of Block Ciphers with Overdefined Systems of Equations

[3] Website of OHB-System AG Germany: http://www.ohb-system.de