SECURE TRANSFER OF DATA FROM SATELLITE TO USER – A CONFIGURABLE SECURITY APPROACH USING A CCSDS COMPLIANT RF TRANSCEIVER

David Selčan [(1)], Gregor Kirbiš [(2)], Dejan Gačnik [(1)], Iztok Kramberger [(2)]

[(1)] SkyLabs d.o,o., Zagrebška cesta 104, 2000 Maribor, Slovenia, david.selcan@skylabs.si
[(2)] University of Maribor, Faculty of Electrical Engineering and Computer Science, Koroška cesta 46, 2000 Maribor, Slovenia

ABSTRACT

In this paper, a configurable approach to securing the data sent to and received from a satellite, based on the use of CCSDS standards, is presented. The application of this approach to the NANOlink communication subsystem is demonstrated. The implementation of the security functions, as well as the limitations arising from implementation limits are shown. The use of CCSDS protocols, with a focus on CCSDS SDLS and CCSDS SDLS-EP standards, to assure secure communication is presented. A limited implementation of CCSDS SDLS-EP PDUs, based on the use of preloaded encryption keys, is demonstrated. Based on the specifics of the security implementation and a security-focused data flow diagram, a threat model of the security functions is analyzed, where it is demonstrated, the proposed solution can be considered sufficiently secure for most satellite operation scenarios. The capability of the proposed security solution to offer a secure link without decreasing the communication bitrate is demonstrated. Finally, the communication performance for a NANOlink operating with the security functions enabled in a 600 km LEO orbit is estimated.

1 INTRODUCTION

Small satellites are gaining incredible traction in the space segment, with more than 2000 [1] new satellites expected to launch in the following 5 years. A combination of ever shorter time-to-space intervals and powerful new capabilities that expand potential applications and service models has made them the ideal platform for gathering, storing and analyzing large amounts of valuable data. However, in the rush to build and launch these new systems, operators and manufacturers have prioritized speed, affordability and flexibility, while security, if considered at all, is often an afterthought. For this reason, small satellites present an underserved market when it comes to off-the-shelf security solutions.

To address this shortcoming, a configurable and customizable security approach, based on the CCSDS SDLS [2] and SDLS-EP [3] standards is envisioned. The proposed approach is realized with the use of a high-throughput S-band SDR-based communication subsystem and is based on the use of AES-256-GCM symmetric authenticated encryption. The proposed approach consists of extending the CCSDS IP core with the features of the CCSDS SDLS protocol, where only a single AES encryption and single AES decryption core is required. In contrast to the traditional approach, where the AES encryption and decryption is performed on an external OBC which is also responsible for processing the communication data, the proposed approach performs the AES encryption and decryption inside the communication subsystem itself, requiring no additional satellite resources to establish and maintain a secure link. As such, the secure link is terminated at the communication subsystem, freeing the satellite designer from having to route encrypted communication packets trough the on-board satellite buses.

The security keys required by the proposed AES cores are stored in a redundant on-board non-

volatile memory, from where they are loaded into the AES cores. A two-level key hierarchy is proposed, where the lower level “transaction” keys are used to transfer data between the GS and the satellite, while the higher level “master” keys are used to manage the security of the link itself. This key-management and other related security functions are managed by following a meticulously reduced subset of the CCSDS SDLS-EP protocol. The keys are preloaded into the transceiver at the time of flight, where a robust EDAC system assures their integrity throughout the whole mission. In addition, the anti-temper architecture of the non-volatile key memories assures that the equipment is protected against key extraction attacks and prevents retrieval of secure keys during on ground activities, like AIV/T.

2 ARCHITECTURE OF SECURITY APPROACH

The NANOlink is a highly miniaturized TM/TC satellite communication subsystem. Its full duplex communication link capabilities, which are based on an SDR architecture, and its best-in-class SWaP (Size, Weight and Performance) characteristics enable improved communication data link budgets, thus assuring outstanding performance for the emerging space market. High reliability is ensured via carefully selected parts and combined with an advanced FDIR approach that supervises the SDR logic and other critical parts of the subsystem. The full duplex communication subsystem is compliant with the CCSDS protocol, while supporting configurable modulation parameters and data rates. A highly efficient add-on RF amplifier module is available which boost the RF output power to 37 dBm. The architecture can be further expanded with the addition of a diplexer with integrated LNA. The primary interface of the NANOlink is a redundant CAN bus, while for high throughput data transfers, a high speed LVDS interface is also available.

The NANOlink is meant for use in three configurations: the base variant NANOlink-base, the variant with an add-on RF amplifier NANOlink-boost and the variant with a diplexer, NANOlink-boost-dp systems.

Figure 1: NANOlink-base S-band communication system

Figure 2: NANOlink-boost S-band communication system

Figure 3: NANOlink-boost-dp S-band communication system with diplexer

From the point of view of the CCSDS functions, NANOlink processes data in the following way. For the uplink, data is digitized and sample by the RF transceiver and forwarded to the demodulator as an IQ data stream. There this stream is filtered and a join frequency and timing synchronization algorithm is applied. Finally, the data stream is O-QPSK demodulated and sent to the CCSDS core. There, each TC packet is decoded and derandomized where finally, the FARM procedure is applied to it. Afterwards, it is stored in a memory, where it can be accessed by the PicoSkyFT processor and finally forwarded to other on-board subsystems via the CAN or LVDS interfaces.

Conversely, on the downlink, data that is received from the previously mentioned interfaces is sent to the CCSDS core, where it is inserted into TM frames. The TM frames are then randomized and encoded, then sent to the modulation core, where the data is modulated, filtered and finally a precorrection filter is applied, before being transferred as an IQ stream to the RF transceiver.

2.1 Implementation of security functions

While the CCSDS SDLS standard specifies many encryption algorithms for potential implementation, the NANOlink security functions are implemented to only support a single

algorithm, which is sufficient to cover all use cases. The AES algorithm was chosen with the following parameters:

- Encryption algorithm: Advanced Encryption Standard (AES) Galois Counter Mode (GCM).
- Authentication bit mask: default according to [2].
- Key length: 256 bits
- MAC length: 128 bits.
- IV length: 96 bits.

The IV field will operate according to a 32-bit fixed field (used to differentiate multiple NANOlinks) and a 64-bit counter. The AES-GCM-256 algorithm is capable of operating in three modes: authenticated encryption, where the data is encrypted as well as authenticated, authenticated-without-encryption, where the data part of the message is only authenticated, without being encrypted and clear mode, where the whole message is neither encrypted or authenticated. The selection of the modes is then based on the risk profile of the satellite.

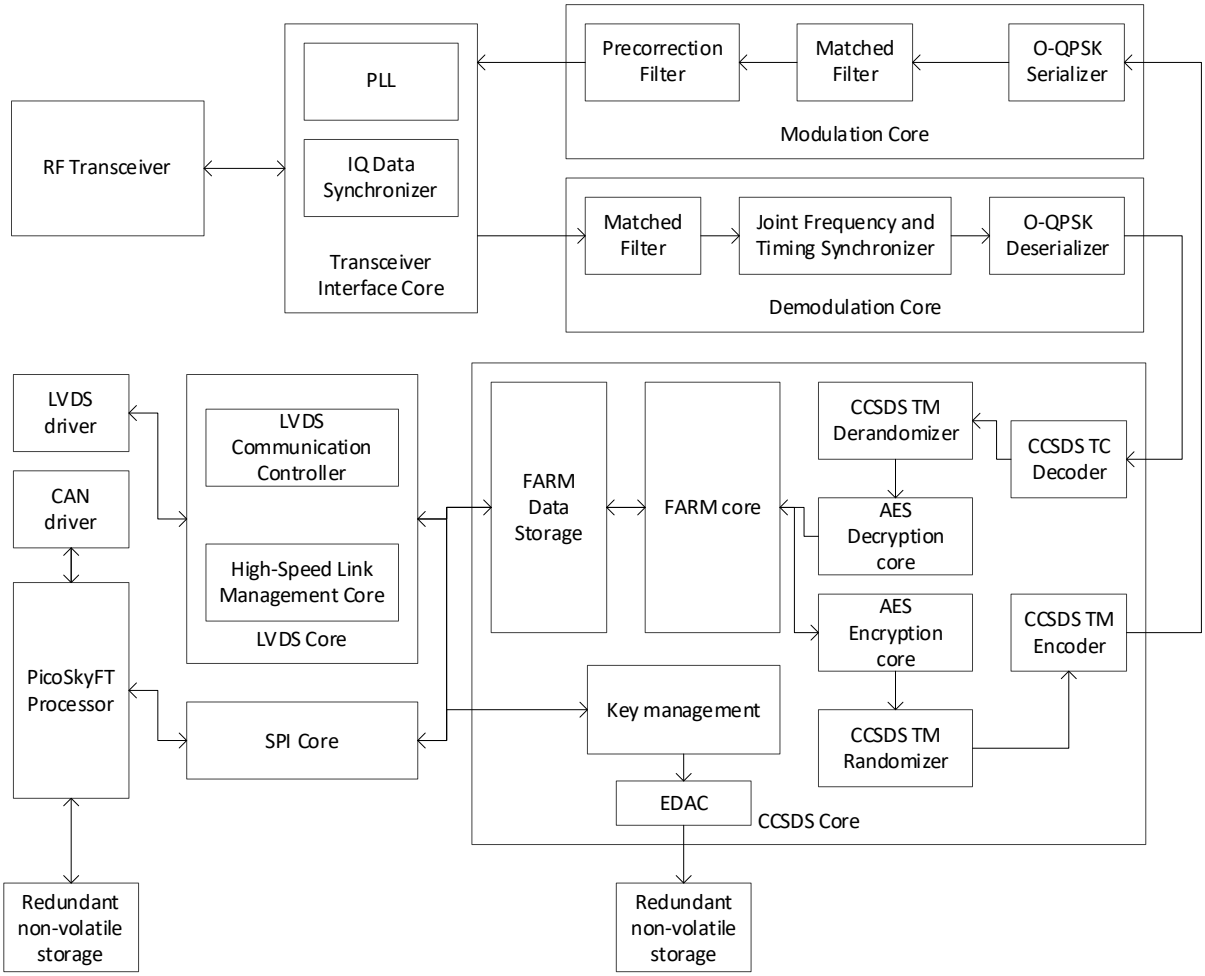

Figure 4: NANOlink security implementation block diagram

An important aspect of the security function is key management. For this reason, we propose a two-level hierarchical key scheme. The highest level is composed of so-called master keys, which are used exclusively for key and security management operations. The lower level is then composed of so-called transaction keys, which are the ones used for actually transmitting the data to and from the satellite. Only a small number of master keys (up to two) is supported, while a larger amount of

transaction keys can be stored.

The keys are stored in a redundant, EDAC protected, non-volatile storage and loaded dynamically into the CCSDS core upon request. The keys can only be written to the key storage in a “write only” manner – the read interface is exposed only to the key management logic, which is then only exposed to the AES encryption and decryption cores. In this way, the possibility of key tampering is severely limited.

Due to the nature of the implementation constraints of the real-time decryption and encryption cores, only a single transaction key can be used at the same time. If a key switch is required, it is in effect immediately on all transactional interfaces. Both master keys are always active.

An additional important aspect of the implementation of the security functions is the prevention of IV (nonce) reuse. Since the AES encryption scheme becomes vulnerable to attack with only a single instance of IV reuse, it is necessary to assure that this does not occur. The most problematic angle is in the case of non-expected power interruptions to the NANOlink, in which case the current IV state is lost. Due to this, the PicoSkyFT processor periodically reads back the current value of all IVs and stores them in a non-volatile storage. Each IV value is stored in three unique locations and protected with a CRC. Upon power-on of the system, the IV values are read back – if any became corrupted, they are ignored. If power was lost during the IV storage update, the largest IV value is used. The IVs are then incremented by small fixed number and used from this point on as the currently active IV numbers.

3 COMMUNICATION PROTOCOLS

The NANOlink supports the following CCSDS protocols:

- TC Synchronization and Channel Coding standard [4],
- TC Space Data Link Protocol [5],
- TM Synchronization and Channel Coding standard [6],
- TM Space Data Link Protocol [7],
- Communication Operation Procedure-1 [8],
- Space Packet Protocol [9].

In order to extend the functionality of the NANOlink with the capability of secure communications, the CCSDS SDLS [2] and CCSDS SDLS-EP [3] are used. This means that each TC and TM packet is extended with an SDLS header and the SDLS footer. Inside these fields, the IV counter, the MAC, the VCN-unique nonce, the User-settable IV field and the SPI (Security Parameter Index) field are transferred.

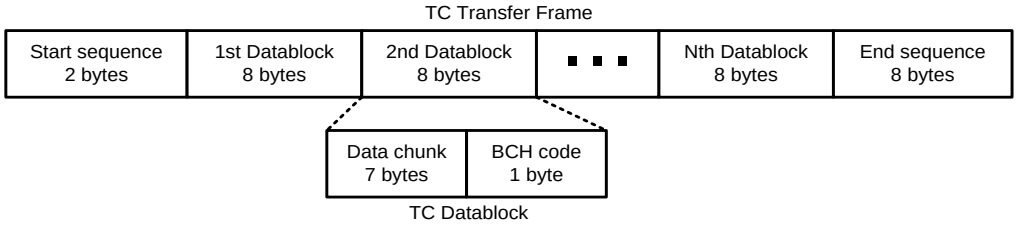

Figure 5: TC Synchronization and Channel Coding sub-layer Transfer Frame

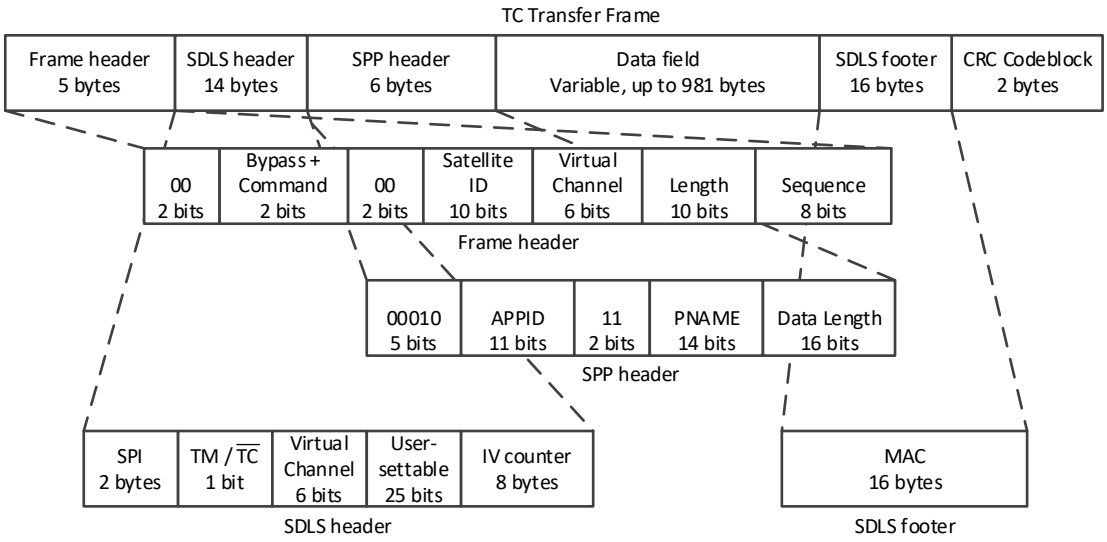

Figure 6: TC Space Data Link Protocol sub-layer Transfer Frame

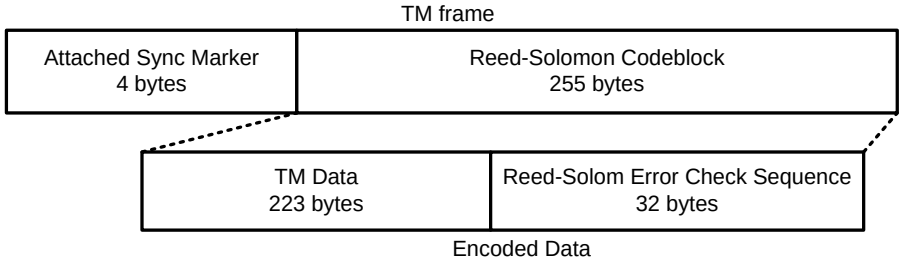

Figure 7: TM Synchronization and Channel Coding sub-layer Transfer Frame

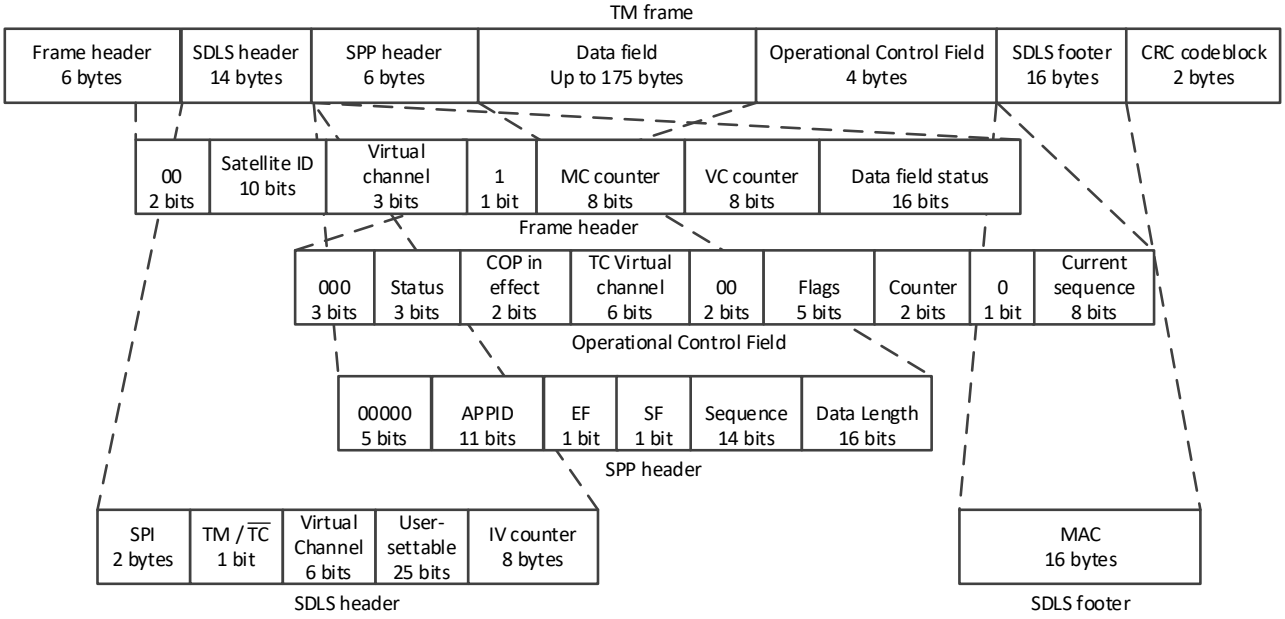

Figure 8: TM Space Data Link Protocol sub-layer Transfer Frame

The SPP header and data fields of the TC and TM frames are sent encrypted (if authenticated encryption is used) using the AES-256 algorithm. The Frame header and SDLS header are masked and used as part of the AAD data. If authentication-without-encryption is used, then the SPP header

and data fields are also processed as AAD data and not encrypted.

The SPI field of the SDLS header specifies which encryption key is in use: values from 1 onward specify which transaction key is in use. Keys are grouped according to VCNs – each VCN has its own security association for the TM packets, while TC packets have only a single SA for all VCNs. Values 65532 and 65533 are used for master keys, and the value 65534 is used for clear mode operation. The IV field is subdivided into two fields, a 4 byte fixed value, that is unique for each device, channel and VCN channel and an 8 byte counter. The MAC is transferred as part of the SDLS footer.

3.1 SDLS-EP implementation

There are two aspects of the SDLS-EP implementation. The first aspect is the use of the FSR reporting field, which is used for reporting of security-related events to the ground. The FSR field is sent alternating with the CLCW field used to manage the COP-1 procedure. The structure of the FSR is shown in the following figure.

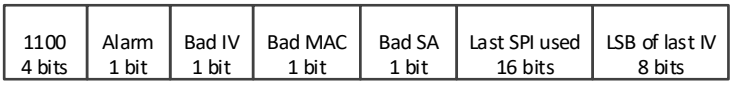

Figure 9: FSR field

The FSR reports, for the last received TC frame, if the IV key, MAC and SPI fields were valid or not. Additionally, the last SPI and IV fields that were received are listed. Additionally, an alarm field is present that is set every time a TC frame is rejected by the security function. The alarm field is only resettable using the SDLS-EP commands.

The second is the method by which SDLS-EP commands (Protocol Data Units – PDUs) are transferred and the list of which commands are implemented. A dedicated VCN is used only for sending and receiving SDLS-EP commands. This is also the only VCN which accepts the master key SPI fields – all the other fields must use transaction keys. For the same reason, this VCN rejects all transaction key SPI fields. The list of supported SDLS-EP commands was determined by including only the commands that are necessary to manage preloaded keys or are necessary for SDLS-EP operation. All other commands are not supported. The list of supported PDUs is:

- Key Activation
- Key Deactivation
- Ping
- Self-Test
- Reset Alarm Flag
- Set Anti-Replay Sequence Number
- Set Anti-Replay Sequence Number Window
- Read Anti-Replay Sequence Number

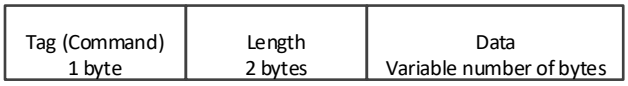

Figure 10: SDLS-EP PDU Structure

The Security Association (SA) model implemented is that each SA supported by the system is associated to a single key stored in the system – this association cannot be changed. For TC packets, that means that the number of SAs is equal to the number of transaction keys stored. For TM

packets, the number of SAs is equal to 8 times the number of transaction keys stored.

The behavior of some SDLS-EP commands differs from the standard – in effect, only a single key can be activated at once, and all SAs that are associated with that key are active once that key is activated. Activating a new key automatically deactivates the previous key. Deactivating a key that is activated transitions the satellite into clear mode.

4 THREAT MODEL

A threat model based on the construction of a Data-Flow Diagram and the subsequent analysis of the encryption algorithm and all associated data processing functions was created. Based on the model, the list of potential vulnerabilities was compiled and evaluated given their risk. The primary limitation of the presented threat model is that it only models the NANOlink itself – the ground station infrastructure is presumed as secure and not analyzed as part of this model.

4.1 AES-GCM-256 analysis

In the context of the threat model, it is necessary to understand the security benefits of using the AES-GCM-256 algorithm as well as its limitations. The AES-GCM-256 algorithm assures the following:

- An adversary that does not possess knowledge of the key used cannot distinguish between the ciphertexts of two equal-length messages encrypted with the AES-GCM-256 algorithm. A consequence of this assurance is that any entity not having knowledge of the key used cannot effectively read the plain text of any message encrypted with the AES-GCM-256 algorithm
- An adversary that does not possess knowledge of the key used cannot forge messages.

However, the assurances listed previously are dependent on a few critical usage limitations:

- The key must be generated uniformly at random and be kept secret from any potential adversary.
- For each message that is sent, a unique IV must be associated with that message. As a consequence of this limit in the context of the chosen IV field structure, up to 2^{64} unique messages can be encrypted and shared for any unique key.
- As a general recommendation of the AES standard [10], less than 2^{64} blocks of plaintext and AAD data should be encrypted for any unique key. A consequence of this limit is that less than 2^{68} bytes of data can be encrypted and shared for any unique key.

4.2 Threat model Data-flow diagram

The threat model data-flow diagram of the NANOlink, presented in the figure below, gives a clear overview of the most relevant processing blocks, storage spaces and interfaces. Based on this threat model, a few things stand out:

- As long as the Ground Station part is presumed secure, all data sent to and received from the NANOlink on a satellite in space can be presumed secure, as long as the keys are kept secure and no fault pertaining to the IV generation occurs.
- The keys, due to the “write only” key update interface cannot be recovered from the key storage itself.
- The IV storage is secure, as long as it experiences no fault and no on-board subsystem attempts to update its contents.

- The PicoSkyFT processor is a critical part of the security policy – as such, any code allowed to execute on it must be checked for tampering.
- There is a data flow loop across the Ground Station to AES decryption to Ground Station blocks. As such, there is a possibility of a timing attack being carried out on the AES decryption core. However, due to the fact that the AES core is implemented as a logic state machine and the fact that the TM reports only a single alert that must be manually cleared, the execution of such an attack over a variable RF link is extremely improbable.

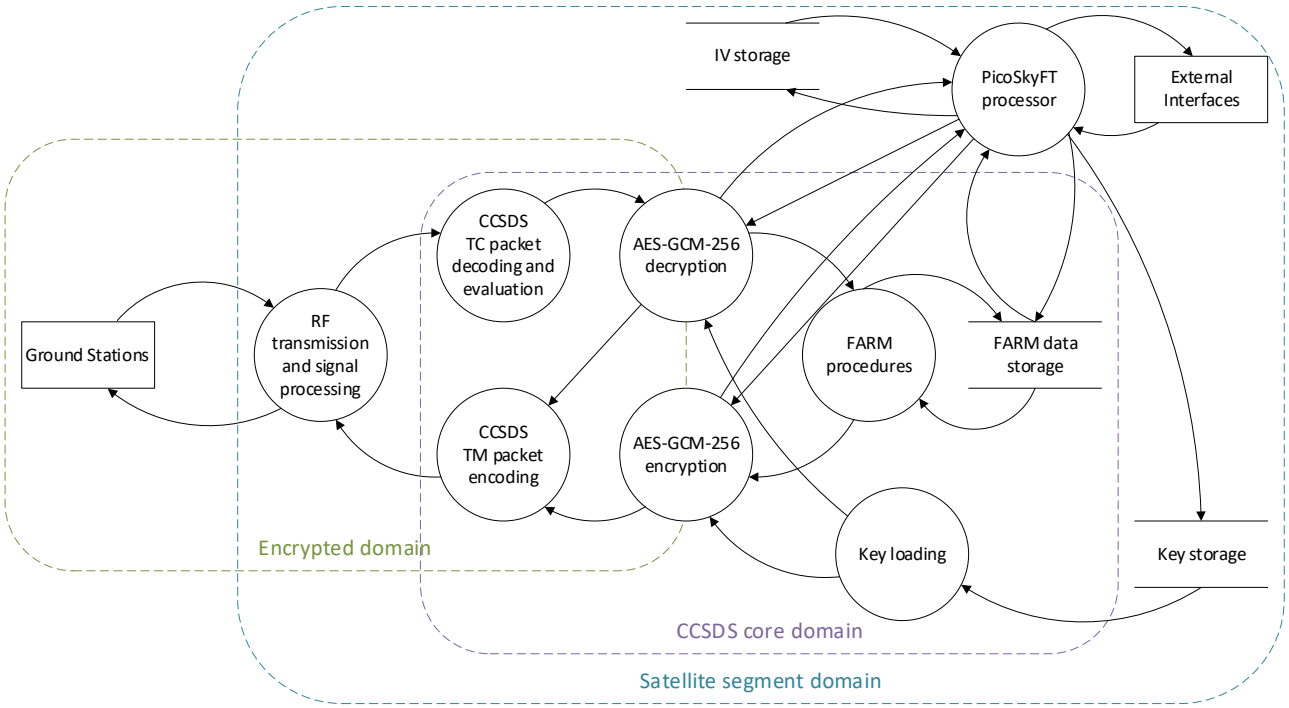

Figure 11: Threat model of the NANOlink security implementation

4.3 List of potential threats, their mitigation and risk assessment

The list of potential threats can be split into several categories. The first two important ones are key exposure threats and IV reuse threats. An additional category that is considered is tampering-related threats. The final category is a lockout from satellite due to the security policy and other miscellaneous situations.

Table 1: List of potential threats

Threat	Mitigation	Risk assessment
Key extracted from NANOlink via external interfaces.	Key storage features a “write only” interface and as such, keys are not accessible from external interfaces.	No risk.
Key extracted from NANOlink via timing attacks.	Due to nature of RF link and direct feedback data exposed over RF link, probability of successful timing attack is very low.	Acceptable amount of risk.
Key extracted from NANOlink via physical access (e. g. power analysis attacks, de-soldering components, signal analysis).	Impossible to prevent fully. Physical access safeguards must be observed when interacting with system with loaded keys by the integrator.	No risk once in orbit. Risk must be assessed from point of view of integration.

Key exposure during upload to NANOlink.	Impossible to prevent fully – keys are vulnerable to extraction when being uploaded. Safeguards must be employed during key uploading process by integrator.	No risk once in orbit. Risk must be assessed from point of view of integration.
Key exposure due to GS insecurity.	Outside the scope of this paper.	Outside the scope of this paper.
IV reuse due to too much messages sent.	If considering a NANOlink operating at maximum bitrate (4 Mbps), a total of more than 600 million years is required to cause IV counter rollover due to message transmission.	No risk.
IV reuse due to on-board fault.	IVs are stored in non-volatile memory, protected by EDAC and CRC and triplicated. A fault in memory device will also render the system unusable.	Acceptable amount of risk.
IV reuse due to command to roll-back IV counter.	Outside the scope of this paper – GS access must be managed so this does not occur.	Outside the scope of this paper.
Tampering with PicoSkyFT processor firmware.	All subsystems connected to CAN bus have capability to overwrite PicoSkyFT firmware – care must be taken that no subsystem has this capability.	Risk must be assessed during mission planning phase.
Tampering with FPGA running CCSDS core logic.	FPGA has dedicated programming path – physical access is required to tamper with it.	No risk once in orbit. Risk must be assessed from point of view of integration.
Tampering with key storage.	A “write only” interface is used – tampering can only cause satellite lockout.	See “Lockout due to key overwrite” entry.
Tampering with IV storage.	Tampering is possible through PicoSkyFT CAN interface – care must be taken that no subsystem has this capability.	See “Lockout due to IV storage overwrite” entry.
Lockout due to IV counter window.	IV counter window is user settable – the risk vs security analysis is required for each individual mission.	Risk must be assessed if any other subsystem is capable of overwriting IV storage without operator supervision.
Lockout due to key overwrite.	Care must be taken that no subsystem on board can initiate the key overwrite procedure without intent.	Risk must be assessed if any other subsystem is capable of overwriting key storage without operator supervision.
Lockout due to IV storage overwrite.	Can only cause lockout due to IV counter window. IV counter window is user settable – the risk vs security analysis is required for each individual mission.	Risk must be assessed if any other subsystem is capable of overwriting IV storage without operator supervision.

5 SECURE LINK PERFORMANCE

The NANOlink is capable of transmitting and receiving data at a raw bitrate of 4 Mbps using O-QPSK modulation. However, due to the use of the CCSDS protocols, some data overhead is present. In order to calculate the effective user-available data rate, the following equations were used, where:

$$R_{USER} = \frac{N_{DATA}}{N_{DATA} + N_{OVERHEAD}} R_{RAW} \quad (1)$$

The following table lists some common bitrates and configuration scenarios and gives their associated user-available data rates.

Table 2: Analysis of achievable user-available bitrate values

Scenario	Data size	Overhead size	Raw bitrate [kbps]	User bitrate [kbps]
Uplink smallest frame	6	60	4000	363.6
			250	22.7
			62.5	5.7
Uplink largest frame	981	200	4000	3322.6
			250	207.7
			62.5	51.9
Downlink full encoding	173	315	4000	1418.0
			250	88.6
			62.5	22.2
Downlink Reed-Solomon encoding	173	56	4000	3021.8
			250	188.9
			62.5	47.2
Downlink Convolutional Code encoding	173	243	4000	1663.5
			250	104.0
			62.5	26.0

In order to assure the performance of the proposed network, the link budget for a communication scenario was calculated. For the GS to Satellite link, a 4000 kbps raw bitrate using a directional antenna was presumed. In addition, a scenario with a 250 kbps raw bitrate using an omnidirectional antenna was also considered. For this scenario, a worst-case elliptic orbit with an apogee height of 750 km and a perigee height of 600 km was used.

Table 3: Slant range to spacecraft vs. Elevation Angle

Parameter	Value	Unit
Earth Radius	6.378.17	km
Height of Apogee (ha)	750	km
Height of Perigee (hp)	600	km
Semi-Major Axis (a)	7.053.17	km
Eccentricity (e)	0.010634	
Inclination (I)	98.61	degrees
Argument of Perigee (w)	180.0	degrees
R.A.A.N. (W)	7.00000	degrees
Mean Anomaly (M)	0.00	degrees
Period	98.250	minutes
dw/dt	-3.1102	deg./day
dW/dt	1.0488	deg./day
Mean Orbit Radius	675.00	km
	7.053.17	km
Sun Synchronous Inclination	98.09	degrees
Elevation Angle (d)	30.0	degrees
Slant Range	1.196.85	km.

Table 4: Proposed scenario link margin – 4000 kbps, directional antenna

Parameter	Value	Unit	Parameter	Value	Unit
Satellite			**Ground Station**		
Transmitter Power Output:	5.0	watts	Transmitter Power Output	50.0	watts
In dBW:	7.0	dBW	In dBW	17.0	dBW
In dBm:	37.0	dBm	In dBm	47.0	dBm
Transmission Line Losses:	-1	dB	Transmission Line Losses	-1.0	dB
Connector and Filter Losses:	0.0	dB	Connector and Filter Losses	-1.0	dB
Antenna Gain:	6	dBiC	Antenna Gain	34.0	dBiC
EIRP:	12	dBW	EIRP	49.0	dBW
Downlink Path			**Uplink Path**		
Antenna Pointing Loss:	-1.0	dB	Antenna Pointing Loss	-1.0	dB
Antenna Polarization Loss:	-1.0	dB	Antenna Polarization Loss	-1.0	dB
Path Loss:	-161.1	dB	Path Loss	-160.3	dB
Atmospheric Loss:	0.0	dB	Atmospheric Loss	0.0	dB
Ionospheric Loss:	0.0	dB	Ionospheric Loss	0.0	dB
Rain Loss:	0.0	dB	Rain Loss	0.0	dB
Isotropic Signal Level at Receiver:	-151.3	dBW	Isotropic Signal Level at Receiver	-114.5	dBW
Ground Station – Eb/No Method			**Satellite – Eb/No Method**		
Antenna Pointing Loss:	-1.0	dB	Antenna Pointing Loss	-1.0	dB
Antenna Gain:	34.0	dBiC	Antenna Gain	6	dBiC
Transmission Line Losses:	-1.0	dB	Transmission Line Losses	-1.0	dB
LNA Noise Temperature:	120.0	K	LNA Noise Temperature	300.0	K
Transmission Line Temp.:	300.0	K	Transmission Line Temperature	270.0	K
Sky Temperature:	450.0	K	Sky Temperature	200.0	K
Transmission Line Coefficient:	0.794		Transmission Line Coefficient	0.794	
Effective Noise Temperature:	539.1	K	Effective Noise Temperature	514	K
Figure of Merrit (G/T):	5.7	dB/K	Figure of Merrit (G/T)	-22.1	dB/K
Signal-to-Noise Power Density:	82	dBHz	Signal-to-Noise Power Density	91	dBHz
System Desired Data Rate:	4000	kbps	System Desired Data Rate	4000	kbps
In dBHz:	66.0	dBHz	In dBHz	66	dBHz
Eb/No:	16	dB	Eb/No	24.9	dB
Required Bit Error Rate:	10^{-6}		Required Bit Error Rate:	10^{-6}	
Required Eb/No:	12.0	dB	Required Eb/No:	12.0	dB
System Link Margin:	**4**	**dB**	**System Link Margin:**	**12.9**	**dB**

Table 5: Proposed scenario link margin – 250 kbps, omnidirectional antenna

Parameter	Value	Unit	Parameter	Value	Unit
Satellite			**Ground Station**		
Transmitter Power Output:	5.0	watts	Transmitter Power Output	50.0	watts
In dBW:	7.0	dBW	In dBW	17.0	dBW
In dBm:	37.0	dBm	In dBm	47.0	dBm
Transmission Line Losses:	-4.5	dB	Transmission Line Losses	-6.0	dB
Connector and Filter Losses:	0.0	dB	Connector and Filter Losses	-1.0	dB
Antenna Gain:	-5.0	dBiC	Antenna Gain	34.0	dBiC
EIRP:	-2.5	dBW	EIRP	44.0	dBW
Downlink Path			**Uplink Path**		
Antenna Pointing Loss:	0.0	dB	Antenna Pointing Loss	0.0	dB
Antenna Polarization Loss:	0.0	dB	Antenna Polarization Loss	0.0	dB
Path Loss:	-161.1	dB	Path Loss	-161.1	dB
Atmospheric Loss:	0.0	dB	Atmospheric Loss	0.0	dB
Ionospheric Loss:	0.0	dB	Ionospheric Loss	0.0	dB
Rain Loss:	0.0	dB	Rain Loss	0.0	dB
Isotropic Signal Level at Receiver:	-163.6	dBW	Isotropic Signal Level at Receiver	-117.1	dBW

Ground Station – Eb/No Method			Satellite – Eb/No Method		
Antenna Pointing Loss:	-1.0	dB	Antenna Pointing Loss	-1.0	dB
Antenna Gain:	34.0	dBiC	Antenna Gain	-5.0	dBiC
Transmission Line Losses:	-1.0	dB	Transmission Line Losses	-4.5	dB
LNA Noise Temperature:	120.0	K	LNA Noise Temperature	300.0	K
Transmission Line Temp.:	300.0	K	Transmission Line Temperature	270.0	K
Sky Temperature:	450.0	K	Sky Temperature	200.0	K
Transmission Line Coefficient:	0.8		Transmission Line Coefficient	0.4	
Effective Noise Temperature:	539.1	K	Effective Noise Temperature	545.2	K
Figure of Merrit (G/T):	5.7	dB/K	Figure of Merrit (G/T)	-36.9	dB/K
Signal-to-Noise Power Density:	68.7	dBHz	Signal-to-Noise Power Density	72.7	dBHz
System Desired Data Rate:	250	kbps	System Desired Data Rate	250	kbps
In dBHz:	54.0	dBHz	In dBHz	54.0	dBHz
Eb/No:	14.7	dB	Eb/No	18.7	dB
Required Bit Error Rate:	10^{-6}		Required Bit Error Rate:	10^{-6}	
Required Eb/No:	12.0	dB	Required Eb/No:	12.0	dB
System Link Margin:	**3.7**	**dB**	**System Link Margin:**	**7.7**	**dB**

The calculated link budgets shows that there is sufficient link margin on the communication link.

6 CONLUSION

The implementation of a practical secure communication link, that is based on the use of the CCSDS SDLS, SDLS-EP and other relevant standards, that was presented in this paper and integrated into the NANOlink communication subsystem, presents a configurable, secure and most importantly, low impact approach to add security to most satellite missions. By utilizing the CCSDS protocols, interoperability with existing ground station solutions is possible. As all the security-related processing is performed inside the RF transceiver, the approach offers to use to basically add-on security to an already existing satellite platform.

An important benefit of the presented approach is its low overhead – since the encryption is done entirely inside the SDR part of the system, no additional transfer latency is present. Additionally, the AES-256-GCM encryption imposes a 30 byte overhead on the uplink and downlink channels per message, in addition to all the other overhead that is a consequence of following CCSDS standards. For maximum sized messages, this means a minimum 3% security-related overhead for uplink messages and a minimum 15% security-related overhead for downlink messages. The security of the proposed implementation was verified by constructing and evaluating a detailed threat model of the transceiver system in combination with a secure Ground Station. Based on the threat model and subsequent vulnerability analysis, it is shown that the security offered by the presented approach is sufficient for most types of satellite missions.

7 REFERENCES

[1] S. DelPozzo and C. Williams, "*Nano-Microsatellite Market Forecast 10th Edition 2020.*" SpaceWorks Enterprises, Inc. (SEI), Feb. 05, 2020.

[2] "*CCSDS 355.0-B-1 - Space Data Link Security Protocol.*" CCSDS Secretariat, Sep. 2015.

[3] "*CCSDS 355.1-B-1 - Space Data Link Security Protocol—Extended Procedures.*" CCSDS Secretariat, Feb. 2020.

[4] "*CCSDS 231.0-B-4 - TC Synchronization and Channel Coding.*" CCSDS Secretariat, Sep. 2010.

[5] "*CCSDS 232.0-B-4 - TC Space Data Link Protocol.*" CCSDS Secretariat, Sep. 2010.

[6] "*CCSDS 131.0-B-3 - TM Synchronization and Channel Coding.*" CCSDS Secretariat, Sep. 2017.

[7] "*CCSDS 132.0-B-2 - TM Space Data Link Protocol.*" CCSDS Secretariat, Sep. 2003.

[8] "*CCSDS 232.1-B-2.1 - Communication Operation Procedure-1.*" CCSDS Secretariat, Sep. 2015.

[9] "*CCSDS 133.0-B-1.2 - Space Packet Protocol.*" CCSDS Secretariat, Sep. 2012.

[10] M. J. Dworkin, "*Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC.*" NIST, Nov. 2007.