# Rationale

## Key Management

Justification

Summary of capabilities

## SA Management

Justification

Summary of capabilities

## Security Unit M&C

Justification

Summary of capabilities

## FSR

Justification

Summary of capabilities

Relation to space link protocols

# Concept of Operations

## Key Management

Refer to the KM Green Book (includes key lifetime, …)

Illustrate key change scenarios (including OTAR, key verification, key change “on the fly” from frame to frame)

Implementing key life cycle with the procedures

Contingency and off nominal scenarios

Master keys versus session keys

## SA Management

Guidelines on planning & assigning SAs

Illustrate normal procedures for SA management: getting SA ready for use, rekeying a SA, ….

Implementing SA life cycle with the EP procedures

Contingency and off nominal scenarios (recovery SA, setARC, modify window, …)

Seamless key change (from frame to frame)

How to handle redundancy (e.g. : reconfiguring redundant command chain using nominal one, logical cross-strapping, …)

## Security Unit M&C

Illustrate nominal procedures for Security Unit M&C

Contingency and off nominal scenarios (using ping, self-test, …)

Rationale, definition and usage of Security Logs

Discussion of self-test (e.g. known answer test (KAT), …)

## FSR

Operating FSR together with Space Link Protocols (alternating CLCW/FSR, …)

How to interpret the flags including the alarm flag (persistant)

Concept of operations for handling alarm flags (e.g.: discriminating transmission problems from security events/attacks, using FSR as a first stage in troubleshooting on the link, …)

## Various types of implementation

Fixed keys, OTAR, dynamic management of SA vs static

EP PDU on-board path/processing (illustrate the different types of on-board architectures, in-band vs out-of-band signaling, implications of routing EP PDUs in OBC, …)