



# Implementing cryptographic security in space

Norsk kryptoseminar 2025, Einar Andreas Øvreneess, EIDEL AS

# ■ INTRODUCTION

## Company:

- **EIDEL AS**
  - 50+ employees at offices in Eidsvoll and Lillestrøm
  - <https://eidel.no/>
  - Founded 1966 in Eidsvoll
- **Products**
  - RCS – Radio Control System
  - RCDS – Remote Crypto Distribution System
  - EDDAS – EIDEL Distributed Data Acquisition System
  - SDL – Secure Data Link
  - SSL – Secure Satellite Link
  - ... and more

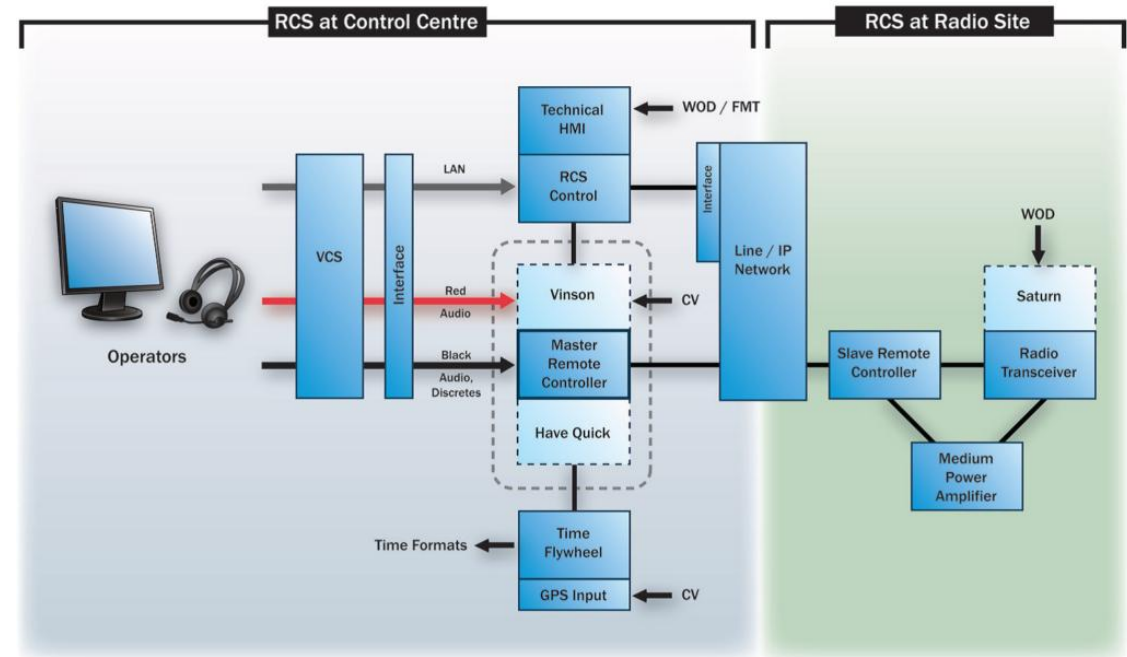
## Me:

- **Einar Andreas Øvreneess**
  - NTNU Technical Cybernetics
  - EIDEL 1997-
- **Systems Engineer**
  - «If possible, then how?»
  - Systems design, development and verification
  - Hardware, Firmware, Software, and some Mechanics and Analysis
  - Installation, training, maintenance and documentation
  - Systems Mid-Life Upgrade
  - ...

# ■ RCS - RADIO CONTROL SYSTEM

## User experience-driven technical design

- User experience gained from signals training, and additional technical training, used for designing the red-black interface in the Radio Control System
- First installation 1999
- 24-7 operation ever since
- System reprogramming time: ~2 years



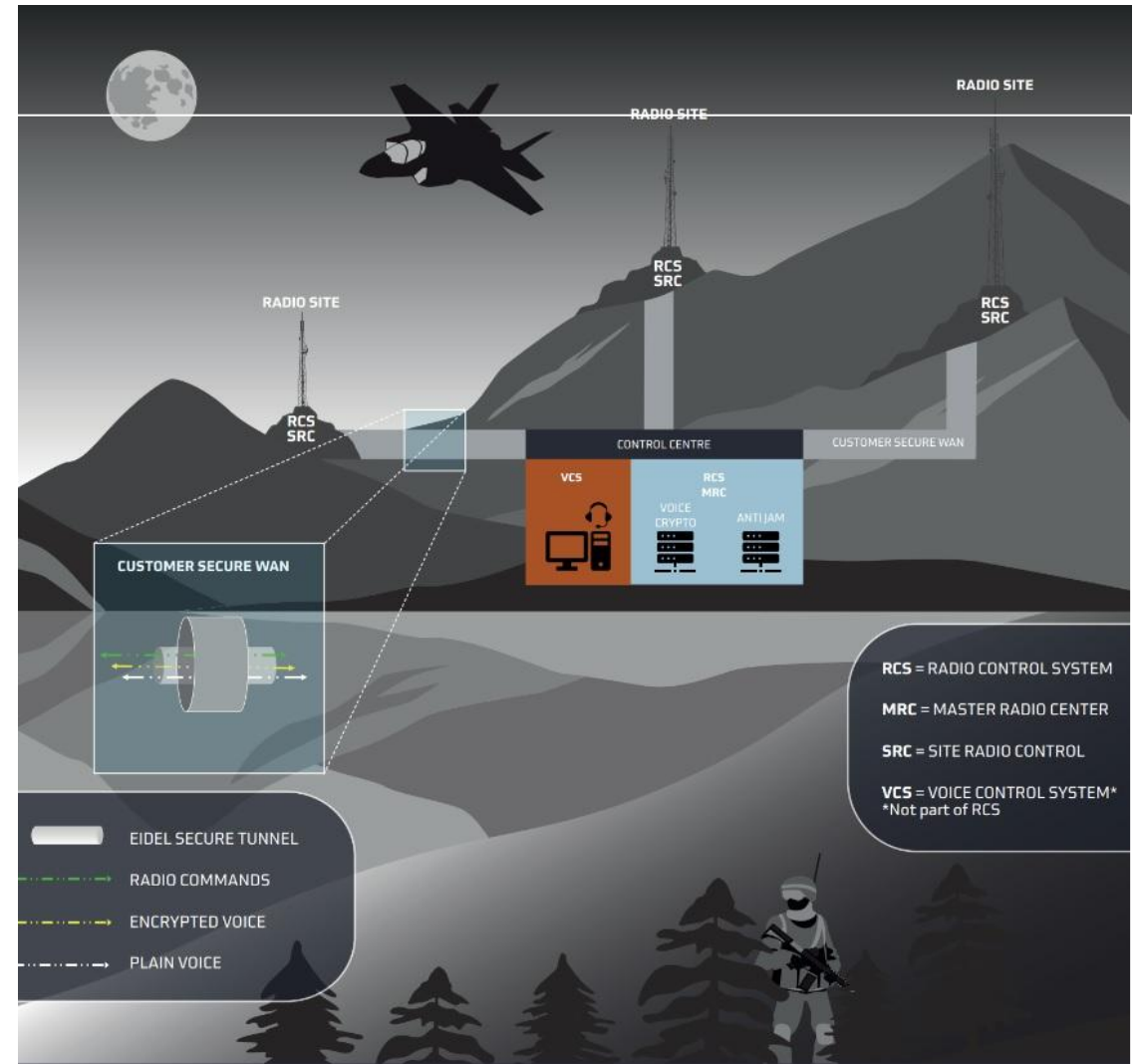
# ■ RCS - RADIO CONTROL SYSTEM

## User experience-driven technical design

- User experience gained from signals training, and additional technical training, used for designing the red-black interface in the Radio Control System
- First installation 1999
- 24-7 operation ever since

## Mid-life upgrade

- Using asymmetric algorithms for cryptographic signature of satellite reprogramming in a bread board demonstration (QUASAR)
- First upgrade 2023
- The red-black interface adopted to networking
- Embedded confidentiality and authentication between nodes for cryptographically protecting core system functions, despite being unclassified:
  - Reprogramming → Incrementally growing functionality
  - System time distribution → Availability



# RCDS – REMOTE CRYPTO DISTRIBUTION SYSTEM

«If possible, then how?»

- Question put forward in 2004
- Laboratory demonstration 2005
- First installation 2010
- NATO SECRET approval 2011
- Growing functionality



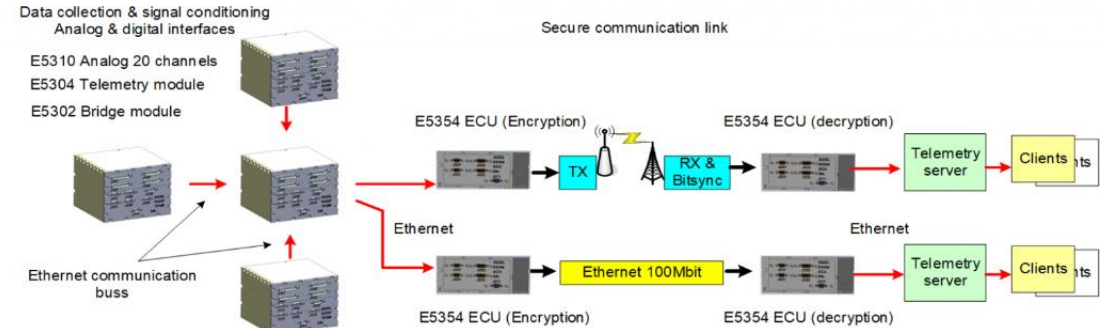
# ■ EDDAS – EIDEL DISTRIBUTED DATA ACQUISITION SYSTEM

## Life-style road-map

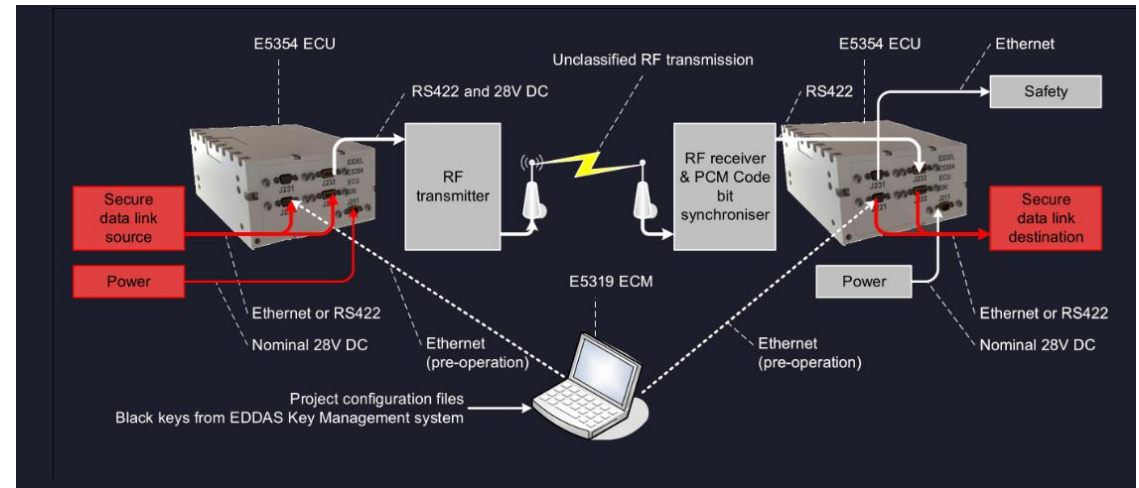
- Using asymmetric algorithms for cryptographic protection of satellite ownership – theoretical study
  - Started out with RSA → Advised by NSM into ECIES for confidentiality and ECDSA for authentication
- Plus, an abruptly terminated telemetry system development project, EDDAS (I)
- New EDDAS project → SDL red-black interface

## SDL - Secure Data Link

- E5354 ECU approval for HEMMELIG in 2014
- AES-256-GCM with cryptographic overhead applied pre-SDLS to the CCSDS TM protocol for a one-way data flow either over RF or over Ethernet
- ECIES-521 and ECDSA-521 protect black keys
- CIK - Crypto Ignition Key, for physical transfer



- Three roles for 5354 ECU:
  - KM – Key Management (Key generation)
  - AS - Acquisition System (i.e., encryption)
  - PS - Presentation System (i.e., decryption)



# ■ SSL – SECURE SATELLITE LINK

## Inspired by EDDAS

- Full duplex by two opposite one-way links
- No ECC, due to awaiting PQC at time of design
- New space+ technology for E5420 NCU for an intended 5+ years operation in LEO polar orbit
- Technology reuse from E5254 ECU for E5421 GCU
- Multiple parallel projects → Multiple variants!
- NorSat-4 launched 14<sup>th</sup> January 2025

*Illustration: FFI*



E5420 NCU

Nano-satellite Crypto Unit

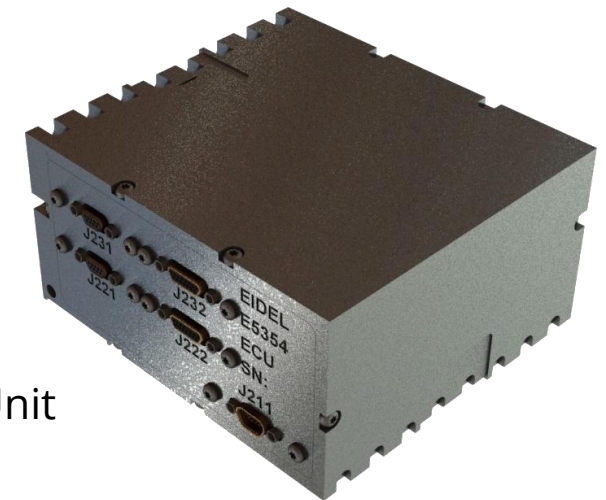


E5421 GCU

Ground-based Crypto Unit

Three roles for GCU:

- KM – Key Management (Key generation)
- KL – Key Loading (i.e., encryption and decryption, for instance being the remote unit at some pre-launch key loading event, where unclassified test keys are replaced by operational keys)
- GS – Ground Support (i.e., encryption and decryption)



# PAYLOAD PHASES

## Space segment

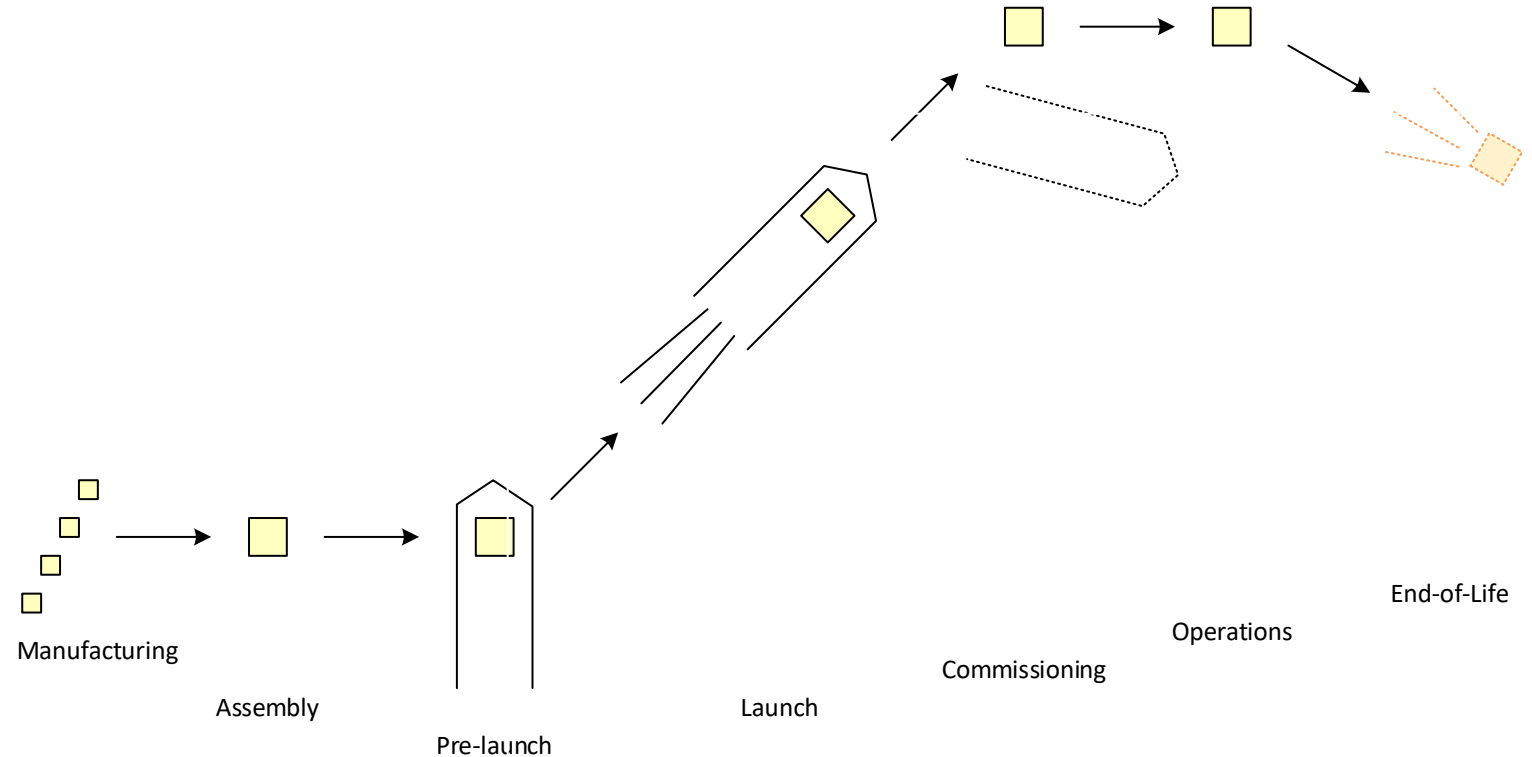
- Manufacture
- Assembly
- Pre-launch
- Launch
- Commissioning
- Operations
- End-of-Life

## Ground segment

- Can follow the same timeline, or
- Can be regarded a continuous support environment

## Constellation

- Individually operated satellites, or
- Satellites that can communicate and operate together



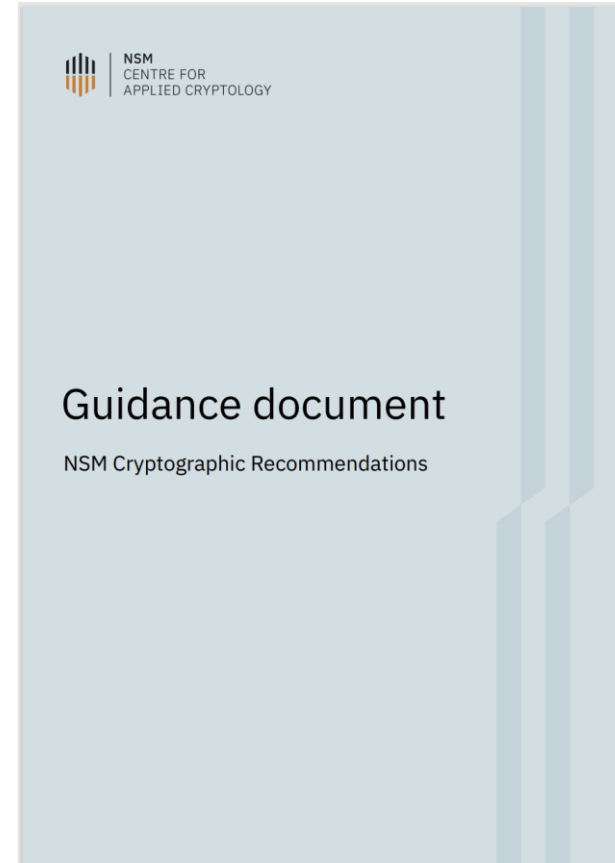
## ■ AND BEYOND?

### Implement PQC

- Hybrid mode i.a.w. NSM Cryptographic Recommendations
- Applicable for:
  - RCDS – cryptographic separation between security levels
  - EDDAS – black keys
  - SSL – multiple security levels, i.e., dual use technology

### Centralized key management

- Look into solutions for one-way links
- Look into link-agnostic key management (end-to-end)
- Look into distributed (national/company) key storage for confidentiality keys (COMSEC)
- Look into system-wide key storage for integrity and authentication (zero-trust)
- Look into solutions for supporting link availability equipment (TRANSEC)



[NSM Cryptographic Recommendations 2025.pdf](#)