IEC 61850 Cyber Resilient Electrical Substation Technologies (CREST)

Linwei Chen

30th October 2019

nationalgrid

Outline

- **Context**
- **Scope**
- **Progress**
- **Next Steps**

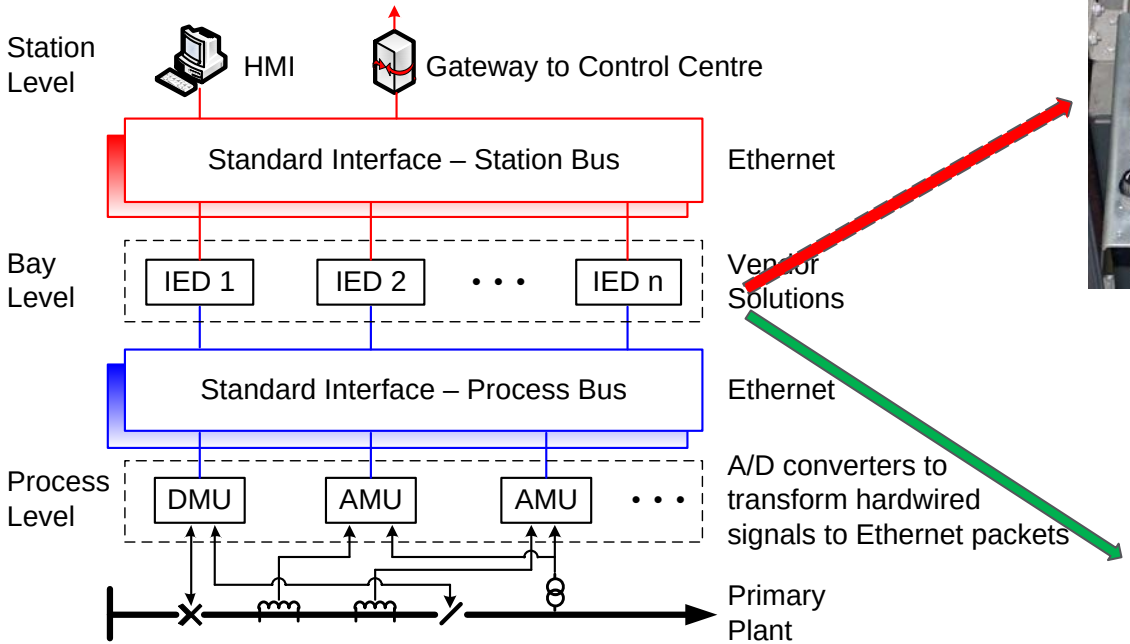
Context

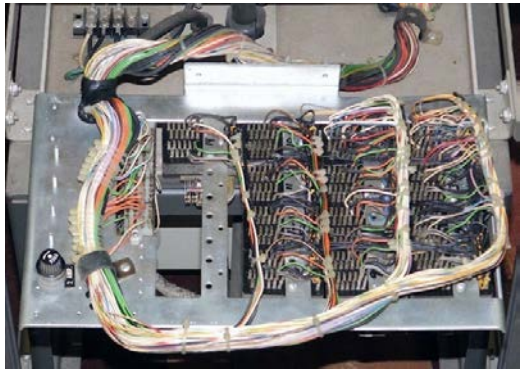
- P&C equipment for conventional substations:
  - Most solutions require hard wired interfaces at process and station level
  - Testing / commissioning requires long outages during installation, maintenance, replacement and extension
  - Equipment obsolescence / support cost

- To improve lifecycle value of P&C solutions, NGET has set up a research programme in 2008 to develop a new Architecture for Substation Secondary System (AS^3) based on IEC 61850.

Context

The AS³ Architecture





Notes:

- AMU: analogue merging unit that converts Amps / Volts to SV packets.
- DMU: digital merging unit, which converts P&C signals to GOOSE packets.

Context

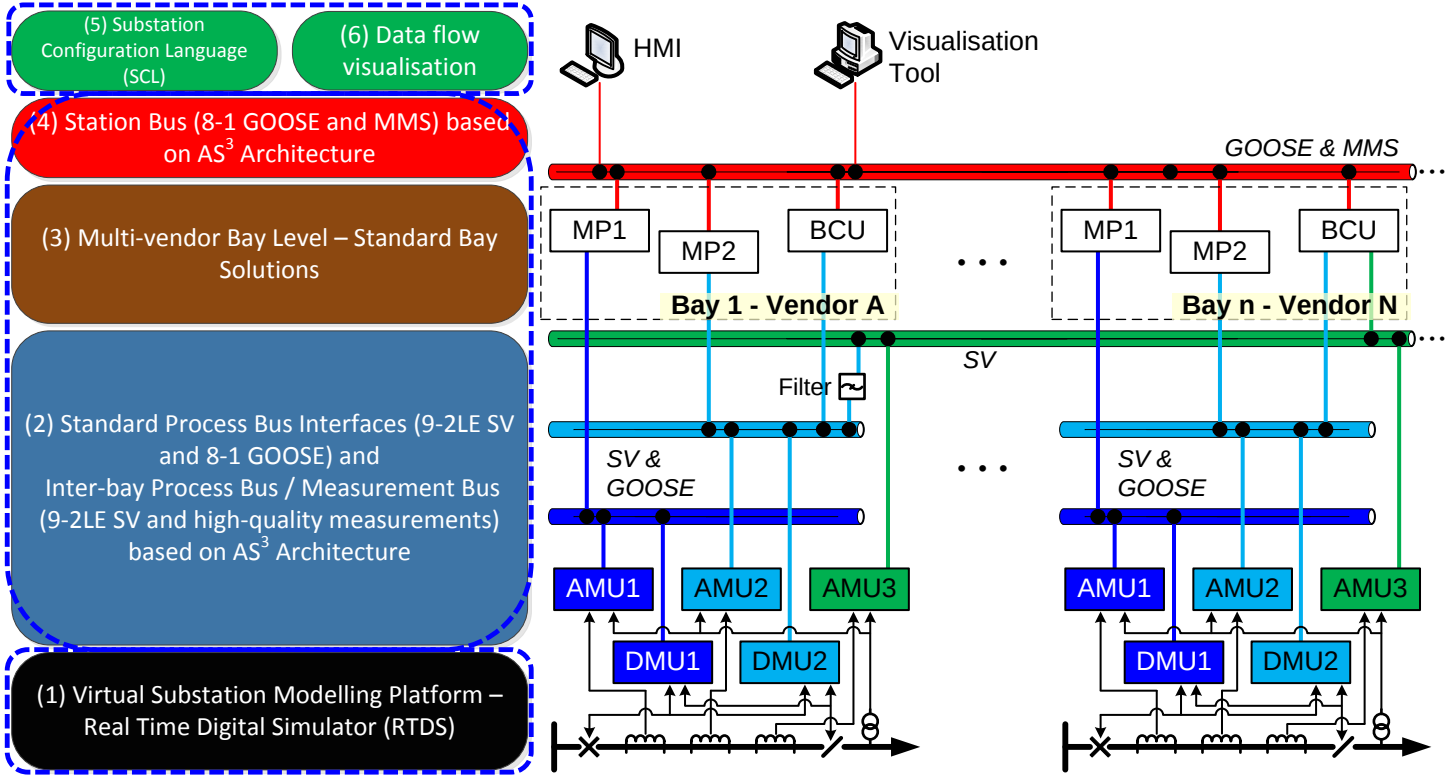
- As a proof of concept, NGET completed the VSATT (Virtual Site Acceptance Testing and Training) project in 2018.

- The project was supported by key suppliers and delivered the following:
  - Development of a multi-vendor IEC 61850 test platform,
  - Development of a visualisation tool to monitor network traffic (GOOSE / SV),
  - Interoperability at process bus and station bus level has been assessed,
  - Engineering process and SCL configuration tools have been investigated.

- Findings and interoperability issues have been fed back to suppliers for following up.

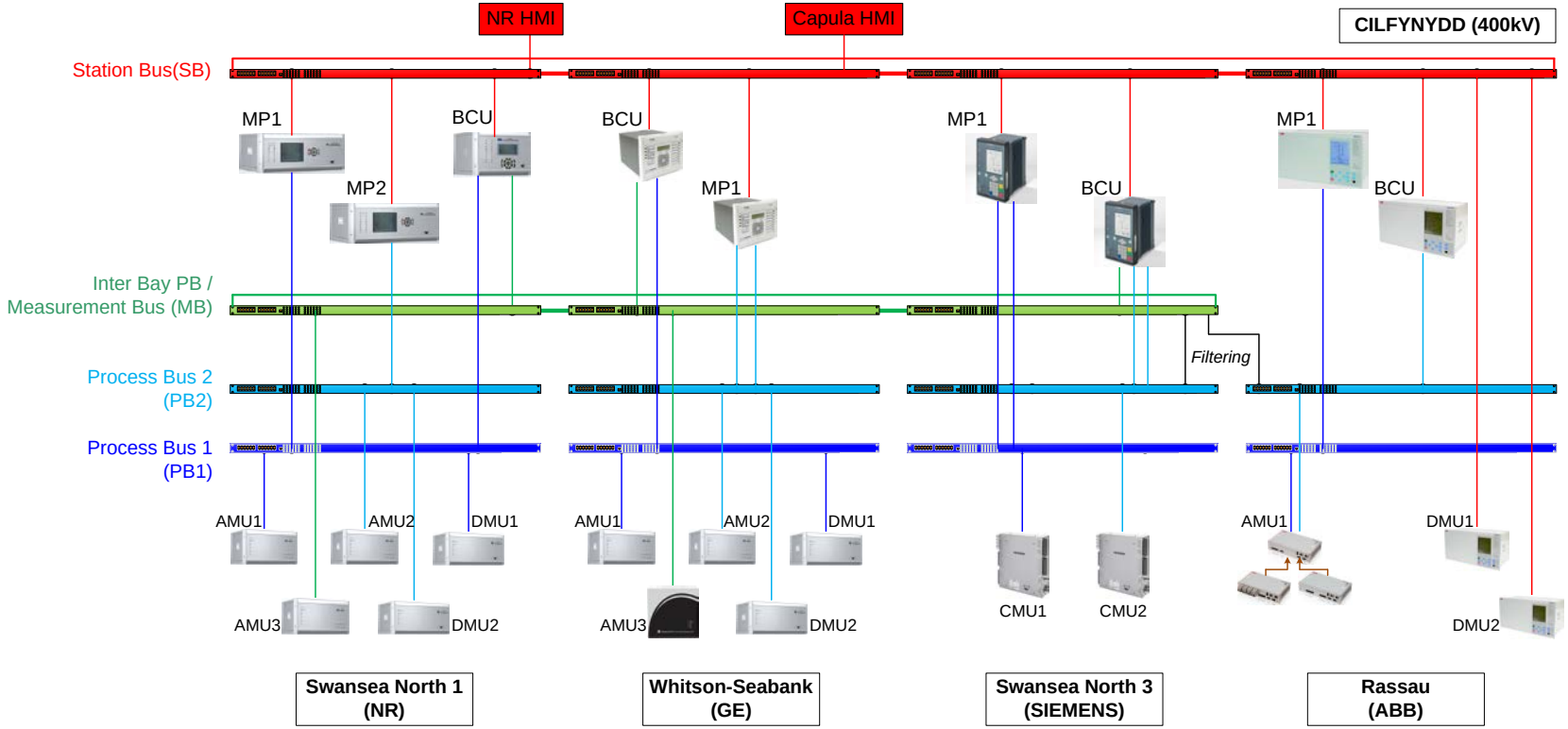
Context

The VSATT Platform – Overview



Context

The VSATT Platform – Multi-vendor Solutions



Context

- VSATT has enabled NG to proceed with the first Process Bus (PB) applications, i.e. PMU
- Further projects are in the pipeline – Busbar Protection (BBP), Delayed Automatic Reclosing (DAR) Blocking
- Follow up technical investigations with business case (RFI)
- During the VSATT project, it became clear that a number of issues merit further investigation, in particular the resilience and cyber security aspect to support wider roll out -> CREST project

CREST Scope

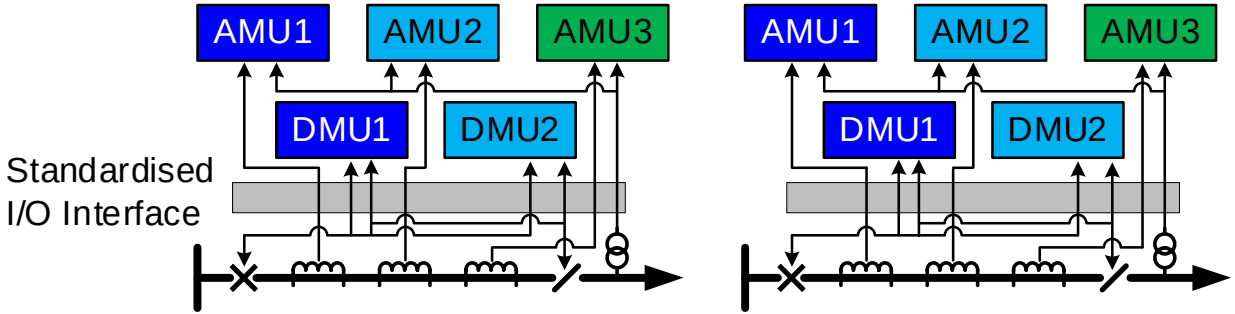
- Review on the current state of the art and available technologies to secure IEC 61850 substation communications and all types of access
- Investigate available tools and technologies that help identify, prevent, detect, respond and recover from cyber related risks and incidents
- Configure and trial available products on the VSATT platform:
  - Intrusion detection systems (IDS),
  - Software defined networking switches,
  - Password management,
  - Secure devices access to operational equipment (checking/cleansing/signing),
  - Possibly global cyber security solution to manage secondary assets.

CREST Scope

- Study the resilience and cyber risk associated with IEC 61850 traffic:
  - SV (Sampled Values) vulnerability tests
  - GOOSE (Generic Object Oriented Substation Event) vulnerability tests
  - MMS (Manufacturing Message Specification) vulnerabilities
  - Failure modes and consequences
  - GPS dependence – particularly for unit protection
- Develop a specification describing how cyber security standards (e.g. IEC 62351 and IEC 62443) are to be applied on the transmission system.
- Develop new ways of protecting S/S P&C equipment - collaborative defence mechanisms, other new.

CREST Scope

- Additional open challenges from VSATT
  - Standardised I/O interface to reduce outage time – define and trial products/solutions,



  - Investigate feasibility of mixed digital and conventional S/S designs:
    - Synchronising of CB closure,
    - Busbar protection.

Progress

Literature Review

- Publications and standards (IEC 62351 and IEC 62443) related to Operational Technology (OT) cyber security:
  - Identify compatible literature from similar areas,
  - Analyse previous cyber events,
  - List preliminary requirements for risk and vulnerability assessment;
  - Identify technologies/solutions that would help protect systems against cyber events;
  - Identify state of the art intrusion detection solutions;
  - Analyse respond and recovery methods to mitigate impacts.

Progress

Technology Review

- Study currently available technologies and solutions to identify gaps:
  - Intrusion detection systems,
  - Software Defined Networking (SDN) based on OpenFlow,
  - Access control, e.g. remote authentication via LDAP/RADIUS,
  - Cryptography for GOOSE based on IEC 62351.

Progress

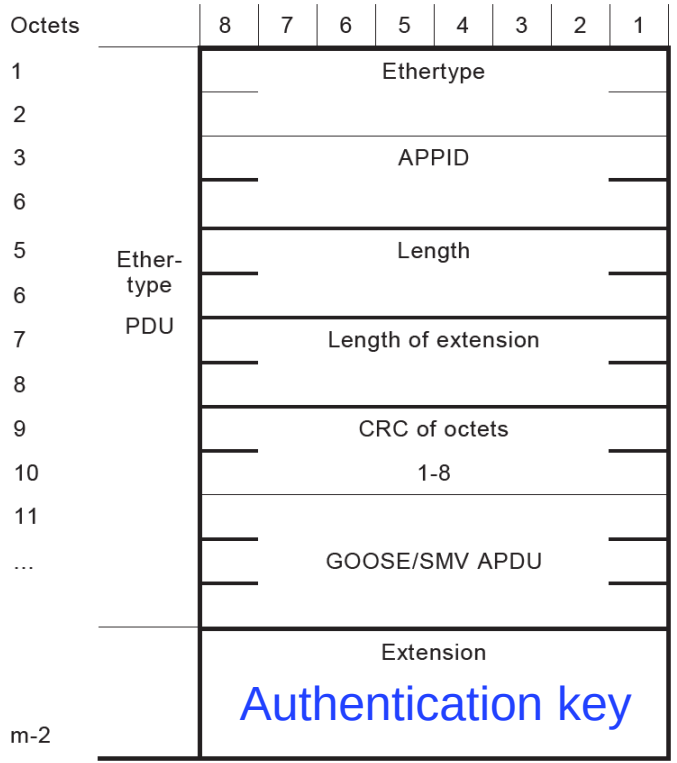
Technology Review

- Software Defined Networking (SDN) based on OpenFlow:
  - OpenFlow is a open protocol to create SDN,
  - It enables the creation of allowed traffic table that should include all substation communications,
  - SDN can facilitate fast recovery from failures,
  - The configuration process might be simplified by importing IEC 61850 Substation Configuration Description (SCD) files,
  - The interoperability between different switches to be reviewed.

Progress

Technology Review

- Cryptography
  - IEC 62351 addresses a number of security issues related to IEC 61850,
  - Message signing - It protects against alteration of data or the injection of malicious GOOSE,
  - Message encryption – besides the benefits introduced by message signing, this adds confidentiality to the data transmitted,
  - The performance of IEC 61850 solutions with cryptography to be reviewed.



Progress

Stakeholder Engagement

- Early engagement meetings with solution providers to trial cyber security products:
  - Intrusion detection systems,
  - SDN switches and controller,
  - Password management based on LDAP/RADIUS,
  - Patch management system for IEDs within a multi-vendor environment,
  - GPS firewall for IEC 61850 differential protection testing.

Progress

Initial IDS Demonstration

- Two intrusion detection systems have been set up on the platform to monitor substation traffic:
  - Mirroring ports created on the Station Bus,
  - Both need to initiate a database:
    - Database A created by importing pre-scanned traffic packets, it has an option to use Machine-Learning to adapt to the traffic changes,
    - Database B created by importing IEC 61850 SCD files.

Progress

Initial IDS Demonstration

- Databases require on-line tuning.
- No false-positive alarms under substation events, e.g. power system faults and remote control.
- A few low-priority alarms were detected:
  - Duplicated GOOSE alarms,
  - VLAN tags missing,
  - GOOSE timestamp not aligned to UTC,
  - Public internet IP address space used.

Next Steps

- Continue IDS testing with:
  - Background traffic injection and packet modification/duplication,
  - Comms/device failures,
  - Maintenance activities, e.g. IED re-configuration and setting update,
- Set up SDN testing for Station Bus / Process Bus
- Develop a collaborative defence mechanism to secure IED responses to cyber events
- Dissemination:
  - IET DPSP 2020,
  - CIGRE Paris 2020.

nationalgrid