Centralised Threat Management

ESB Networks

Jonathan Sandham

Future Networks
ESB Group:-

- ESB – Generation, Supply, DNO
- Population 4 M - 2,2m Electricity Customers
- Dispersed Population
  - 200,000kM Network
  - 230,000 Transformers
- System Peak: 5,035 MW
- 78% Wind integration
- 30% of daily peak is data
Short History of Telecoms in ESB

1960's
- Analog uWave
- DCC

1970's
- Digital uWave
- FO/OpMux

1980's
- Satellite
- CU Cable

1990's
- Polling Radio/PMR

2000's
- GPRS

60s 70s 80s 90s 00s
Extensive Telecommunications Network Built Up

- Fibre Network
- Microwave Radio
- Polling Radio
Current Grid Requirements

- Power Line Carrier
  - Teleprotection systems
- Point-to-Point Circuits
  - Teleprotection systems
  - OMS
  - TSO SCADA circuits
  - Energy Management Systems
  - Energy metering
  - Event recorders
- Disturbance recorders
- Polling radio network
- DSO Networks SCADA circuits
- OpTel - Operational Voice Services
- Private Mobile Radio
  - Private Mobile Radio
  - TETRA
  - Hand portable Radio Systems
- General site alarms
  - General Station Alarm
Future “smarter” Grid Requirements

- IP based SCADA communications.
- IP enabled polling radio. (also capable of supporting legacy SCADA protocols)
- Enhanced communications for secondary substations.
- Sensor Network communications.
- Smart Grid backhaul.
- Improved communications for energy meters & quality of service monitoring.
- Time distribution using IEEE 1588– alternative to GPS.
- Private IP Mobile Radio Network.
- Physical site security using IP Video surveillance.
- Physical site security using access control mechanisms.
- Smart Metering communications.
- IEC 61850 based communications.
- Smart Metering/AMI (1.4 million urban, 0.8 million rural)
- HV demand response
- Substation & Distribution Automation
- Embedded Generation
- LV control and loop automation
- Demand side management
- Other
  - Emergency Telephony
  - Outage and Fault Management
  - Asset Management and Monitoring
  - Mobile Workforce Management

www.esb.ie/esbnetworks
The Communications Challenge

Solutions

- GPS
- Fibre
- PLC
- Microwave
- Satellite
- Mimomax
- Copper
- GPS
- Polling Radio
- 4G Wireless/Wimax/LTE (Public/Private)
- Global M2M
- 2G Wireless (GPRS)
- Mesh Radio
- PLC

Criticality

ESB Network Volume

- 400 kV: 4 → 7
- 220 kV: 32 → 38
- 110 kV: 168 → 200
- 38 kV: 505 → 535
- 20 kV/10 kV: 230,000
- Meters: 2,200,200

Smart Grid

www.esb.ie/esbnetworks
What Exists today?

- Enterprise network – standardised, modular, centralised, understood, high levels of change, medium levels of change control
- Control system Network – decentralised understood but complex, resilient by design, managed 24x7x365, outages are not tolerated
- Operations and Control - centralised understood but complex, resilient by design, managed 24x7x365, outages are not tolerated
- Security and physical site management control
Security to date

- An addition
- A cost
- Useless
- An Inconvenience
- An Overhead
A historical perception of security

- Security is in a silo
- Systems cannot exercise their effectiveness or benefit
- Reporting failed to reflect benefit
- Single use case associated with Security Systems and services
A new approach?

- Introduce mechanisms to monitor, visualise and measure security at all levels
- Integrate security into day to day processes and disperse the function across your organisation
- Create benefit from the integration
- Understand and leverage all opportunities presented by security
- Maintain vision
How do we approach radical change?

- **Influence**
  - Organisation
    - Legislation
    - Regulation
    - Monetisation
    - Risk ... ation
  - User
    - Awareness
    - Best practice
    - Approach
We don’t have to do security… yet
Safety is a core, Security should be too.
Take a global view, identify influencers from external points
Liaise with groups which have influence and ensure organisation is directed in the correct manner
- Price review - tie security to CI
- CERT
- Information Exchanges
- Government
Users – the weak link?

- Users are not security conscious – no,
- Users are not aware of security in the context of cyber
- Incentivise the contextualisation of security
  - Training – It’s the most effective mechanism engine you have
  - Approach
  - Best practice
  - Competance
iSOC – Integration… into what?

- Socialisation of security at all levels within the organisation.
  - Vigilance and consistency are key
  - Drive from a single policy and justify based on common sense, add value by securing employees approach to security outside the workplace

- Day to day processes and existing known centres of strength and excellence
  - Enterprise/Operational NOC’s - Physical Security Centers - Operation centers work into their processes and ways of work – create value and incentive

- Communicate with key parties
  - Working Groups - Information Exchanges - Your national CERT – Government - Intelligence groups

- BUILD TRUST internally and externally
ESB’s SNOC vision

- **Existing Networks Operations Centre**
  - Purely customer focused – commercial and internal
  - Efficient operations and incident management – ITIL
  - Incidents and change a realised threat is just an incident

- **Connect with everything – leverage operational benefit**
  - SNMP
  - SCADA
  - Syslog
  - Reuse and recycle
  - Colocation or collaborative connectivity between all centres

- **Connect with people – Build relationships – build trust**
  - Internal groups
Effective organisation wide, threat management:

- Organisational awareness
- Secure living and practices in the workplace
- Preparing for failure
- Security providing organisational value
- Enabling vision into process and organisational state

Effective centralised threat management is

- A framework to collaborate
- A platform which seamlessly integrates
- A resource which has value to ALL stakeholders
- Derived from existing organisational strengths
Thank you