Energy Cyber Security Joint Operator and Vendor Seminar

Procuring secure operational technology

Justin Lowe

7 February 2018

Setting clear procurement requirements for OT is essential

Any changes to existing systems or services, or new assets or systems, require careful considerations for security:

- Unless you specify security requirements you are likely not to get any security

  - Commercial pressures mean that vendors and integrators generally do not include security features by default

- Bolting-on cyber security controls later is more costly and often less effective

- Increasing regulation means that there now potential penalties for security incidents increasing the need to get it right from the start

- Changes to existing systems can introduce security risks to an existing secure system

Setting clear procurement requirements for OT is essential *but not easy to do*

Why not?

- Security in ICS / OT is still maturing

- Many systems vendors and integrators are still building cyber capability (human and technology)

- Incompatible security solutions

- Operators being locked in to vendors' favoured security solutions

- High change control costs for adding in security later in the procurement process

- Existing guidance exists but isn't easy to use

Three principles for ensuring effective security requirements in OT procurement

1. Ensure systems and services are Secure by Design – and by default

- Ensure that security requirements are being thought about from the very early stages of the design – in parallel and in conjunction with functionality
- Sometimes simple design modifications at an early stage can reduce security risk

2. Treat security requirements in the same way as functional and non-functional requirements

- Security requirements are not special – they are just like other functional and non-functional requirements
- Ensure OT and security specialists work together to develop the security requirements

3. Include assurance of adherence to requirements in the process

- Build testing of security functionality and penetration testing into factory and site acceptance tests (FAT, SAT)
- Consider a blend of vendor provided assurance and independent testing
- Needs to be more than just a vanilla IT pen test

ENA/BEIS Energy Delivery Systems – Cyber Security Procurement Guidance

Designed specifically for Energy Delivery System OT procurements however may be applicable to other sectors

Developed by PA for BEIS and ENA in conjunction with industry and NCSC

Aligns IEC 62443, Smart Grid Architecture Model (SGAM) and NIS.

Audience – Procurement teams, project managers, those developing specifications, innovation teams, purchasers of systems or services, vendors and systems integrators.

Key elements

- **EDS Cyber Security Reference Model (CSRM)**

- **Process & guidance**

- **Procurement statements**

http://www.energynetworks.org/electricity/engineering/cyber-security-procurement-language-guidance.html
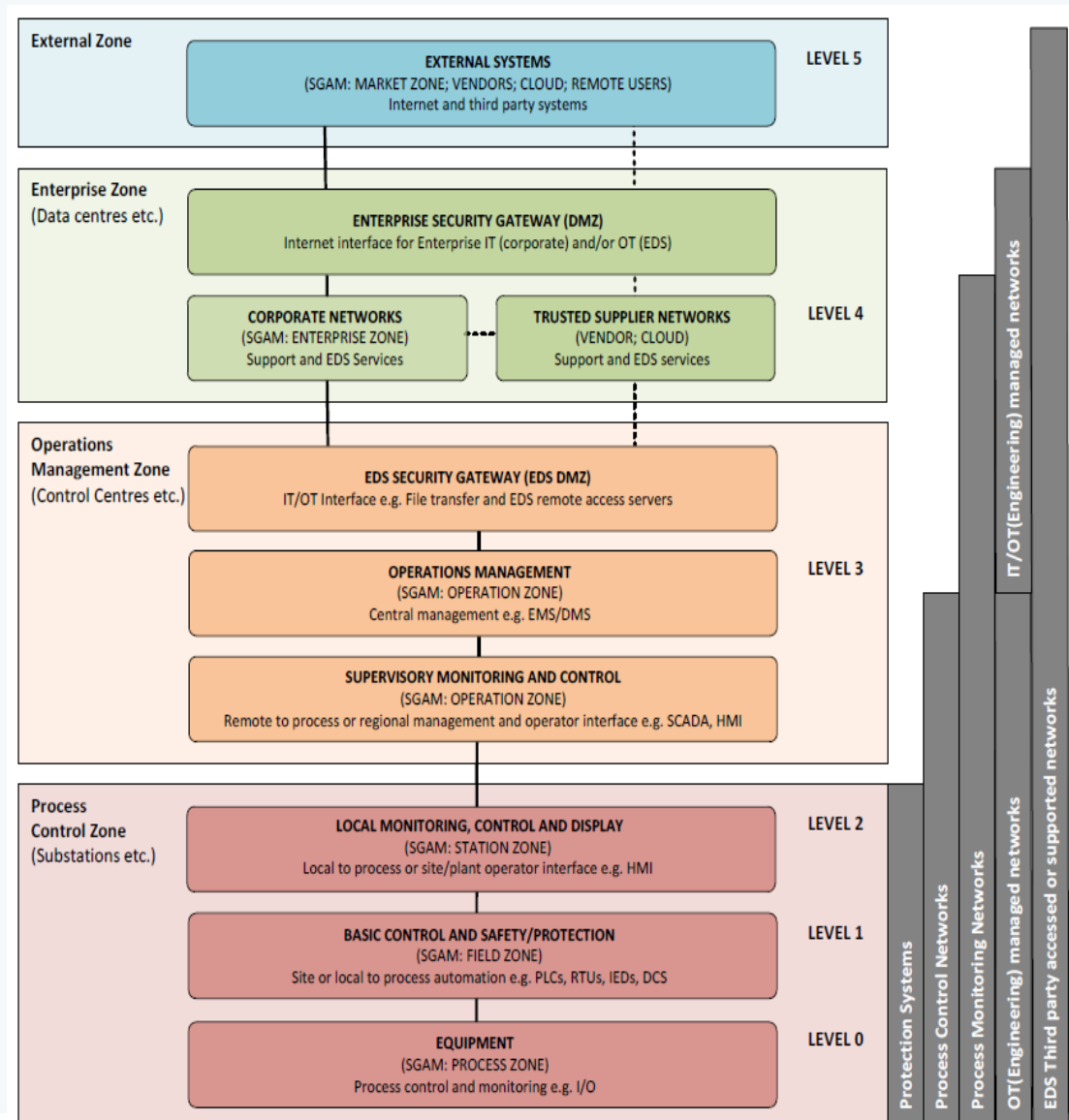
Using the Energy Delivery Systems Cyber Security Procurement Guidance to develop procurement requirements

Selecting Security Procurement Statements

1. Identify the reference security zone

2. Understand the security level

3. Select the reference statements

4. Tailor for use in the procurement process

5. Provide relevant information to the third party

6. Provide assurance that requirements have been met

Example Procurement Statements

The EDS – CSPG provides:

- **Aligned framework with common reference model**
- **Common terminology to enable operators, vendors, integrators and service providers to use the same 'language'**
- **A pragmatic process for defining security requirements for OT systems and services**

About PA.

An innovation and transformation consultancy, we believe in the power of ingenuity to build a positive human future in a technology-driven world.

As strategies, technologies and innovation collide, we turn complexity into opportunity.

Our diverse teams of experts combine innovative thinking and breakthrough technologies to progress further, faster. Our clients adapt and transform, and together we achieve enduring results.

We are over 2,600 specialists in consumer, defence and security, energy and utilities, financial services, government, healthcare, life sciences, manufacturing, and transport, travel and logistics. And we operate globally from offices across the Americas, Europe, the Nordics and the Gulf.

PA. Bringing Ingenuity to Life.