

# Use of certification when qualifying COTS Smart Devices – EDF Energy UK perspective

Dr. Silke Kuball, TCO, EDF Energy UK

19<sup>th</sup> May 2022

# Brief Introduction

## EDF Energy UK:



Part of EDF group,  
Major electricity provider in UK:  
**Generation:** Operating AGRs, PWR and Thermal, also  
Decommissioning activities.  
**New Build:** HPC EPR  
**Future:** SZC EPR



The work presented here draws on experience across the above (nuclear) fleet.

**My role:** Technical Lead of Software Assurance Team within TCO.

**TCO:** Technical Client Organisation: Provides Technical Capability and Subject Matter Expertise to all Licensees, exercises Intelligent Customer Role.

**Location:** Gloucester, UK; *Bristol, UK; Bridgewater, UK.*

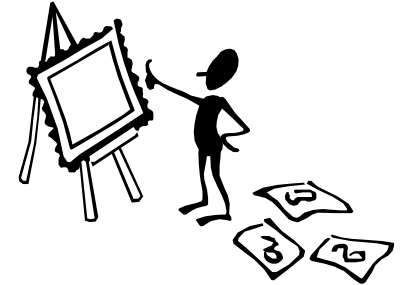
# Terminology: “Smart Device” ~ COTS digital device

Definition Smart Device (UK nuclear context):

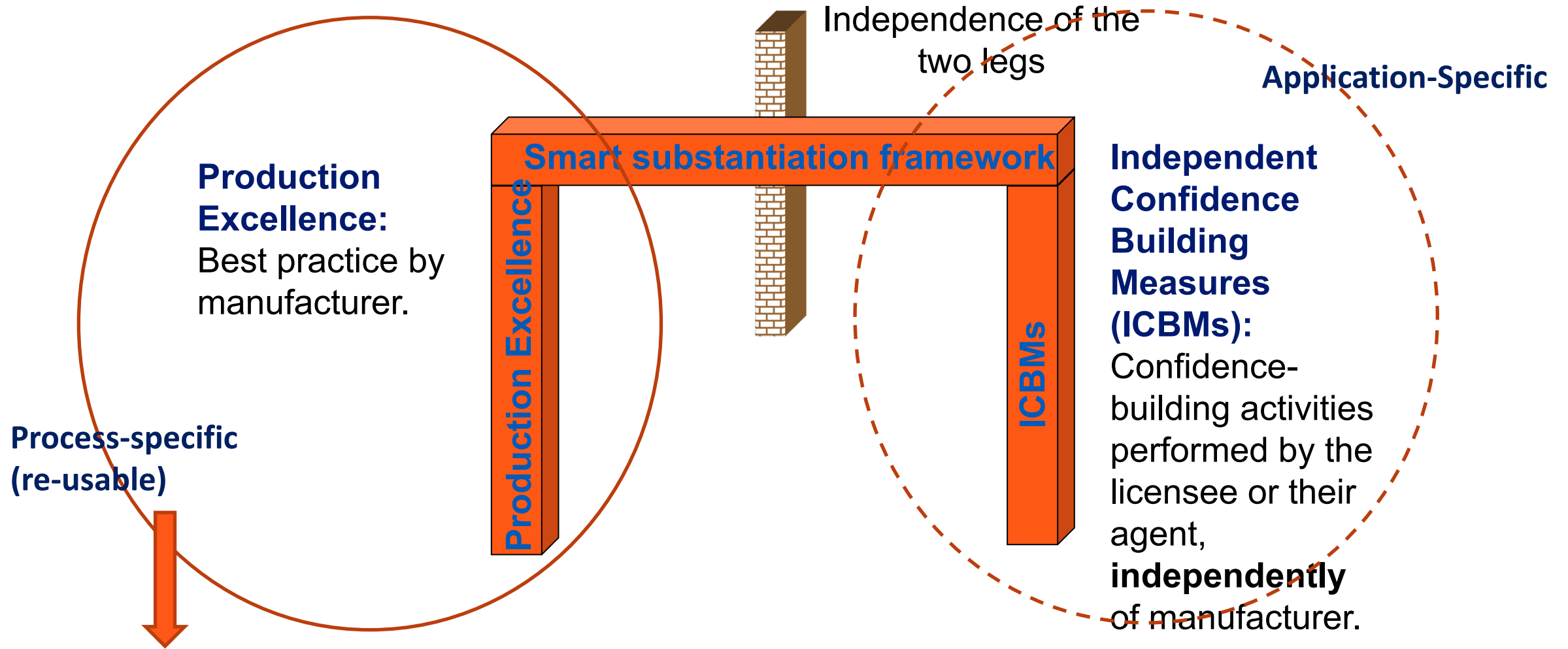
“Commercial off the shelf devices that perform a defined function, contain **intelligence in the form of** software, firmware or HDL-based components and are **not programmed by the end user – only limited configuration** is possible”

Note:

The end-user can usually configure the device to perform the functions required by their system. It may be possible to choose a processing algorithm or an operating range but it is not possible to add a completely new algorithm or range.



## Context: Smart Device Qualification in UK nuclear industry



**EDF “in-house certification” element for COTS Smart Devices**

# How do we demonstrate Production Excellence in EDF context?

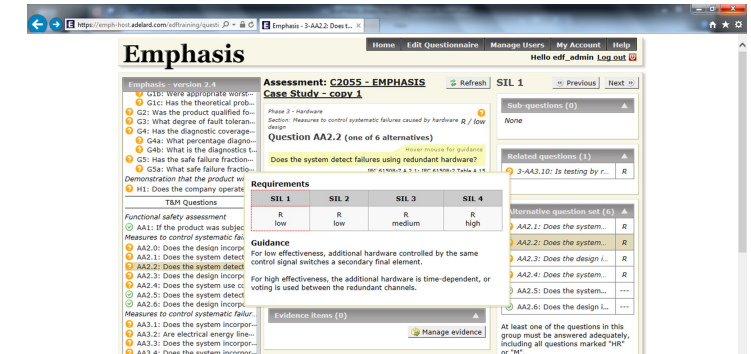
## 1) Existing Nuclear Generation :

Production Excellence: Delivered via EMPHASIS (based on IEC 61508 questions and T&M's but modified).EMPHASIS-assessed product. Assessed Devices database.

## 2) In New Build (HPC):

Production Excellence achieved via several options:

- EMPHASIS. As above. *Tried and tested.*
- For class 3  $10^{-1}$  (SIL 1): Audit at system supplier/manufacturer's site based on existing certification report and evidence. Sampling of evidence across lifecycle steps. Principle: Use certification report analysis as initial step and identify evidence to be viewed. *Awaiting first trial.*
- Other: Nuclear standards and IEC 62671.



↔ **Production Excellence can be seen as EDF “in-house method” of achieving “certification”**



←

→

https://emph-host.adelard.com/edftraining/questi

Emphasis - 3-AA2.2: Does t...

Home

Edit Questionnaire

Manage Users

My Account

Help

Hello edf\_admin

Log out

Emphasis - version 2.4

G1b: Were appropriate worst...

G1c: Has the theoretical prob...

G2: Was the product qualified fo...

G3: What degree of fault toleran...

G4: Has the diagnostic coverage...

G4a: What percentage diagno...

G4b: What is the diagnostics t...

G5: Has the safe failure fraction...

G5a: What safe failure fractio...

Demonstration that the product wi...

H1: Does the company operate

T&M Questions

Functional safety assessment

AA1: If the product was subjec

Measures to control systematic fai...

AA2.0: Does the design incorpo

AA2.1: Does the system detect

AA2.2: Does the system detect

AA2.3: Does the design incorpo

AA2.4: Does the system use co

AA2.5: Does the system detect

AA2.6: Does the design incorpo

Measures to control systematic failur...

AA3.1: Does the system incorpor...

AA3.2: Are electrical energy line...

AA3.3: Does the system incorpor...

AA3.4: Does the system incorpor...

Assessment: C2055 - EMPHASIS

Case Study - copy 1

Phase 3 - Hardware

Section: Measures to control systematic failures caused by hardware R / low design

Question AA2.2 (one of 6 alternatives)

Does the system detect failures using redundant hardware?

IEC 61508-7 A.2.1: IEC 61508-2 Table A.15

Refresh

SIL 1

Previous

Next

Sub-questions (0)

None

Related questions (1)

3-AA3.10: Is testing by r... R

Alternative question set (6)

AA2.1: Does the system... R

AA2.2: Does the system... R

AA2.3: Does the design i... R

AA2.4: Does the system... R

AA2.5: Does the system... ---

AA2.6: Does the design i... ---

Evidence items (0)

Manage evidence

At least one of the questions in this group must be answered adequately, including all questions marked "HR" or "M".

Requirements

SIL 1	SIL 2	SIL 3	SIL 4
R low	R low	R medium	R high

Guidance

For low effectiveness, additional hardware controlled by the same control signal switches a secondary final element.

For high effectiveness, the additional hardware is time-dependent, or voting is used between the redundant channels.

6

ENERGIFORSK Workshop COTS May 2022 | TCO PWR Technology I&C Branch | © Copyright 2022 NNB Generation Company (HPC) Limited. All rights reserved.

EDF

HPC

ENERGY

CCGN

# Current Role of **pre-existing** 3<sup>rd</sup> party certification (eg TUV, Exida...)

## 1) Existing Nuclear Generation Processes:

Production Excellence: Delivered via EMPHASIS (based on IEC 61508 questions and T&M's but modified), **IEC 61508 certification provides good basis for manufacturer having required evidence available but does not replace EMPHASIS process, does not play big role in EMPHASIS.**

## 2) In New Build (HPC):

Production Excellence achieved via several options:

- EMPHASIS. *As above.*
- For class 3  $10^{-1}$  (SIL 1): **Audit at system supplier/manufacturer's site based on existing IEC 61508 certification report and evidence.** Sampling of evidence across lifecycle steps. Principle: Use cert report analysis as initial step and identify evidence to be viewed. *Awaiting first trial.*
- Other: Nuclear standards and IEC 62671.

Requires  
manufacturer  
resource



## Historically: “Mixed feelings” regarding use of 3<sup>rd</sup> Party certification

- *“Certification should provide a level of confidence in the product and this should reduce the amount of effort required for qualification”.*
  - However, experience with 3<sup>rd</sup> Party 61508 certification has not been entirely positive.
  - Issues: high SIL claimed by manufacturer yet s/w development not part of certification; report not demonstrating adequate interpretation and scrutiny of and T&Ms; high-level statements in report with no avenue to retrieving detailed arguments or evidence.
  - Certification sponsored by manufacturer, does this influence rigour of assessment?
- ➡ 3<sup>rd</sup> party certification was hardly drawn on for qualification other than as “making it easier to assess”, and possibly as “additional compensatory evidence”.

- (How) Can we change this?





# First steps

- Difference between EMPHASIS and 3<sup>rd</sup> party IEC 61508 certification?
  - In principle the topics covered should be similar, the evidence required comparable.
  - How about the rigour of assessing evidence and dealing with non-compliances?
- In 2019 made initial contact with two organisations carrying out IEC 61508 certification (Org 1, Org 2).
- In-depth conversations with Org 1:
  - They had assessed a device D-1 that EDF was interested in.
  - They had good representation of assessors in UK.
- Org 1 presented their way of working, discussions with staff involved.
- Presentation on D-1 assessment.
- In alignment with EDF expectations.
- Agreement to conduct trial project, funded by EDF. Manufacturer agreed.




# Trial project



- Qualification of a valve actuator, which EDF require at SIL 2.
- Note: SIL 2 EMPHASIS requires high level of work and input from manufacturer.
- Aim: Identify whether/how Org 1 assessment (report, staff, work done, evidence) can be **transferred into a complete and accepted EMPHASIS assessment report**.
  - See what the differences/gaps are.
  - Identify whether existing Org 1 certification can be seen as equivalent to EMPHASIS assessment and under which conditions.
  - Draw on Org 1 and EDF staff, i.e. minimal use of manufacturer resource.

# Project Plan



ACTION PLAN			
WHO	WHAT	WHEN	HOW

- Steps:
  - Agree work scope (EMPHASIS assessment and report at SIL 2) and resource.
  - Place contract with Org 1.
  - NDA (EDF, Org 1, manufacturer).
  - Org 1 transferred references to evidence, knowledge and judgements into EMPHASIS question set.
  - Review by EDF.
  - Identify any outstanding points to be addressed with manufacturer of D-1.
  - Resolve gaps.
  - Write final report including lessons learned.
- Executed mostly during 2020-2021.

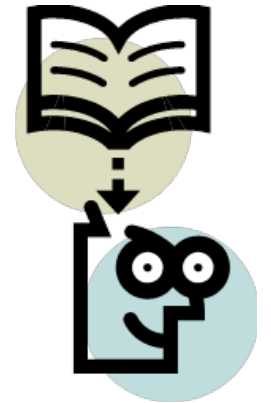
## Findings - 1



- High percentage of EMPHASIS requirements fulfilled by “porting” evidence and knowledge from CASS assessment into EMPHASIS.
- Some discrepancies identified, categorised, mitigated by other evidence or posed as additional questions to manufacturer.
- Required 2 hour meeting with manufacturer to close out open points and regular progress discussions with Org 1.
- Remote discussions between EDF and Org 1 due to Covid restrictions. Discussions were detailed w.r.t. T&M questions.
- Some discussions required involving the original assessors especially on sw-related questions.
- Due to resource issues, an “evidence sampling” activity between EDF and Org 1 has not yet been conducted. Planned under additional contract. Purpose is to validate process.

## Findings - 2

- CASS covers more s/w T&M questions (questions marked “R”) than EMPHASIS. This can be helpful to provide compensation against gaps against EMPHASIS elsewhere. It is useful to gather as much information as available rather than restrict to “checklist”.
- Certain questions in EMPHASIS missing from CASS templates, example:
  - How field data are monitored and analysed.
  - Informing customers of significant defects.
  - S/w with limited lifespan (cut-off dates etc).
  - Allow for primary output to be overridden.
  - Password protection of configuration parameters.
  - Independence between development staff and testers.
  - Tolerance to operator error, information to operator.
  - Behaviour under power recycle or loss of power. ETC
- Some of these can potentially be mitigated by alternative evidence from the CASS assessment.
- This was done for trial project but could be investigated generically.
- Need to review and re-assess EMPHASIS questions.
- Identify generic additional questions to address in addition to certification evidence.



# Results

- NDA still required covering all parties.
- Minimal assessment impact on manufacturer resource.
- Hopefully this process could achieve easier manufacturer “buy-in” than new assessment.
- Cost of external support (Org-1): was circa 40K for trial project. For SIL 2 assessment probably already cost-saving and no additional cost from manufacturer.
- Approach “merges” assessor role and role of “evidence-holder” into one.  
Beneficial since less onus on manufacturer and pre-existing familiarity with product.
- However: requires alignment between certifying organisation and UK licensee expectations.

## Next steps:

- Develop generic process for use of existing certification based on evidence-porting by a certification body into company-specific assessment process.
- Trial again (different device, different certifying organisation).
- Determine whether/how increasing confidence in certifying organisation would reduce need for sampling or even porting information.
- Revisit EMPHASIS questions, any changes?



## Open Questions/Points

- The more we work with a certification body, will it get easier to “reuse” existing certification conducted by them?
- The level to which we will need to sample evidence ourselves would need to be reviewed, would this reduce over time (or not)?
- What are our criteria on cert body in order to accept their work as “equivalent”, or to engage with them as “assessors” based on work they have already done?
- EPRI have guidance for cert bodies, is this helpful to us?

**Thank you!**

**Questions/Comments?**