Black Box Testing for Functional Safety

Dr. Silke Kuball
EDF Energy - Nuclear Services
Cyber and Software Assurance Group
20 November 2024

T6A Members

EDF Nuclear Services – who we are

- Part of the EDF nuclear family.
- Nuclear Services: Specialist technical business unit with niche skills.
- Supporting all of EDF Energy (UK) nuclear licensees (5 generating stations, 3 stations in defuelling, 2 new build projects: HPC and SZC).

Nuclear Services - C&I Cyber and Software Assurance Group:

- Security assessments for CBSIS (systems and devices, setting standards and expectations etc).
- Qualification of software-based safety related systems and devices (assessments, static analysis, testing, wider substantiation cases, innovation of reliability substantiation etc).
- Contributing to internal and external standards and Tech Reports.

Qualification of s/w based safety related components

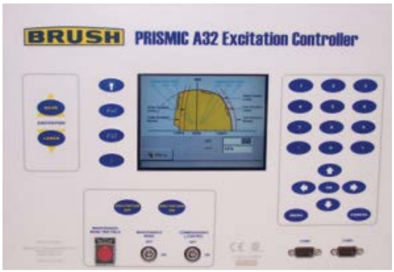
Aim: To implement technical measures to control and avoid systematic failure mechanisms of software – and complex-logic-based devices where they have nuclear safety significance → Risk Reduction.

Variable speed drives

Gamma monitor

Example devices

Safety Trip Alarm

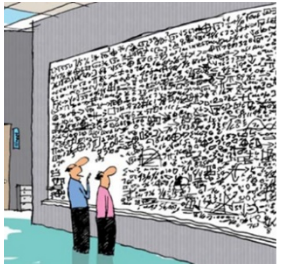


Automated Voltage Controller

Electrical protection relay

How do we achieve Functional Safety Aims?

EDF Nuclear Services



Use "qualification frameworks";

- Based on setting a target for required functional safety/ systematic failure probability (class/SIL/pfd etc).
- Employ qualification approaches to gain confidence that the device can meet target(s).

Qualification Frameworks:

Firstly: Standards compliance (e.g. IEC 61508, IEC 62138, IEC 60880 etc);

In addition: Use of additional specialist techniques to build confidence in:

- Properties.
- Absence/Mitigation of Vulnerabilities.

Example qualification framework -

For Software based Commercial Off the Shelf (COTS) devices

EDF Nuclear Services

Production Excellence

Emphasis Assessment

Leg 1

IEC 61508-based (Parts 1-3)

IEC 61508/ EMPHASIS

Assessment of manufacturer processes

Compensating Activities

Depends upon gaps found in Production Excellence e.g.
Review of CVs (By Licensee)
Module Tests (by Manufacturer)
Statistical Tests (by either)
SCA
etc.

Support

Independent Confidence Building Measures

Select From:

Leg 2

EIMT Records
Proof Test Records
Commissioning Tests
Hardware Reliability Analysis
Certification
Supplier Pedigree
Review of Tools
Prior Use
Static Code Analysis
Dynamic Analysis
Black-box testing
Others…

Additional Confidence Building - by Licensee or their agent. Application focussed

Assurance Techniques- similar to IEC 61508 T&Ms

Independence of the two legs

IEC 61508 Techniques & Measures Tables

- Black-box testing activities are listed for example as T&M for "software aspects of system validation"

Table C.7 – Properties for systematic safety integrity – Software aspects of system safety validation

(See 7.7. Referenced by Table A.7)

	Technique/Measure	Properties			
		Completeness of validation with respect to the software Design Specification	**Correctness of validation with respect to the software Design Specification (successful completion)**	**Repeatability**	**Precisely defined validation configuration**
1	Probabilistic testing	R1 (R2 if operational profile coverage targets are defined, justified and met)	R1 (R2 if required outputs are defined, justified and met)	–	–
2	Process simulation	R1	R1 (R2 if required outputs are defined, justified and met)	–	R2 Gives a definition of the external environment
3	Functional and black-box testing	R1 (R2 if operational profile coverage targets are defined, justified and met)	R1 (R2 if required outputs are defined, justified and met)	–	–
4	Forward traceability between the software safety requirements specification and the software safety validation plan	R1 Confidence that the software safety validation plan addresses the software safety requirements	–	–	R2 Confidence with a clear baseline of requirements under test
5	Backward traceability between the software safety validation plan and the software safety requirements specification	–	R1 Confidence that software safety validation plan contains no unnecessary complexity	–	R2 Confidence with a clear baseline of requirements under test

2 Types of Black Box Testing for Confidence Building

EDF Nuclear Services

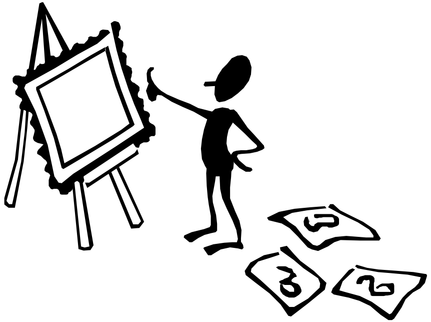
- **1) Statistical Testing (ST):**
  - **Tests are random generated from a probabilistic model of the device's anticipated operational use environment (model: Operational Profile).**
  - **Statistical tests are s-independent and identically distributed (**Result of any test not influenced by history/previous test-runs).
  - **Any occurring failure is detected.** Correctness checker needed (Oracle).
  - **Link to quantitative metric for probability of failure on demand (upper bound) and confidence level.**

α	pfd	N (number of failure-free ST tests)
0.9	0.01	230
0.95	0.01	298
0.95	0.001	2994
0.99	0.01	458
0.99	0.001	4602
0.99	0.0001	46049

- **2) Enhanced Functional testing (EFT):**
  - Collective term, sits between ST and traditional functional testing.
  - Informed by operational usage scenarios and application environment;
  - Tests can be specified to address weaknesses in the overall qualification or target specific areas of concern related to the application.
  - Can still use random variation of test parameters but: does not need to model operational usage distributions or s-independence between tests.
  - **Does not provide link to quantitative confidence in dependability (pfd/pfa) but qualitative confidence in areas of concern;**

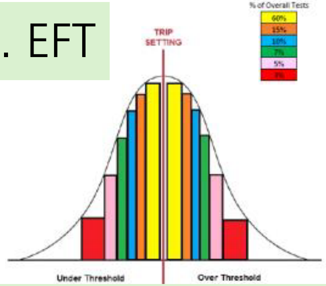
Specialist Black-Box Testing for Confidence Building

- EDF Energy NS use: Especially for higher integrity requirements or/and where there are significant gaps in standards compliance.
- How you employ these depends on the aim of the testing.
- SQEP input required to determine most appropriate testing approach.
- **Next: Some examples…**



Example 1: ST and EFT on Motor Protection Relays (Gas Circulators)

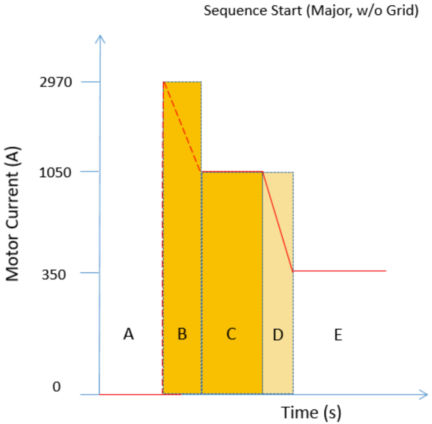
1. EFT



- Realistic checks of configuration
- Checks for spurious actuation

2. ST

- Confidence building in operation



Functions:

- Instantaneous Overcurrent (ANSI 50)
- Instantaneous Earth Fault (ANSI 50n/64)
- Thermal Overload (ANSI 26)
- Phase Imbalance (ANSI 46)

	Protection Function Weighting				
Profile	**Inst. O/C**	**Inst. E/F**	**TOL (Cold)**	**TOL (Hot)**	**Unbalance (PI)**
Unit Start-Up Sequence	0.25	0.25	0.25	N/A	0.25
Normal Operation Sequence	0.25	0.25	N/A	0.25	0.25
Depressurisation With Grid Sequence	0.25	0.25	N/A	0.25	0.25
Depressurisation Without Grid Sequence	0.25	0.25	N/A	0.25	0.25

Example 1- Outcomes

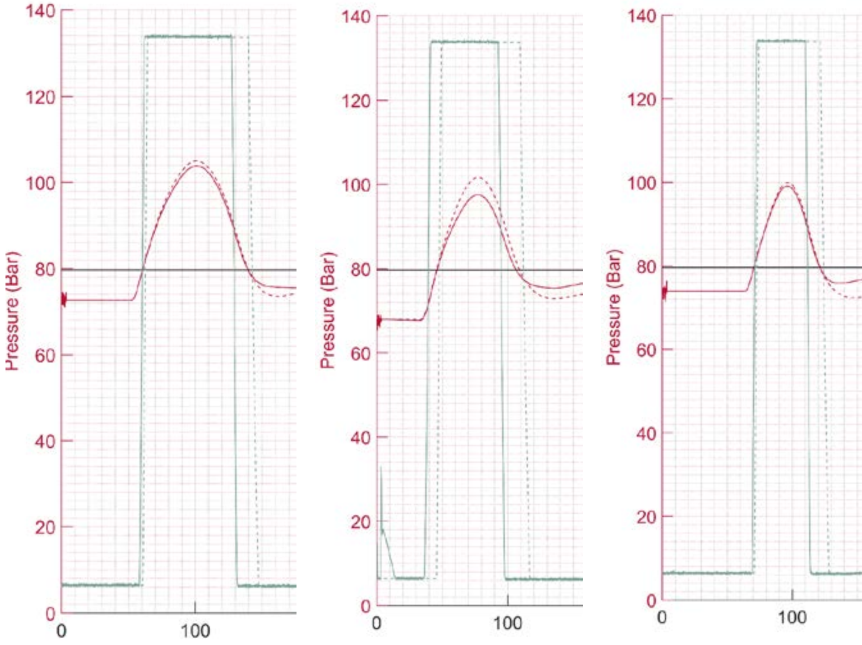
Time and Cost
- **Cost: Approx. (£50-70k) to perform testing**
- **Time taken: ~2 years but impacted by covid restrictions (approx. 3-6 months to specify tests and approx. 6 months to execute and analyse).**

Results
- **Combination of statistical testing and enhanced functional testing performed to support the test aims and the safety case requirements**
  - **Pfd better than 10^{-2} with high confidence demonstrated**
  - **Confirmation of correct configuration and suitability of the dual relay configuration**
- **Use of OEM facilities and expertise provided cost and time savings**
  - **OEM stated they would look to utilise some of these concepts going forward as part of their design activities.**

Devices are now installed on site and have been operating with no issues for over two years.

Example 2: ST on Pressure Relief Valve Controller

- Replacement of obsolete controller for venting Steam Generator pressure in controlled manner.
- Restrictions on production excellence assessment: ST chosen to build additional confidence.
- Plant model implemented using Simulink.
- Statistically representative variation of pressure transients:
  - Steam mains volume;
  - Starting pressure;
  - Pressure rise and decrease parameters.
- Oracle: new controller behaviour compared against a model controller and the obsolete controller.
- Testing detected a configuration issue.
  Due to lack of information on internal control algorithm (PI vs PID control).
- Rectified configuration and all tests passed.

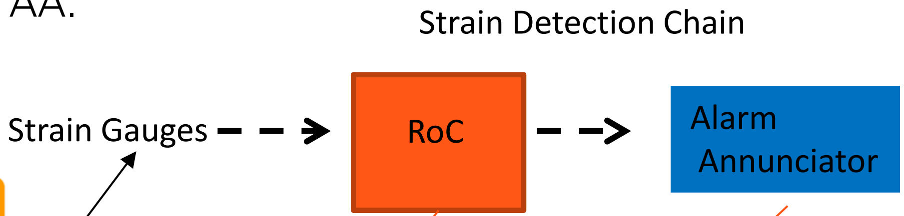


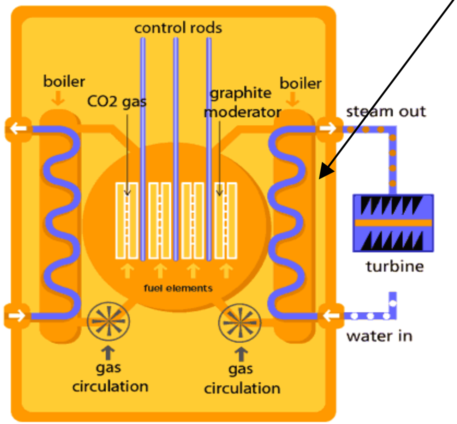
Example 3 –ST : Spine Break Detection

Aim of testing:

- Achieve confidence in a chain of 2 devices executing in sequence.
    - o Rate of Change detector (RoC);
    - o Alarm Annunciator (AA).
- Existing qualification no issue but: original target SIL’s not sufficient to combine into 10^{-2} **for ch**
- Extensive previous testing done but not on RoC alarm.
- Use of software-based config tool on AA.

⇨ ST chosen.



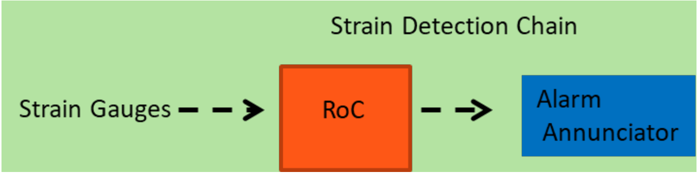


Devices’ under test (DUT)’s role:

- Detect when strain changes by more than 60 units over 7 seconds
- Alarm on ROC

Example 3 –ST : Spine Break Detection

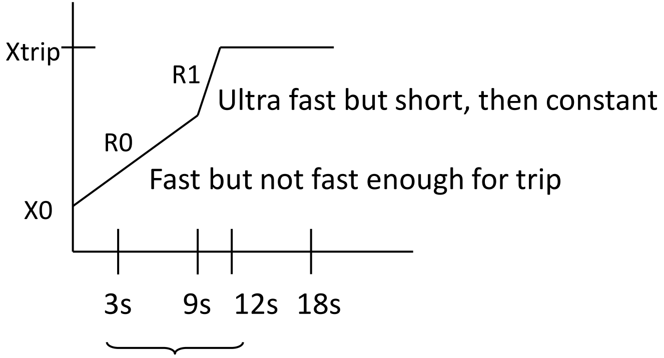
- No facility to test the sequence as a whole with large number of tests.
- Testing split over both devices with lower pfd target for each.



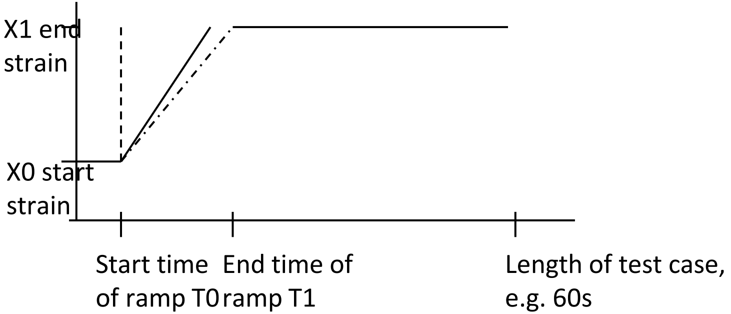
- **For AA:**
  - 50 sec long sequences of binary inputs feeding 4 group alarms simulating randomised input from RoC device.
  - Fault scenarios inserted on some (Power recycle, oscillation etc.) with random variation.
  - Circa 3000 tests in total.
- **For RoC:**
  - Simplified ramp types with randomisation - based on expert input.
  - > 3000 tests of circa 60 sec length each.
  - ~10% error insertion: (Broken Wire, Power recycle, Loss of power).

Example 3 –ST : Spine Break Detection

- **RoC device simplified ramps for ST testing:**



Achieves trip level between 3s and 12s but not in [0,7s] or [9s,18s]



Example 3 - Outcomes

RoC device tests:

- Initially Test results analysis (test failures) identified the following issue:
  - Failure to alarm for certain ramps close to but beyond trip condition.
- **Cause:** Undocumented feature in DUT which rounds down delta T in configuration to nearest 5 sec. Needs to be considered in configuring device.
- DUT re-configured to take into account the above.
- **Fresh set of tests rerun with no failures.**

Alarm Annunciator:

- Device restart time after power loss longer than expected.
- Device max response time longer than expected.
- Output flashing on input state change.
- **Clarified with manufacturer, accepted and added to operating instructions.**

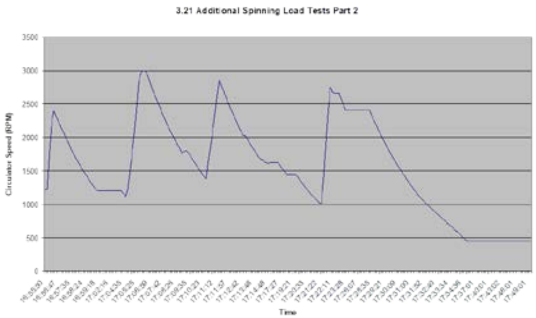
Overall: Test success and clarification of config requirements and device behaviour under meaningful operational sequences.

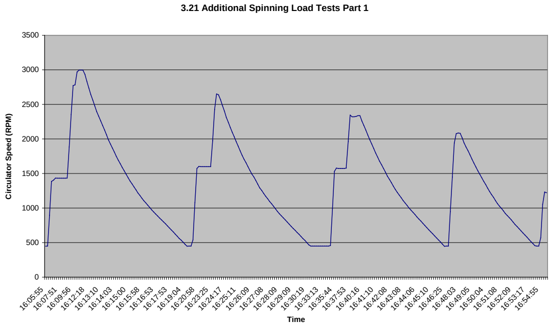
Example 4: Speed Drives – Gas Circulator Motors - EFT

EDF Nuclear Services

- FSA/EMPHASIS performed but some significant gaps.
- Drive not developed according to IEC 61508 lifecycle and use on EDF plant differs from standard u
- Reliability target SIL1/10^{-2} pfd due to system architecture.
- Compensatory activities performed. Testing one of them:
    - Addition to SAT: Testing of variations of motor starts, run ups and flycatching.
    - Tests of restarting drive after coasted down to variation of speeds.
    - No claim to be statistically representative of what will happen on plant, but:
        - Qualitative confidence in speed drive behaviour under variation of credible scenarios.
        - Additional validation of configuration tool.
- Testing successful and supported installation.

Example tests





Summary

- Statistical and other black box testing form very important and effective part of overall software-based system/device qualification.
- The aim of the testing needs to be clear: e.g.
  - Underwrite *quantitative* confidence in pfd upper limit claims;
  - *Qualitative* confidence e.g. under specific scenarios (edge cases, high risk demands, all usage scenarios etc);
  - Validation of requirements ("is this the right product given the real-world/plant environment?").
  - A combination of the above …
- Different aims suggest different approaches to black box testing.
- We use a variety of approaches informed by safety case need.
- Suitably Qualified and Experienced Personnel (SQEP) involvement required to design appropriate test regime.
- **For more information… talk to a member of our team.**

Thank You

Slot	Start Time	Paper	Workshop	Finish
9	14:35	Machinery Functional Safety with IEC 62061 and ISO 13849	Functional Safety Tool Qualification	15:05
-	15:05	**SHORT COMFORT BREAK** (Oak Room)		15:25