EQSA

Equipment Qualification
Services Alliance

tecnatom TÜVRheinland® element wood.

EQSA

Equipment Qualification
Services Alliance

tecnatom TÜVRheinland element wood.

Qualification of Smart Devices

Alan Poole
Wood

Introduction

- Qualification of Smart Devices
  - The presentation will focus on the qualification (substantiation) of smart devices (instruments) to perform their safety function and not the environmental qualification.
    - The term qualification is used generally to cover both environmental and performance demonstration
      - For the qualification of a device to perform its safety function substantiation or justification are often used.

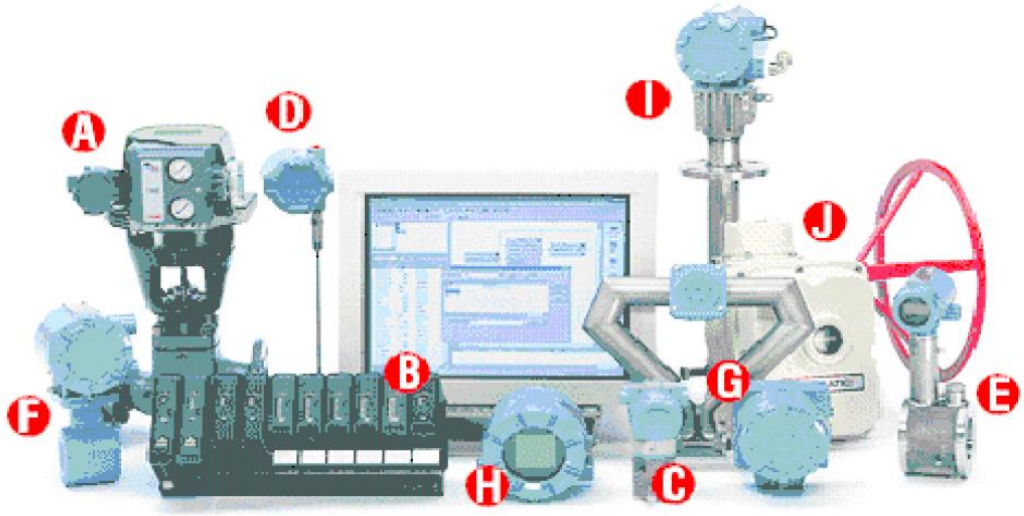
Presentation Topics

- What is a Smart device
- Why do smart devices need to be treated differently than non-smart devices
- UK Regulatory Expectations
- International Guidance
- Use of Standards
- Intelligent Customer Role
- Research
- Amount of effort for qualification
- Working Groups
- Challenges
- The golden thread

What is a Smart device?

What is a Smart instrument?

A=Modulating Valve, B=PLC/SCADA, C=Pressure,
D=Temperature, E=Vortex Flow, F=Magnetic Flow,
G=Coreolis Flow, H=pH, I=O_2, J=Motorised Valve



What is a Smart device?

- Definition in BS IEC 62671 - Nuclear power plants — Instrumentation and control important to safety — Selection and use of industrial digital devices of limited functionality

5.2.2 Applicability criteria for this standard

A digital device to which this standard may be applied shall comply with the following criteria:

a) The device is a pre-existing digital device that contains pre-developed software or programmed logic (e.g. an HPD) and is a candidate for use in an application important to safety.

b) The primary function performed is well-defined and applicable to only one type of application within an I&C system, such as measuring a temperature or pressure, positioning a valve, or controlling speed of a mechanical device, or performing an alarm function.

c) The primary function performed is conceptually simple and limited in scope (although the manner of accomplishing this internally may be complex).

d) The device is not designed so that it is re-programmable after manufacturing nor can the device functions be altered in a general way so that it performs a conceptually different function: only pre-defined parameters can be configured by users.

e) If the primary device function can be tuned or configured, then this capability is restricted to parameters related to the process (such as process range), performance (speed or timing), signal interface adjustment (such as selection of voltage or current range), or gains (such as adjustment of proportional band).

What is a Smart device?

- Examples of smart devices from BS IEC 62671
  - Pressure sensors
  - Temperature sensors
  - Smart sensor e.g. pressure transmitter
  - Valve positioner
  - Electrical protective devices, such as over-voltage/over-current relays
  - Motor Starters
  - Dedicated display units e.g. multi-segment LED bar displays or simple communications interfaces
- Other smart devices
  - Generator load shedding systems

What is a Smart device?

- Examples of devices that do not fall into the criteria in BS IEC 62671
  - Programmable Logic Controllers (PLC)
  - Devices provided with a programmable language, regardless of its restricted nature (in terms of number of function blocks (or equivalent) or inputs and outputs), where such devices have been designed to allow them to be configured for more than one application
    - E.g. single loop digital controller with a function block language.
  - Additional techniques are required to qualify PLCs

Why should smart devices be treated differently?

- The reliability of analogue and digital devices, which do not use software or firmware, can be calculated using standard techniques.
  - Failures rates of individual components can be used to calculate the overall failure rate of this type of device.
- Smart devices by their nature use software/firmware to deliver their function and the reliability of these types of devices cannot be easily obtained.
- ONR therefore expect additional tools and techniques to be applied to demonstrate the smart device can adequately perform its safety function.
  - Real life experience has identified latent errors that have caused erroneous operation.

UK Regulatory expectations

- ONR's Safety Assessment Principles

Engineering principles: safety systems	Computer-based safety systems	ESS.27
Where the system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design.		

422. The rigour of the standards and practices applied should be commensurate with the level of reliability required. The standards and practices should demonstrate 'production excellence' and, through the application of 'confidence-building' measures, provide proportionate confidence in the final design.

UK Regulatory expectations

423. ‘Production excellence’ is a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system. It should include the following elements:

(a) thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems;

(b) implementation of a modern standards quality management system; and

(c) application of a comprehensive testing programme formulated to check every system function, including:

(i) prior to installation on site, the verification of all phases of the system production process and the validation of the integrated system against its specification by persons not involved in the specification and design activities;

(ii) following installation on site, a demonstration that the safety system, in conjunction with the plant, performs in accordance with its specification. This demonstration should be devised by persons not involved in the system’s specification, design or manufacture; and

(iii) a programme of dynamic testing, applied to the complete system to demonstrate that the system is functioning as intended.

UK Regulatory expectations

424. Independent ‘confidence-building’ should provide an independent and thorough assessment of the safety system’s fitness for purpose. This should include the following elements:

(a) complete, and preferably diverse, checking of the finally validated production software by a team that is independent of the system’s suppliers, including:

(i) independent product checking that provides a searching analysis of the final system;

UK Regulatory expectations

(ii) independent checking of the design and production processes, including the activities undertaken to confirm the realisation of the design intent; and

(b) independent assessment of the comprehensive testing programme covering the full scope of the test activities.

425. When demonstrating 'production excellence' and applying 'confidence-building' measures for computer-based safety systems:

- verification is the process of ensuring that a phase in the system lifecycle meets the requirements imposed on it by the previous phase; and
- validation is the process of testing and evaluation of the integrated computer system (hardware and software) to ensure compliance with functional, performance and interface requirements.

426. Statistical testing is highly recommended as an approach for demonstrating the numerical reliability of computer-based safety systems. Such testing may play a role in both 'production excellence' and 'confidence-building' aspects of the safety justification.

427. If weaknesses are identified in the production process, compensating measures should be applied to address these. The choice of compensating measures and their effectiveness should be justified in the safety case.

UK Regulatory expectations

- ONR Guidance for the assessment of Computer Based Safety Systems is captured in Technical Assessment Guide NS-TAST-GD-046
  - Known as TAG -046
    - ➢ Additional guidance for smart devices added to the April 2019 revision
    - ➢ Gives greater clarity on regulatory expectations for each Safety Classification (Class 1 to 3 BS EN 61226)
      - ➢ Appendix 2
        - ➢ Table 2 Production Excellence and Confidence Building Measures examples

International Guidance

- C & I IAEA Standards and Guidance SSG-39.

6.82. Equipment qualification should be based on a selection of the following methods:

— Use of engineering and manufacturing processes in compliance with recognized standards;
— Reliability demonstration;
— Past experience in similar applications;
— Type tests;
— Testing of supplied equipment;
— Analysis for extrapolating test results or operating experience under relevant conditions;
— Evaluation of manufacturer production processes;
— Inspection of components during manufacture.

International Guidance

QUALIFICATION OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY FOR SAFETY APPLICATIONS

7.165. This section provides guidance on the qualification of industrial digital devices of limited functionality that are to be used in nuclear power plant safety systems, but that have not been developed specifically for use in such applications. This guidance describes an approach to fulfilling the qualification recommendations of paras 6.78–6.134 for devices in this category.

7.166. A device of limited functionality has the following characteristics:

— It contains predeveloped software or programmed logic;
— It is autonomous and performs only one conceptually simple principal function, which is defined by the manufacturer and which is not modifiable by the user;
— It is not designed to be reprogrammable;
— If it is reconfigurable, the configurability is limited to parameters relating to compatibility with the process being monitored or controlled, or interfaces with connected equipment.

7.167. All other devices are not 'industrial digital devices of limited functionality', i.e. they have the following characteristics:

— They use commercial computers (such as personal computers, industrial computers or programmable logic controllers);
— They are developed for an I&C platform; or
— They are specifically developed for the nuclear industry.

EQUIPMENT QUALIFICATION

6.77. Requirement 30 of SSR-2/1 (Rev. 1) [1] states:

> "A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing."

6.78. I&C systems and components should be qualified for their intended function during their service life.

6.79. The qualification of I&C components should include their software, hardware description language and process interfaces, if any.

6.80. The qualification should provide a degree of confidence commensurate with the importance to safety of the system or component.

Smart Device Qualification - Standards

- Principal standards ONR include in assessments
  - For the design of E, C & I based safety systems ONR (and HSE) recognise BS EN 61508 as relevant good practice (RGP).
    - Standards recognised as RGP are not explicitly stated as such but are referenced in ONR's TAGs
  - As BS EN 61508 is the parent standard for sector specific standards ONR expect BS EN 61513 (Nuclear power plants — Instrumentation and control important to safety — General requirements for systems) to be applied to any design (or equivalence is demonstrated)
  - From the referenced standards BS EN 61226 - Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions is considered to be fundamental by ONR.
    - Qualification/Substantiation requirements are proportional to the safety classification of the equipment

Intelligent Customer Role

- ONR's expectations are that Nuclear Site Licensee's should act as intelligent customers.

Leadership and management for safety	Capable organisation	MS.2
The organisation should have the capability to secure and maintain the safety of its undertakings.		

66. Being a capable organisation requires the retention and use of knowledge so that safety requirements are understood and risks are controlled throughout all activities, including those undertaken by contractors at all levels within the supply chain. An ***'intelligent customer'*** capability should therefore be maintained to ensure that the use of contractors in any part of the organisation does not adversely affect its ability to manage safety.

Intelligent Customer Role

- The activities required to support the “Intelligent Customer” expectations related to smart device qualification include:
  - Detailed understanding of the design of the equipment that is supplied
    - This requires the licensee to review all information that supports the safety claim made on equipment and to gain confidence that any equipment is suitable for use.
      - Includes the review of third party certification
        - » Not taking certification on face value

C&I system qualification - Research

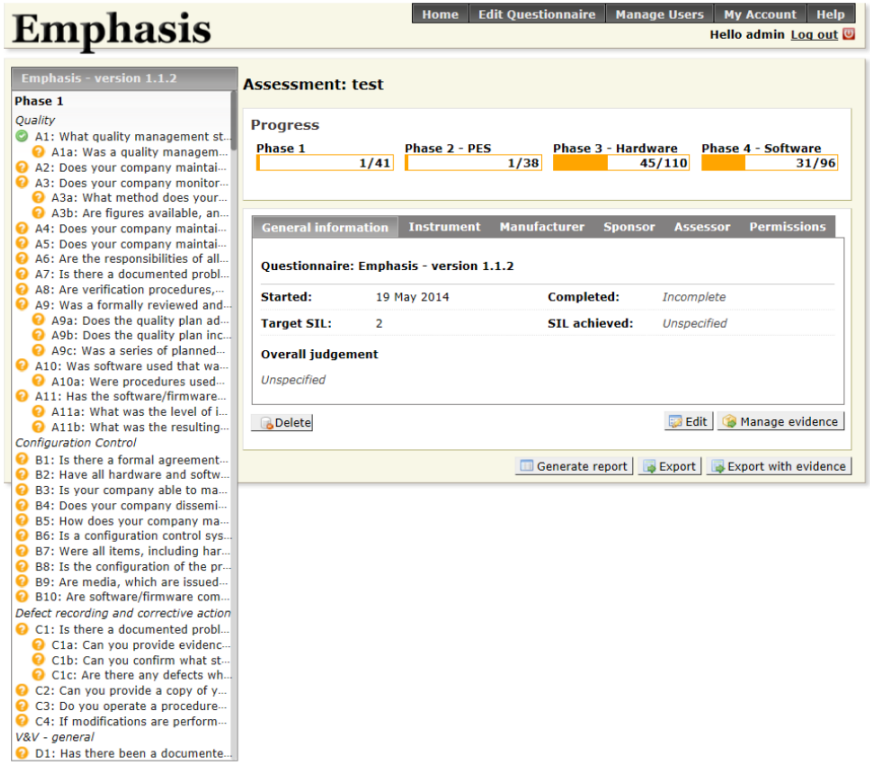
- Research into the qualification of smart devices
  - The Energy Act 2013 enables ONR to carry out or commission research in connection with its purposes, in support of its vision of being an exemplary regulator that inspires respect, trust and confidence.
  - ONR encourages licensees to participate in and fund research.
    - Research topics are captured in the ONR Research Register (http://www.onr.org.uk/research/regulatory-research-register.htm)
      - » Currently there are 14 E, C & I related projects (June 2019)

C&I system qualification - Research

- Research into the qualification of smart devices
  - Conducted by the Control and Instrumentation Nuclear Industry Forum (CINIF)
    - Comprises of Site Licensees and new build Requesting Parties.
      - Research carried out on behalf of CINIF by Universities and consultants.
    - Output used by CINIF Members to develop their own internal guidance.
      - Research output only available to CINIF members

C&I system qualification - Research

- EMPHASIS Tool was an output from CINIF research
  - ➢The **E**valuation of **M**ission im**P**erative, **H**igh-integrity **A**pplications of **S**mart **I**nstruments for **S**afety
    - ➢High-level tool to support qualification against BS EN 61508



C&I system qualification – amount of effort

- Typical duration of substantiation
  - 6 to 12 months for instruments
    - Depending on Safety Classification, availability of information and gaps found
  - For a system could be > 12 months
    - Statistical testing could require significant time to perform tests
- Typical costs for substantiating one instrument
  - >£50K

C&I system qualification – Working Groups

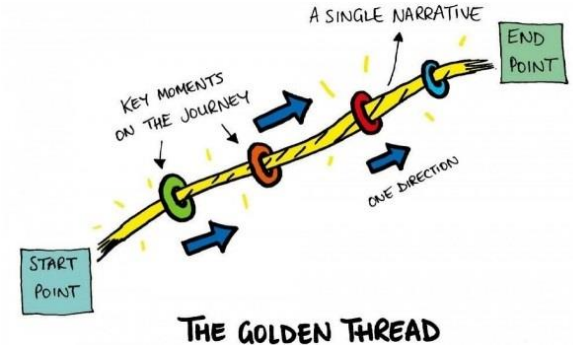
- To share the effort in qualifying a smart device ONR encourage the sharing of qualification reports
  - This has challenges
    - Non-Disclosure Agreements between manufacturers and site licensees
    - Commercial arrangements
  - A Working Group has been established to supporting sharing of reports
    - Nuclear Industry Smart Instrument Working Group (NISIWG)

C&I system qualification - Challenges

- Challenges
  - Initial challenge is to identify which devices are smart
    - Diversity of vendor manufacturing facilities
    - Engagement with vendors and their commitment to support assessment
    - Intellectual Property protection concerns
    - Location of available information
      - » Sometimes only available at vendors premises under supervision
    - Sharing of substantiation reports across the industry to reduce the overall cost

C&I system qualification – The Golden Thread

- The Golden Thread that links the safety case to the supplied equipment



Safety Case
Engineering
Qualification
Procurement
Supply Chain

EQSA

Equipment Qualification
Services Alliance

tecnatom TÜVRheinland® element wood.

Seismic Testing – LIVE Demonstration

EQSA
Equipment Qualification Services Alliance

Group A	Group B
Richard McLaren	Zhenlai Zhai
Ann Walker	Andrew Douglas
Ben Pyne	Callum McNaught
Tom Reed	Emmanuelle Chardon
Bob Storey	Steve Waywell
Victoria Smith	Liam Pendlebury
Chris Berry	Kirk Cunliffe
Mika Price	Sarah Hyde
Francesco Pellegrino	Simon Greatorex
Wang Yongjiao	Stuart Hanson
Lievre Alban	Mike Scragg
Azham Khan	Gareth Whitcombe
Gavin Colliar	Nie Yan
Alan Fergusson	Thorsten Kaiser
Jordan Lessarre	Xiaochun Zha
Qijin Peng	Chris Bark

EQSA

Equipment Qualification
Services Alliance

tecnatom TÜVRheinland® element wood.

EQSA

Equipment Qualification
Services Alliance

tecnatom TÜVRheinland® element wood.

EQSA

Equipment Qualification
Services Alliance

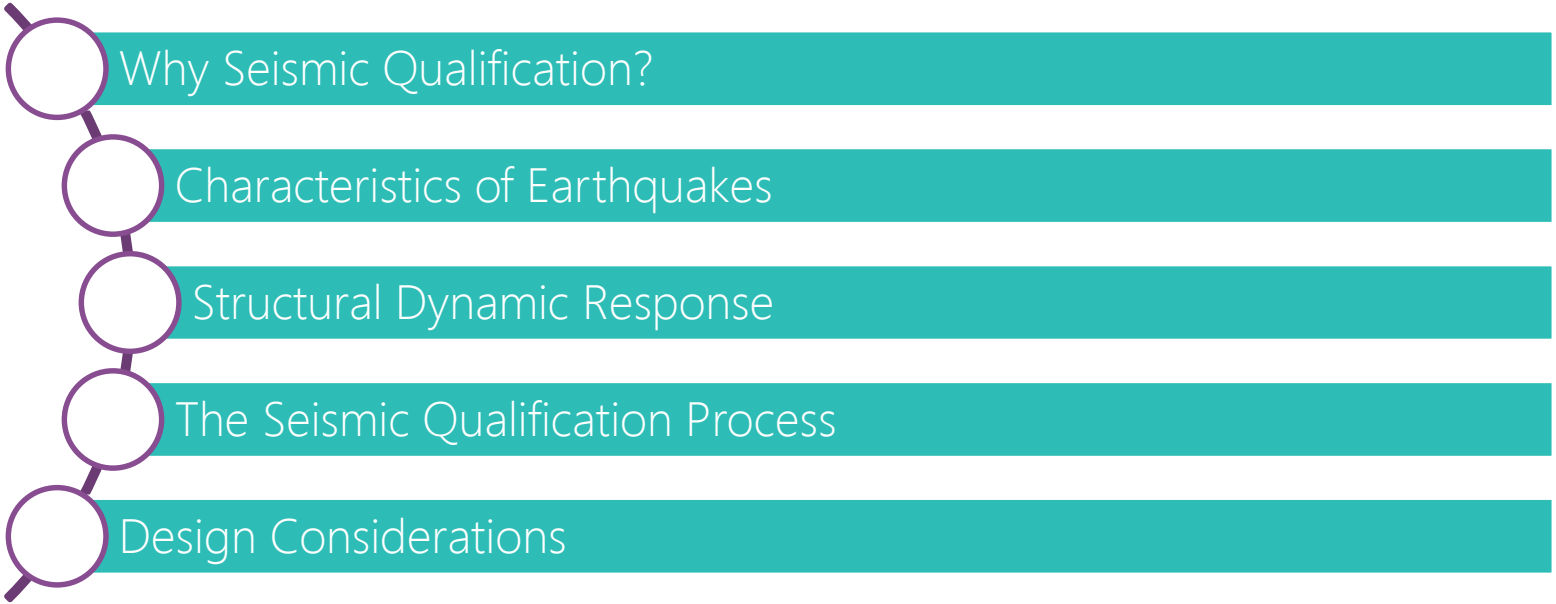
tecnatom TÜVRheinland® element wood.

Seismic Qualification

Chris Stone
Element

Friday 11 March 2011

Presentation



Why Seismic Qualification?

2010 Chile Earthquake

Earthquake Damage

2010 magnitude – 8.8 Chile Earthquake

1999 magnitude – 6.7 Izmit, Turkey Earthquake

Who Needs Seismic Qualification

Nuclear Industry:
Power stations, Processing Plants and Submarine bases

Telecoms Industry:
Equipment (cabinets and contents) 99999s Requirement for installation in Europe / USA / Japan / Taiwan etc.

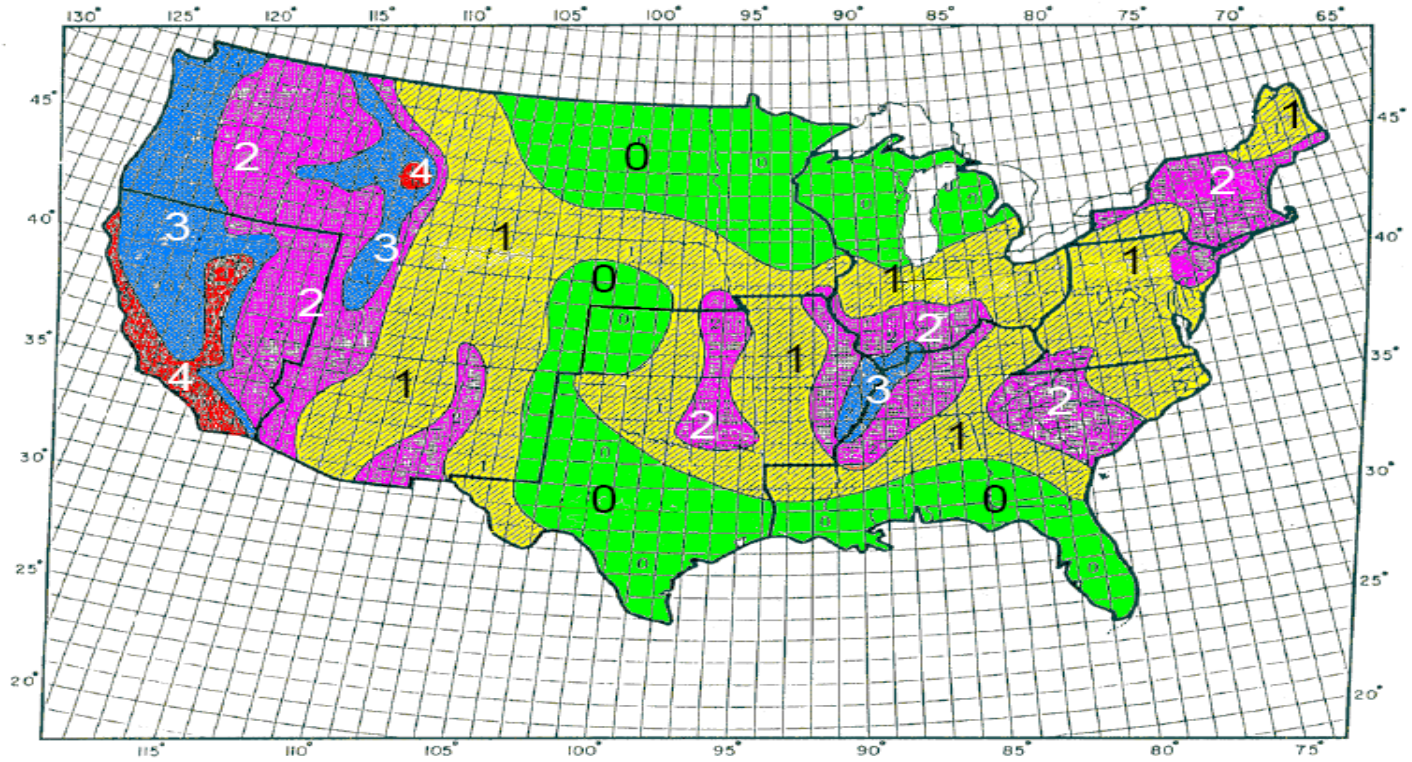
Oil, Gas and Power Generation Industries
Control and Containment

Engineering Consultancies:
Validation of FE analysis e.g. non-linear dynamic contact elements

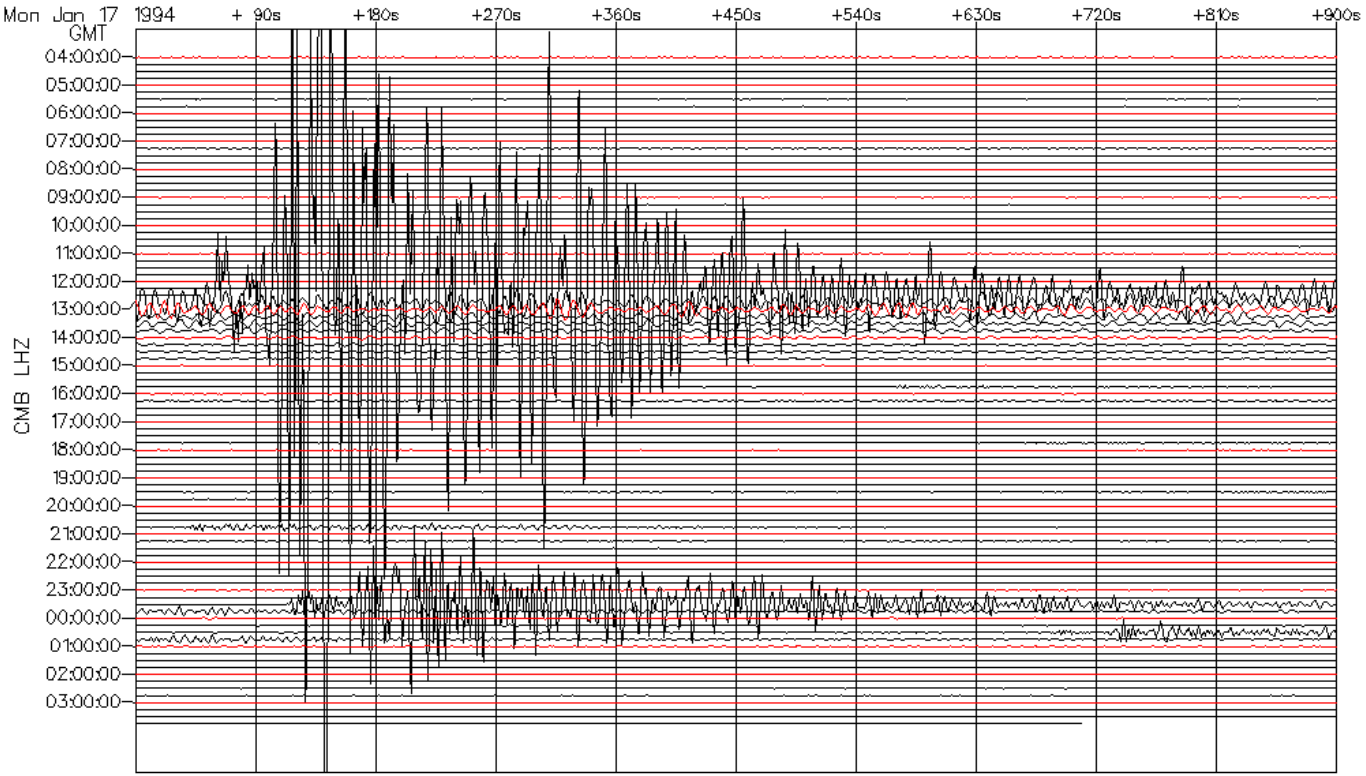
Engineering Contractors:
Testing of new materials / construction techniques

Characteristics of Earthquakes

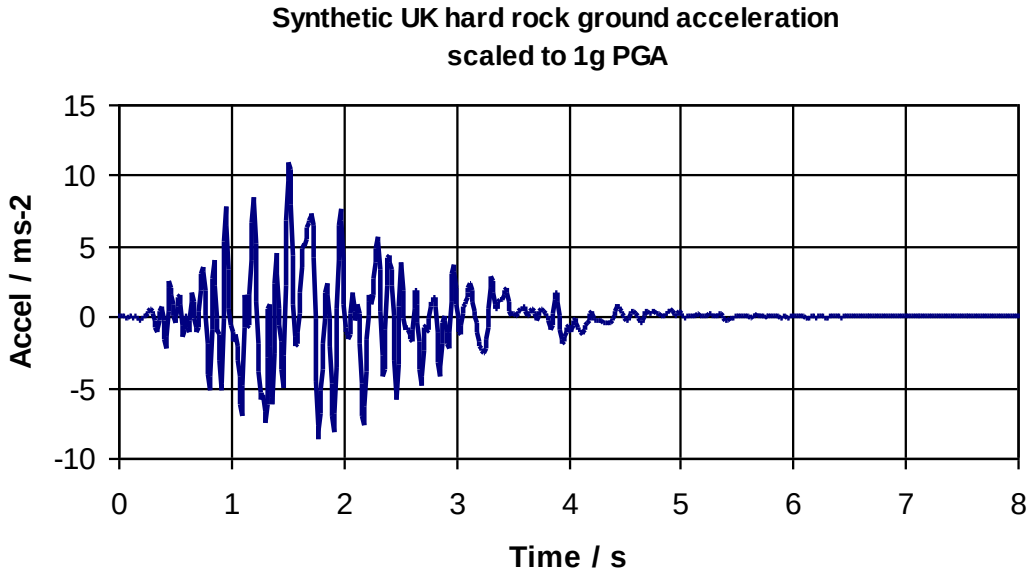
Zones and Regions



Northridge, California, Earthquake, 1994

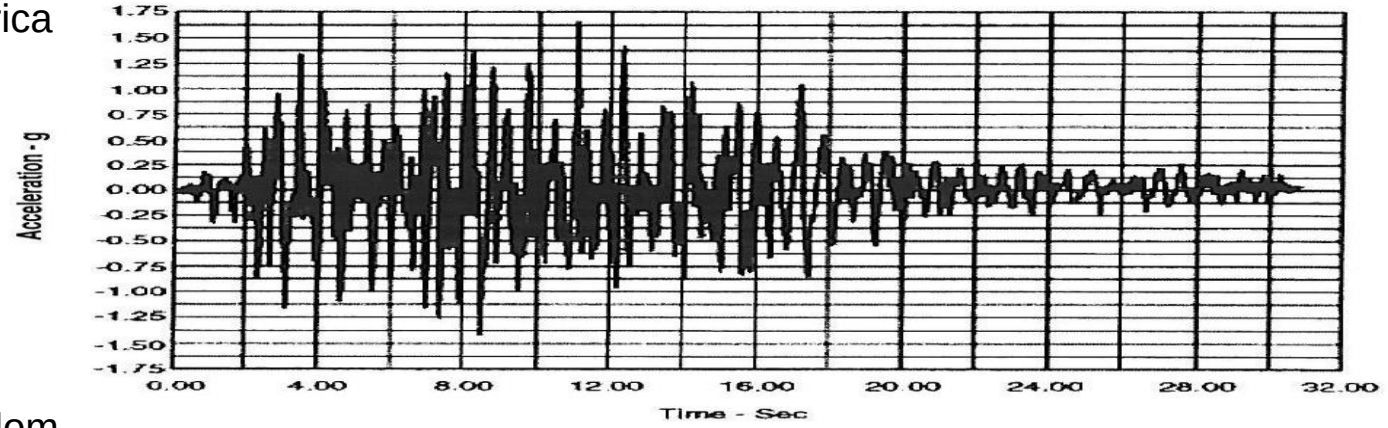


UK strong ground motion

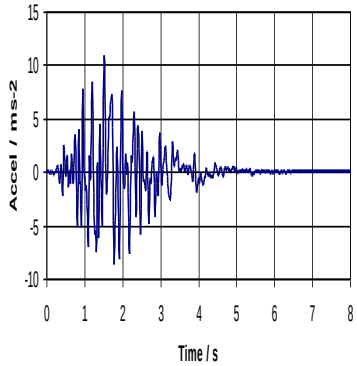


Strong Ground Motion

North America

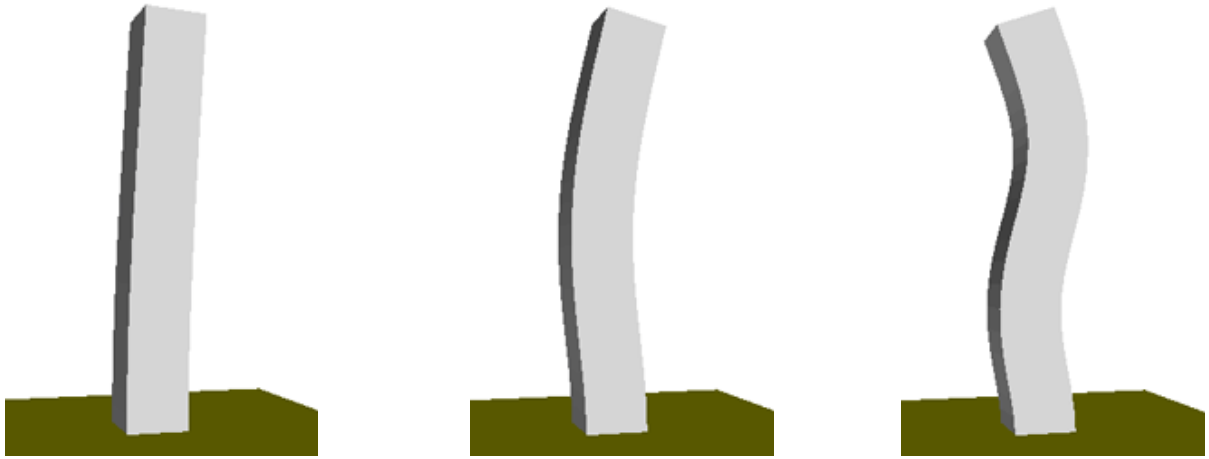


United Kingdom



Structural Response To Earthquakes

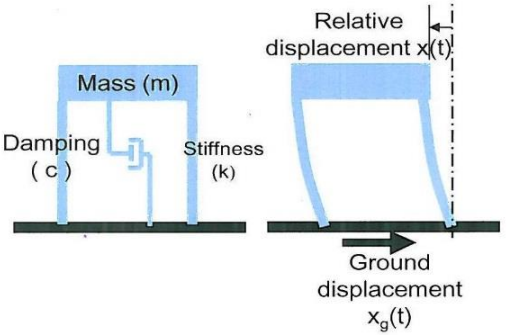
Elastic Structural Dynamic Response



Dynamic model

- Natural frequency and period

$$\omega = \sqrt{\frac{k}{m}} rad/s \qquad T = \frac{2\pi}{\omega} \; seconds$$



- Mass - m
- Stiffness - k
- Damping – c
- Displacement - x

- Equation of motion

Internal inertia force

Internal damping force

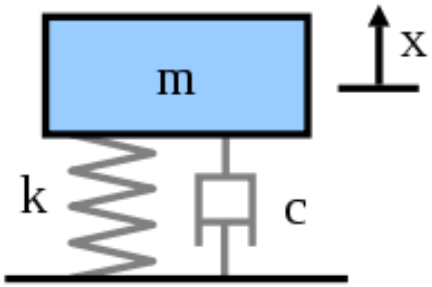
Internal 'stiffness' force

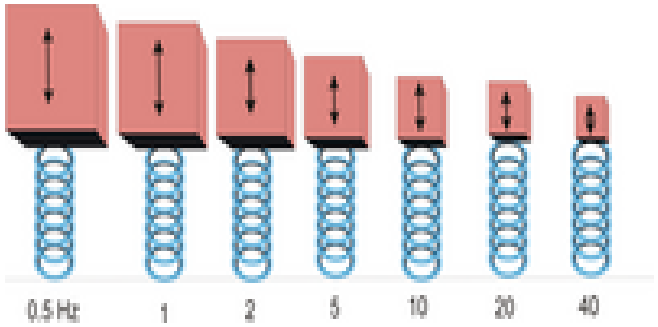
External (earthquake) force

$$m\ddot{x} + c\dot{x} + kx = P(t) = -m\ddot{x}_g$$

Response Spectrum

The peak or steady-state response (displacement, velocity or acceleration) of a series of oscillators of varying natural frequency, that are forced into motion by the same base vibration or shock





Response Spectra

Response of an infinite series of damped elastic SDOF systems

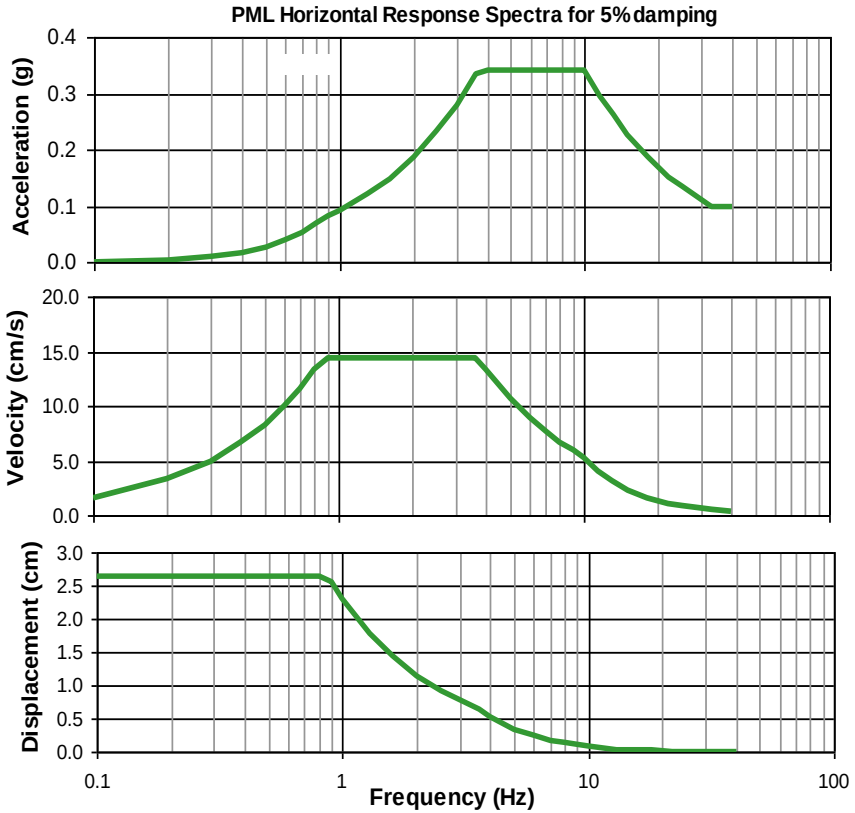
Graphs of the maximum values of

- acceleration,
- velocity, and/or
- displacement

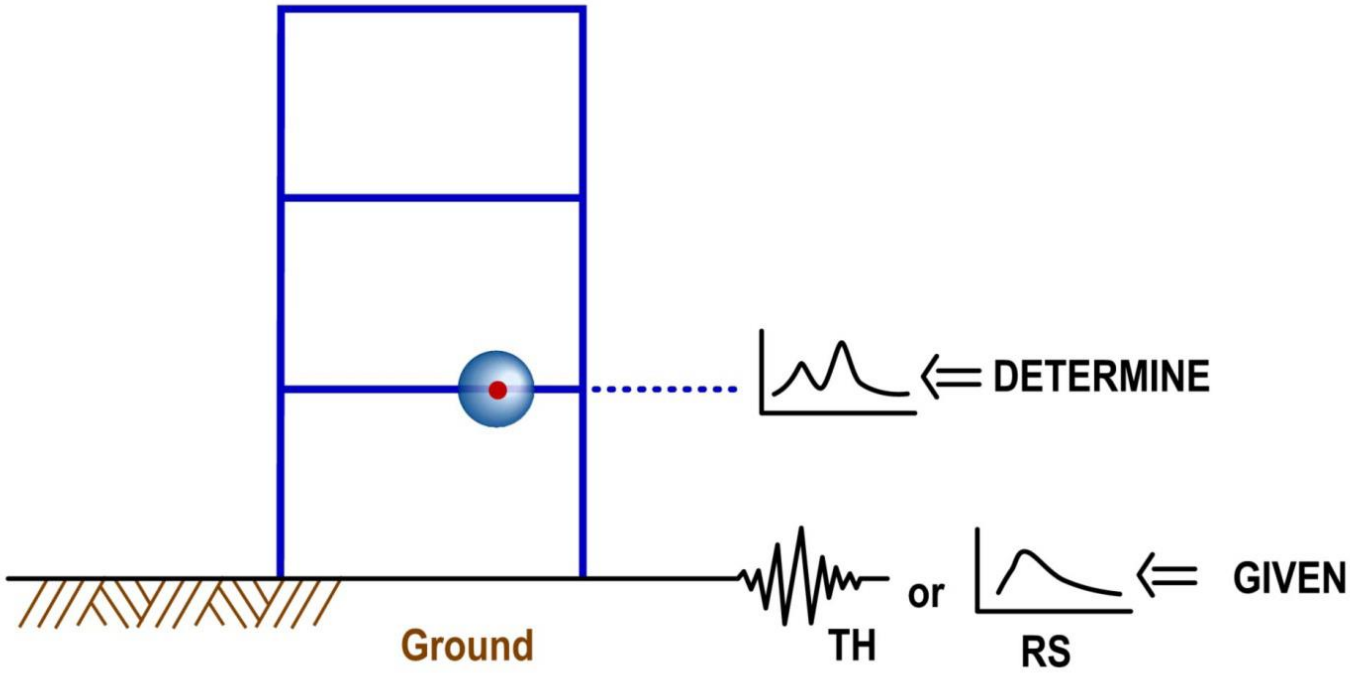
Maximum response values for several levels of damping

Plotted against undamped natural frequency or period

Response Spectra



Secondary Response Spectra



Why Secondary Response Spectra

Non structural elements difficult to analyse

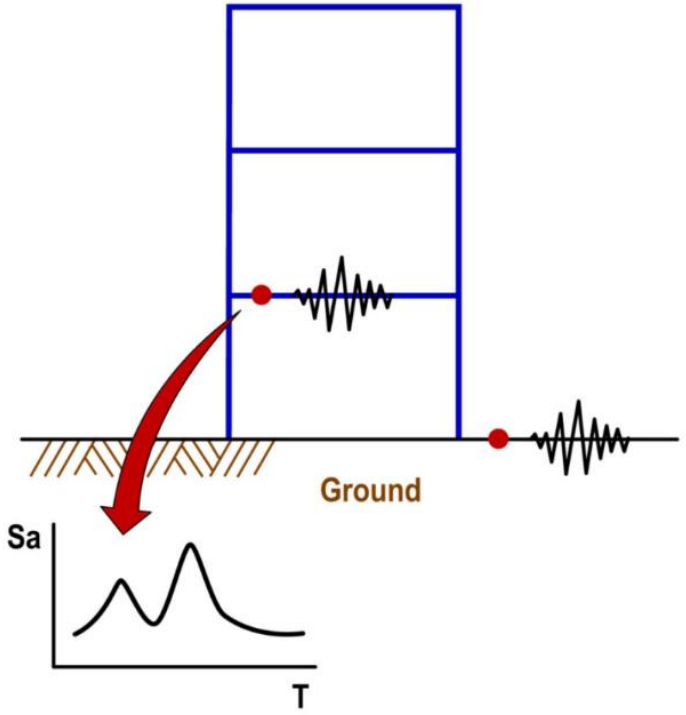
- Complex
- Relatively small

Large models required

Different design teams/companies

Secondary Response Overview

- Synthesise time histories
- Compute motion at point of interest
- Compute secondary response spectra



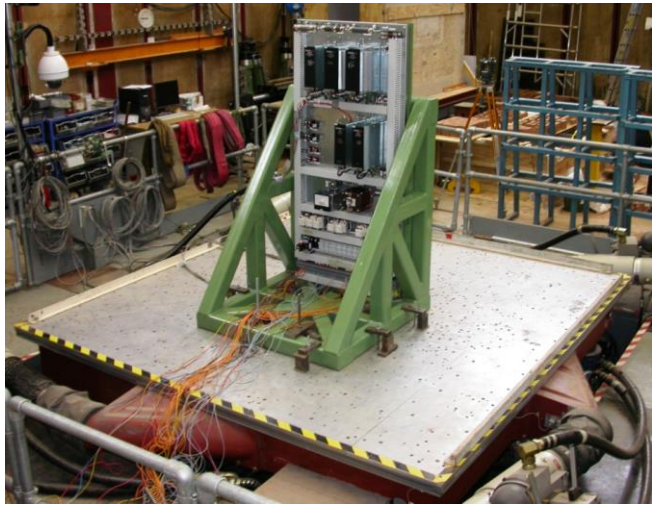
The Seismic Qualification Process

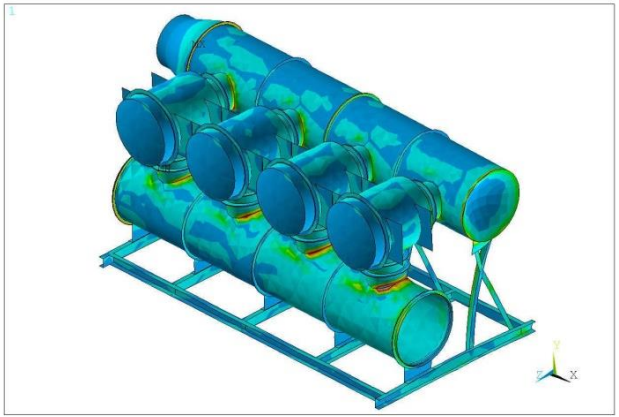
Seismic Qualification with Element

- 25 Years Experience – Post Sizewell B
- Wide Range of Industries and Products Qualified
  - Over 200 triaxial seismic test programmes successfully completed
- Partnership with University of Bristol
- Up To Date Knowledge of Specifications
- Support at Tender Stage Through to Final Qualification Report and Documentation

Seismic Qualification

- Seismic Testing
  - Functionality,
  - Physical Limits
- Modelling
  - FEA
- Experience





Typical Process of Qualification by Test

Preliminary meetings to agree test specification including
- Equipment requirements
- Main test spectra
- Number and amplitude of shakes
- Exploratory test requirements
- Details of function testing

Preparation of test documentation – Detailed Test Plan, Inspection Plan, Functional Test Plan

Generate shakes ready for testing

Arrival of specimen, examination for transport damage

Mount specimen on shaking table

Install instrumentation

Functional tests

Exploratory tests

Functional tests

Main seismic tests including basic data processing

Functional tests

Remove specimen from shaking table and return to client

Final data processing and produce test report

Test Specifications

IEEE 344 – 2013 IEEE Recommended Practice for the Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

IEEE 693 – IEEE Recommended Practice for the Design of Substations

RCC-E Design and Construction Rules for Electrical Equipment of Nuclear Islands

BTRs (Books of Technical Rules)

BTR 91 C 112 EPRUK Equipment Seismic Qualification Testing (RCC-E)

ASCE 7-10 Minimum Design Loads for Buildings and Other Structures (AC156)

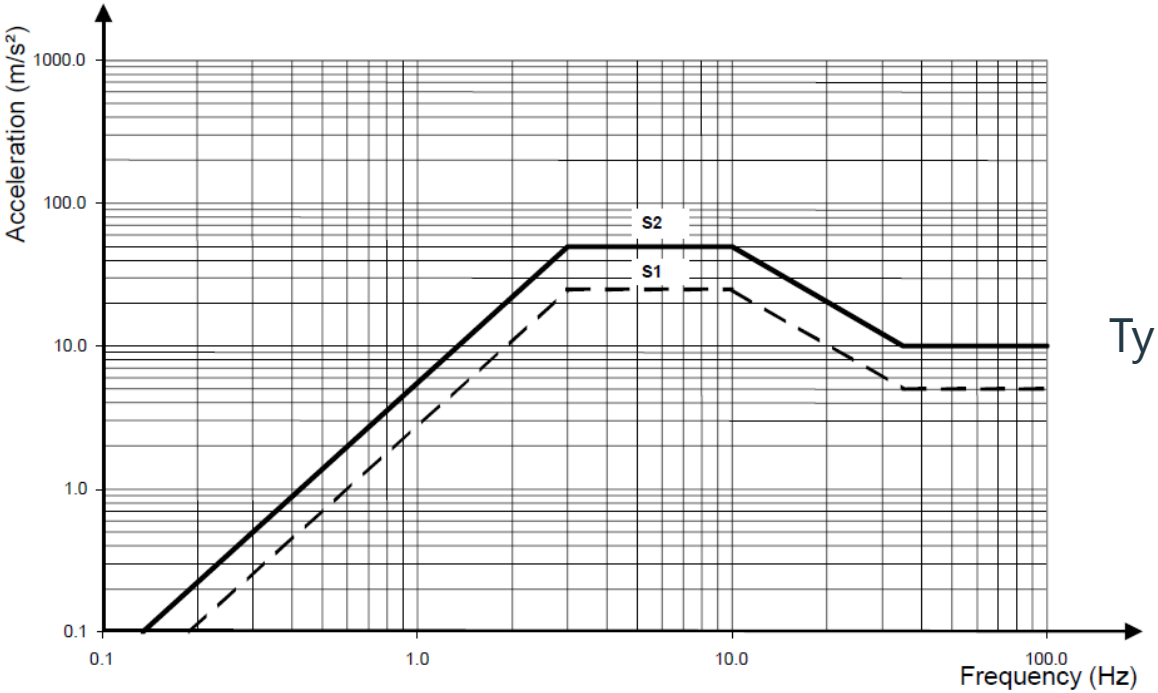
IEC 980 Recommended Practice for the Seismic Qualification of Electrical Equipment of the Safety System for Nuclear Generating Stations

IEC 60068-2-57 International Test Standard Environmental testing –

Part 2-57: Tests – Test Ff: Vibration – Time-history method

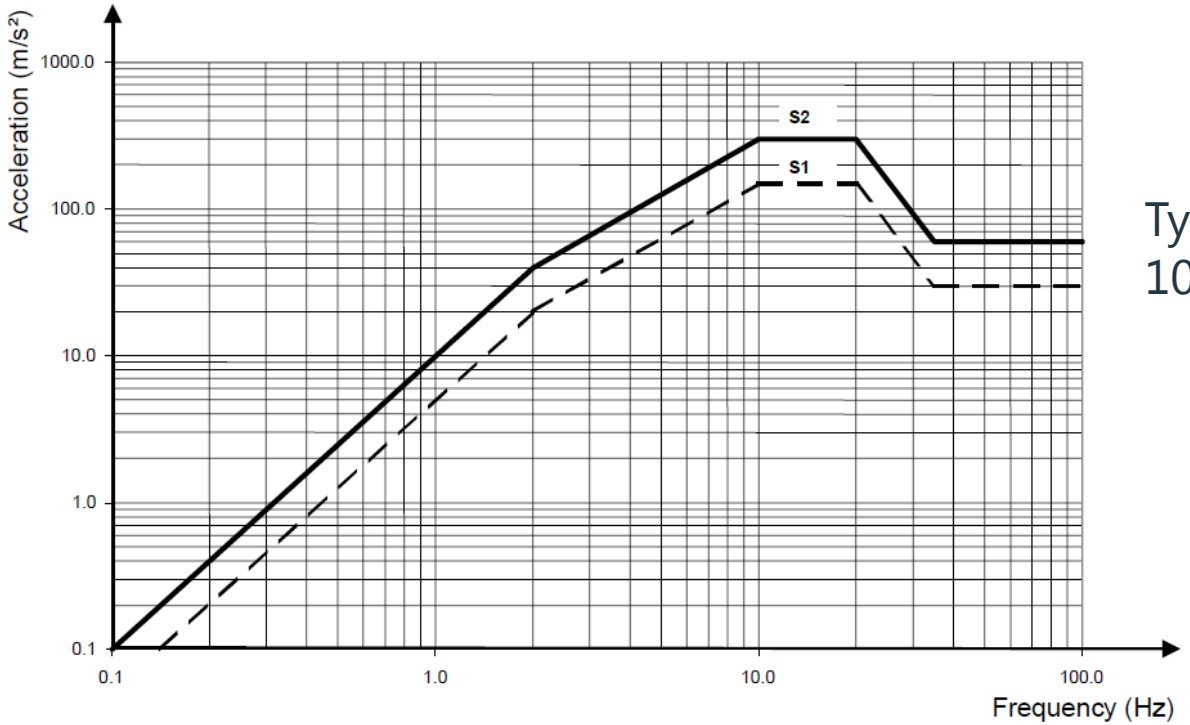
Sellafield ET372, British Energy, BNG, Site Specific etc

Required Response Spectra – Assemblies



Typically 1g zpa

Required Response Spectra – Components

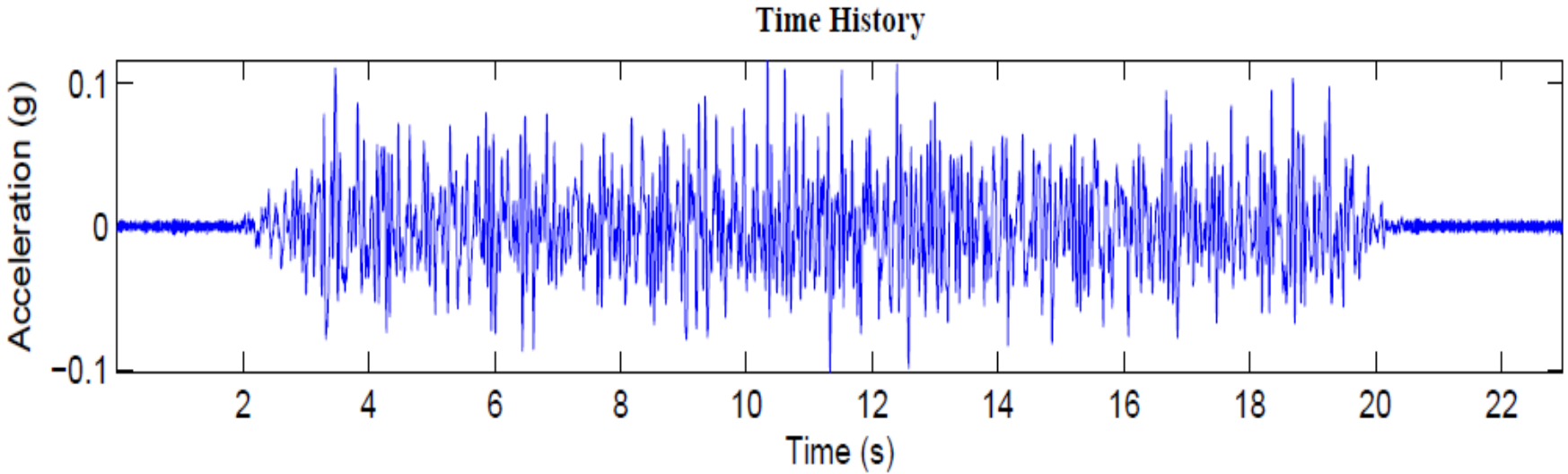


Typically 6g to 10g zpa

Test Durations

Ramping

Strong Motion



Test Sequences

Triaxial Shakes:

25%, 50%, 75%, 100%, 140% *(and back down)*

5 at 25%, 1 at 100%, 1 at 140%

5 at OBE, 1 DBE, 1 SSE (SME)

5 at S1 (OBE), 1 at S2 (SSE)

Other combinations are possible

Shakes more than 100% are used to check for “cliff edge” effects

Ageing

Dynamic Testing

- Vibration
- Shock and bump
- Bench handling
- Transportation bounce
- Acceleration

Radiation

Thermal Cycling

Ageing

Climatic Testing

- Temperature, humidity, altitude, icing
- Driving sand & dust
- Ingress protection (IP)
- Salt corrosion
- Solar radiation/heating
- Fluid Contamination

Specimen Mounting

Representative of In-Service Conditions or Rigidly Mounted

Orientation wrt gravity

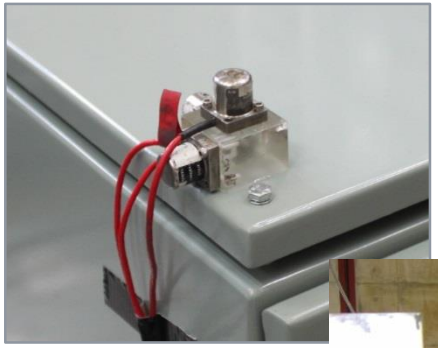
Test Fixturing

– cabling/pipework

Mounting Bolts

Tightening Torques

Response Measurements



Typically: acceleration, displacement and strain

Functional Testing

Safety Critical

Continuity

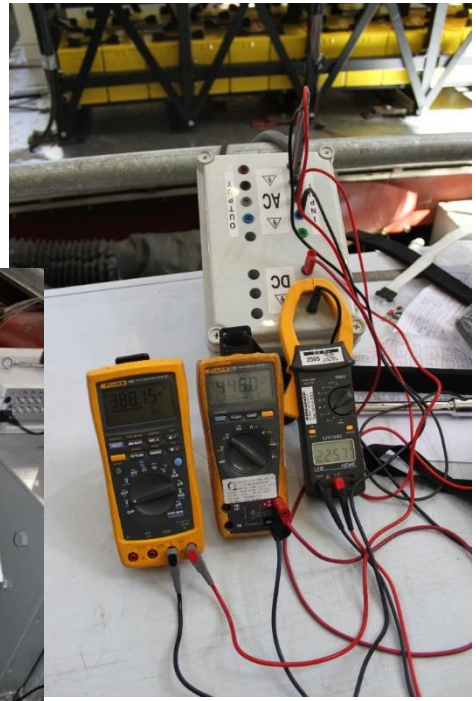
Change of State

Containment

Data Transfer

Acceptable Limits

Pass/Fail Criteria



Qualification Documents

Test Plan

Test and Inspection Log

Test Report – Test Laboratory

Test or Qualification Report

- Incorporating functional test results

Post Test Modification and Qualification

Partnership

Element has a Heads of Agreement with BEELAB

Bristol Earthquake and Engineering Laboratory Ltd, BEELAB, wholly owned by the University of Bristol, was established to market expertise, promote collaboration with industry and generate income to support further research

Twelve year partnership – established relationship

Head of Civil Eng Dept, Research Associates and Technicians

Research – BEELAB leads this work with input from Element

Long-term, evolving programme, on and off the facility, informal reporting

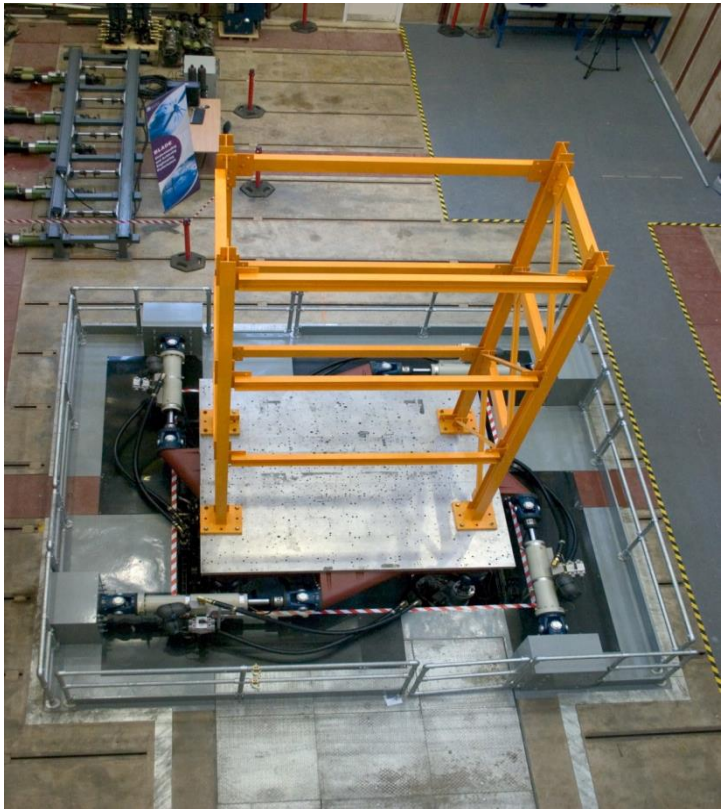
Commercial/Qualification Testing – Element leads this work, which is performed by BEELAB

Element Test Plan, fully specified activities, one hit test, formal qualification documents

UKAS Accreditation

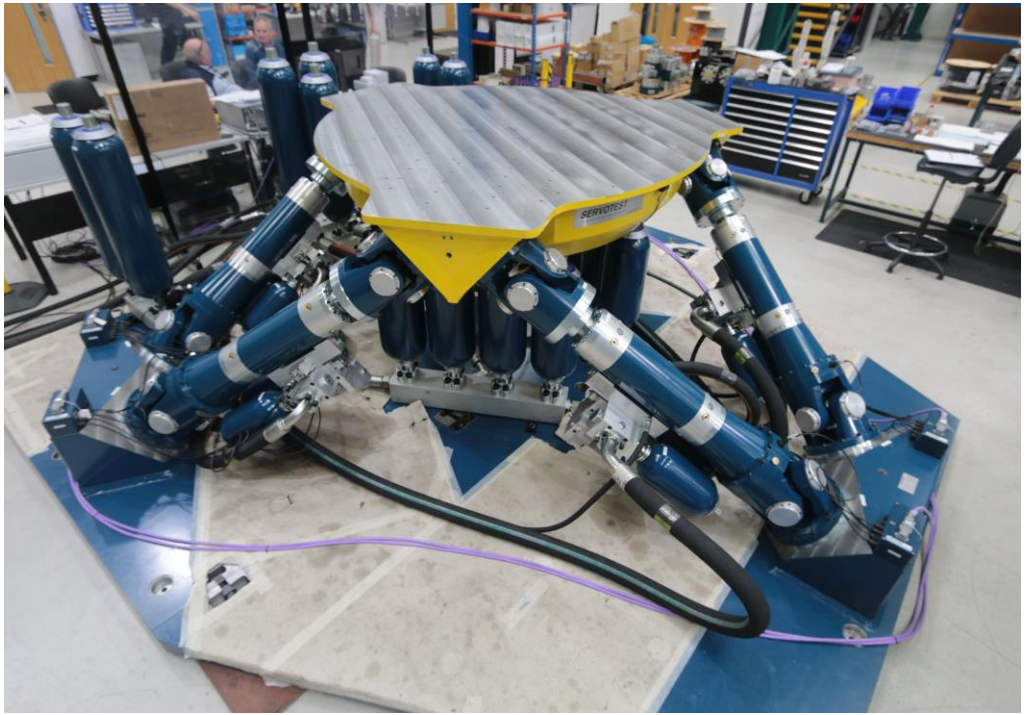
Earthquake Test Lab to become an extension of Element's UKAS Facilities

Existing Shaking Table



Size	3 m by 3 m
Axes	6
Construction	4 piece cast aluminium
Mass	3.8 tonnes
Max payload	15 tonnes
Max payload height	15 m
Max payload C of G	5 m
Craneage capacity	2 x 10 tonnes
Operational frequency:	0 -100 Hz
Longitudinal (X) and lateral (Y) actuators:	4 at 70 kN
Horizontal acceleration (no payload):	3.7 g*
Horizontal velocity:	1.2 m/s
Horizontal displacement	± 150mm
Yaw rotation	± 3.6 degrees
Vertical acceleration (no payload)	5.6 g*
Vertical velocity	1.2 m/s
Vertical displacement	± 150mm
Pitch/roll rotation	± 5.2 degrees

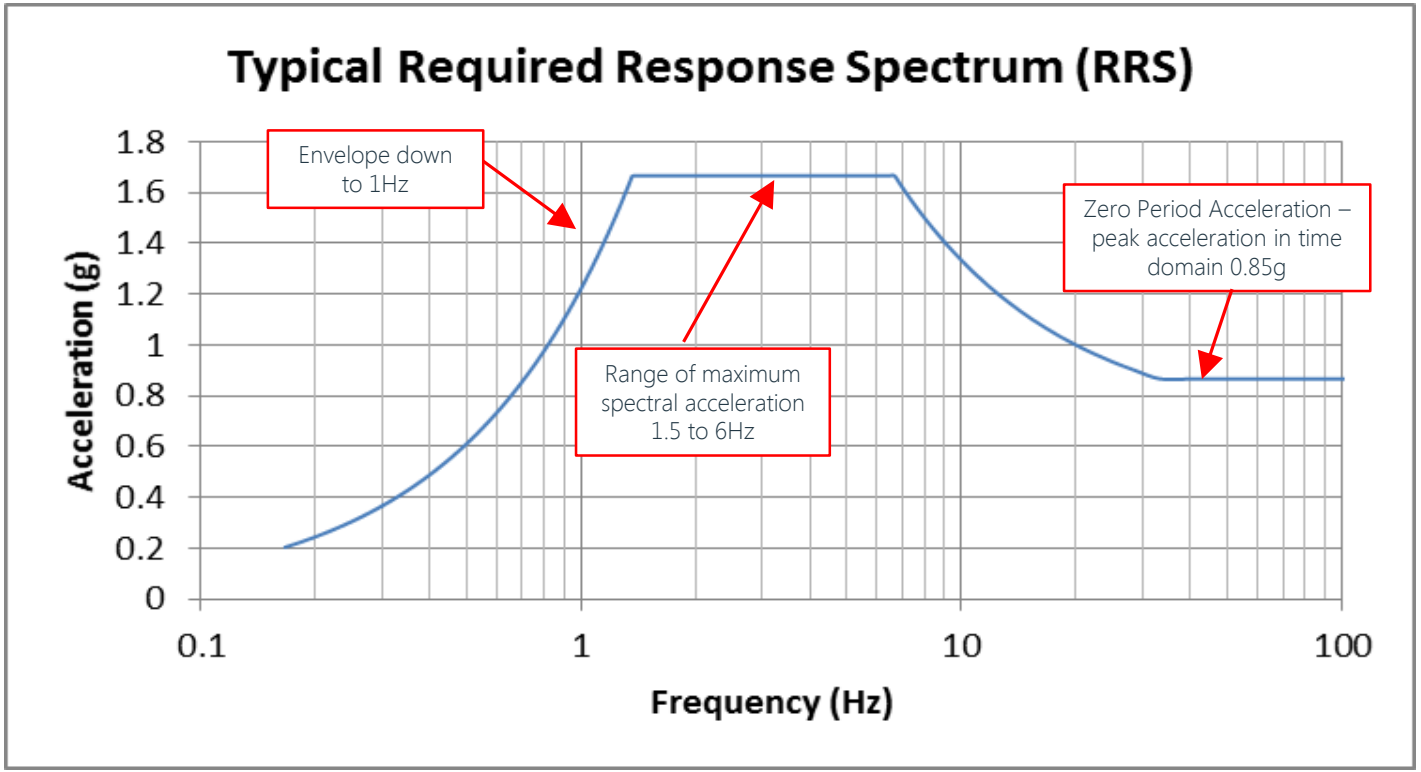
New Shaking Table



Size	1.2 m by 1.2 m
Axes	6
Construction	Steel platform
Mass	2.4 tonnes
Max payload	800kg
Max payload height	15 m
Max payload C of G	0.4 m
Craneage capacity	2 x 10 tonnes
Operational frequency:	0 -150 Hz
Actuators:	6 at 30 kN
Horizontal velocity:	1.2 m/s
Displacement	± 80mm triaxial
Rotation	± 10 degrees
Horizontal and Vertical acceleration (no payload)	10g
Vertical velocity	1.2 m/s
Vertical displacement	± 120mm
Pitch/roll rotation	± 10 degrees

Design Considerations
Dynamic Characteristics

Required Response Spectra – What to look for



Thanks
Any Questions?