HORIZON
NUCLEAR POWER

ENERGY WORKING FOR BRITAIN

Use of FPGA technology in a (UK) Nuclear Protection System

Demanding regulatory regime (IEC 61226, 61513, IEC 60880, TAG 46)

Cezar Georgescu
December, 2017

Contents

- Horizon Nuclear Power overview
- C&I Architecture and development of FPGA-based platform
- ICBMs of the FPGA-based Class 1 Platform

Contents

- **Horizon Nuclear Power overview**
- C&I Architecture and development of FPGA-based platform
- ICBM of the FPGA-based Class 1 Platform

Horizon Nuclear Power overview

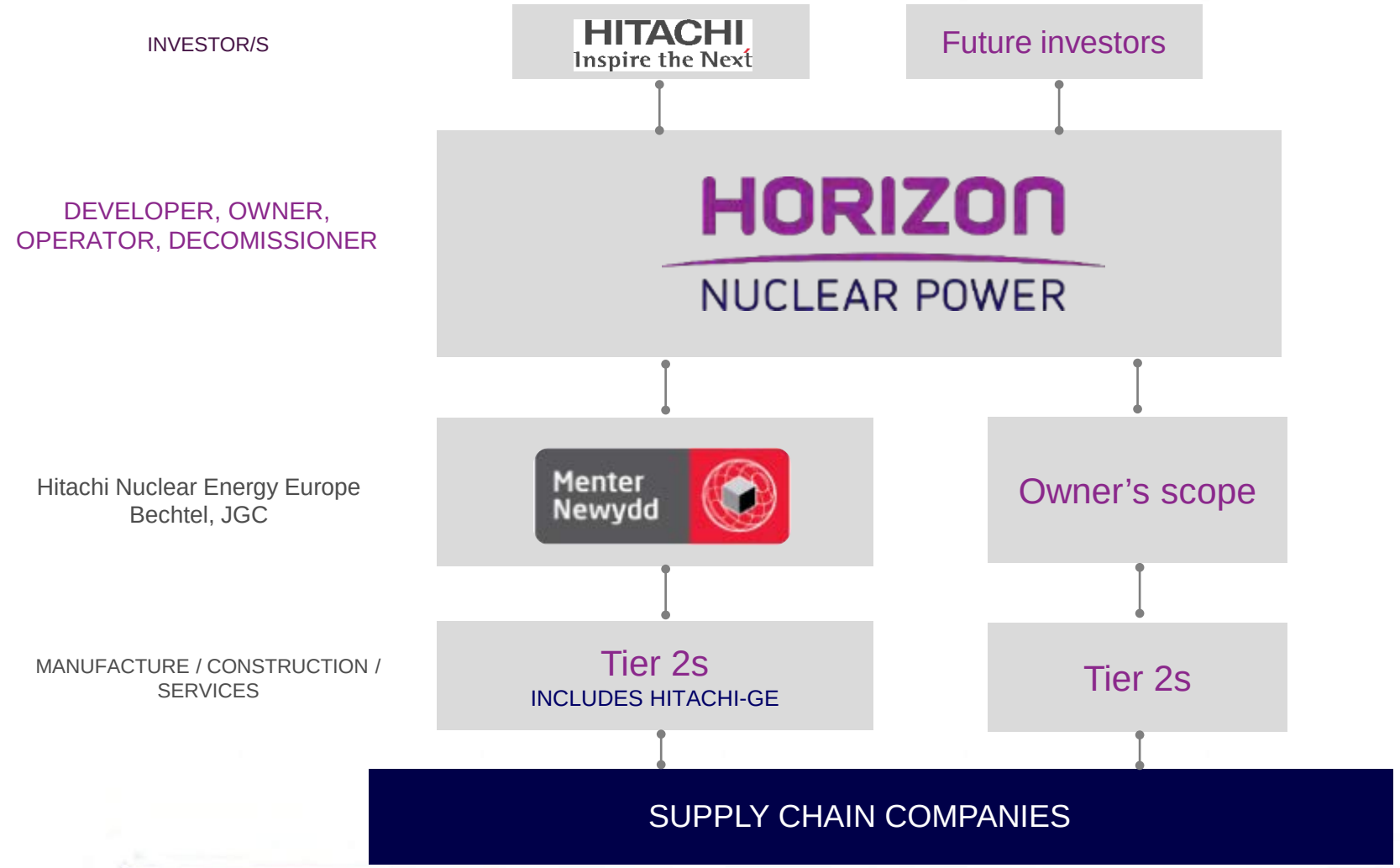
- Established in 2009 and acquired by Hitachi in November 2012
- Established to help meet the need for new, secure low carbon power
- Making steady progress past milestones for lead Wylfa Newydd project, with Oldbury to follow
- Will deploy tried and tested Hitachi-GE ABWRs which have been built to time and budget in Japan
- c.£20billion investment in the UK - up to 60% of project value could be spent in UK, creating opportunities for British businesses

GLOUCESTER HQ

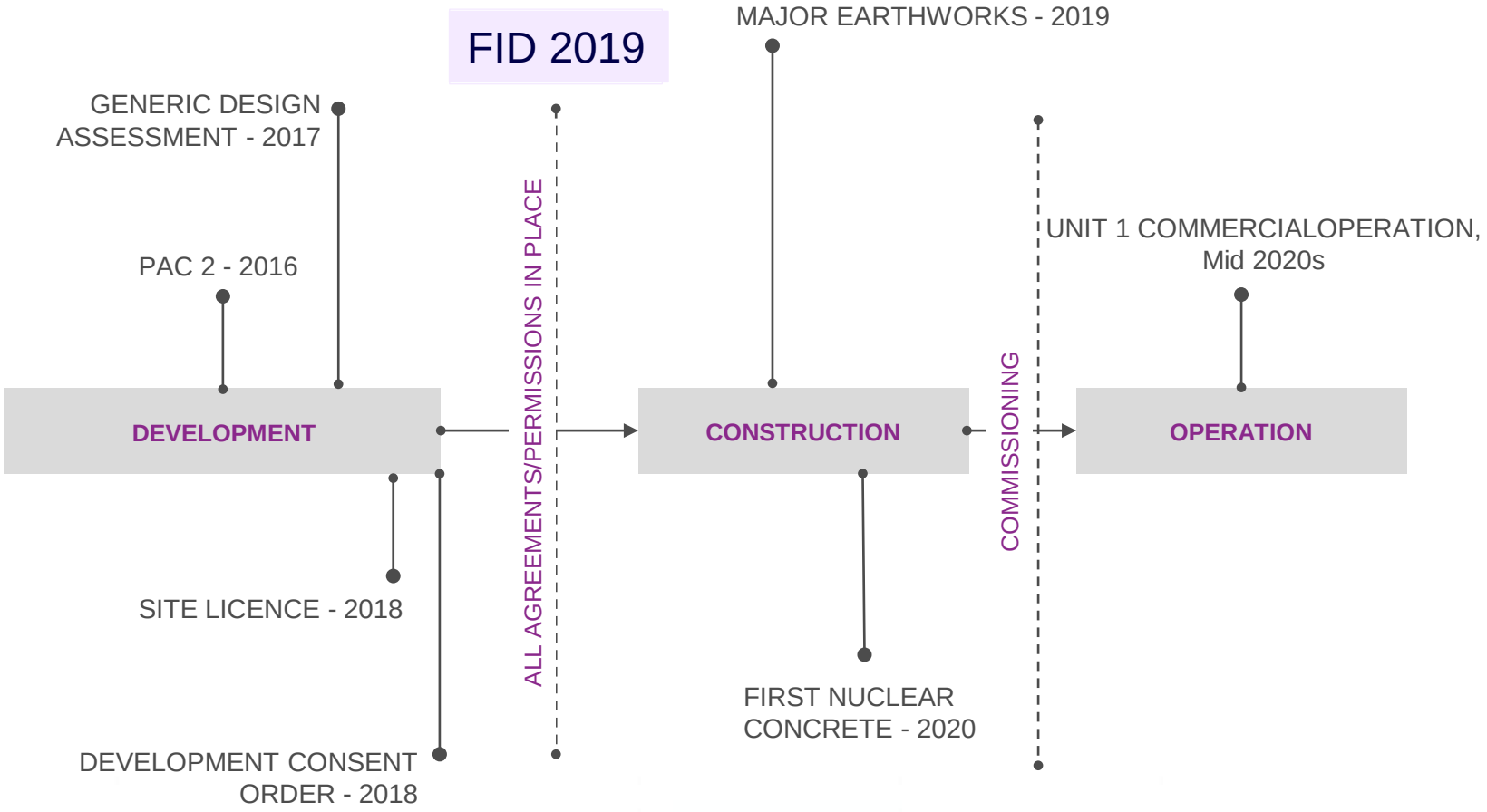
WYLFA NEWYDD

OLDBURY

Project structure



Baseline schedule



Recent progress

- Detailed discussions on a financial support model with UK Government and Government of Japan
- ABWR moving through fourth and final stage of the Generic Design Assessment
- Operations Partnership announced with Exelon Generation
- Clearance to begin purchase of reactor components
- Menter Newydd JV approaching second year of preparatory work for Horizon
- Further nuclear expertise added to Horizon Board
- Second intake of Horizon Apprentices launched
- £1 million of funding for Coleg Menai to build a new Engineering Centre on Anglesey
- Preparing for Site Licence Application (end March)

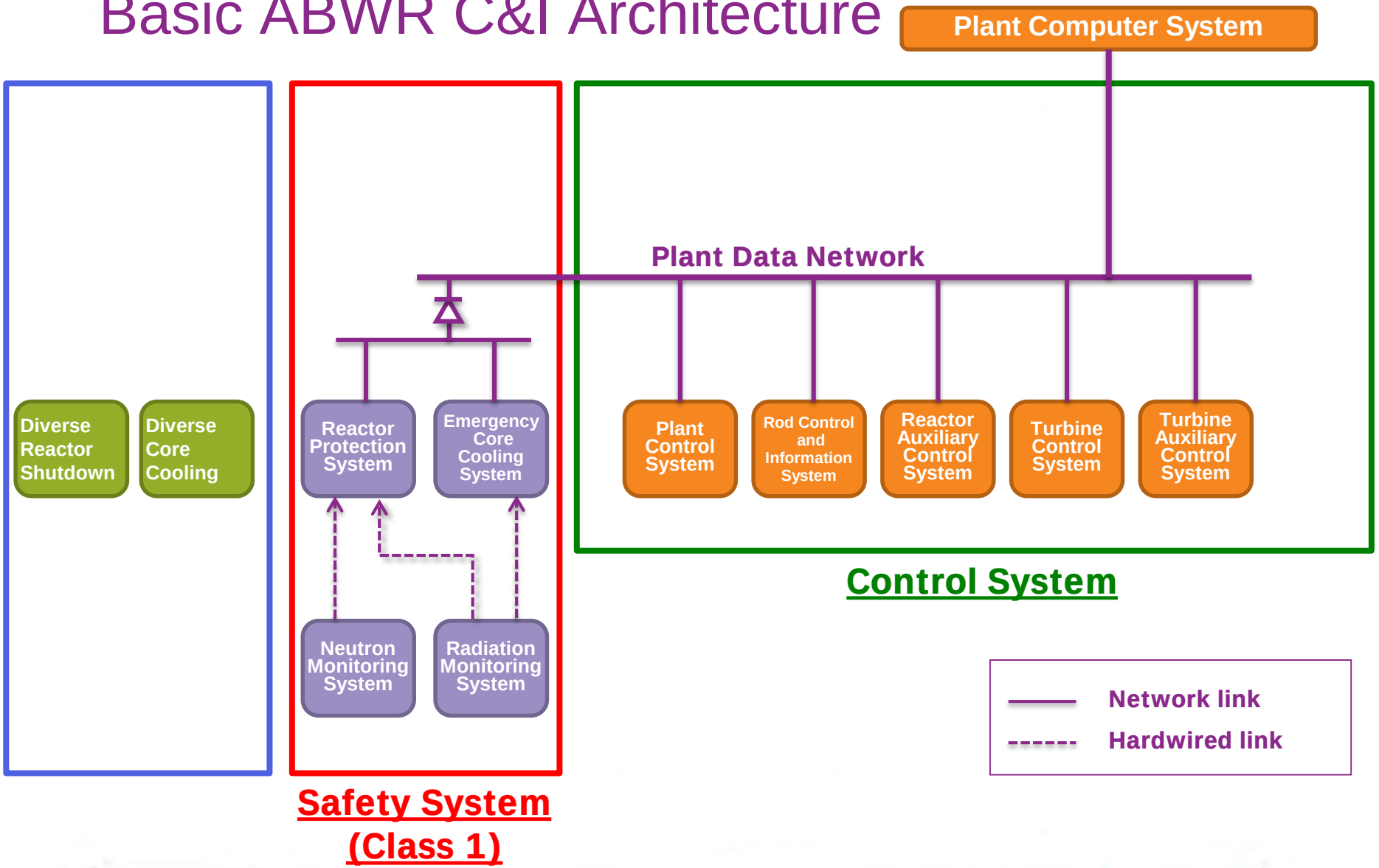
Delivering Wylfa Newydd

- Technology approval
- Planning permissions
- Nuclear Site Licence
- Site development
- Environmental permits

Contents

- Horizon Nuclear Power overview
- **C&I Architecture and development of FPGA-based platform**
- ICBM of the FPGA-based Class 1 Platform

Basic ABWR C&I Architecture

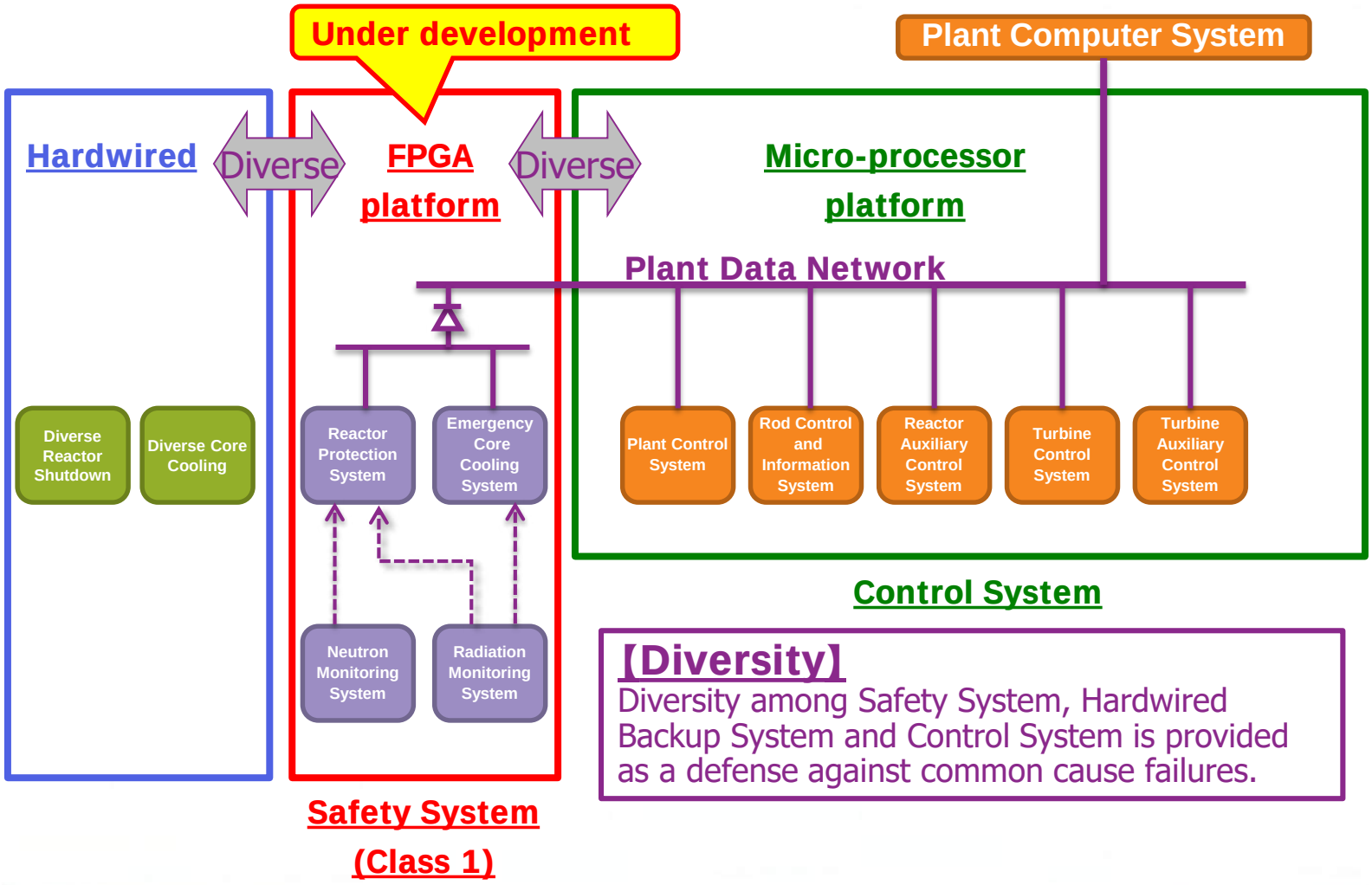


C&I Architecture Introduction

- In Japanese designs the Control System and the Safety System are both Hitachi products
- Need for additional diversity to meet UK relevant good practice and expectations
- Hence Hitachi decided to develop a new Class 1 Platform – using FPGA technology

The Key UK Regulatory Expectation

Diversity between systems



[Diversity]

Diversity among Safety System, Hardwired Backup System and Control System is provided as a defense against common cause failures.

Safety System Architecture

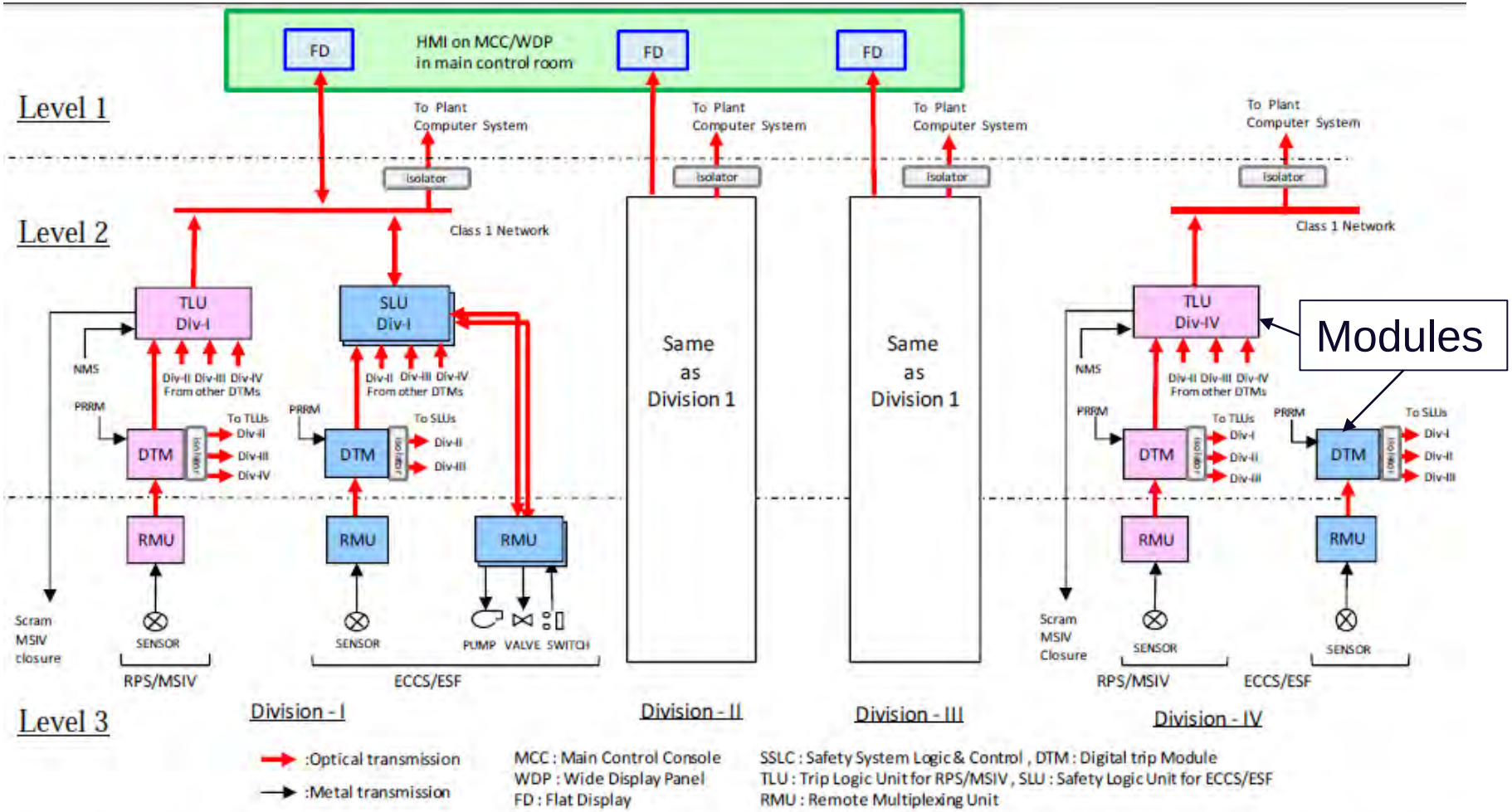
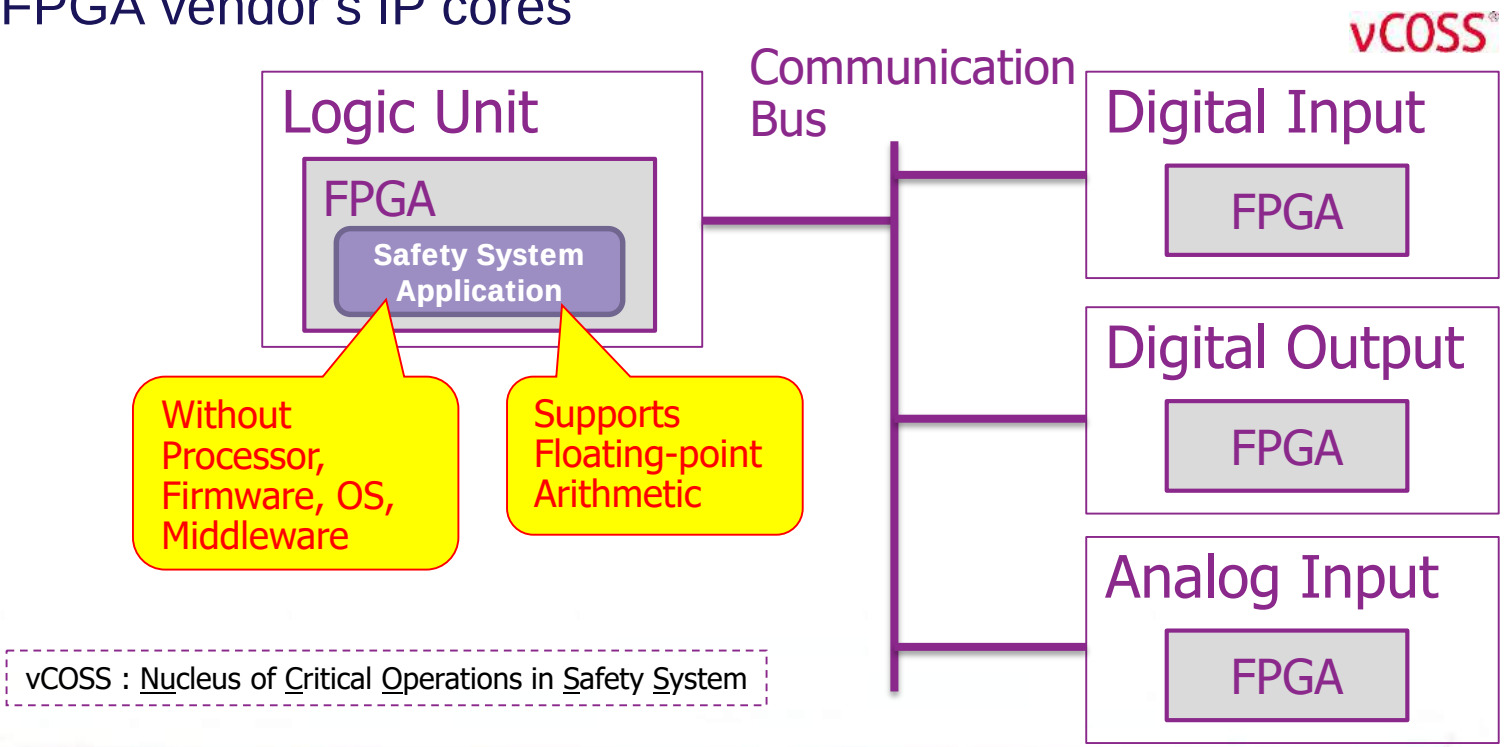


Figure 14.4-4: C&I Architecture of Safety System Logic and Control System (SSLC)

General Configuration

Class 1 FPGA Platform

- Each module is built up of units containing FPGAs
- Units are connected by a communication bus
- The Logic Unit is the heart of each module and does not rely on an FPGA vendor's IP cores



Contents

- Horizon Nuclear Power overview
- C&I Architecture and development of FPGA-based platform
- **UK specific requirements: ICBMs**

Regulatory guidance

- Objective based regulations
- N+2
- The Office for Nuclear Regulations require the FPGA development process to be treated as a form of software development
- Safety Assessment Principles (SAPs) and Technical Assessment Guides (TAGs)
  - Engineering Principles: safety systems (SAP) ESS.27, Computer-based safety systems, life cycle demands
  - TAG 46, Computer Based Safety Systems
- Relevant Good Practice:

IEC 61226 **IEC 61513**

IEC 60880 (for Cat A) **IEC 61508**

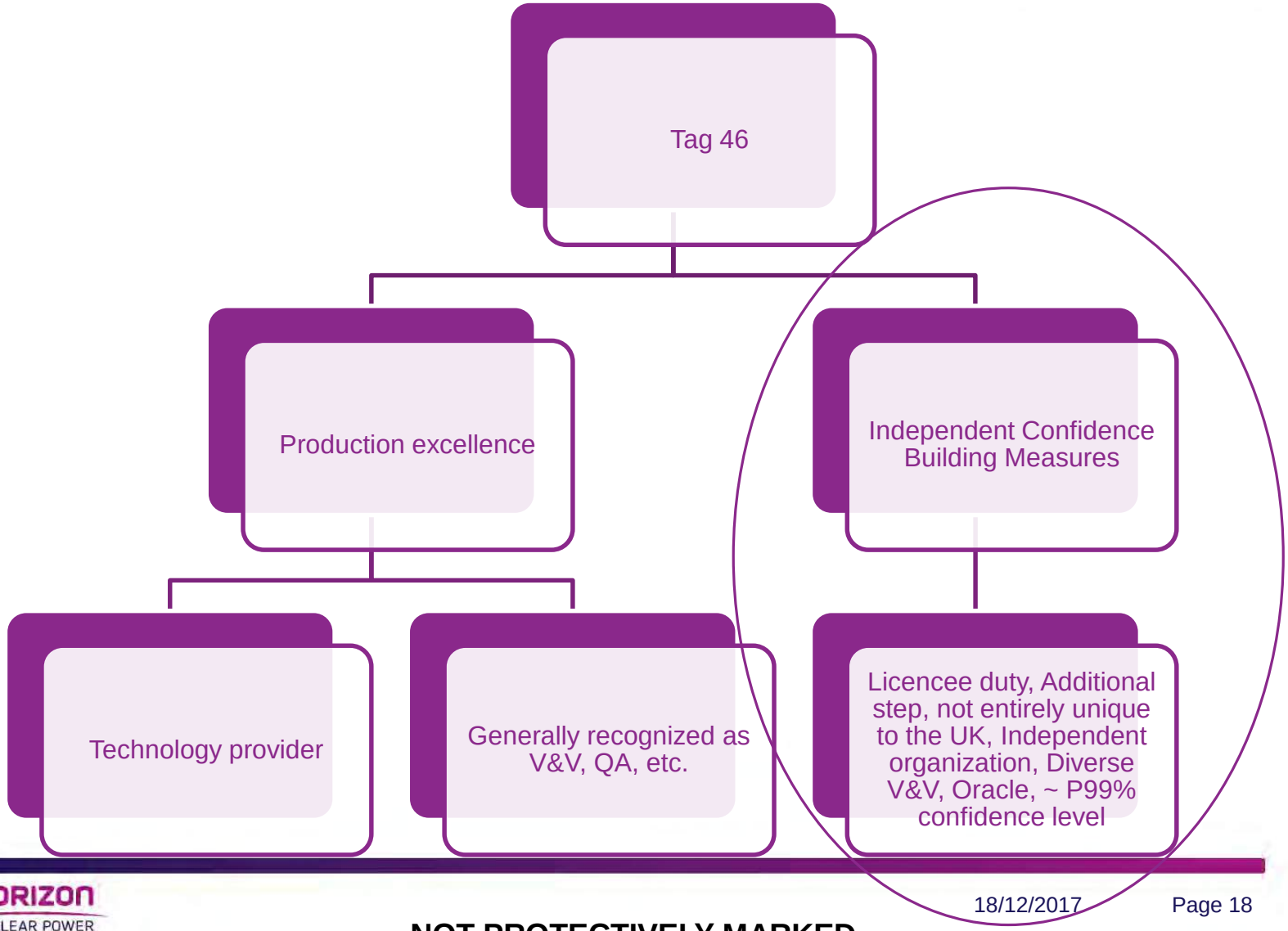
What is ICBM?

From TAG 46, Computer Based Safety Systems

- Safety Assessment Principle (SAP) ESS.27 has two key legs, *Production Excellence* (PE) demonstration and *Independent Confidence Building Measures* (ICBM).
- The philosophy of the multi-legged procedure is that system acceptance centres on the demonstrated high quality production and an independent searching examination of the systems' fitness for purpose that finds no significant number of errors.
- *Production Excellence* is for Hitachi to perform and demonstrate.
- *Independent Confidence Building* is for Horizon, as nuclear site licensee, to perform and demonstrate.
- *Graded*, based on the *Class of the system*; most demanding for the (FPGA-based) Class 1 Platform

A two V&V approach: PE vs. ICBMS

From TAG 46, Computer Based Safety Systems



ICBM of FPGA-based Platform

Some Issues

- Need for independent, competent organization
- ICBM of FPGA-based platform new to civil nuclear
- Timing Issues to answer the high number of tests
- No actual visibility of what is in the final configured FPGA chip (place and route); integrity demonstration

ICBM of the FPGA-based Platform

Formal methods now in PE

- Means different mix of PE/ ICBM techniques
- For ICBM
  - Review of PE
  - Dynamic Analysis/testing, simulator-based with coverage metrics
  - Statistical Testing
- No separate Static Analysis as this is in PE
  - Including no further formal verification as this is in PE

ICBM of the FPGA-based Platform

Timing Issues

- Concurrency Analysis
- FPGAs exhibit parallel rather than serial operation
  - Previous ICBM experience largely with microprocessor-based systems exhibiting serial operation
- The FPGA-based Platform configuration results in a mixture of synchronous and asynchronous behaviours
- Proposed ICBM approach
  1) Detailed architectural analysis to identify vulnerabilities
  2) Detailed analysis of each identified vulnerability
  3) Use of nuXMV tool for synchronous and SPIN for asynchronous concurrency analysis

ICBM of the FPGA-based Platform

What is in the final configured FPGA chip?

- FPGAs provide no visibility to what's in the chip
  - Can't be read back – at least not with any confidence
- Bitstream is proprietary – and encrypted
  - Even if it could be read it still doesn't actually tell you what actually ends up in the FPGA chip
- Hence have to be reliant on testing at the FPGA chip boundary to build confidence;
  - Dynamic Testing
  - Statistical Testing

ICBM of the FPGA-based Platform

Real engineering challenges

- 99% confidence level, 10-4 pdf
- Time to perform ~ 50,000 statistical tests
  - Licencee's position:
    - Reduce confidence level down to PSA's P50 (hence, number of test)
    - Use early 5th and a 6th division as a representative test bed
    - Solve timing issues
- Digital systems unavoidable, Nuclear cannot be left behind
- Challenges not unique to well controlled RPS/ SSLC technology provider
  - See Class 1 systems such as Emergency power generators and switchgear, HMIs, HVACs, etc.

ICBM of the FPGA-based Platform

One Big Advantage!

- New FPGA-based Platform is being developed in the knowledge that ICBMs have to be carried
- Hence platform is being developed to make it “ICBM-capable”
  - For example – design will provide quick and complete reset for use between statistical tests
- Horizon/Hitachi taking specialist advice on this
- GDA Pilot exercise

HORIZON NUCLEAR POWER

ENERGY WORKING FOR BRITAIN

Use of FPGA technology in a (UK) Nuclear Protection System

Cezar Georgescu

December, 2017