Introduction of Class 1 FPGA Platform for the UK ABWR

Junichi Kumagai
Toru Motoya
Hitachi, Ltd.
Contents

1. About Hitachi and Hitachi’s C&I
2. UK ABWR Project Overview
3. UK ABWR C&I System Architecture
4. Class 1 FPGA Platform
Contents

1. About Hitachi and Hitachi’s C&I
2. UK ABWR Project Overview
3. UK ABWR C&I System Architecture
4. Class 1 FPGA Platform
About Hitachi, Ltd. (FY2017)

Revenues
$85.5 billion

- Construction Machinery: 11%
- Electronic Systems & Equipment: 23%
- Social Infrastructure & Industrial Systems: 20%
- Information & Telecommunication Systems: 6%
- Smart Life & Ecofriendly Systems: 5%
- Automotive Systems: 10%
- High Functional Materials & Components: 16%
- Others: 9%
Global Expansion* (FY2017)

**Europe**
- Revenues: $8.8 billion
- Number of companies: 139
- Number of employees: 16 thousand

**Asia (incl. China)**
- Revenues: $9.5 billion yen
- Number of companies: 143
- Number of employees: 44 thousand

**North America**
- Revenues: $10.7 billion
- Number of companies: 100
- Number of employees: 21 thousand

**Japan**
- Revenues: $42.4 billion
- Number of companies: 202
- Number of employees: 168 thousand

**Other Areas**
- Revenues: $4.5 billion
- Number of companies: 106
- Number of employees: 12 thousand

---

<table>
<thead>
<tr>
<th>Region</th>
<th>Revenues ($ billion)</th>
<th>Number of companies</th>
<th>Number of employees (thousand)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>$42.4</td>
<td>202</td>
<td>168</td>
</tr>
<tr>
<td>Outside Japan</td>
<td>$43.1</td>
<td>677</td>
<td>139</td>
</tr>
<tr>
<td>Total</td>
<td>$85.5</td>
<td>879</td>
<td>307</td>
</tr>
</tbody>
</table>

* Revenues: FY2017, Number of companies and employees: As of end of FY2017 © Hitachi-GE Nuclear Energy, Ltd., Hitachi, Ltd. 2018. All rights reserved.
Hitachi Nuclear Application History

DCS: Distributed Control System  Note: Definition of Safety System and Safety Related System is based on IAEA Safety Glossary 2007
ABWR Operating Experience by Hitachi Digital C&I System

- Kashiwazaki-Kariwa Unit 6 (TI), C/O in 1996
- Unit 7 (NI), C/O in 1997

- Ohma Unit 1 (NI and TI), FAT finished (FSS), completed in 2016

- Shika Unit 2 (NI and TI), C/O in 2006

- Hamaoka Unit 5 (TI), C/O in 2005

- Shimane Unit 3 (NI and TI), under preoperational test at the site (FSS), completed in 2009

C/O: Commercial Operation
NI: Nuclear Island
TI: Turbine Island
FSS: Full Scope Simulator
FAT: Factory Acceptance Test
Contents

1. About Hitachi and Hitachi’s C&I
2. UK ABWR Project Overview
3. UK ABWR C&I System Architecture
4. Class 1 FPGA Platform
UK ABWR Project Overview

- Horizon Nuclear Power is planning to build 1,350 MWe class Advanced Boiling Water Reactors (ABWR) in Wylfa and Oldbury.
- The primary focus is to secure all key agreements and permissions in place for the Final Investment Decision in 2019.
- Commercial operation of the 1st unit at Wylfa is planned to be in the middle 2020s.
UK ABWR Project Assessment Status

- Final process of Step-4 was completed in December 2017.
- Currently at pre-engineering phase.

Dec. 2017 GDA completed within the target period of 5 years

Contents

1. About Hitachi and Hitachi’s C&I
2. UK ABWR Project Overview
3. UK ABWR C&I System Architecture
4. Class 1 FPGA Platform
UK regulatory expectations

UK regulatory expectations for C&I are;

- Complying with International Code and Standards such as IEC 61513
- Referring to assessment guides such as SAP, TAGs
- Referring to relevant good practice such as feedbacks from other GDA

Based on the above expectations, Design features of UK ABWR system are determined, such as;

- System reliability according to Category & Class
- Redundancy
- Separation
- Diversity

SAP: Safety Assessment Principle
TAG: Technical Assessment Guide
IEC: International Electro technical Commission
Overall UK ABWR C&I Architecture

Hardwired Backup System

Safety System (Class 1)

Control System

Reliability:
- Complied with required reliability value for each system (e.g. reliability of SSLC is assigned $10^{-4}$ PFD.)

SSLC: Safety System Logic and Control system
PFD: Probability of Failure on Demand
Overall UK ABWR C&I Architecture

Hardwired Backup System

Safety System (Class 1)

Control System

Redundancy:
- Each safety system satisfies N+2 requirement.
- Each division has 2 out of 4 voting logic.
Overall UK ABWR C&I Architecture

- **Hardwired**
  - Diverse Reactor Shutdown
  - Diverse Core Cooling

- **FPGA platform**
  - Reactor Protection System
  - Emergency Core Cooling System
  - Neutron Monitoring System
  - Radiation Monitoring System

- **μ processor platform**
  - Plant Control System
  - Rod Control and Information System
  - Reactor Auxiliary Control System
  - Turbine Control System
  - Turbine Auxiliary Control System

- **Plant Computer System**

- **Plant Data Network**

**Control System**
- Separation;
  - Class 1 network is isolated from non-class 1 by data diode.
  - Class 1 control panels of each division are installed in different room.
Overall UK ABWR C&I Architecture

Hardwired

Control System

Diversity;
- Different platforms are adopted for safety system, HWBS and control system to secure defense against Common Caused Failure.

Plant Data Network

Safety System (Class 1)

Hardwired Backup System

Diverse Reactor Protection System
Diverse Emergency Core Cooling System

FPGA
- platform

µ processor
- platform

Plant Computer System

Network link
Hardwired link

Hardwired

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse

Diverse
Contents

1. About Hitachi and Hitachi’s C&I
2. UK ABWR Project Overview
3. UK ABWR C&I System Architecture
4. Class 1 FPGA Platform
Overview of the Class 1 FPGA Platform

Hitachi developed a Class 1 Platform vCOSS S-zero

The main features are:

- Each module has FPGAs inside and connected to safety field bus.
- Development process complies with IEC 61513, 62566, 61508 and 62443
- Without processor, firmware, OS, middleware
- Supporting floating-point arithmetic without FPGA vendor’s floating-point IP cores
Certification for the Class 1 FPGA Platform

Reliability requirement assigned to SSLC is $10^{-4}$ [PFD]. The platform is required IEC 61508 SIL 3 as single configuration in order to satisfying $10^{-4}$ PFD as a whole system.

Certified as following from TÜV Rheinland in Jan. 2018.

- **vCOSS S-zero** complies with IEC 61508 **SIL 3** as single configuration.
- Measures for fault avoidance is applied in accordance with IEC 61508 **SIL 4**.
- Furthermore, Certified as SL 1 (Cyber Security Standard)
  - IEC 62443-4-1:2018 (Edition 1.0),
  - IEC 62443-4-2:2017 (65/663/CDV)

SSLC: Safety System Logic and Control system
PFD: Probability of Failure on Demand

No.:968/FSP 1119.07/18
The figure focuses on the range of the FPGA bit stream from the specification.
We applied the formal verification to the files generated from the specification to comply with SIL 4.
Calculation Macros

- Allow user to design as function block diagram using general design tool
- Support wide variety macros which are developed as white-box
  - Essential analog macro; about 10 types (+, −, ×, ÷, √...)
  - Simple digital macro; about 30 types (AND, OR, Flip Flop, ...)
  - Advanced function macro; about 30 types (PID control, Switch, ...)
  - The others are under development.

Users are able to use over 10,000 macros per one LU and design flexibly!!
Hitachi completed GDA on schedule without GDA issues including C&I field.

Our design features

- Different Platforms are adopted to achieve the diversity.
- Developed vCOSS S-zero in accordance with IEC 61513 series.
- vCOSS S-zero has been certified for single SIL 3 according to IEC 61508. Furthermore, the certificate confirmed that measures for fault avoidance is applied in accordance with IEC 61508 SIL 4.
- vCOSS S-zero has also been certified for Security Level 1 according to IEC 62443-4.
Introduction of Class 1 FPGA Platform for the UK ABWR

Junichi Kumagai
Toru Motoya
Hitachi, Ltd.