ADELARD

Use and licensing of COTS digital devices in safety critical industries

Sofia Guerra

Eoin Butler, Gareth Fletcher, Samuel George, Heidy Khlaaf

22 October 2019

PT/713/150004/4

Adelard LLP, 24 Waterside, 44-48 Wharf Road, London N1 7UX
T +44 20 7832 5850   E office@adelard.com   W www.adelard.com

ABOUT ADELARD

- Adelard LLP is an independent company founded in 1987
- Working on safety, security and dependability of computer-based system
- Product and services company

- Assessment and justification of computer-based safety systems
  - PLCs, FPGAs, PCs, smart devices
- Safety case development and tool support
- Guidance and standards development
- System and software assessment, analysis and testing

OUTLINE

- Background to the project and objectives
- Approach
- Coverage
- Analysis
- Conclusions

SMART DEVICES

Smart devices

Commercial off the shelf devices, containing both hardware and software that perform a defined function, and may be configured, but not programmed by the end user.

WHY SMART SENSORS?

- Pure analogue sensors disappearing
- Improved functionality
  - Better accuracy
  - Better noise filtering
  - In-built linearisation
  - Better on-line calibration
  - Better diagnostic features
- Often less expensive

SMART SENSORS -> SMART DEVICES

- Embedded industrial systems
  - Commercial-Off-The-Shelf
  - Perform a defined function
  - Smart or intelligent – microprocessor or microcontrollers
  - Configurable but not programmable – fixed firmware
  - Have a safety role
  - Examples qualified include
    - Temperature transmitters
    - Pressure transmitters
    - Voltage regulators
    - Gas analysers
    - Boiler controllers
    - And
      Relays, UPS, Radiation monitors

Safety demonstration of smarts – Why is it difficult?

- Safety demonstration requires information about product and process and knowledge of internal structure - supplier's IP
- Usually sold as black-box
- Nuclear industry is a small customer, so does not have much leverage with the manufacturers

- It is usually done by attempting to show compliance with development standards
  - Not developed to nuclear standards

- Analysis techniques do not necessarily suitable to be applied
- Safety justification may required (static of formal) analysis of the software

PROJECT OBJECTIVES AND APPROACH

- Review use of COTS components in safety and safety related applications
- Both nuclear and other sectors
- Focus on software aspects of justification, not aspects of the justification common to analogue devices
- Approach
  - Information from
    - Consultations
    - Review of publicly available information
    - Information already known to Adelard
  - Set of questions/topics to be covered defined for project use

TOPICS COVERED

- Types of COTS
- Applications
- Regulatory requirements
- Categorisation
- Compliance with standards
- Role of third-party certification
- Evidence required
- Assurance activities carried out by the licensee
- Reuse of licensing activities in different applications

COVERAGE

Nuclear	Other sectors
Finland	Oil and gas (UK)
Sweden	Rail industry (UK)
UK	Aviation (USA)
USA	Automotive (UK)
France	
Germany	
Canada	

OIL AND GAS

- Expectation that the following exists
  - Safety manual
  - Functional safety assessment
  - Certification – IEC 61511
- Overall process follows IEC 61511
- Mainly SIL 1, and some SIL 2. SIL 3 typically require diversity

ANALYSIS

- Use of smart devices vs programmable products
- Compliance with standards
- Use of third-party certifications
- Assurance activities independent of the manufacturer/supplier
- Sector-specific supply chains
- Generic and application-specific assessments
- Categorisation and classification

ANALYSIS

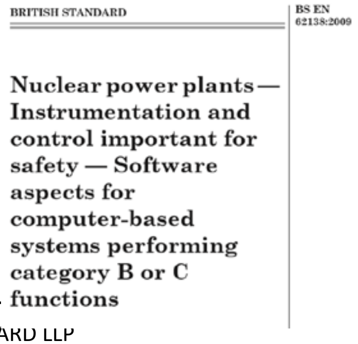
Use of smart device vs programmable products

- Some industries do not commonly use smart/COTS component
  - Avionics, automotive
- Space and weight drive the development of integrated solutions
- Enabled by dedicated supply chains

ANALYSIS

Compliance with standards

- All sectors and countries , compliance of the development process and quality assurance approaches with relevant standards played an important role
- Standards vary
- The way compliance is assessed also varies



BRITISH STANDARD

BS EN 62138:2009

Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions

Software Considerations in Airborne Systems and Equipment Certification

BRITISH STANDARD

BS EN 50155:2007

Incorporating corrigendum May 2010

Railway applications — Electronic equipment used on rolling stock

BS EN IEC 61000-6-2:2019

Incorporating corrigendum March 2019

ndards Publication

magnetic compatibility (EMC)

Part 6-2: Generic standards - Immunity standard for industrial environments

ANALYSIS

Use of third-party certifications

- Certain industries rely heavily on the use of third-party certifications
  - Independent assessor (may be funded by manufacturer) performed an assessment and produces a certificate
- In certain industries, certification does not replace the need for examining evidence
- Most commonly used standards is IEC 61508
- Most use of certification is confined to lower integrity levels
- The use of certification is to an extent linked to liability and risk ownership

ANALYSIS

Assurance activities independent of the manufacturer/supplier

- In all cases, the end user must perform some level of assurance activities themselves
- This is independent of the level of certification that is used/accepted
- It varies from test to source code analysis

ANALYSIS

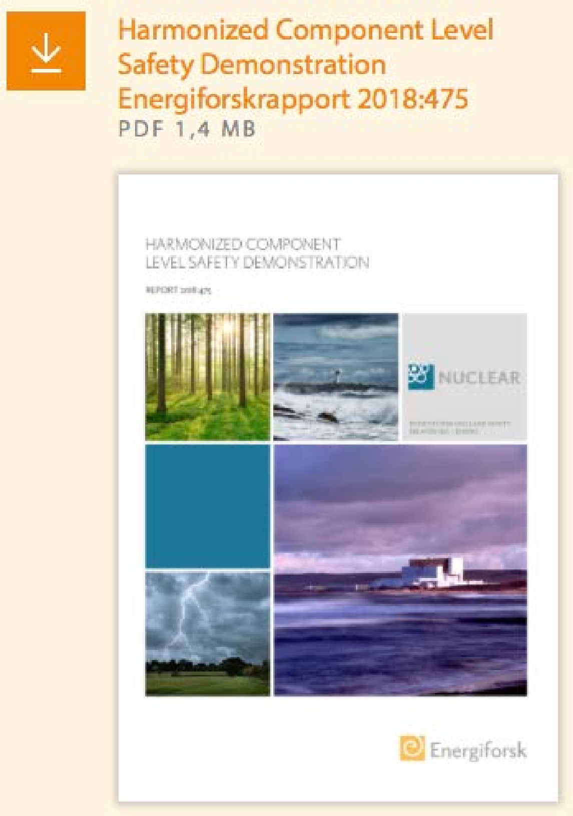
Sector-specific supply chains

- Sectors with large markets and stringent requirements tend to attract sector-specific devices
- These are designed to relevant standards
- Nuclear markets tend to be smaller, specially for general-purpose components
- Interesting questions are whether
  - Internationally the nuclear market might be significant to attract more supplier engagement
  - Products developed for industries are suitable for use in the nuclear industry

ANALYSIS

Generic and application-specific assessments

- Vary from sector to sector
  - Common in rail
  - Not used in avionics
- Nuclear industry exploring/using generic assessments
- Driver is re-use and associated cost reduction



Harmonized Component Level Safety Demonstration
Energiforskrapport 2018:475
PDF 1,4 MB

ANALYSIS

Categorisation and classification

- In all cases, the end user must perform some level of assurance activities themselves
- This is independent of the level of certification that is used/accepted
- It varies from test to source code analysis

CONCLUSIONS

- COTS digital components becoming more common in a number of industries
- Compliance with standards is ubiquitous
- Commercial factors drive the availability of components (and the ability of assessing the components)
- A more harmonised approach and cross-country sharing might increase the ability of suppliers willing to support the nuclear industry