Ada Europe 2014
Industrial Sessions: Ada in Railways

Critical software For the First European Rail Traffic Management System

Ana Rodríguez
June 2014
Contents

- Corporate Overview
- ERTMS - European Rail Traffic Management System
- RBC (Radio Block Centre)
- Conclusions and opportunities
Corporate Overview
Service Portfolio

Safety-critical Electronic Systems Engineering

<table>
<thead>
<tr>
<th>Engineering</th>
<th>Consulting</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Engineering</td>
<td>System Consulting</td>
<td>HIL Test Systems</td>
</tr>
<tr>
<td>Hardware Engineering</td>
<td>Technology Consulting</td>
<td>Simulators</td>
</tr>
<tr>
<td>RAMS Engineering</td>
<td>Process Consulting</td>
<td>Test Benches</td>
</tr>
<tr>
<td>Software Engineering</td>
<td></td>
<td>Electronic Control Units</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Development Tools</td>
</tr>
</tbody>
</table>

In-house
On-site
Assystem is an Industrial Engineering company listed in NYSE Euro next Paris. Offices in 14 countries, employs approximately 11,100 people worldwide and reported €871.4 M in revenue in 2013. 2013 Consolidated Revenue Up 1.8%
Corporate Overview
Quality – Standards – Memberships

<table>
<thead>
<tr>
<th>Accreditations</th>
<th>Industry Standards</th>
<th>Memberships</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIN EN ISO 9001:2008</td>
<td>IEC 61508</td>
<td>Cetren</td>
</tr>
<tr>
<td></td>
<td>ISO 26262</td>
<td>ECPE</td>
</tr>
<tr>
<td></td>
<td>RTCA</td>
<td>FlexRay</td>
</tr>
<tr>
<td></td>
<td>CENELEC</td>
<td>Open-DO</td>
</tr>
<tr>
<td></td>
<td>EN 50126, EN 50128 &amp; EN 50129</td>
<td>VDA</td>
</tr>
<tr>
<td></td>
<td>BS IEC 60880-2:2000</td>
<td>ZAL</td>
</tr>
<tr>
<td></td>
<td>MISRA</td>
<td>Shitf2RAIL</td>
</tr>
<tr>
<td></td>
<td>ECSS</td>
<td></td>
</tr>
</tbody>
</table>
Corporate Overview

Key Customers and Locations

- London Underground
- Westinghouse Rail Systems
- BAE Systems
- Augusta Westlands
- Ultra Electronics
- Meggitt

Key Customers:
- Westinghouse Rail Systems
- GE Aviation
- Ultra Electronics
- Goodrich
- GE Transportation
- GE Aviation
- Hamilton Sundstrand

Silver Atena Locations:
- Audi
- BMW
- Daimler
- Volkswagen
- Robert Bosch
- ZF Lenksysteme
- IAI
- Snecma
- Alstom
- Airbus DS
- Siemens
- THALES Group
- CAF
- Eliop
- Bombardier
- Airbus
- EADS
- MTU Aero Engines
- Airbus
- BAE Systems
- Meggitt
- Ultra Electronics
- Augusta Westlands
- Westinghouse Rail Systems
- Hamilton Sundstrand
- GE Transportation
- GE Aviation
- Goodrich
- London Underground
- Silver Atena Locations
- Key Customer
Corporate Overview

Railways Competences

- Software Engineering, Hardware Engineering and Test Facilities
- RAMS (Reliability, Availability, Maintainability and Safety) Program
  - Safety Management: Safety Plan, Hazard Analysis, Preliminary Hazard Analysis, Hazard Log, V&V reports Safety Case
  - Independent Safety Assessment
  - RAMS proven methodology (tool-set, methods and techniques)
- Safety Integrity Level (SIL): SIL 4, 3 and 2
- Consultancy on processes, products deployments, safety issues and software technologies
- H2020 SHIFT²RAIL Innovation Program
  - On-board Train Integrity; Zero Field Testing; Formal Methods and Standardisation for Smart Signalling Systems; Traffic Management System
Contents

- Corporate Overview
- ERTMS - European Rail Traffic Management System
- RBC (Radio Block Centre)
- Conclusions and opportunities
ERTMS
European Rail Traffic Management System

- ERTMS aims to enable intelligent train traffic management with interoperable driving systems and optimise capacity, reliability and minimise life-cycle cost
- European Train Control System (ERTMS/ETCS) developed to establish common standards for on-board systems, connection/communication interfaces between modules and the development of common procedures
- Specifications of ERTMS/ETCS requirements are public, and define the so-called kernel and its interfaces with the ground
- ... and now being deployed across Europe

Assist our clients in the development and prove of ERTMS/ETCS equipments, which is intended to achieve this interoperability with safety
ERTMS
ERTMS/ETCS

- The ERTMS/ETCS system provides the driver, in a standard format, with all the information needed for optimum driving, constantly controlling the effect of every action taken in terms of train safety, and activating emergency braking should the train speed exceed the maximum safety limits

- There are three levels of application

<table>
<thead>
<tr>
<th>ERTMS/ETCS level</th>
<th>On board</th>
<th>Track-side</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Check of train integrity</td>
<td>Data transmission</td>
</tr>
<tr>
<td>1</td>
<td>no</td>
<td>balises+loops (option)</td>
</tr>
<tr>
<td>2</td>
<td>no</td>
<td>balises+radio</td>
</tr>
<tr>
<td>3 (planned)</td>
<td>yes</td>
<td>balises+radio</td>
</tr>
</tbody>
</table>
ERTMS
ERTMS/ETCS - Radio Block Centre

- Projects on Advance Traffic Management & Control Systems for a new generation of signalling and control systems, building on current ERTMS/ETCS
  - Bombardier: Improvement of Rio de Janeiro commuter lines that is the first ERTMS solution deployed in South America
  - Siemens Rail Automation Division (former Invensys Rail Dimetronic): Development of the Radio Block Centre (RBC), ERTMS interoperability requirements for the data exchange between the RBC and the on-board sub-system

- On the basis of the state of the infrastructure (free line, routes in the stations, train speeds, slowdowns) and the position of the train, the RBC transmits authorisation to proceed data to the on-train unit, giving details of the free distance and the maximum permitted speed at the point
Contents

- Corporate Overview

- ERTMS - European Rail Traffic Management System

- RBC (Radio Block Centre)

- Conclusions and opportunities
Radio Block Centre

ERTMS/ETCS level 2’s ground technology

- ERTMS/ETCS level 2’s ground system comprises a RBC central unit, installed in specific central posts, from which railway circulation is managed and controlled through the System of Command and Control (SCC).

- The RBC continuously transmits to every train, via GSM-R radio, the speed and the train distance, the constraints imposed by the track, and the position of the trains.

SCC © Cetren
Radio Block Centre

System Operation

- RBC: bi-directional continuous information by GSM-R Euro-radio (SIL4 Ada Software)
- CEC - Command and control of all the RBCs in a line
- JRU – black-box unit
- Maintenance Assistance Unit
- I/C Control equipment
- Local ERTMS Control, operator commands console

©Siemens
Radio Block Centre
Safety & Integrity Requirements

- ERTMS/ETCS – Baseline 3 - System Requirements Specification
- High integrity requirements for RBC data generation: maintaining and assuring the accuracy, consistency and validity of data.
- RBC messages generation function: Safety Integrity Level 4 (SIL4)
- Strict life-cycle development to eliminate (minimize) threats to data integrity
- Develop controls to eliminate or reduce the probability or severity of each hazard, to lower the overall risk
Radio Block Centre
Safety & Integrity processes and techniques

- CENELEC standards

![CENELEC Standards Diagram]

- Independent teams: Design& Development, V&V and safety auditor (Independent Safety Assessment)

Table A.9 – Software Quality Assurance (SQA)

<table>
<thead>
<tr>
<th>TECHNIQUE/MEASURE</th>
<th>Ref</th>
<th>SIL 0</th>
<th>SIL 1</th>
<th>SIL 2</th>
<th>SIL 3</th>
<th>SIL 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Accredited to EN ISO 9001</td>
<td>7.1</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>2. Compliant with EN ISO 9001</td>
<td>7.1</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>3. Compliant with ISO/IEC 90003</td>
<td>7.1</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>4. Company Quality System</td>
<td>7.1</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>5. Software Configuration Management</td>
<td>D.40</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>6. Checklists</td>
<td>D.7</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>7. Traceability</td>
<td>D.50</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>8. Data Recording and Analysis</td>
<td>D.12</td>
<td>HR</td>
<td>HR</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

Requirement:

1) This table shall be applied to different roles and all phases.
Radio Block Centre

Safety & Integrity Requirements

- RBC embedded software:
  - Safety-critical Software (software which can directly create or control a hazard).
  - Software that provides information required for a safety-related decision falls into the safety-critical category

- Designing for Safety SW is designing for minimum risk: Hazard risk (likelihood and severity), risk of software defects, risk of human operator errors, and other types of risk (such as programmatic, cost, schedule, etc.)

- The RBC software is implemented in Ada95 Language:
  - Ada is widely used for railways critical (SIL4 and SIL3) developments
  - Ada enforces good programming practices, makes bugs easier for the compiler to find, and incorporates elements that make the software easier to verify
Radio Block Centre
Safety & Integrity Requirements

- RBC embedded software:
  - Safety-critical Software (software which can directly create or control a hazard).
  - Software that provides information required for a safety-related decision falls into the safety-critical category.

- Designing for Safety SW is designing for minimum risk: Hazard risk (likelihood and severity), risk of software defects, risk of human operator errors, and other types of risk (such as programmatic, cost, schedule, etc.)

- The RBC software is implemented in Ada95 Language:
  - Ada is widely used for railways critical (SIL4 and SIL3) developments.
  - Ada enforces good programming practices, makes bugs easier for the compiler to find, and incorporates elements that make the software easier to verify.
RBC
Safety Process – RAMS program

RAMS Engineering processes, tools and techniques used to manage, development and assessment of high-integrity systems:

- Preliminary Hazard Analysis
- System Hazard Analysis
- System Safety Assessment
- Safety Case
- Independent Safety Assessment

Early risk appreciation

Quantitative measurements of reliability, availability and maintainability through a RAM program

ISA recognized by Spanish Railway Authority
- Design, specification and implementation of the RBC V&V Program
- Functional testing, integration and performance testing

**SIL4 Lifecycle**

- **Requirements Analysis**
  - Modelling, UML, RTSA

- **Design**
  - UML, RTSD, Model Based Design

- **Coding**
  - Ada, Assembler

- **V&V**
  - Dynamic and Static Analysis
    - Code Inspection, Unit Test

- **Integration**
  - SW/SW Integration, SW/HW Integration

**Additional Processes**

- Project Management
- Quality Management
- Risk Management
- Configuration Management
Radio Block Centre
RBC – SW & Validation Development

- Test Bench based on Silver-Atena testing product
  - Simulation of Equipments interfacing RBC
  - Messages logger
  - Automatic test scenarios and scripts generation
Contents

- Corporate Overview
- ERTMS - European Rail Traffic Management System
- RBC (Radio Block Centre)
- Conclusions and opportunities
Radio Block Centre

Conclusion and opportunities

- Spain: ERTMS/ETMS largest deployment in Europe
- Consolidated technologies and capacities
- Good opportunities for Spanish railways industry (AVE La Meca-Medina)
- New challenges for the deployment of ERTMS/ETCS level 2 and 3
  - Introduction of satellite assets for improving safety at railway level crossings
  - Employ Satellite Communication and Satellite Navigation in conjunction with existing terrestrial assets/systems
Conclusion and opportunities

- Ada Language and development tools are commonly used for SIL4 and SIL3 projects
- Needs for improvement of safety assurance processes, both deployment and operations of the train lines
  - The “safeness” and reliability of a system depend on many factors
  - Humans are involved in all aspects of the process, quite capable of subverting even the “safest” of languages
Radio Block Centre

Conclusion and opportunities

- Expert report commissioned by the Spanish government (June 2014)
- The cause of the crash was “excess speed resulting from the driving personnel’s failure to comply with speed limit regulations”
- Adif, the state railway infrastructure manager failed to install the kind of technology that can automatically slow down a train in the event of human error.
- Recommendations: ERTMS signs warning drivers and security mechanisms to automatically slow down speeding trains, a safer internal communications system
Thank you for your attention!

Ana Rodríguez - Aerospace Business Unit Manager  
ana.rodriguez@silver-ataena.es  
Ronda de Poniente 5, 28760 Tres Cantos, Madrid  
Telf. +34 608754488