SILVER ATENA
AN ASSYSTEM COMPANY

Ada Europe 2014
Industrial Sessions: Ada in Railways

Critical software For the First European Rail Traffic Management System

Ana Rodríguez
June 2014

assystem

Contents

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

Corporate Overview

Service Porfolio






Safety-critical Electronic Systems Engineering

Engineering	Consulting	Products
▪ System Engineering ▪ Hardware Engineering ▪ RAMS Engineering ▪ Software Engineering	▪ System Consulting ▪ Technology Consulting ▪ Process Consulting	▪ HIL Test Systems ▪ Simulators ▪ Test Benches ▪ Electronic Control Units ▪ Development Tools

In-house	On-site

Corporate Overview

Silver Atena Group

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

Accreditations

- AS 9100C (EN 9100:2009)
- DIN EN ISO 9001:2008

CMMI LEVEL 3

ISO 9001

VIT

AS 9100

ENAC INSPECCIÓN Nº 286/EI490

Industry Standards

- RTCA DO-160, DO-178B, DO-248B & DO-254
- IEC 61508
- ISO 26262
- CENELEC EN 50126, EN 50128 & EN 50129
- BS IEC 60880-2:2000
- MISRA
- ECSS

CENELEC

RTCA

BSI

European Commission

IEC

ISO

MISRA

Memberships

- Aerospace Cluster
- Cetren
- ECPE
- FlexRay
- Open-DO
- VDA
- ZAL
- Shitf2RAIL

Ada europe

Madrid Network CLUSTER AEROESPACIAL

ZAL Zentrum für Angewandte Luftfahrtforschung GmbH

Cetren CERTIFICACIÓN

bavAIRia Europe's heart of aerospace and navigation

SHIFT2RAIL

ECPE

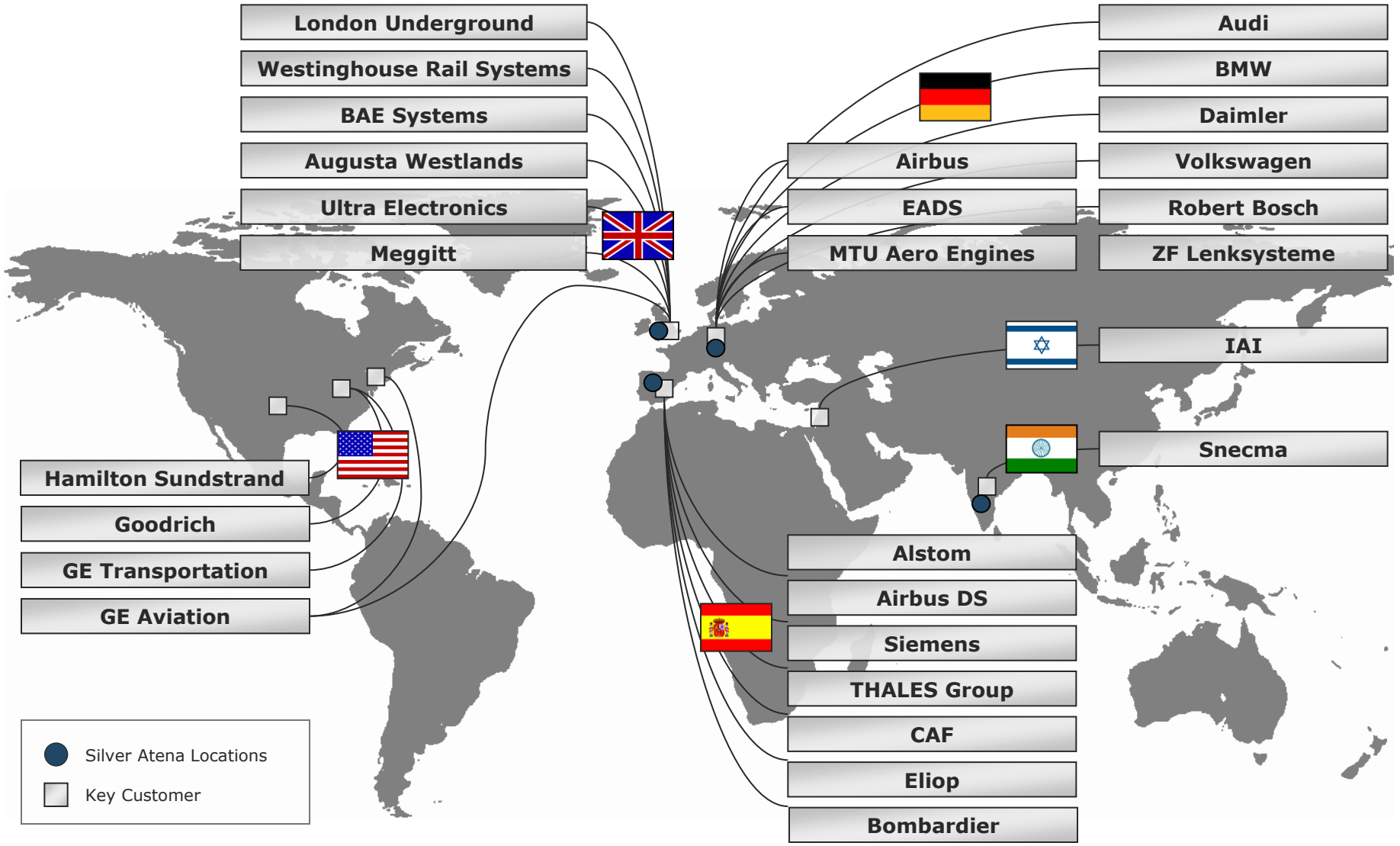
FlexRay™

openDO

VDA

Corporate Overview

Key Customers and Locations



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 1 ERTMS/ETCS equipment

	On board		Track-side			
ERTMS/ETCS level	Check of train integrity	Data transmission	Lineside electronic units	Lineside signals	Track occupancy detection	Radioblock
1	no	balises+loops *(option)*	yes	yes	yes	no
2	no	balises+radio	no	no	yes	yes
3 *(planned)*	yes	balises+radio	no	no	no	yes

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

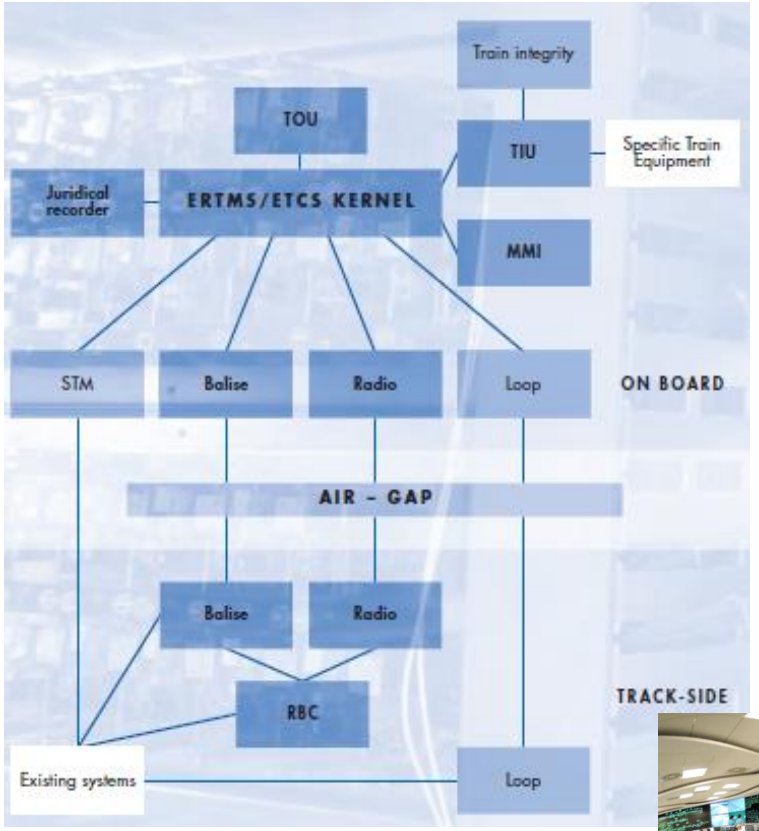
Contents

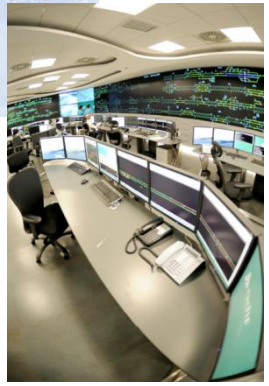
- Corporate Overview
- ERTMS - European Rail Traffic Management System
- RBC (Radio Block Centre)
- Conclusions and opportunities

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



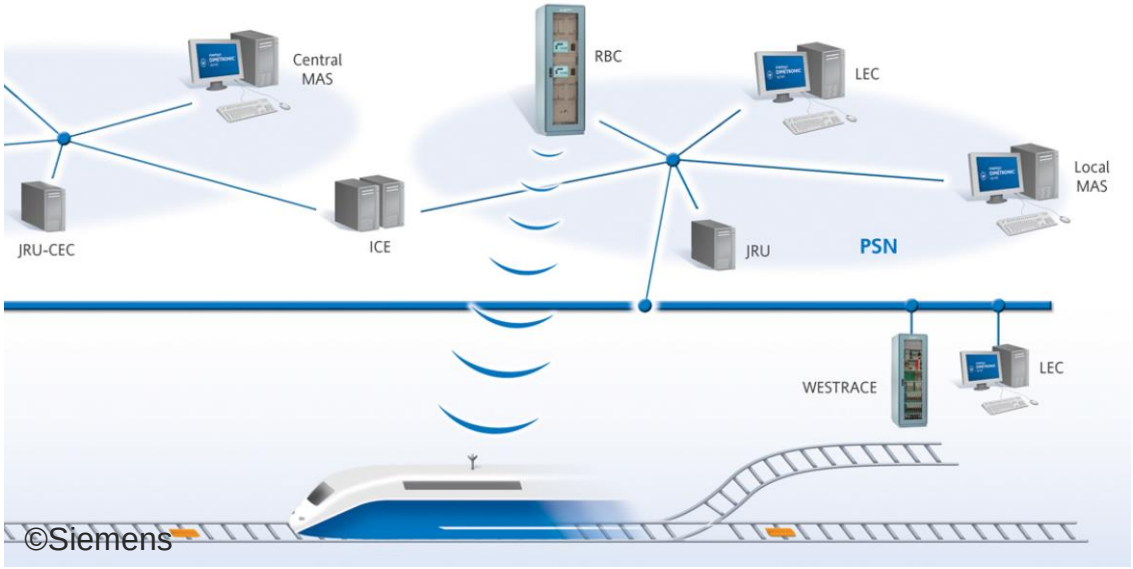


SCC © Cetren

Radio Block Centre

System Operation

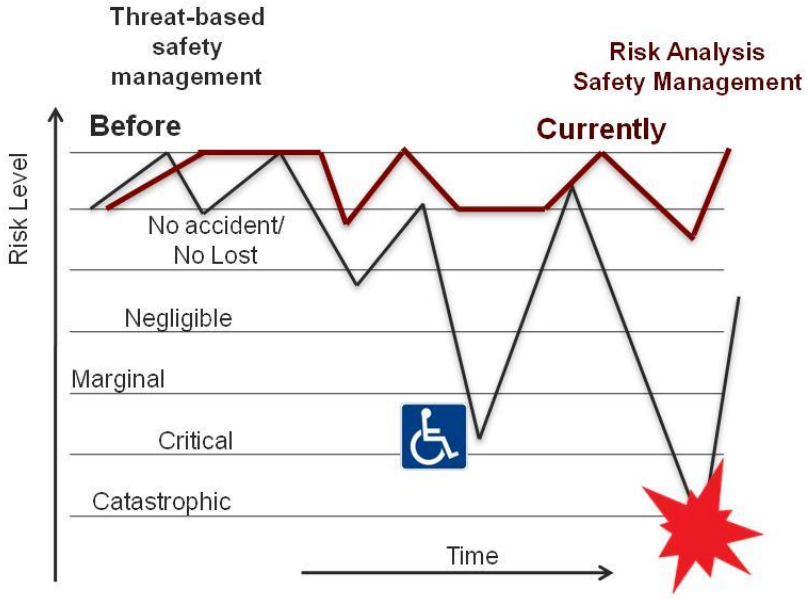
- RBC: bi-directional continuous information by GSM-R Euro-radio (SIL4 Ada Software)
- CEC- Command and control of all the RBCs in a line
- JRU – black-box unit
- Maintenance Assistance Unit
- I/C Control equipment
- Local ERTMS Control, operator commands console



Radio Block Centre

Safety & Integrity Requirements

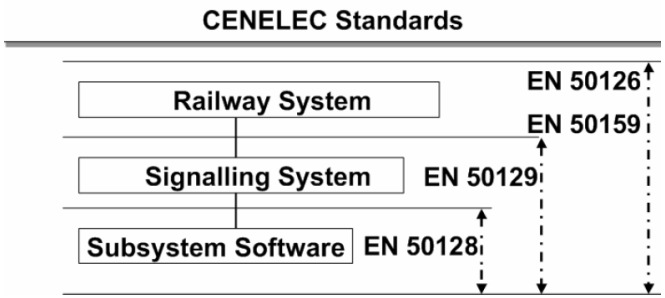
- ERTMS/ETCS – Baseline 3 - System Requirements Specification
- High integrity requirements for RBC data generation: maintaining and assuring the accuracy, consistency and validity of data.
- RBC messages generation function: Safety Integrity Level 4 (SIL4)
- Strict life-cycle development to eliminate (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



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

Table A.9 – Software Quality Assurance (6.5)

TECHNIQUE/MEASURE	Ref	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. Accredited to EN ISO 9001	7.1	R	HR	HR	HR	HR
2. Compliant with EN ISO 9001	7.1	M	M	M	M	M
3. Compliant with ISO/IEC 90003	7.1	R	R	R	R	R
4. Company Quality System	7.1	M	M	M	M	M
5. Software Configuration Management	D.48	M	M	M	M	M
6. Checklists	D.7	R	HR	HR	HR	HR
7. Traceability	D.58	R	HR	HR	M	M
8. Data Recording and Analysis	D.12	HR	HR	HR	M	M
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

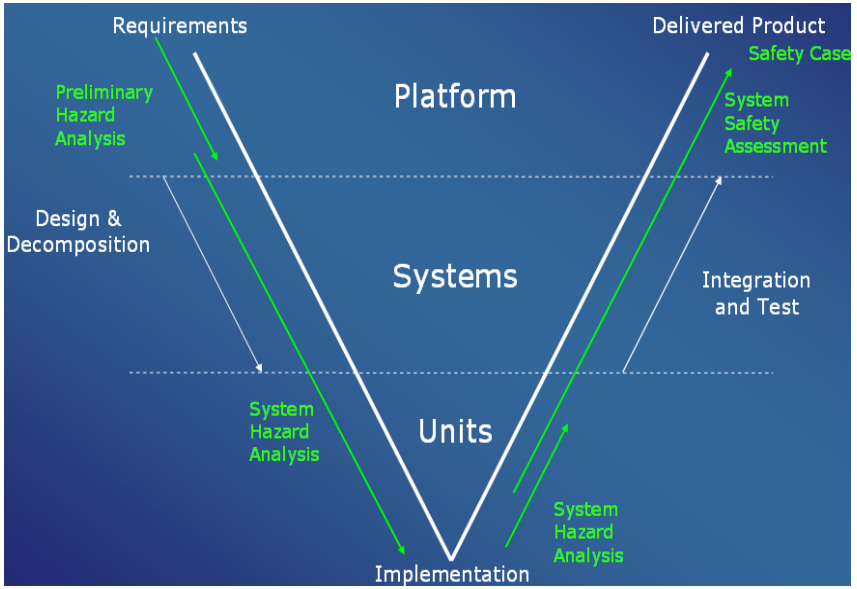
Safety Process – RAMS program

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



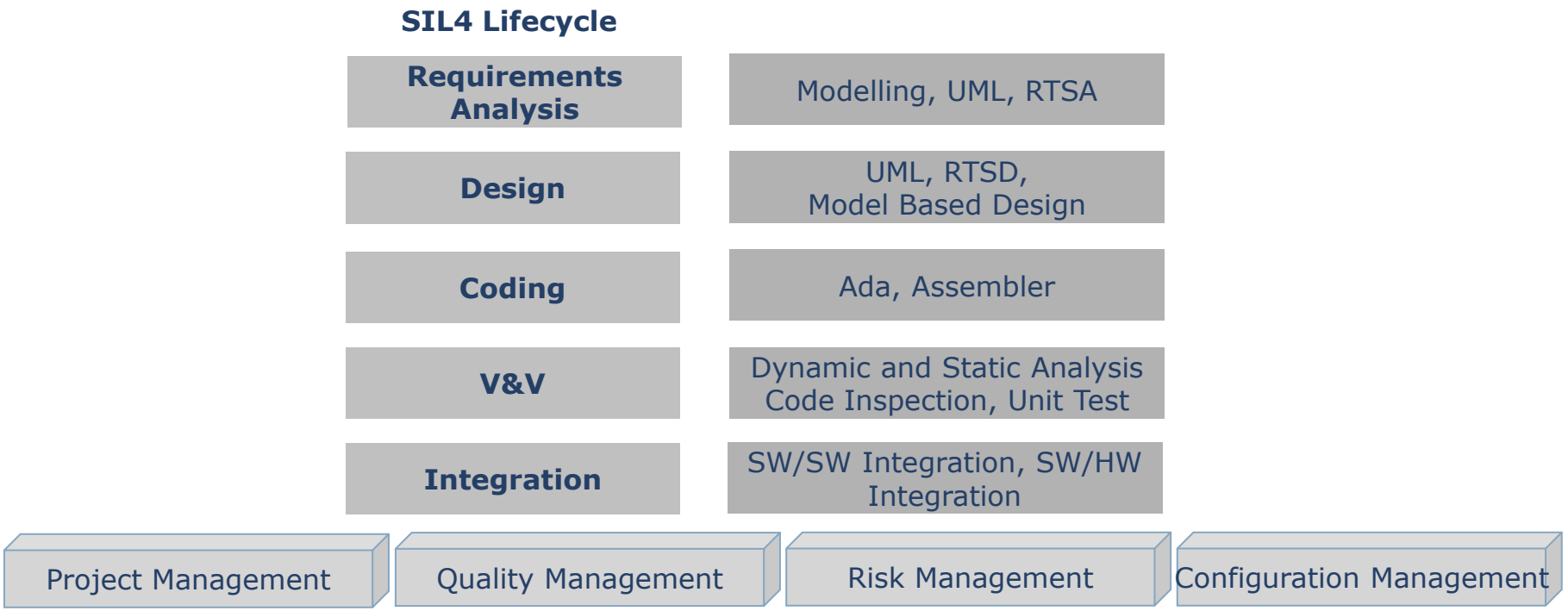
CENELC EN 50128

ISA recognized by Spanish Railway Authority

Radio Block Centre

V&V

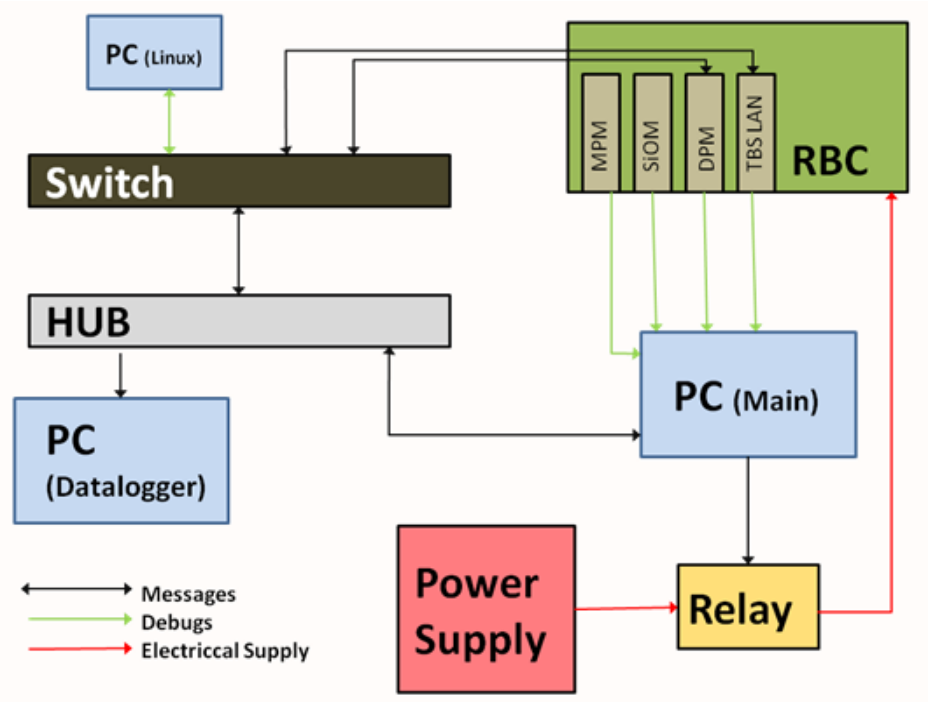
- Design, specification and implementation of the RBC V&V Program
- Functional testing, integration and performance testing



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



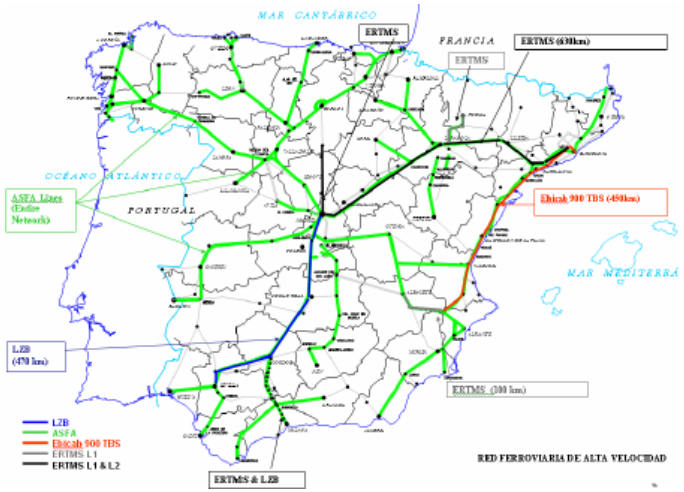
Contents

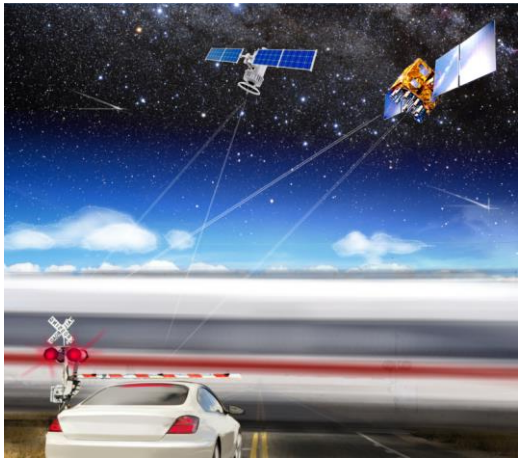
- Corporate Overview
- ERTMS - European Rail Traffic Management System
- RBC (Radio Block Centre)
- Conclusions and opportunities

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





Radio Block Centre

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

The Santiago de Compostela derailment on July 2013: Europe’s worst rail accident in recent history.

Thank you for your attention!

Ana Rodríguez - Aerospace Business Unit Manager

ana.rodriguez@silver-atena.es

Ronda de Poniente 5, 28760 Tres Cantos, Madrid

Telf. +34 608754488

Engineering | Product| Consulting
www.silver-atena.com
www.assystem.com