ERA conference
ERTMS Users Group
FA 12-11-2013

Part 1: New functions: GPRS & carrier independent solutions
Part 2: Key management & system security

Part 1: ETCS communications
Part 2: Secure ETCS communications
Part 1: ETCS communications

ETCS over GPRS

ERT: Euroradio Replacement Technology

Part 2: Secure ETCS communications

KMS Evolution

ERT: Euroradio Replacement Technology

12-11-2013
Part 1 / Best Possible Next Step

Best Possible Next Step = **ETCS over GPRS**

Best Possible Future Aim: **Euroradio Replacement Technology**
The activity aims at developing ETCS over GPRS specifications and demonstrating the suitability of a packet switching technology, such as GPRS, as a transmission system for ETCS. The ETCS over GPRS specifications will be developed with the aim to achieve a bearer independent system, and the interface description with the communication system in order to allow the data transmission over a packet switched technology, such as GPRS, while maintaining the current capabilities (transmission over a circuit switched technology – GSM-R).
## ETCS over GPRS – Status today

### Development >>>>>>>>>>>>

<table>
<thead>
<tr>
<th>Testing Phase 1</th>
<th>Testing Phase 2</th>
<th>Testing Phase 3</th>
<th>Testing Phase 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPRS LAB</td>
<td>GPRS FIELD</td>
<td>ETCS over GPRS FIELD</td>
<td>GPRS FIELD – Cross border</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ETCS over GPRS FIELD – Conventional speed</td>
<td></td>
</tr>
</tbody>
</table>

**TODAY**

EEIG ERTMS Users Group presentation at CCRCC
ETCS over GPRS - Development status today

11E017-1 ETCS over GPRS principles and functional requirements

ETCS
- Subset 026
- Subset 037
- Subset 092
- Subset 093

GPRS
- GPRS for ETCS Engineering Requirements
  - O-2475

FFIS for Euroradio

Project
ETCS over GPRS - testing status today: Phase 1 test report under preparation. Successful transition from Phase 1 to Phase 2

<table>
<thead>
<tr>
<th>Development</th>
<th>Testing Phase 1</th>
<th>Testing Phase 2</th>
<th>Testing Phase 3</th>
<th>Testing Phase 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPRS LAB</td>
<td>GPRS FIELD</td>
<td>ETCS over GPRS FIELD</td>
<td>ETCS over GPRS FIELD</td>
<td>ETCS over GPRS FIELD</td>
</tr>
<tr>
<td>Conventional speed</td>
<td>High speed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross border</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EEIG ERTMS Users Group presentation at CCRCC

12-11-2013

TODAY
ETCS over GPRS brings no principal changes
ETCS over GPRS brings no principal changes
Think of the DNS as a simple look-up table

<table>
<thead>
<tr>
<th>ETCS ID of RBC’s connected to that network</th>
<th>Corresponding IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>255.255.255.001</td>
</tr>
<tr>
<td>102</td>
<td>255.255.255.002</td>
</tr>
<tr>
<td>103</td>
<td>255.255.255.003</td>
</tr>
<tr>
<td>104</td>
<td>255.255.255.004</td>
</tr>
<tr>
<td>105</td>
<td>255.255.255.005</td>
</tr>
<tr>
<td>106</td>
<td>255.255.255.006</td>
</tr>
<tr>
<td>.................</td>
<td>255.255.255........</td>
</tr>
</tbody>
</table>
ETCS over GPRS brings no principal changes
ETCS over GPRS brings no principal changes
ETCS over GPRS brings no principal changes

Maximum time allowed for Service Registration

Maximum time allowed for establishing ETCS Session

Balise sending the order to do Service Registration

Balise sending the order to establish ETCS Session

RESULT

RESULT

RESULT

RESULT
Best Possible Next Step (2015): ETCS over GPRS
Part 1 / Best Possible Next Step

Best Possible Next Step = ETCS over GPRS

Best Possible Future Aim:
ETCS over any radio bearer
Part 1 / Best Possible Future Aim

Best Possible Next Step =
ETCS over GPRS

Best Possible Future Aim:
Euroradio Replacement Technology
Best Possible Future Aim (2022)
Future ETCS communications - utopian scenario
Attractive future concept
Attractive future concept
The technology independence achieved with a mobile communications router could lead to more freedom and opportunities in future network ownership business models.
Onboard technology overview. Euroradio Replacement Technology (ERT) means that:
Universal IP family technology completely replaces Euroradio.
End of Part 1

Questions?
Part 1: ETCS communications

Part 2: Secure ETCS communications
Best Possible Next Step = KMS Evolution

Best Possible Future Aim = Euroradio Replacement Technology
Background of the KMS Evolution activity

MAP2012: Facilitating and speeding up ERTMS deployment - 2nd phase / Activity 8 Key Management systems

<table>
<thead>
<tr>
<th>Sub Activity 8.1: KMS security analysis and recommendations</th>
<th>Sub Activity 8.2: KMS Evolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The work has resulted in a report that covers not only KMS security but also ERTMS security in general</td>
<td>KMS Evolution Strategy</td>
</tr>
<tr>
<td></td>
<td>KMS Evolution FRS+ORS</td>
</tr>
<tr>
<td></td>
<td>KMS Evolution SRS</td>
</tr>
</tbody>
</table>

To download the public report, go to: ertms.be
ETCS security report

• Management Summary of
  – Results
  – Overview of Threat Identification, Risk Analysis and Recommendations

• Threat Identification Reference Case

• Appendices, e.g.:
  – Hacker terminology/Cybercrime
  – Introduction to symmetric encryption technologies
ETCS Security Reference Case

Scope for the Reference Case

- GSM-R circuit switched transmission system including Euroradio
- ERTMS Application Level 2 relevant components including track side and onboard equipment
- The offline KMS used for the European Train Control System

Scope for Variations

- GSM-R packet switched (GPRS) transmission system including Euroradio
- ERTMS Application Level 3
- Variations in implementation choices but conforming to the ERTMS standards
ETCS Security Recommendations

• Governance
  – Policies, procedures, guidelines and roles on secure life cycle management of all ERTMS related equipment
  – Minimize manual handling of cryptographic material
  – Apply transition from a safety mindset to a safety and security mindset

• People
  – ERTMS security awareness training

• Process
  – Incident response procedures
  – Access control, system monitoring, system verification
  – Business Continuity and Disaster Recovery

• Technology
  – System hardening
    • Correct system patching
    • Remove not need functionality
    • Disable unnecessary services
    • Limit user rights to what they need
    • Antivirus protection
Background of the KMS Evolution activity

Security recommendations directly related to KMS Evolution

- Governance
- Technology
- People
- Process
Best Possible Future Aim = Euroradio Replacement Technology

Best Possible Next Step = KMS Evolution
Best possible next step - 2015

Universal IP family security infrastructure

OKMS

GSM-R CSD

GPRS / EDGE

ETCS

DNS
Best possible future aim - 2022

Universal IP family security infrastructure

ETCS

GPRS / EDGE

LTE

TETRA

Wi-Fi

XYZ
Onboard technology overview. Euroradio Replacement Technology (ERT) means that: Universal IP family technology completely replaces Euroradio.
Part 1: ETCS communications

ETCS over GPRS

ERT: Euroradio Replacement Technology

Part 2: Secure ETCS communications

KMS Evolution

ERT: Euroradio Replacement Technology
End of Part 2
Questions?
Thank you for your attention