# ALARP - A railway automatic track warning system based on distributed personal mobile terminals

**Andrea Bondavalli**

**Resilient Computing Lab**
**Dipartimento di Sistemi e Informatica**
**Università degli Studi di Firenze**

**61° IFIP WG 10.4 Meeting**
**Martinique France, January 26-30, 2012**

# Outline

- ALARP project motivations, facts and objectives
- The ALARP system
  - The MT (design and ongoing prototyping)
  - The TPAD (design and ongoing prototyping)
  - The communication solution
- Validation of the ALARP solution
- Conclusions

# Motivations

## Rail maintenance worker killed by train

Updated April 13, 2010 8:16:00

**A man has died after being hit by a train while carrying out maintenance work on the tracks in Sydney's south.**

The man was one of four people carrying out track maintenance at Kogarah when a train approached at about 1:00am (AEST).

ABCnews

## BNSF Railroad Worker Killed in Amarillo, TX Rail Yard Accident

By felalawyer on January 12, 2012 | From gordon-elias.com

AMARILLO, TX – A BNSF railroad worker was killed on Monday, January 9, 2012 in an Amarillo rail yard while moving a piece of railroad maintenance equipment.

zimbio.com

## 3 rail engineers killed during test run

Three rail engineers of Alstom were killed yesterday after being struck by a train at Bar-le-Duc during the test run of a Regiolis train. Alstom has taken a 15-year lease from Reseau Ferre de France of an 8-mile stretch of track between Loxeville and Willeroncourt in the Meuse for the purpose of test runs. Around 20 engineers were involved in the test, apart from the fatalities another 5 were injured. 2nd December 2011

safetynews.co.uk

wikipedia

## Tebay rail accident

From Wikipedia, the free encyclopedia

*This article is about the engineering accident. For the passenger train accide*

The **Tebay rail accident** occurred when four railway workers working on the West Coast Main Line were killed by a runaway wagon near Tebay, Cumbria, England in the early hours of 15 February 2004.

## Safety of workers in the railway scenario is a serious concern

- trackside workers are exposed to injuries and fatalities since vehicles are constrained to tracks and drivers have little margins to react
- For example: in U.S. railways during 1993-2002 there were 460 fatal railroad-related work injuries within railroading workers and 761 fatal railroad-related work injuries involving workers not from the railroad field
  - Druidi, D., "Railroad-related work injury fatalities," Monthly Labor

# Current solutions for track warning

Traditional Lookout

Autoprowa

# The ALARP project

**A railway automatic track warning system based on distributed personal mobile terminals**

**http://www.alarp.eu/**

**RTD project funded within the EU FP7 Transport programme**

- **call FP7-SST-2008-RTD-1**
- **EU Grant no. 234088**
- **EU contribution of € 2,626,610**

**Started on January 1st 2010 and now entered its final year**

**7 partners: 2 SMEs, 2 large companies, 3 research partners**

AnsaldoSTS Finmeccanica Company — Italy

ResilTech Technologies for Resilience

PROR — UK

ftw Creating Communication Technologies — Austria

TECHNISCHE UNIVERSITÄT DARMSTADT — Germany

Elbit Systems — Israel

# Objectives

**Recall the attention of a workgroup operating on a railway worksite about the presence of a train approaching**

- **design, develop and validate an innovative Automatic Track Warning System (ATWS) to improve the safety of railway trackside workers.**

**The ALARP ATWS aims to:**

- **Inform the trackside workers about approaching trains, emergencies on tracks and tunnels nearby the workers (e.g. fires, toxic smoke), escape routes,**
- **Keep track of the status and localisation of the workers and of the operating conditions of devices**

# Key ALARP requirements

**ALARP worksite is structured in two different zone**

- **Red (Risk) zone** is an area not protected from rolling stock movements (working limit of a red zone are defined according to the different national regulations)
- **Green (Safe) zone** is the safe area outside of the limits of the Red Zone

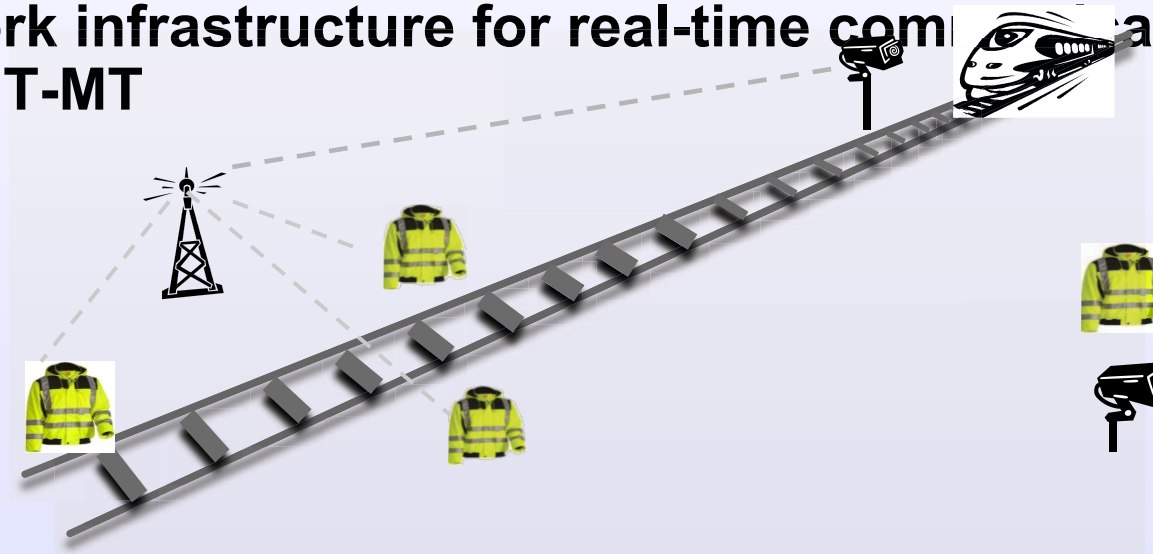
**ALARP is meant to be a SIL 2 ($10^{-7} \leq THR \leq 10^{-6}$) system designed to protect working gangs providing:**

- **ALERT** when workers are at risk (e.g., train approaching and worker in red zone), allowing them to reach a safe position (with notice time according to the different national regulations)
  - Also used when workers are not responding (injuries or health problems)
- **WARNING** signals are sent only to raise their attention

# The ALARP SIL 2 system

## Key components:

- one or more track-side Train Presence Alert Devices (TPADs), able to sense an approaching train on the interested track without interfering with the signaling system . Distance from working side depending on expected max speed (could be up to 5 Km.)
- a set of distributed, Mobile Terminals (MTs) (low-cost, wearable, context-aware, trustable and highly reliable, wireless, COTS) to inform the workers about approaching trains and/or other events that could harm their safety
- network infrastructure for real-time com ation of TPAD-MT and MT-MT

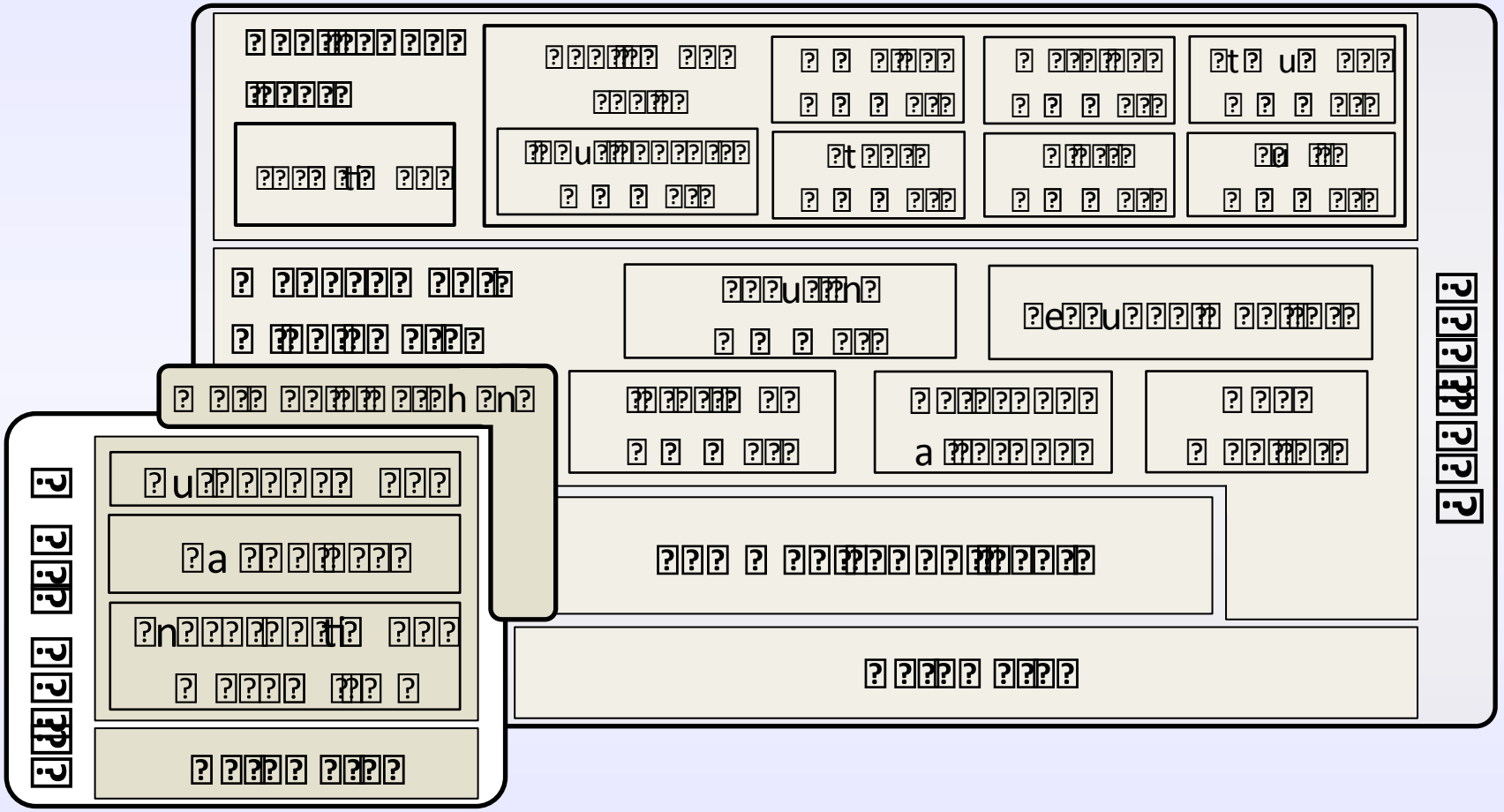


# The Mobile Terminal (MT)

**Based on the hybrid distributed system model, the MT is organized in two subsystems with different sets of requirements in terms of security and timeliness.**

- **The first (wormhole) contains simple but critical middleware services; it executes on a very basic hardware, that ease monitoring and assessing its behaviour.**
  - **Contains time-related services (resilient clock, synchronization protocols), ciphering and authentication services**
- **The second (payload) executes on a different hardware than the first; it requires localization , networking and I/O devices to interact with the workers, the TPADs and the MTs**

# Architecture of the MT



# The MT prototype

- A prototype construction is underway
- First prototype with MT composed of two small pcs for (WH and PL) linked together, basic localization and no special devices
- Final prototype (one year from now) using virtual machines on Asymmetric Multiprocessing and an OTS multicore processor, more sophisticated localization and ergonomic devices

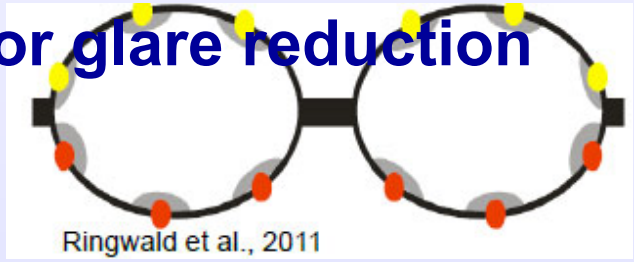
# Ergonomics -Warning/alerting signals

bone conductor (www.bhm-tech.at)


safety glasses

- Electrical signals are transformed into mechanical vibrations, which are transmitted by bone conduction to the inner ear
- Communication can be maintained in a very noisy environment while using ear protection

- 6 blinking LEDs (3 red; 3 yellow)
- LED Position on the upper and lower end of the visual range
- Diffuse and adaptive light for glare reduction



# The TPAD

**TPAD is composed by the following main blocks:**

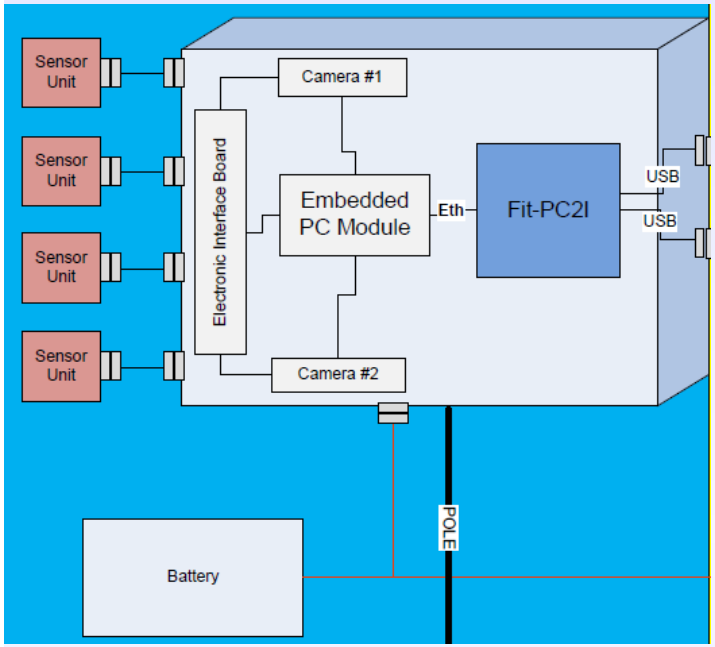
- **Block I (Low power) triggers the TPAD from a *ready state* to *full functionalities*, due to a train detection. The triggering is performed by a sub-block which consists of geophone and an accelerometer sensors.**
- **Block II (High power) consists of additional sensors (both geophone and accelerometer) and cameras. This block is activated by Block I and works in higher power consumption levels.**

**Block I is "extra sensitive" (using very high gain detectors circuits) enabling a very high probability of detection (POD), but also a high False Alarm Rate (FAR).**

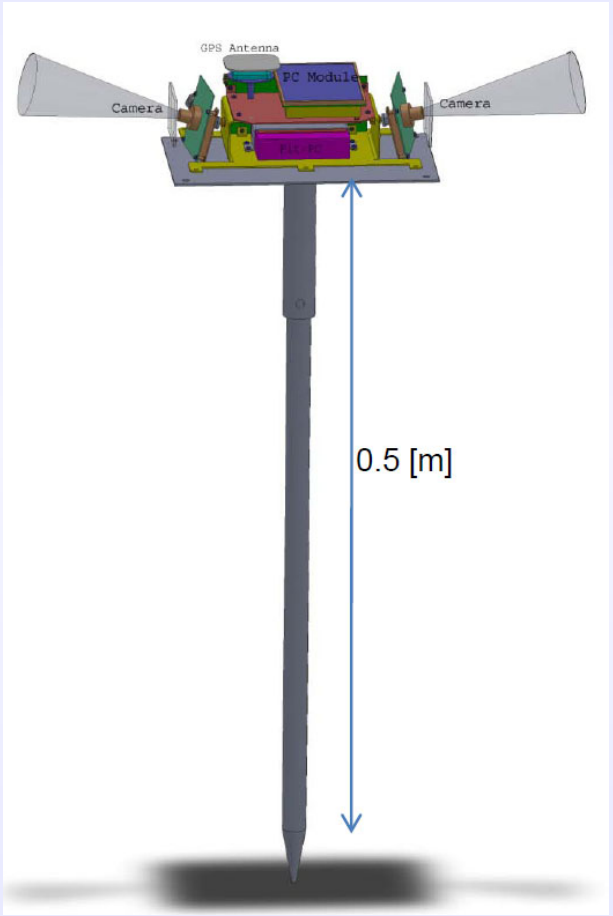
**Block II has mid to high POD and a low to none FAR.**

**On the whole, the combination of both blocks shall result in a very high POD and a very low FAR.**

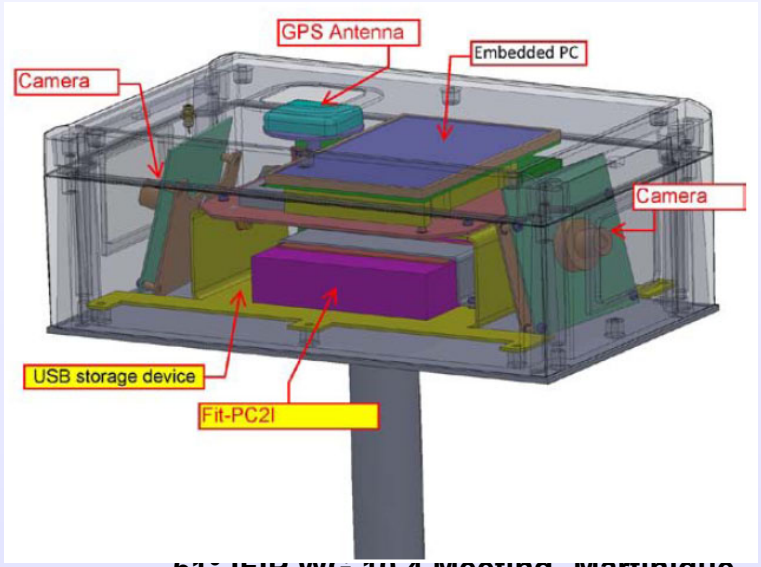
# TPAD block diagram and prototype




Interface towards TPAD external comm module



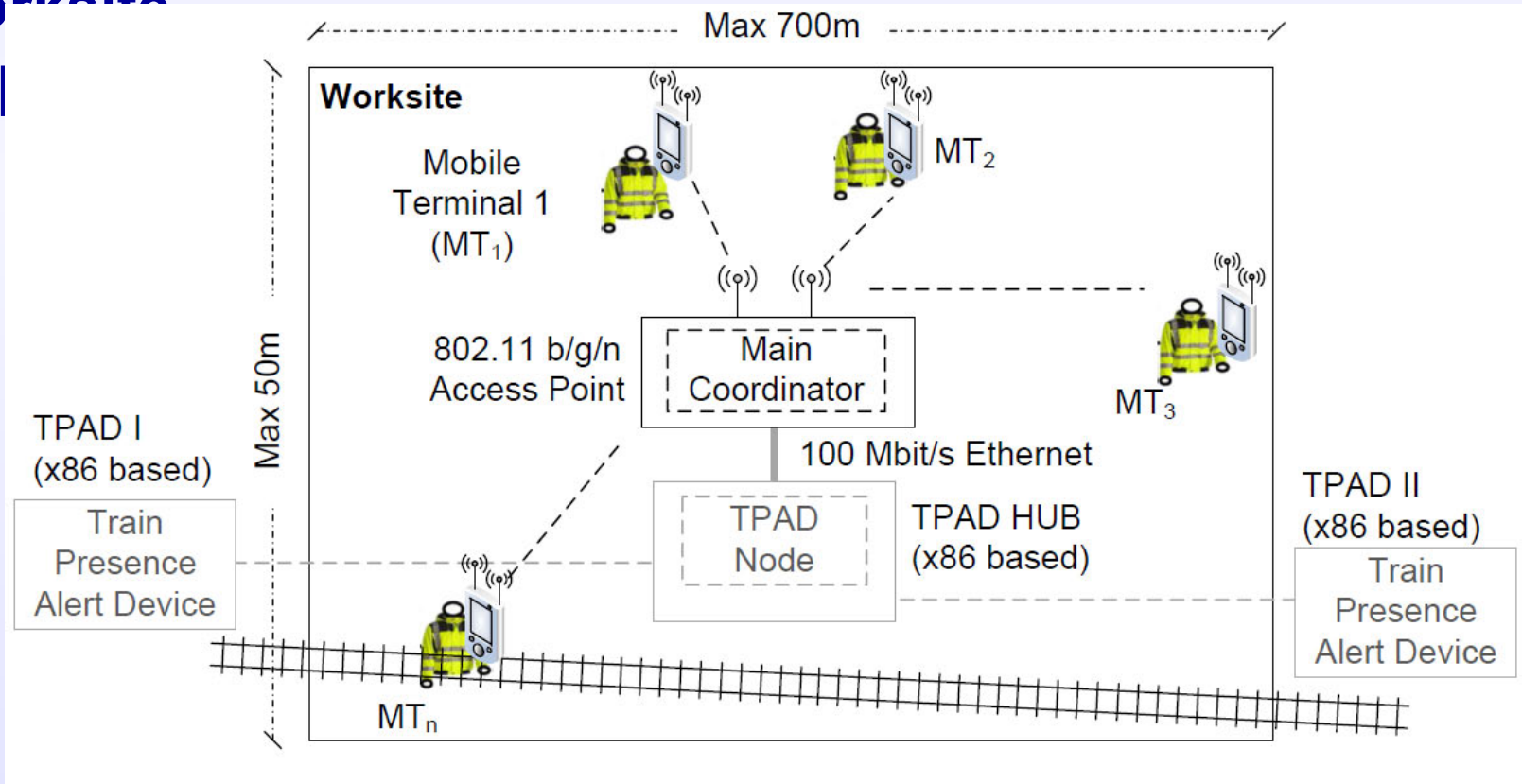

Dimension: 330x200x120 mm
Weight: < 5 KG



# Communications

## Real-time wireless communication.

- long range between TPADS and a TPAD HUB located in the worksite
- IEEE 802.11 (MTs and an Access Point) within the worksite
- Both



# Real-time communication in the worksite

## The Real-time Group Communication Protocol basis for the worksite communication protocol between MTs and TPAD HUB)

- Relying on IEEE 802.11 PCF "Contention Free Period", a coordinator (Access Point) polls node s in a round-based style.
- An omission degree is assumed for consecutive losses (to trigger a transition to safe state)
- A resiliency degree value allows specifying the maximum number of retransmissions of each message, at the price of

E. Nett and S. Schemmer, "Reliable real-time communication in cooperative mobile applications," IEEE Trans. Computers, vol. 52, no. 2, pp. 166-180, 2003.

## Modifications were introduced to fit the ALARP requirements

-no need to guarantee agreement and ordering

-solutions for multicast and unicast are introduced

-Three different resiliency degrees to match three different

# ALARP Verification and Validation

**The ALARP system installation s will need to be certified according to the railway EN50126/ IEC 50128/50129 reference standards.**

**The project has thus considered certifiability as the main assessment objective.**

**A Verification and Validation Plan (V&V Plan), has been defined for a complete future ALARP product**

**In addition the subset of V&V activities doable within the project lifetime have been identified and are being performed**

# ALARP V&V activities performed in the research project

- **Risk Analysis (RA):**
  - **Hazard Identification, Hazard Analysis & Identification of necessary countermeasures**
- **Quantitative modelling of ALARP solutions and components (e.g comm protocols, architectural choices)**
  - **In particular with respect to THR objectives for SIL2**
- **Software Testing, Quality and Rule Check (MISRA C++)**
- **Requirements Traceability at different levels**
- **Testing on Prototypes (single components and full prototype)**

# Conclusions

The ALARP project aims to improve safety of railway trackside worker by devising a SIL 2 real-time ATWS

- Architecture Composed of one or more TPADs, a set of MTs and communication infrastructure to provide TPAD-MT and MT-MT communication
- MT design based on hybrid architecture, localization and ergonomic concerns.
- The project is currently in its last year, finalizing implementation of concept to get to a feasibility prototype and on-field demonstrations.
- Ongoing assessment and validation activities

**More at http://www.alarp.eu/**

# THANK YOU for your attention.

## Questions?