**Transport (including Aeronautics)**

Grant Agreement for: Collaborative Project (Small or medium-scale focused research project)

---

**Annex 1 - “Description of Work”**

<table>
<thead>
<tr>
<th>Project acronym:</th>
<th>ALARP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project full title:</td>
<td>A railway automatic track warning system based on distributed personal mobile terminals</td>
</tr>
<tr>
<td>Grant Agreement no.:</td>
<td>234088</td>
</tr>
<tr>
<td>Date of preparation of Annex I (latest version):</td>
<td>02/10/2009</td>
</tr>
<tr>
<td>Date of approval of Annex I by Commission:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Beneficiary no.</th>
<th>Beneficiary organisation name</th>
<th>Beneficiary Short name</th>
<th>Country</th>
<th>Date enter project</th>
<th>Date enter project</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ansaldo STS S.p.A.</td>
<td>ASTS</td>
<td>IT</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>2</td>
<td>Forschungszentrum Telekommunikation Wien</td>
<td>FTW</td>
<td>AT</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>3</td>
<td>Università degli Studi di Firenze</td>
<td>UNIFI</td>
<td>IT</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>4</td>
<td>ResilTech S.r.l.</td>
<td>RT</td>
<td>IT</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>5</td>
<td>Elbit Systems</td>
<td>ESL</td>
<td>IL</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>6</td>
<td>PROPRS Ltd.</td>
<td>PRO</td>
<td>UK</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>7</td>
<td>Darmstadt University of Technology - Institute for Ergonomics</td>
<td>IAD</td>
<td>DE</td>
<td>M1</td>
<td>M36</td>
</tr>
</tbody>
</table>
# Table of contents

Table of contents ............................................................................................................. 2  
Part A ................................................................................................................................... 5  
Part B ................................................................................................................................... 7  

B1  Concept and objectives, progress beyond state-of-the-art, S/T methodology and work plan 7  
  B1.1  Concept and project objective(s) ........................................................................... 7  
    B1.1.1  Safety of railway workers ............................................................................... 7  
    B1.1.2  The need for an Automatic Track Warning System (ATWS) ....................... 8  
    B1.1.3  Project objectives ......................................................................................... 9  
  B1.2  Progress beyond the state of the art ................................................................. 11  
    B1.2.1  Technical progress .................................................................................... 11  
      B1.2.1.1  Resilient wireless communications .................................................. 11  
      B1.2.1.2  Safe & resilient architectures............................................................ 12  
      B1.2.1.3  Modelling, verification, validation and evaluation ............................. 12  
    B1.2.2  Commercial Automatic Track Warning Systems (ATWS) ...................... 13  
  B1.3  S/T Methodology and associated work plan .................................................... 14  
    B1.3.1  Overall strategy and general description .................................................. 14  
      B1.3.1.1  System foundations ................................................................. 14  
      B1.3.1.2  Resilient wireless communication .................................................. 16  
      B1.3.1.3  Mobile Terminal (MT) .................................................................... 18  
      B1.3.1.4  Train presence alert device .............................................................. 20  
      B1.3.1.5  Integration and proof-of-concept ....................................................... 23  
      B1.3.1.6  Modelling, verification, validation and evaluation ............................. 24  
      B1.3.1.7  Risks appraisal and management ....................................................... 27  
    B1.3.2  Timing of work packages and their components ....................................... 28  
      B1.3.2.1  Structure of work-packages .............................................................. 28  
      B1.3.2.2  Timing of work packages and their components .............................. 32  
    B1.3.3  Work package list / overview ..................................................................... 33  
      B1.3.3.1  Work-package list ............................................................................ 33  
    B1.3.4  Deliverables list ......................................................................................... 34  
    B1.3.5  Work package descriptions ....................................................................... 36  
    B1.3.6  Efforts for the full duration of the project ............................................... 49  
      B1.3.6.1  Indicative efforts per beneficiary per WP ......................................... 49  
      B1.3.6.2  Indicative efforts per activity type per beneficiary ............................ 49  
    B1.3.7  List of milestones and planning of reviews .............................................. 50  
      B1.3.7.1  List of milestones ............................................................................. 50  
      B1.3.7.2  Planning of reviews ......................................................................... 51  

B2  Implementation ........................................................................................................... 52
B2.1 Management structure and procedures ................................................................. 52
  B2.1.1 Introduction ....................................................................................................... 52
  B2.1.2 The project management structure .................................................................. 52
  B2.1.3 Meetings ........................................................................................................... 53
  B2.1.4 Conflict resolution ......................................................................................... 53
  B2.1.5 Quality Assurance (QA) .................................................................................. 53
  B2.1.6 Communication Strategy .............................................................................. 53
  B2.1.7 Project risk management ................................................................................ 53
B2.2 Beneficiaries .......................................................................................................... 54
  B2.2.1 ANSALDO STS S.p.A. (ASTS) ......................................................................... 54
    B2.2.1.1 Brief description of the organization ....................................................... 54
    B2.2.1.2 Main task(s) in the project ..................................................................... 54
    B2.2.1.3 Short profile(s) of the staff members .................................................... 55
  B2.2.2 Forschungszentrum Telekommunikation Wien (FTW) ..................................... 55
    B2.2.2.1 Brief description of the organization ....................................................... 55
    B2.2.2.2 Main task(s) in the project ..................................................................... 56
    B2.2.2.3 Short profile(s) of the staff members .................................................... 56
  B2.2.3 Università degli Studi di Firenze (UNIFI) ......................................................... 57
    B2.2.3.1 Brief description of the organization ....................................................... 57
    B2.2.3.2 Main task(s) in the project ..................................................................... 57
    B2.2.3.3 Short profile(s) of the staff members .................................................... 57
  B2.2.4 ResilTech S.r.l. (RT) ........................................................................................ 58
    B2.2.4.1 Brief description of the organization ....................................................... 58
    B2.2.4.2 Main task(s) in the project ..................................................................... 58
    B2.2.4.3 Short profile(s) of the staff members .................................................... 59
  B2.2.5 ELBIT Systems Ltd. (ESL) .............................................................................. 59
    B2.2.5.1 Brief description of the organization ....................................................... 59
    B2.2.5.2 Main task(s) in the project ..................................................................... 59
    B2.2.5.3 Short profile(s) of the staff members .................................................... 60
  B2.2.6 PROPRS Ltd. (PROPRS) ................................................................................. 60
    B2.2.6.1 Brief description of the organization ....................................................... 60
    B2.2.6.2 Main task(s) in the project ..................................................................... 60
    B2.2.6.3 Short profile(s) of the staff members .................................................... 61
  B2.2.7 Institute of Ergonomics at Darmstadt University of Technology (IAD) ............ 61
    B2.2.7.1 Brief description of the organization ....................................................... 61
    B2.2.7.2 Main task(s) in the project ..................................................................... 62
    B2.2.7.3 Short profile(s) of the staff members .................................................... 62
B2.3 Consortium as a whole .......................................................................................... 63
  B2.3.1 Consortium complementarity ......................................................................... 63
B2.3.2 Industrial/commercial involvement............................................................................ 63
B2.3.3 SMEs involvement ................................................................................................ 64
B2.3.4 Sub-contracting ................................................................................................... 64
B2.3.5 Other countries.................................................................................................... 64
B2.3.6 Additional partners ............................................................................................. 64
B2.4 Resources to be committed .................................................................................... 65

B3 Impact............................................................................................................................ 69

B3.1 Strategic impact......................................................................................................... 69
B3.1.1 Impacts listed in the work programme ................................................................ 69
B3.1.2 RIMINI Standard .................................................................................................. 70
B3.1.3 Interactions with the European Railway Agency (ERA) ........................................ 70
B3.1.4 Market opportunities for European industry ....................................................... 70

B3.2 Plan for the use and dissemination of foreground ................................................. 71
B3.2.1 Dissemination of project results........................................................................... 71
B3.2.1.1 Dissemination to the public ........................................................................... 71
B3.2.1.2 Dissemination among the Consortium and to the scientific community .......... 71
B3.2.1.3 Dissemination to stakeholders and the Stakeholder Group ............................ 71
B3.2.1.4 Communication Matrix.................................................................................. 72
B3.2.2 Knowledge Management, IPR and exploitation ................................................ 72
B3.2.2.1 Knowledge management............................................................................... 72
B3.2.2.2 Intellectual Property Rights (IPR) management........................................... 72
B3.2.2.3 Exploitation strategy..................................................................................... 73

B4 Ethical issues.................................................................................................................. 76
B4.1 Privacy of workers .................................................................................................... 76
B4.2 Dual use ..................................................................................................................... 77

B5 References.................................................................................................................... 78
<table>
<thead>
<tr>
<th>Beneficiary no.</th>
<th>Beneficiary organisation name</th>
<th>Beneficiary Short name</th>
<th>Country</th>
<th>Date enter project</th>
<th>Date enter project</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ansaldo STS S.p.A.</td>
<td>ASTS</td>
<td>IT</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>2</td>
<td>Forschungszentrum Telekommunikation Wien</td>
<td>FTW</td>
<td>AT</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>3</td>
<td>Università degli Studi di Firenze</td>
<td>UNIFI</td>
<td>IT</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>4</td>
<td>ResilTech S.r.l.</td>
<td>RT</td>
<td>IT</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>5</td>
<td>Elbit Systems</td>
<td>ESL</td>
<td>IL</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>6</td>
<td>PROPRS Ltd.</td>
<td>PRO</td>
<td>UK</td>
<td>M1</td>
<td>M36</td>
</tr>
<tr>
<td>7</td>
<td>Darmstadt University of Technology - Institute for Ergonomics</td>
<td>IAD</td>
<td>DE</td>
<td>M1</td>
<td>M36</td>
</tr>
</tbody>
</table>

Table 3 - List of Beneficiaries
Part B

B1 CONCEPT AND OBJECTIVES, PROGRESS BEYOND STATE-OF-THE-ART, S/T METHODOLOGY AND WORK PLAN

B1.1 CONCEPT AND PROJECT OBJECTIVE(S)

B1.1.1 Safety of railway workers

Safety of workers is a serious concern of the most industrialised countries. Surface transport workers are facing very high risks since they often operate without service interruptions. In railway situation is even more peculiar, since vehicles are constrained to tracks and therefore drivers have much less margins to react in case of emergencies and therefore workers are much more exposed to injuries and fatalities.

This vision is supported by many independent analyses and published reports, e.g.:

- **UIC Safety Database Activity Report 2007 key findings:**
  - Most staff fatalities and serious injuries continue to be as a result of being hit by a train;
  - Most staff member deaths occurred in open line accidents, whereas most serious injuries to staff members were incurred in accidents in stations.

- **Risk to the workforce from The Railway Strategic Safety Plan 2005 and 2006 of the UK Rail Safety and Standards Board (RSSB):**
  - It is a matter of very serious concern that railway trackside work has one of the highest fatality rates for all employment sectors in the UK, notably comparing unfavourably with the construction industry.
  - In the past decade, risk to the railway workforce has been reduced, but incidents such as the accident at Tebay in 2004, in which a runaway vehicle killed four workers, show that track workers continue to face significant risk within their work.
  - The industry is committed to improvement in this area and to the reduction of risk to track workers through better planning and the development and adoption of good working practices.
  - Workers who are required to go on or about the track from time to time are exposed to the possibility of being struck by trains, including on-track plant, as well as hazards such as live rails. All hazards are heightened at night when visibility is reduced. Track workers – whose primary role involves maintenance and renewal of the infrastructure – are most exposed.

- **Workforce safety performance report (Nov. 2006) of the UK Rail Safety and Standards Board (RSSB):**
  - Track workers are the most exposed group (34.8%) to fatal risk.
  - Track workers, including infrastructure inspection, maintenance and upgrade occupations, account for over half the fatalities (57%).
  - Track worker is perceived as being working in the most hazardous environment when compared with train crew and other workforce.
  - The main activity leading to workforce major injuries is track maintenance.
  - The hazardous events exhibiting the greatest level of fatality risk to track workers are “Track worker struck/crush by train” and “Worker electric shock”.

In synthesis, the above independent studies demonstrate that:

- most railway staff fatalities and serious injuries are the result of being hit by a train or by an electric shock;
- trackside work has one of the highest fatality rates in the railway sectors;
there is a clear need for a trusted and dependable device informing railway workers in a personalized, timely, and reliable manner about events that may temporarily increase their risks while working trackside.

Even recently accidents to railway workers happened around the world:

- on 9th January 2008 a man working for the Union Pacific railroad was struck and killed by a commuter train at the Waukegan (USA) Metra station while he was throwing a switch to let a northbound Metra train pass;
- on 25th January 2008 a high-speed train ran into a railroad work site in the Shandong Province of Eastern China, killing 18 people and injuring another nine. Railroad workers were relocating tracks when a train slammed into their work site at 120 km/h (75 mph), according to the Xinhua news agency. The workers had entered the work area several hours ahead of schedule;
- on 11th February 2008 an NJ Transit employee died in Bergen County, N.J. (USA), after a Suffern-bound train struck him while he was working on the tracks near where he was struck;
- on 6th March 2008 a 50-year-old worker, in charge of an enterprise working for the state railways has been hit and killed by a train travelling near the work site. The incident occurred over the night in Milan (Italy), on the city outskirts along the Turin-Milan railway, where a work site is open even at night.

More in general the UK RSSB has estimated that, considering UK only, the track workers category counts more than 25 Fatalities and Weighted Injuries (FWI) per year.

Workers injuries and/or fatalities may also have an obvious secondary side-effect on quality of service of the railway concerned due to the line interruption.

B1.1.2 The need for an Automatic Track Warning System (ATWS)

This text is extracted from the UK Office of Rail Regulation (ORR) web site:

"The maintenance and renewal of the railway infrastructure takes place daily. This work must often be carried out close to or on the running track known as 'the line'. Some work can be done by machine but often people also have to be involved and this can present the considerable risk of being struck by trains. It is the responsibility of Network Rail and its contractors to plan ahead and manage renewal and maintenance work to minimise safety risks and disruption.

The safest way of undertaking maintenance and renewal work is to separate workers from trains. On Network Rail controlled infrastructure, this is known as 'green zone working' and involves blocking one or more lines to trains and/or setting up protected areas away from running lines.

It is not always possible to block lines to traffic and some work known as 'red zone working' on lines where trains are running takes place. This involves warning workers of approaching trains in time to get clear of the line and into a 'position of safety' well before the train arrives. This type of working requires very strict safety systems to be in place."

There are clear recommendations (no. 9 and 10) from ORR:

- Railtrack should require the use of automatic track warning systems for large scale works and those of significant duration, unless it is not reasonably practicable to do so. Such decisions should be clearly documented in the project safety plan.
- HMRI should implement a strategy to encourage the increased use of automatic track warning systems at such locations, both through liaison with Railtrack Headquarters and Zones, and

1 The term FWI is a measure that combines fatalities and injuries. With this measure, 200 minor injuries and 10 major injuries are each considered to be equal to one fatality.

2 UK Office of Rail Regulation http://www.rail-reg.gov.uk/

3 Red/green zone working - A report on maximisation of green zone working on Railtrack infrastructure.

4 HMRI (Her Majesty's Railway Inspectorate) is the British organisation responsible for overseeing safety on Britain's railway
when considering the robustness of safety plans associated with CDM\textsuperscript{5} Regulations. Formal enforcement should be taken where justified.

This has led to the RIMINI (risk minimisation) standard that contains a hierarchy of protection methods, with green zone working as the first choice, followed by red zone working with an automatic means of warning, and finally red zone working with human lookouts as a last resort.

Some existing ATWS (see more details in section B1.2.2) have been tested in recent years but the following intrinsic problems have hindered a widespread use of these devices:

- they are expensive;
- systems are complex to install and use;
- they rely on existing signalling systems and therefore not usable in scarce traffic lines without signalling;
- training is time consuming and complex.

B1.1.3 Project objectives

The objective of the ALARP project is therefore to study, design and develop an innovative more efficient Automatic Track Warning System (ATWS) to improve the safety of railway trackside workers.

ALARP ATWS will be able to:

- selectively inform the trackside workers about:
  - approaching trains on the track,
  - maintenance events on power lines and/or safety equipment in the concerned tracks that may put at risk workers’ safety (e.g. being hit by a train or by an electric shock),
  - emergencies on tracks and tunnels nearby the workers (e.g. fires in a tunnel, toxic smoke, etc.),
  - escape routes in case of emergencies;
- keep track of the status and localisation of the workers (and especially those at risk, not responding) and of the operating conditions of devices.

The proposed ALARP concept (see an example of a possible configuration in Figure 1) will be based on the following main components:

- the track-side train presence alert device (TPAD), able to sense an approaching train on the interested track without interfering with the signalling system;
- a set of distributed, low-cost, wearable, context-aware, robust, trustable and highly reliable, wireless Mobile Terminals (MTs) to inform the workers about possible approaching trains and/or other events that could put at risk their safety.

The proposed Train Presence Alert Device (TPAD) will have the following characteristics:

- able to detect a train approaching the “red zone” without interfering at all with existing signalling systems (and therefore able to sense the approaching train also in case of low density traffic lines without signalling systems\textsuperscript{6});
- based on a multi-spectral camera to detect approaching trains in all lighting and weather conditions;

\textsuperscript{5} Construction Design and Management

\textsuperscript{6} e.g. in Spain out of the 12.140 km of the conventional system, 5.510 km are single-track without signalling, out of which 4.763 km are managed by means of block signalling by telephone (2006)
The proposed Mobile Terminal (MT) will have the following main characteristics:

- **low-cost, self-powered and portable and easily movable** in different places of work;
- equipped with an **anti-theft system**.

### 1. Mobile Terminal Characteristics

- able to generate **alarm perceivable in harsh conditions** (e.g. high noise, low light, etc.);
- of **small size** to be wearable without interfering with the worker’s job (e.g. embedded in the helmet), with **ergonomic design** and **interface** easy for different users;
- **able to communicate and interact** through **wireless** connections with other MTs and the track-side train presence alert devices together with mechanisms to check validity and trust-levels for this ad-hoc communication;
- able to **localise itself** on the railway fusing information from GPS/EGNOSS\(^7\) and/or the wireless network(s) and/or Inertial Measurement Units (IMUs) and the railway map;
- able to **eavesdrop on wireless signalling communication** links (e.g. ERTMS) to obtain information on approaching trains or other local emergencies;
- it will have the possibility to use **multi-lingual and/or mimics** interface to be used in **interoperable cross-border services**;
- able to **identify the direction of the movement of the worker** in case of emergencies to verify if he is using the correct escape routes and possibly suggest alternatives if these are compromised (e.g. in case of smoke in a tunnel);
- able to be **coupled with a specific worker** through biometric sensors to avoid possible misuses of the device by the worker (e.g. abandoning it close to trackside);
- **robust, highly-reliable and available** to be **trusted** by the workers;
- able to assume the **leader functionality** in order to manage trackside workers teams both in normal work and emergencies.
- **low-cost** and based on **COTS\(^8\)** to be adopted in large scale and **sustainable** in low and medium scale.

---

\(^7\) EGNOSS: European Geo-stationary Navigation Overlay System

\(^8\) COTS: Components-Off-The-Shelf
B1.2  PROGRESS BEYOND THE STATE OF THE ART

B1.2.1  Technical progress

B1.2.1.1  RESILIENT WIRELESS COMMUNICATIONS

ALARP resilient wireless communication infrastructure will be based on (i) of-the-shelf wireless access technologies, with candidate solutions including WLAN 802.11 like, Bluetooth, WIMAX, and cellular (GPRS/UMTS), and (ii) standard protocols for multi-hop forwarding in ad hoc networks (including broadcast, unicast, geo-cast). These solutions will be used to develop the topology and group management solution for guaranteed delivery of safety-critical alerts.

Accordingly, research challenges include

- redundant use of, and handoff between, different access technologies
- adaptive use of ad hoc routing protocols for guaranteed dissemination in the alert regime, and for minimized overhead in the stand-by regime given the required level of resilience
- managing sufficient context information for appropriate context-aware end-user alerting

Vertical handoff between different access technologies is of a particular current research interest as it combines the benefits offered by cellular (GPRS/UMTS) technologies supporting always on connectivity, with the high bandwidth/cost ratio that WLAN technology can offer within limited areas [1]. Handoff decision can be made based on a combination of parameters, including bandwidth, reliability, latency, and cost. Particularly context-aware services, such as the ALARP alerting, require roaming based on multiple parameters including user preferences. For multi-parameter decision making, different approaches are proposed including pattern recognition algorithms and fuzzy logic ([2], [3]). The ALARP project will investigate multi-criteria decision methods for establishing pro-active or reactive redundancy over different access technology. The benefit of redundancy in the topology will be investigated in a trade-off with reduced battery life-times due to higher energy consumption.

A broad variety of existing ad-hoc protocols for multi-hop forwarding (broadcast, geo-cast and unicast), can be considered as candidates for reliable dissemination in ALARP.

(i) Broadcast and geo-cast mechanisms are particularly suitable when certain messages have to be disseminated to all devices within a specific geographic area. However, a simple flooding approach is not appropriate because of a broadcast storm problem [4], and the lack of guaranteed reliability. Most existing work addressing the reliability aspect of broadcast in multi-hop wireless networks focuses on providing higher (but not-guaranteed) message coverage by, e.g., introducing redundancy into the procedure, so that a node can tolerate at least one failure in reception ([6], [7]). Broadcast reliability may be also achieved by means of acknowledgments [5]. Geo-cast, as a special case of broadcast, is particularly efficient because nodes forward packets based on the local geographic position of neighbouring nodes [8]. Particularly relevant for ALARP scenario is an approach where geo-cast approach is used for low-cost geographic neighbourhood discovery [9], and where a geo-aware group management supports reliable communication [10].

(ii) The use-case for a specific unicast routing protocol critically depends on the mobility patterns, available communication resources, and type and requirements of the application traffic. They differ in the approach to route and neighbourhood discovery/maintenance which is central to building a local topology view, and a group management. While, the proactive protocols such as OLSR [11] regularly perform network wide update of the link-state information, the reactive protocols (e.g., AODV [12]) support route discovery upon the existing traffic request. The hybrid protocols (e.g., ZRP) support complete update of the routes within the k-hop neighbourhood, and discovery outside it, and can be optimally configured for a particular scenario [13].
The ALARP project does not intend to develop new ad-hoc routing protocols, but a careful selection and parameter configuration of the existing candidates will be performed. Regarding the security of communication the similar approach will be adopted: the appropriate existing key management schemes and security protocols will be selected and the suitable configurations for their operation will be determined.

**Context-aware** communication has attracted considerable attention in the research community. It exploits the capability of sensor-enabled systems to assess context parameters, e.g., location information of the relevant devices, environment conditions, system self-diagnosis information, as well as high-level mission schedule. Solutions for management of general context information developed previously ([29], [30]), as well as general frameworks for context-sensitive networking, e.g., context management in Personal Networks [14], and the Ad-hoc Context Aware Network architecture (ACAN) [15], have to be extended to meet the safety requirements of the ALARP system. In ALARP, the relevant context information for the resilient topology and group management will need to be carefully designed, together with a cost-efficient approach to acquiring this information.

**B1.2.1.2 SAFE & RESILIENT ARCHITECTURES**

Achieving dependability and security despite accidental and malicious faults in networks composed by mobile nodes is particularly challenging due to their intrinsic asynchrony. Several factors imply the asynchrony in mobile systems based on wireless communication between them: the unreliability of the communication, the network partitioning, the changes in the network topology and the consequent absence of continuous connectivity to global resources. Furthermore, the threats to resilience and safety are particularly severe: device lifetime and communication are severely limited by scarcity of power; use of wireless links means susceptibility to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion; poor physical protection of mobile devices (especially in a hostile environment like the one considered in ALARP) makes them susceptible to physical damage, and vulnerable to theft or subversion.

The ALARP project will propose middleware solutions for enhancing resilience, availability and security in the wireless domain. The proposed solutions will accommodate a balanced harmonization among security/trustworthiness, availability/performance and reliability/safety aspects. The plan is to define the MT architecture using principles like architectural hybridisation, which allow to painlessly enhancing a given original architecture in its timeliness, security and in general quality of service. This approach was successfully used as basic paradigm for the definition of the system architecture in other EU projects, like CRUTIAL [16], HIDENETS [24] and MAFTIA [17].

The proposal of the MT safe and resilient architecture will enhance the state of the art since it will include new paradigms and architectural constructs to secure resilience properties in spite of uncertainty factors, and new algorithms suited for wireless domains providing availability and reliability, while maintaining high performance and security levels. In particular, aspects like uncertainty in the positioning of the MT (mobile devices) in space and in time will be a part in which ALARP project will significantly advance the state of the art, proposing new mechanisms and algorithms exploiting this information at the middleware and application level.

**B1.2.1.3 MODELLING, VERIFICATION, VALIDATION AND EVALUATION**

State-space models are commonly used for dependability modelling of computing systems, since they are able to capture various functional and stochastic dependencies among components and allow evaluation of various measures related to dependability and performance (performability) based on the same model. The main problem raised by the establishment of a state-based model being truly representative of the behaviour of a complex system is that of controlling the explosion in the number of states (state space explosion problem). Significant progress has been made in addressing the challenges raised by the large size of models both in the model construction and model solution phases, using a combination of techniques that can be categorized with respect to their purpose (largeness avoidance and largeness tolerance, see [18] for a comprehensive survey).
In ALARP we will advance the state-of-the-art developing modelling construction and solution techniques specifically tailored for the dependability assessment of dynamic, unreliable, evolvable, safety-critical systems, subject both to accidental and malicious threats. Quantitative evaluation techniques have been mainly used to evaluate the impact of accidental faults on systems dependability, while the evaluation of security has been mainly based on qualitative evaluation criteria. Besides assessing the impact of accidental threats, extensions are needed to quantify the impact of malicious threats. Therefore, in ALARP we will develop a comprehensive modelling framework that can be used to assess the impact of accidental faults as well as malicious threats in an integrated way.

It is well established and widely recognized that modelling and experimentation complement each other, at least at the conceptual level, but the two approaches have seldom been used in the literature to evaluate real-life systems. The most comprehensive method addressing the construction of analysis models on the basis of measurements performed in a running prototype or in a full deployment has been developed in [19] for performance and performability analysis: software performance models of distributed applications are extracted from traces recorded during execution. A similar approach is recording error propagation traces induced by fault injection experiments [20] to support the construction of error propagation models. Other works (e.g., [21]) derive high-level form of behavioural models using experimental measurements obtained from fault injection experiments, while in other papers (e.g., [22]) the values provided from field data are used to setup parameters of analytical models. Other attempts in exploiting the potential interactions among different evaluation approaches were reported in the context of two European projects: DBench [23] and HIDENETS [24]. In DBench, a framework for dependability benchmarking based on modelling and experimentation was defined, focusing on On-Line Transactional systems. In HIDENETS, a holistic approach for the analysis of distributed applications and mobile services on dynamic and open communications infrastructure has been presented.

ALARP will take on the challenge of providing a composite V&V (verification and validation) framework for dynamic, critical systems and infrastructures where evolution and resiliency/safety are paramount, thus attacking very complex and difficult problems for system evaluation, at the frontier of the state of the art. The framework will include both model-based analysis and experimentation (testing), exploiting their potential interactions. Mechanisms will be developed to ensure the cooperation and the integration of these techniques, in order to provide realistic assessments of architectural solutions and of systems in their operational environments.

For the analysis of the experimental results, in ALARP we will adopt the approach proposed in [25]. In particular, the authors propose to use OLAP (On-Line Analytical processing) techniques supported by data collected in Data Warehouse that allows: i) to analyze the usually large amount of raw data proposed in evaluation experiments, ii) to compare results from different experiments, and iii) to share experimental results obtained by different research teams. In this context, we will also explore the possibility to adopt the same approach for collecting and analyzing results coming from the model-based evaluation activity, so as to simplify and increase the possibility of sharing results obtained by the different analysis techniques.

**B1.2.2 Commercial Automatic Track Warning Systems (ATWS)**

On the market there are few existing Automatic Track Warning Systems:

- MINIMEL by Schweizer Electronic;
- Securail by Infra Safety Services;
- Autoprowa by Zöllner GmbH.

All the above systems are based either on a device connected with the signalling system or on a train detection tool (typically magnetic) sending (via wired or wireless connection) the alarm to an horn- and/or flash-based warning system.

First of all the existing commercial ATWS suffer for the following aspects:

- expensive;
ALARP intends to overcome the above defects by proposing:

- a **low-cost personalised safe** MT (e.g. a bracelet- or a watch-type device) with a sounding and/or flashing and/or vibrating alarm providing a personalised and therefore safest alarm to each worker;
- a **much simpler system to carry, install and use** through an accurate and innovative design;
- a device with **limited training needs** through a much simpler user interface to be developed during the project’s life.

Moreover, the ALARP ATWS will have the following competitive advantages over existing devices:

- it is **completely independent from a signalling system**, making it usable on any type of railway, including scarce traffic and regional lines;
- being a **personalised solution** it offers an higher trustability and the possibility to give advice/directions to the workers to reach safe areas;
- it has **staff monitoring capabilities** ("who is where?");
- it offers the possibility to include a **wider range of alarm causes** including images and messages of what caused the alarm (thus **increasing the trustability** of the system);
- it **does not depend on a centralised control room** and each Mobile Terminal can assume the leader role thus increasing dependability and availability.

### B1.3 S/T METHODOLOGY AND ASSOCIATED WORK PLAN

**B1.3.1 Overall strategy and general description**

**B1.3.1.1 SYSTEM FOUNDATIONS**

**B1.3.1.1.1 Risk analysis and requirements specification**

The risk is defined as the product of consequence of a hazardous event and the frequency, or probability, of its occurrence. Thus a risk can be reduced by decreasing the event frequency or its consequence. A thorough risk analysis will be part of the system design and will be based on a system approach in which the TPAD and MT systems will be assessed in conjunction with the human elements their environment, communication interfaces and the approaching train. Specifically ALARP will follow a standard approach as outlined in Figure 2.
Referring to this figure the following tasks will be undertaken:

1) Define System Boundaries It is essential to define precisely the physical and operational boundaries of the ALARP system: this will include the area occupied by the workers their equipment in relation to the track and incoming trains, their telecommunication equipment and their interfaces and will involve the normal operation of the system and their processes.

2) Define Risk Criteria The risk criteria will need to be defined in order to be sure what criteria will be used to judge the tolerability of the predicted risks. There are several options that must be considered, mainly, general principle of risk control, the risk envelope, average or peak risk, measure of risk, and values of risk limits. The best option will be considered and applied taking into consideration the various regulatory regimes under which the ALARP system will operate.

3) Identify Hazards The success of a risk analysis depends on the identification of potential hazards. Hazards may emanate from two categories a) Internal Hazards - Hazards intrinsic to the site or activity associated with the mode of operation or from b) External Hazards - emanating from outside the defined operational boundaries. To help in a systematic hazard identification, a structural technique such as hazard and operability study (HAZOP) or failure mode and effect analysis (FMEA) will be used to ensure that the list of hazards is as comprehensive as possible. The identified hazard list will be then used to generate potential accident scenarios for subsequent risk analysis. This can include events in which the workers on the line don’t response to the alarms because of the environmental weather conditions etc.

4) Assess probabilities To assess the probabilities of initial hazardous events, an analysis of historical data applicable (e.g. from the accident database of the European Railway Agency) to
the given situation will be carried out, or in the event of very limited data, formalised techniques of elicitation of expert judgement could be applied. Alternatively a fault tree analysis (using component and human reliability data), when a combination of failure events is required may be applied.

5) Assess consequences The consequence of the postulated accidents will be assessed considering the transient behaviour of the processes involved. The consequences leading to worker fatalities and different degree of injuries will be considered.

6) Assess Risk For each potential hazard considered a risk will be evaluated from the level of consequence and the probability of the event.

7) Assess against criteria Once the risk level is evaluated it will be assessed against defined risk criteria. For events exceeding the criteria measures will be postulated for risk reduction.

8) Risk reduction measure/ modification For risk in excess of risk criteria measures to meet the risk limit or to satisfy ALARP principle will be proposed.

Using the above method level of protection allocation (most likely as a SIL target) will be fed back into the design specification for the ALARP system.

B1.3.1.1.2 Overall architecture

The ALARP system will consist of a set of Train Presence Alert Device (TPAD) and Mobile Terminals (MT) where the TPADs provide information (can be seen as a set of sensors) and the set of MTs are a distributed system in which the individual nodes

- can perform asymmetric roles (e.g. a leader and the flock);
- are able to reach agreement and to disseminate information they get from other nodes or devices or generated locally.

Such a system has to operate in networking environments with wireless multi-hop communication which presents a number of characteristics that will be specifically accounted for in ALARP in particular when the appropriate architecture. These characteristics include:

- unreliable communication due to the presence of wireless links;
- uncertain operational conditions, due to operation in open environments, with variable numbers of users or traffic flows, and due to dynamic network topologies;
- variable failure modes, ranging from simpler accidental faults to malicious faults (attacks and intrusions), due to operation in open and weakly controlled environments.

Because of these characteristics, and having in mind the resilience and safety objectives previously stated in Section B1.1.3, the fundamental challenges in ALARP will be to:

- reconcile the needs for predictability and timeliness with the uncertainty of the environment;
- improve reliability and availability despite the unreliability of the communication and of the system components;
- ensure secure and trustworthy operation in the presence of non-trusted parties.

In ALARP we propose to address these challenges not only by designing new algorithmic solutions, new protocols and new services, but also by applying or devising innovative architectural solutions. In particular, the ALARP architecture will be based on a hybrid architecture, which allows subdividing the system in two parts, one "simple and trusted" and one "complex", having different sets of properties and relying on different sets of assumptions, namely in terms of faults and synchronism. For example, we can consider the subsystem "simple and trusted" as synchronous with a crash fault model, and use lighter assumptions, such as asynchronous with arbitrary faults of processes and communications, on the rest of the system.

B1.3.1.2 Resilient wireless communication

Wireless Communication in the ALARP system is utilized for several purposes:
1. Between the **Train Presence Alert Device (TPAD)** and the **Mobile Terminals (MT)** of the workers: Distances here are in the order of few km and solutions based on medium range (e.g., WIMAX), or short-range multi-hop (WLAN 802.11 like) ad-hoc communication are possible. Furthermore, the use of cellular technologies can be an alternative, involving that way also third party infrastructure-based operator networks.

2. **Between the MTs** of the ALARP system: utilizing multi-hop forwarding, short-range technologies such as WLAN 802.11 or Bluetooth type can be sufficient. However, for resilience purposes, alternative means, e.g. via cellular networks or track-side access points, need to be investigated.

3. **Between the MTs and other sources of information** (e.g. the signalling systems, civil protection emergency rooms, etc.): this source of information can be one of the on-site devices, then this is equivalent to Case 2. It could however also be placed in a remote, server based control centre, in which scenario the connection to infrastructure networks is required.

The ALARP project will design the architecture and develop the necessary communication protocols to achieve a timely and resilient inter-device communication in the above three scenarios, facing the challenges created by the dynamics caused by mobility and changing link properties. The solutions will thereby use off-the-shelf wireless technologies, with WLAN 802.11, Bluetooth, WIMAX, and cellular (GPRS/UMTS) as candidates.

In order to achieve resilient communication and to be able to provide safety guarantees, the following functionalities will be investigated:

- **Neighbour discovery and (remote) monitoring of device connectivity and activity status:** Disconnected situations and crash faults of neighbouring devices need to be immediately detected by the ALARP system in order to trigger the correct countermeasures, ranging from recovery actions (e.g., switching to other interfaces) or issuing warning messages to the control unit about potential unsafe situations of the warning system itself. Hello messages enriched by positioning information sent in adaptive transmission periods can be used for this purpose. The adoption strategy has to be tuned to meet the safety and performance requirements of the ALARP scenarios.

- **Resilience via multi-interface and multi-technology devices:** In order to meet the resilience requirements, the ALARP Personal devices and the track-side monitoring unit will be equipped with multiple interface cards of potentially heterogeneous Layer 1/2 technology. The management and usage for pro-active or reactive redundancy however needs to be investigated in trade-off with reduced battery life-times due to higher energy consumption.

- **Reliable broadcasting and multi-hop forwarding:** Certain warning situations will lead to broadcast messages that have to be reliably received by all personal devices in the geographic area. Mechanisms to achieve this reliability without causing broadcast storm problems have to be investigated for the ALARP scenarios. Both for unicast and broadcast message, multi-hop forwarding will be needed. The project does not intend to develop new ad-hoc routing protocols, but a careful selection and parameter configuration of the existing candidates (e.g. OLSR, AODV, etc.) will be performed. Proactive routing protocols may be preferred in the ALARP scenarios, as continuous knowledge about the presence and connectivity of the personal devices is desirable (see Bullet 1).

- **Data integrity and authenticity via off-the shelf security protocols:** Again, the project will not design new protocols but rather select the appropriate key management and security protocols and determine the suitable configurations for their operation. Candidates include IPsec and TLS.

The functionalities mentioned above have to be considered to meet the basic requirements of the ALARP system. In addition to that, some optional extensions will be investigated on the level of a feasibility study. Those are:

- **Technological solutions to obtain information from the signalling system** in a non-intrusive way: these approaches include **eavesdropping** on the GSM-R communication. However, challenges due to message encryption with dynamic session keys need to be addressed.
- **Safe management of context information**: context information includes positioning info of the relevant devices, environment conditions, information about the state of the communication solution, as well as general background information (timed mission plan, etc.). Solutions for management of general context information have been developed previously [14], but they have to be extended to meet the safety requirements of the ALARP system.

**B1.3.1.3  MOBILE TERMINAL (MT)**

**B1.3.1.3.1  Safe and resilient architecture**

Achieving dependability and security despite accidental and malicious faults in networks of mobile nodes is particularly challenging due to their intrinsic asynchrony (unreliable communication, partitioning, mobility, etc.) and the consequent absence of continuous connectivity to global resources such as certification and authorization servers, system wide stable storage, a global time reference, etc. Furthermore, the threats to resilience and safety are particularly severe: device lifetime and communication are severely limited by scarcity of power; use of wireless links means susceptibility to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion; poor physical protection of mobile devices (especially in a hostile environment) makes them susceptible to physical damage, and vulnerable to theft or subversion.

In this context, we will propose middleware solutions for enhancing resilience, availability and security in the wireless domain. The solutions have to accommodate a balanced harmonization among security/trustworthiness, availability/performance and reliability/safety aspects. These solutions range from algorithms and higher layer protocols to actual services. For this we plan to apply principles like architectural hybridisation, which allow to painlessly enhancing a given original architecture, in terms of timeliness, security, quality of service, etc.

**B1.3.1.3.2  Self-localisation in harsh environments**

Satellite-based localization solutions have become meanwhile quite mature and lead to good localisation accuracy; however they require line of sight to a sufficient number of satellites. This condition may not be fulfilled in certain scenarios, e.g. shadowing due to large buildings in urban scenarios or in mountain areas. In particular for track-side work in tunnels, such satellite-based solutions need to be complemented by additional mechanisms to achieve always available, accurate, and timely positioning.

In order to improve accuracy or achieve positioning even in scenarios of complete absence of GPS/Galileo signals, measurement of properties of wireless communication links can be utilized. For long-range, cellular technologies, typically Time of Arrival or Time difference of Arrival measurements are utilized [26], for short-range ad-hoc communication estimators frequently rely on received signal strength [27]. Localization based on the fusion of measurements from a larger set of ad-hoc links and long-range wireless technology is still a research topic [28]. In addition, for safety-critical use-cases as in the ALARP scenarios, it is also necessary to develop mechanisms to obtain online upper bounds on the accuracy of the obtained positioning information. Furthermore, the mobility models that act as basis for improved continuous tracking can be tuned to ALARP scenarios, as the nature of the mission is known a-priori. The message exchange for wireless positioning on the ad-hoc links should thereby not interfere with other potentially safety-critical communications.

The information from movement sensors can provide additional accuracy enhancement and also allow to obtain directional information, which can e.g. be used in emergency scenarios to make the device show the direction to the worker about possible emergency routes.

The ALARP project will select, adapt, and extend existing algorithms to obtain positioning information and accuracy bounds based on the fusion of satellite based information (if available) and measurements of the different wireless links in the ALARP system. For the algorithmic part, a collaboration with the FP7 IST project WHERE [28] is intended. Finally, the necessary protocols for information exchange and the mechanisms to determine timeliness of positioning info will be developed and implemented in close collaboration to the Wireless Communication work of ALARP.
B1.3.1.3.3 Application logic

The application logic for the operation of alarms for the safety of line workers will be assessed and the level set by considering the results of the risk assessment and recommendation from human factor analysis. The analysis will be specific to the alarm types incorporated into ALARP MTs which could be based on visual, sound or vibration modes or combination of these. The level of the alarm will need to be set in relation to the risk level, the local environment and type of detector. This will be incorporated into the ALARP MT using a real-time expert system with its own built intelligence that will advise on the appropriate alarm level, and guide the user to the appropriate action to be taken, from doing nothing to an appropriate escape route. The MT will be able to operate in two modes of operation:

a) training mode

b) operational mode.

In training mode the MT will be used as a training tool in which the trainee will be able to study about alarms level, the action to be taken including evacuation modes.

In the operational mode - monitoring scope, the MT will operate in an advisory capacity. The system will be updated to assess any new site or incorporation of any new devices into an ALARP system. The system will contain its own knowledge base so that its predictions can be intermittently updated. It will operate within a probabilistic framework to provide proper treatment of the inherent uncertainties and allowing various outputs to be generated in the form of advice in terms of the most likely outcomes.

The application logic will be based on a rule base and data for risk, and the appropriate alarms level and the required actions, defined by the developers of ALARP system with the help from the knowledge engineer to ensure completeness, consistency and acceptability. This will be achieved by direct mapping of the areas of concern (to the users of the system) monitoring devices, to discrete rule base modules. This will enable them (users) to agree the functionality and the accuracy of the advisory modules.

The uncertainties in the system will be treated using a combination of fuzzy logic and probabilistic methods. Using such methods, decisions will be made on the basis of the balance of probability, or the most likely outcome, and degrees of confidence could be also assigned to these decisions.

Amongst all other functions, the application logic will allow to assign to one MT of the group the leader role. This role will allow the staff manager to:

- dispatch an alarm message to the team;
- send personalized messages to one or more workers on the track;
- manage and control a group of MTs and therefore to manage the team of trackside workers during both in normal work situations and during emergencies.

B1.3.1.3.4 Human machine interface and ergonomics

The ISO 13407 standard [33] provides guidance on achieving high usability of products by incorporating user centred design activities throughout the life cycle of interactive computer-based systems. It describes user centred design as a multi-disciplinary activity, which incorporates human factors and ergonomic knowledge and techniques with the objective of enhancing effectiveness and productivity, improving human working conditions, and counteracting the possible adverse effects of use on human health, safety and performance. There are four user centred design activities that need to perform in the project. These are:

- to understand and specify the context of use;
- to specify the user and organisational requirements;
- to produce design solutions;
- to evaluate designs against requirements.
The iterative nature of these activities together with connections to content of work package structure of the proposal is illustrated in Figure 3.

![Diagram of user centred design activities]

**Figure 3 - The interdependence of user centred design activities**

The sequence in which activities are performed and the level of effort and detail that is appropriate varies depending on the design environment and the stage of the design process.

The approach will be subdivided into 6 steps:

1. definition of requirements and analysis (task analysis, functions analysis, user-analysis/focus group, prioritisation of cases of usage);
2. exploration or alternative design mock-ups (development of idea draft concept, look and feel, interfaces, design exploration, first prototype concept, review usability);
3. synthesis (concept evaluation, recombination of concept, design developing, second prototype concept, usability testing);
4. evaluation of concepts (comprehensibility: core design elements, cooperative usability testing, evaluation sheets for each concept, preference rating of tested concepts, findings discussion);
5. implementation and design (design exploration, prototype implementation, usability review);
6. design evaluation against user requirements (checklists).

**B1.3.1.3.5 Safeguards to secure workers’ privacy**

The project will:

- design the MT to safeguard privacy of workers through
  - limited storage of data,
  - anonymisation of individual devices,
  - turn-off options;
  - insurance that privacy safeguards will not be controllable by the employer;
- integrate the above safeguards into the final devices.

**B1.3.1.4 TRAIN PRESENCE ALERT DEVICE**

One of the main components of the ALARP system is the Train Presence Alert Device (TPAD). The TPAD will be designed to be an autonomous, self-powered alerting system that will serve a virtual gate and will deliver wirelessly an alarm to all the people within the relevant site through a dedicated wireless channel. In order to provide sufficient time to evacuate the repair site, it is imminent that the virtual gate will be located at least 5 km away, providing at least 60 seconds to
clear the area if working on a high speed train rail. Obviously the TPAD can be located closer to the working site pending train speed and required alerting time.

The basic concept of the virtual gate (TPAD location) and the working sight is shown in Figure 4.

![Figure 4 - The TPAD basic concept](image)

The main challenges of the TPAD are described below. The means of how we are planning to take care of these challenges are also discussed.

**B1.3.1.4.1 Low false alarm rate with high probability of detection:**

One of the most critical features of the system is its ability to properly detect, analyze and communicate any train hazard without any false alarms. This has to be done on a mobile, reliable, and easy-to-use system, that has to function independently from the rail system. The architecture that we propose to use will be based on the following functionalities:

- **Multi-Spectral Sensing:** The TPAD will operate with two low-power spectral sensors, a colour day camera, and a uncooled FLIR camera. In addition the TPAD will include an acoustic sensor that will work in parallel to the two imaging sensors. Due to power issues (discussed below), we will operate the system with the day and acoustic sensors as the detection sensors while the uncooled FLIR will serve as a verifying sensor. Since each sensor by itself is sufficient to detect with high probability the event of a passing train we foresee that the multi-spectral sensing operation will provide adequate performance.

- **Very Low False Alarm Rates:** One of the major challenges in similar systems is the ability to persuade the user that the system is reliable and functioning correctly. Due to the nature of the rail system it is possible that the TPAD will alert the sight workers long before they can actually identify it by themselves (visually or acoustically). The method that we are planning to implement is to keep the man-in-the-loop concept by sending a visual snapshot image of the occurrence that triggered the virtual gate through the communication channel. In case an alert is received by the sight workers through the MT, they can verify the threat visually and define the action. The TPAD will also try and define through video content analysis the train speed and time of arrival to the site area. Figure 5 illustrates a possible image being sent to the MT device.

- **High Reliability:** The ALARP system is fully dependent on the TPAD to function properly. Failure of one of its components may cause a critical failure to the whole system. Since not all of the components of the TPAD are redundant we find ourselves with a critical system with single points of failure. In order to overcome the problem we plan to use a fail-safe Built In Test (BIT).

- **Robustness:** The TPAD will be packaged such that it will withstand the environmental requirements of similar electro-optical track systems.
B1.3.1.4.2 Easy to Install/Self Calibration System

The TPAD will be designed as a simple autonomous mobile device that will be easily installed near the rail track. The system will not require any interaction with the rail track or rail system (including power). Once positioned and secured near the rail track, the user will operate the system and initiate the self-calibrating procedure. Throughout this full process, the system will define its location (through GPS), test all sub-units, calibrate its imaging sensors, and define its Line Of Site (LOS). The LOS image will define the region of interest and will make sure that the system is looking at the correct track. This process should be short and require no more than a few minutes.

B1.3.1.4.3 Energy Efficient

The TPAD is to be designed for at least one full week of work without any maintenance. One of the important issues that need to be dealt is the power source and management scheme. Assuming a secondary battery package, 0 °C average ambient temperature and system weight limitation that allows hand carrying of the system (we foresee that the battery pack should weigh less than 8-10Kg), we can achieve approx 1000Wh total capacity or approx 6W per hour average power.

The TPAD system includes the sensor module (day camera, uncooled FLIR, and acoustic sensor), communication module, the central processing and storage unit, display UI module, and the power module. In its peak power when all units are functioning we can expect power consumption of more than 10W per hour therefore a power management scheme should be developed. The general guidelines that we will follow in the power management module are:

- Minimize the use of sensors - In general we will aim to use the day sensor and the acoustic sensors as the primary detection sensors while keeping the uncooled FLIR sensor as the verifying imager (mainly at night).
- The communication module - will function only during a gate passing event or a predefined event (BIT event showing that the system is alive and properly functioning). Between these periods the communication module will be in idle mode.
- Central processing and storage unit - will function in a low power level performing minimal tasks till a gate passing event or other pre-defined maintenance event. For example, the storage sub-unit including all compression hardware and software will remain idle until a gate event.

The TPAD will report its power status during the CBIT messages thus enabling battery replacement in time.

B1.3.1.4.4 Anti-Theft

The TPAD includes an inherent Anti-Theft mechanism by utilizing the CBIT function. In case of theft, the system will report a CBIT failure due to the mismatch between the Calibrated LOS and
the CBIT LOS. The system will continue to report its position and status to the MTs through the communication channel thus enabling to follow the TPAD even when moved away from its initial location. If required the TPAD may include an internal sound alarm unit.

TPAD Architecture

The TPAD architecture will be built around the building blocks described in Figure 6.

Day CMOS Camera - The definition of the camera parameters will be done during the development phase and will include resolution, shutter type, shutter speed, frame rate, dynamic range, sensitivity (mainly in low light), depth of field, focus mechanism (if required), power, and digital interface. The objective lens will be impacted mainly by the detection distance, F# and required Field of View of the image. The captured image will be sent to the Central Processing Unit through a digital interface channel.

FLIR Camera - The uncooled FLIR camera will function in parallel to the day camera. The requirements of the camera will be defined during the first phases of the program and will include resolution, sensitivity (NETD), frame rate, FOV (F#), time from stand-by to operation, power consumption, and input/output interface. Similar to the day camera, the FLIR captured image will be sent to the Central Processing Unit through a digital or analog interface channel.

Acoustic Sensor - The Acoustic sensing device will complement the day and FLIR cameras as a detection device. In difference to acoustic sensors that are physically connected to the track (measuring the acoustic vibration), the proposed sensor is used in a remote manner detecting the actual acoustic Doppler effect.

Central Processing and Storage Unit - This is the heart of the TPAD that interfaces the three sensor devices, hosts the algorithm layer (detection, communication, BIT, power management, video compression, UI, Setup), and controls the display, communication and power units. The CPU requirements and architecture will be defined throughout the first stages of the project.

Communication Unit - The resilient wireless communication unit will be defined in WP2. The communication unit will enable data communication between the TPAD and the MTs at distances of up to 5+ km without direct sight between the two. The communication unit should also maintain robust and fail safe mechanisms packaged in a small low power unit.

Display Unit - Serves as the interface unit of the TPAD. The Display Unit is controlled and driven by the Central Processing Unit.

Power Unit - Includes the Battery, DC to DC converters, power interfaces with all the sub units, charging mechanism (including safe charge), short circuit and reversed connection prevention mechanisms, and digital interface to the Central Processing Unit.

B1.3.1.5 INTEGRATION AND PROOF-OF-CONCEPT

B1.3.1.5.1 System integration and proof-of-concept

The System Integration and Proof-Of-Concept is the most critical part of the program. This effort will start with a clear definition of the Integration Procedure and Test Plan, followed by actual
system integration testing, development iterations if fixes are identified, and finalized with a test report.

There are two important gates that need to be successfully passed before entering the ALARP System integration phase and include:

- **Mobile Terminal Integration** - Including the software/hardware integration, communication, mechanical, UI, and others. This effort will be discussed separately in Section B1.3.1.5.2.

- **Train Presence Alert Device Integration** - This integration effort will verify that all aspects of the TPAD are functioning properly as designed. The TPAD integration will include the sensor level (day, FLIR, acoustic), the wireless communication unit, the display unit, the power unit the Central Processing and Storage Unit including applications i.e. detection, communication, BIT, power management, video compression, UI, Setup applications.

**B1.3.1.5.2 MT integration**

The MT integration effort is one of the most challenging activities within the program due to the fact that it is required to integrate various multidisciplinary capabilities into one small device that has to directly interact with the worker. The methodology of the integration is similar to the full system integration expressed above and includes MT integration and test plan definition, actual integration and testing and additional system fixes (if required).

The MT integration effort will include among others:

- **Hardware-Software Integration** - which will checkout the integrity of the safe resilient middleware and algorithms and verify proper functionality. In addition we will checkout the functionality of the higher level applications including the Application Logic: Training and Operational Modes, User Interface, Situational Awareness Program, MT/TPAD communication software, and others.

- **Self Localisation** - The self localization system provides the positioning data of each and every one of the MTs and TPADs. In addition, it also verifies that the user is "alive" i.e. moving with the MT. The integration effort will verify the functionality both outdoor and indoor and also in poor weather environments.

- **Wireless Communication** - WP2 will define the wireless communication method between the MTs, and between the MTs and the TPAD. During the MT integration phase we will verify proper functionality of the Wireless Communication Link, including neighbour discovery and remote device monitoring, multi-hop forwarding, and data authentication / security protocols.

- **Human Machine Interface** - This effort will include integration and testing of the various modes of operation on the user on the correct position of the MT. This will include initial tests that will verify proper ability to function with the system thus minimizing disturbance to the ongoing site activities. Further and more enhanced testing will be done in WP6 (evaluation phase).

- During the MT integration phase we will verify the functionality of the entire unit in different environmental situations including various temperature ranges, humidity, random vibration, and shock. In addition we will test the power management scheme and verify that it meets the MTs requirement specifications.

**B1.3.1.6 MODELLING, VERIFICATION, VALIDATION AND EVALUATION**

The verification and validation process in ALARP will be based both on modelling and on experimental dependability evaluations. The analyzed objects will be both single components/mechanisms proposed in the other WPs and a more comprehensive set of final components integrated in the proof-of-concept. The different evaluation approaches to the analysis will be integrated in a unique framework exploiting their potential interactions, for example allowing cross-validation and cross-fertilization of the obtained results.

**B1.3.1.6.1 Quantitative modelling**

In ALARP the main topics that will be developed in the context of modelling will be:
i) **quantitative model-based evaluations** for early validation of components, mechanisms and design of the overall architecture: to this regard, attention will be paid to the model construction and solution process. Model-based evaluation, in particular stochastic state-based (e.g., Stochastic Petri Nets and their extensions), is commonly used since it is able to capture various functional and stochastic dependencies among components and allows the evaluation of various measures related to dependability performance. The difficulties in handling such models are mainly related to model largeness and state explosion problem; significant progress has been obtained during the last years for addressing such problems, e.g., the use of hierarchical approaches, composition rules or model decompositions. In ALARP we will identify the appropriate modelling construction and solution approaches capable to address the significant challenges raising from the ALARP characteristics, like the varying operational conditions (e.g., in terms of involved users and available wireless connections) and the presence of both accidental and malicious faults. Among the possible research directions, we will also explore the feasibility of adopting a Multiple Phased System (MPS) approach to represent the different operational phases (e.g., before or during a malicious attack), as well as the (automatic/semi-automatic) derivation of dependability analysis models from high-level specification formalisms, like UML diagrams.

ii) **modelling as support for experimentation**: modeling helps in **selecting the features and measures of interest** to be evaluated experimentally, as well as the right inputs to be provided for experimentation.

iii) in ALARP experimentation will be also used as a support for modelling. Integration of model-based and experimental evaluation has additional advantages:

- mitigation of the system complexity, since the system can be analyzed at different levels of abstraction, and we are able to feed a high-level model with values derived through experimental measurements;

- possibility to cross-validate results obtained for the same indicator using different techniques.

In ALARP we will explore the feasibility of using Data Warehouse as support for collection of results of experimentation and modelling, with OLAP techniques for a fast, easy and powerful access to the results. The usage of a Data Warehousing approach will simplify and increase the possibility of sharing results obtained by different analysis techniques.

### B1.3.1.6.2 Verification and validation

Verification and validation are essential in the life cycle of any safety critical system. The development of any system is incomplete without rigorous testing and verification that the implementation is consistent with the specifications. Verification and validation (V&V) are nowadays extremely important, especially in software, as the complexity of software in systems has increased, and planning for V&V is necessary from the beginning of the development life cycle [32]. In addition, V&V is very closely linked with certification: it is the major component in support of certification.

While the terms verification and validation are often used in papers and texts, there are distinct differences in their terminology. According to the IEEE Standard Glossary of Software Engineering Terminology [31], verification is defined as "The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase". Validation, on the other hand, is defined as "The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements". So verification simply demonstrates whether the output of a phase conforms to the input of a phase as opposed to showing that the output is actually correct. Verification will not detect errors resulting from incorrect input specification and these errors may propagate without detection through later stages in the development cycle. It is not enough to only depend on verification, so validation is necessary to check for problems with the specification and to demonstrate that the system is operational.

For these motivations, in ALARP we see both Verification and Validation as needed. In ALARP we see Verification and Validation highly integrated with the design and implementation processes;
V&V will be practiced over the entire system life cycle. We will develop early in the project a V&V plan that will guide these processes. The requirements will be early defined in order to plan as soon as possible verification and validation activities and to guarantee traceability of the requirements in the project. The V&V Plan will describe approaches and methods for single components verification, integration verification, qualification testing, and overall system verification. Verification procedures involve step by step instructions that implement the inspection, demonstration, testing, and analysis required by the Verification Plan. The V&V activities will include both software and hardware aspects.

V&V techniques that we plan to use in ALARP include:

- **Dynamic testing**: testing involving the execution of the overall system or of single component (e.g. middleware services);
- **Measurement techniques**: used to measure quality of service properties (measurements of the system of its components will be strongly related to modeling processes as described in 1.1.4.6.1);
- **Dependability analysis and Hazard analysis**: validation techniques in which attention will be paid in the identification of hazards, their root causes, and possible countermeasures.

*B1.3.1.6.3 Testing and evaluation*

Testing and evaluation will be carried out according to the following phases:

- A **first phase (PH1)** that will be carried out in laboratory, to test and evaluate the single ALARP components in a controlled environment.

- A **second phase (PH2)** that will be carried out in the field (most likely in one of the ASTS installations) to test and evaluate the basic functionalities of the ALARP system. In particular, we envisage to test all the TPAD and MT functionalities with the exception of the following MT advanced characteristics:
  
  - eavesdropping on wireless signalling communication;
  - the ability to identify the direction of the movement of the worker;
  - the biometric coupling between the MT and the worker.

  This phase will allow to verify the concept feasibility and highlights those parts of the design that need refinements and/or improvements.

- Finally, a **third phase (PH3)** in which the entire ALARP system will be tested and evaluated in the field against requirements covering all planned characteristics.

*B1.3.1.6.4 Validation scenarios*

The validation scenarios definition are part of the work specified in WP1.1 and WP6.2, but it is possible to anticipate the following 3 scenarios (corresponding to the 3 evaluation phases PH1, PH2 and PH3 described in §B1.3.1.6.3):

- in the laboratory (phase PH1), in which all the single ALARP components are tested and evaluated in controlled environments for the specific functionalities;
- in the ASTS railway test track for phase PH2, where
  - the TPAD will be tested with real trains running on the track, in day- and night-time conditions, with artificially-generated environmental conditions (e.g. smoke, fog, etc.),
  - the MT will be tested in controlled field environment to evaluate the robustness to noise, temperature, electromagnetic noise, etc.;
- in real railway lines to have a real scenario (still in a controlled environment) with specific infrastructures like tunnels, bridges, etc. where it will be possible to reproduce the environmental conditions already tested in the ASTS railway test track.

The validation scenarios will be defined in WP1.1 according to the following methodology:

1. identification of hazardous events;
2. determination of hazardous conditions (i.e. the characteristics and circumstances surrounding a railway accident);
3. evaluation of the relationships between hazardous conditions and events;
4. definition of accident scenarios by generating a railway accident table;
5. verification of the feasibility of the relationships between elements of hazardous conditions to filter out unfeasible scenarios;
6. calculation of the weighting of each scenario to prioritise the list;
7. clustering of the accident scenarios to limit the number of possible scenarios.

B1.3.1.6.5 Final assessment and guidelines
The final assessment will be conducted in the application environment by considering different validation scenarios that focus on the behaviour in presence of different kinds of events that could affect workers’ safety and by exemplifying the scenarios that benefit from the solutions developed in WP2, WP3 and WP4. Then the results of the previous work will be consolidated and the guidelines will be prepared that are necessary to utilize
(i) the new technical solutions,
(ii) the modelling, verification, validation and evaluation methodologies and
(iii) the proof-of-concept framework.

B1.3.1.6.6 Informed consent
The project will ensure that all the workers participating into the project testing and evaluation phases will fill an informed consent form. A copy of the informed consent will be submitted to the European Commission.

B1.3.1.7 RISKS APPRAISAL AND MANAGEMENT
There are a series of key risks, ranging from technical to exploitation risks, associated with the project that need to be specifically managed. A non-exhaustive example areas that will be taken into account by the project are:

- **Availability of COTS components.** The project intends to use as much as possible COTS components. There is a risk that the market does not offer the required components. This risk is limited by the internal competences of both ASTS and ESL that can design in-house the required missing HW components.

- **Eavesdropping on wireless signalling communication.** This expected characteristic of the MT can be hindered by the level of protection existing on wireless signalling systems (e.g. cryptography in ERTMS radio transmission). As already described in the text, ALARP system does not rely on existing signalling systems and therefore this characteristic, despite its potential, is not mandatory for a successful completion of the project. Moreover, longstanding experience of ASTS in signalling systems design and development will ensure that this risk will be carefully managed.

- **Coupling MT with a specific worker.** There is the risk that the existing biometric devices will not allow a reliable and/or ergonomic coupling between the worker and the MT. The downscaling of this requirement to a more classical authentication solution will not infringe the validity of the overall ALARP concept.

- **Workers acceptance.** The acceptance of workers of a device like the ALARP ATWS is a key parameter for the success. Acceptance will depend on many aspects including the ergonomics and the trustability. The ergonomics aspects will be guaranteed to the strict adherence to the ISO 13407 standard and to the feedback from the Stakeholder Forum that, will involve, amongst others, also workers organisations. Trustability is granted by the proposed approaches for reaching adequate safety integrity levels (SIL) on the system and by the
additional features (e.g. the possibility to send an image of the train detected by the TPAD) forecasted for the ALARP system. Also in this case the risk is mitigated by the long-standing experience in developing safety-related equipments of both ASTS and ESL.

- **Cost.** As pointed out in section B1.1.3, the MT must be low-cost to be adopted in large scale and have sustainable costs for low- and medium-scale adoption. MT costs will drive the entire design process and in particular the selection of the COTS platform and the real-time operating system and related SW. This attention to costs is guaranteed by the large experience of Elbit Systems in designing and producing IT devices for large scale adoption both in the civil and military markets.

**B1.3.2 Timing of work packages and their components**

**B1.3.2.1 STRUCTURE OF WORK-PACKAGES**

The project is based on 8 work-packages, 6 of which are technical (WP1 to WP6) while WP0 is dealing with project management and WP7 with dissemination and exploitation issues.

The diagram in Figure 7 represents the interdependencies between the ALARP work-packages. WP0 (project management) and WP7 (dissemination and exploitation) control and get input from all the technical work-packages (WP2, WP3, WP4, WP5 and WP6).

![Figure 7 - WP interdependencies](image)

WP1 will set-up the system foundations through

- the risk analysis and requirements and validation scenarios specification (WP1.1);
- the design of the overall architecture (WP1.2).

The need for requested effort in WP1 (see the resource allocation per beneficiary and per WP in Table 8 at page 50) over the planned period is justified by the following reasons:

- The system foundation work has to start almost from scratch without the possibility to use past experiences (and therefore a significant effort is required) since:
The proposed system is very innovative for the railway sector and, at the same time, no similar solutions can be mediated from other application sectors.

The ALARP system is aimed at solving an issue that, despite its importance, has been never deeply considered and analysed in terms of risk analysis and requirements definition by railway operators. This is due to the fact that in most cases the workers are not belonging to the railway operators.

- The risk analysis and the user requirements definition tasks are iterative and time-consuming processes, involving also the use of models, since:
  - ALARP deals with workers safety and consequent human factors that have significant aspects that are country-dependent and therefore thorough analysis are needed (e.g. the already implemented safety procedures, the level of training of workers, etc.).
  - The regulations on safety procedures and on privacy are not uniform across Europe and therefore also in this case a detailed and time-consuming analysis is required.

- Being based on system and on a holistic approach which deals with safety aspects, the Risk assessment is quite a convoluted process, and some tasks require special attention:
  - Hazard identification can identify many hazards, the HAZOP process requires several participants, experts in different disciplines postulating different events which will need to be analysed.
  - Assessment of probabilities for the postulated events will require quite a lot database searches and adaptation to an ALARP project. Where the data will not exist, again group data elicitation will be required (several experts).
  - Risk assessment will require to take account of uncertainty in data and processes as well as to take account of data and event correlations which will require special attention.
  - Several iterations for the assessment will be required to come to final system specification.

- The risk analysis and the requirements scenario definition will lead to the specification of the validation scenarios that are also part of WP1.1 and then refined in WP6.2;

- The design of the overall ALARP architecture requires the claimed effort for the following reasons (that have also an impact on the development of the Mobile Terminal in WP3):
  - The ALARP system is a safety-critical system with peculiar characteristics requiring a thorough and integrated approach in the design:
    - it must be trustable by workers and therefore it needs to have very high reliability;
    - the Mobile Terminal must be wearable mostly by low-trained staff and therefore requires an extra effort in the design phase for what concerns the ergonomics (alert system, symbols to guide the workers to escape paths, etc.);
    - it requires interactions between Mobile Terminals in harsh environment.
  - The envisioned ALARP architecture will incorporate the concept of architectural hybridisation, a paradigm to construct systems with wormholes, i.e. special components that present improved characteristics with respect to the remaining components of the system. Because of that, the architecture will include two kinds of services:
    - generic middleware services, which contribute to the overall resilience improvement because of the functionality they offer,
    - and timeliness and trustworthiness oracles, which are fundamental because (but not exclusively) of their improved properties regarding timeliness or security, when compared to the remaining middleware services.
In fact, the architectural hybridization principle allows subdividing the system in two parts, one “simple and trusted” and one “complex”. The power of the wormholes model originates from the possibility of using a different model for the two subsystems, both for the synchrony and for the failure models: for example, we can consider the subsystem “simple and trusted” as synchronous with a crash fault model, and use lighter assumptions, as asynchronous with arbitrary faults of processes and communications, on the rest of the system.

- The ALARP system has to deal with the issue of workers’ privacy: specific solutions to cope with privacy without infringing system functionalities have to be considered. This will contribute to add complexity to the overall architecture design.

- The effort for WP1 cannot be extended beyond the 9 months period since, given the complexity of the ALARP system, the development phases in WP2, WP3 and WP4 as well as the integration (WP5) and validation (WP6) phases have to start quite early in the project.

Then, on the basis of the findings of WP1, three work packages will start in parallel with the design of the main ALARP components: the Mobile Terminal (MT), the Train Presence Alert Device (TPAD) and the resilient wireless communication system:

WP2 will design the resilient wireless communication system through:
- the definition of the overall communication architecture (WP2.1);
- the development of adaptive protocols for enhanced resilience (WP2.2);
- iterations on the solution approaches on the basis of model-based early evaluation outcomes (WP2.3).

The WP3 “Mobile Terminal design” includes the definition and design tasks and the development of the main SW modules of the Mobile Terminal:
- the resilient core (wormhole);
- the middleware;
- the self-localisation SW;
- the application logic;
- the Human-Machine Interface.

WP3 will be developed according to the following phases:
- design of the safe and resilient architecture and development of the resilient core and the middleware (WP3.1);
- selection of the COTS platform (WP3.2);
- design and development of the methodology for the self-localisation in harsh environments (WP3.3);
- design and development of the application logic (WP3.4);
- design of the ergonomics and development of the Human Machine Interface (WP3.5).

WP4 will concentrate on the design of the TPAD according to the following activities:
- TPAD system requirements definition (WP4.1)
- Hazard Analysis through analytical modelling of the detection model (WP4.2)
- TPAD Architecture Detailed Design (WP4.3)
- Development of TPAD subunit components (WP4.4)
• Development of TPAD application SW (WP4.5)

The outcome of the three design work-packages will be the input of the integration and proof-of-concept work-package (WP5) that will involve the following activities:

• MT integration (WP5.1);
• TPAD integration (WP5.2);
• ALARP system integration and proof-of-concept implementation (WP5.3)

Finally the modelling, verification, validation and evaluation work-package (WP6) is a vertical work-package that will serve the entire project with the following activities in support to both the design and testing phases:

• quantitative modelling (WP6.1);
• verification and validation (WP6.2);
• testing and evaluation (WP6.3);
• final assessment and guidelines (WP6.4).
### B1.3.2.2 Timing of Work Packages and Their Components

<table>
<thead>
<tr>
<th>ID</th>
<th>Work Packages/Tasks</th>
<th>Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WP0 Project Management</td>
<td>01/01/2010</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>2</td>
<td>WP1 System foundations</td>
<td>01/01/2010</td>
<td>30/09/2010</td>
</tr>
<tr>
<td>3</td>
<td>WP1.1 Risk analysis and requirements and scenarios specifications</td>
<td>01/01/2010</td>
<td>01/06/2010</td>
</tr>
<tr>
<td>4</td>
<td>WP1.2 Design of the overall architecture</td>
<td>01/03/2010</td>
<td>30/09/2010</td>
</tr>
<tr>
<td>5</td>
<td>WP2 Resilient wireless architecture design</td>
<td>01/04/2010</td>
<td>29/09/2012</td>
</tr>
<tr>
<td>6</td>
<td>WP2.1 Definition of the overall communication architecture</td>
<td>01/04/2010</td>
<td>31/12/2010</td>
</tr>
<tr>
<td>7</td>
<td>WP2.2 Development adaptive protocols for enhanced resilience</td>
<td>01/10/2010</td>
<td>30/12/2011</td>
</tr>
<tr>
<td>8</td>
<td>WP2.3 Iterations on solution approaches</td>
<td>01/07/2011</td>
<td>29/06/2012</td>
</tr>
<tr>
<td>9</td>
<td>WP3 MT design</td>
<td>01/03/2010</td>
<td>29/06/2012</td>
</tr>
<tr>
<td>10</td>
<td>WP3.1 Safe and resilient architecture design and development</td>
<td>01/03/2010</td>
<td>31/12/2010</td>
</tr>
<tr>
<td>11</td>
<td>WP3.2 COTS platform selection</td>
<td>02/09/2010</td>
<td>30/09/2011</td>
</tr>
<tr>
<td>12</td>
<td>WP3.3 Design and development of the self-localisation solution</td>
<td>02/09/2010</td>
<td>30/12/2011</td>
</tr>
<tr>
<td>13</td>
<td>WP3.4 Application logic design and development</td>
<td>02/09/2010</td>
<td>29/09/2012</td>
</tr>
<tr>
<td>14</td>
<td>WP3.5 Economics and HMI design and development</td>
<td>01/03/2010</td>
<td>29/09/2012</td>
</tr>
<tr>
<td>15</td>
<td>WP4 TPAD design</td>
<td>01/03/2010</td>
<td>29/06/2012</td>
</tr>
<tr>
<td>16</td>
<td>WP4.1 TPAD system requirement definition</td>
<td>01/03/2010</td>
<td>30/09/2010</td>
</tr>
<tr>
<td>17</td>
<td>WP4.2 TPAD analytical hazard analysis</td>
<td>01/06/2010</td>
<td>30/09/2010</td>
</tr>
<tr>
<td>18</td>
<td>WP4.3 TPAD detailed architecture design</td>
<td>02/08/2010</td>
<td>30/09/2011</td>
</tr>
<tr>
<td>19</td>
<td>WP4.4 HW units development</td>
<td>03/01/2011</td>
<td>29/09/2012</td>
</tr>
<tr>
<td>20</td>
<td>WP4.5 SW application development</td>
<td>03/01/2011</td>
<td>29/09/2012</td>
</tr>
<tr>
<td>21</td>
<td>WP5 Integration and proof-of-concept</td>
<td>03/01/2011</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>22</td>
<td>WP5.1 MT integration</td>
<td>03/01/2011</td>
<td>29/09/2012</td>
</tr>
<tr>
<td>23</td>
<td>WP5.2 TPAD integration</td>
<td>03/01/2011</td>
<td>29/09/2012</td>
</tr>
<tr>
<td>24</td>
<td>WP5.3 System integration and proof-of-concept implementation</td>
<td>01/07/2011</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>25</td>
<td>WP6 Modelling, verification, validation and evaluation</td>
<td>01/04/2010</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>26</td>
<td>WP6.1 Quantitative modelling</td>
<td>01/04/2010</td>
<td>31/01/2012</td>
</tr>
<tr>
<td>27</td>
<td>WP6.2 Verification and validation</td>
<td>01/07/2010</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>28</td>
<td>WP6.3 Testing and evaluation</td>
<td>03/01/2011</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>29</td>
<td>WP6.4 Final assessment and guidelines</td>
<td>02/07/2013</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>30</td>
<td>WP7 Dissemination and exploitation</td>
<td>01/01/2010</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>31</td>
<td>WP7.1 Dissemination</td>
<td>01/01/2010</td>
<td>31/12/2012</td>
</tr>
<tr>
<td>32</td>
<td>WP7.2 Exploitation</td>
<td>01/01/2010</td>
<td>31/12/2012</td>
</tr>
</tbody>
</table>
# B1.3.3 Work package list / overview

## B1.3.3.1 WORK-PACKAGE LIST

<table>
<thead>
<tr>
<th>WP No</th>
<th>Work-package title</th>
<th>Lead beneficiary No</th>
<th>Lead beneficiary short name</th>
<th>Person-months</th>
<th>Start month</th>
<th>End month</th>
<th>Deliverable No</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP0</td>
<td>Project management</td>
<td>1</td>
<td>ASTS</td>
<td>20</td>
<td>M1</td>
<td>M36</td>
<td>D0.1.n, D0.2, D0.3, D0.4, D0.5, D0.6</td>
</tr>
<tr>
<td>WP1</td>
<td>System foundations</td>
<td>1</td>
<td>ASTS</td>
<td>46</td>
<td>M1</td>
<td>M9</td>
<td>D1.1, D1.2, D1.3, D1.4</td>
</tr>
<tr>
<td>WP2</td>
<td>Resilient wireless communication design</td>
<td>2</td>
<td>FTW</td>
<td>34</td>
<td>M4</td>
<td>M30</td>
<td>D2.1, D2.2, D2.3</td>
</tr>
<tr>
<td>WP3</td>
<td>Mobile Terminal (MT) design</td>
<td>3</td>
<td>UNIFI</td>
<td>96</td>
<td>M4</td>
<td>M30</td>
<td>D3.1, D3.2, D3.3, D3.4</td>
</tr>
<tr>
<td>WP4</td>
<td>Train Presence Alert Device (TPAD) design</td>
<td>5</td>
<td>ESL</td>
<td>52</td>
<td>M4</td>
<td>M30</td>
<td>D4.1, D4.2, D4.3, D4.4</td>
</tr>
<tr>
<td>WP5</td>
<td>Integration and proof-of-concept</td>
<td>5</td>
<td>ESL</td>
<td>70</td>
<td>M13</td>
<td>M36</td>
<td>D5.1, D5.2, D5.3, D5.4, D5.5, D5.6, D5.7, D5.8</td>
</tr>
<tr>
<td>WP6</td>
<td>Modelling, verification, validation and evaluation</td>
<td>4</td>
<td>RT</td>
<td>60</td>
<td>M4</td>
<td>M36</td>
<td>D6.1, D6.2, D6.3, D6.4, D6.5, D6.6,</td>
</tr>
<tr>
<td>WP7</td>
<td>Dissemination and exploitation</td>
<td>1</td>
<td>ASTS</td>
<td>15</td>
<td>M1</td>
<td>M36</td>
<td>D7.1.n, D7.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TOTAL</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>393</td>
</tr>
</tbody>
</table>

Table 4 - Work package list
### B1.3.4 Deliverables list

<table>
<thead>
<tr>
<th>Deliverable No</th>
<th>Deliverable name</th>
<th>WP no.</th>
<th>Lead beneficiary no.</th>
<th>Lead beneficiary short name</th>
<th>Estimated indicative person-months</th>
<th>Delivery date(s)</th>
<th>Nature*</th>
<th>Dissemination level¹⁰</th>
</tr>
</thead>
<tbody>
<tr>
<td>D0.1.n</td>
<td>Six-monthly management reports (n = 1 ... 6)</td>
<td>WP0</td>
<td>1</td>
<td>ASTS</td>
<td>16</td>
<td>M(n*6)</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D0.2</td>
<td>Quality Assurance Plan</td>
<td>WP0</td>
<td>1</td>
<td>ASTS</td>
<td>1</td>
<td>M3</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D0.3</td>
<td>Final report</td>
<td>WP0</td>
<td>1</td>
<td>ASTS</td>
<td>1</td>
<td>M36</td>
<td>R</td>
<td>P</td>
</tr>
<tr>
<td>D0.4</td>
<td>Interim Periodic Management Report</td>
<td>WP0</td>
<td>1</td>
<td>ASTS</td>
<td>1</td>
<td>M18</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D0.5</td>
<td>Final Periodic Management Report</td>
<td>WP0</td>
<td>1</td>
<td>ASTS</td>
<td>1</td>
<td>M36</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D0.6</td>
<td>Report on the distribution of the Community financial contribution between beneficiaries</td>
<td>WP0</td>
<td>1</td>
<td>ASTS</td>
<td>N.A.</td>
<td>30 days after receipt of final payment</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D1.1</td>
<td>Risk analysis</td>
<td>WP1</td>
<td>6</td>
<td>PRO</td>
<td>10</td>
<td>M6</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D1.2</td>
<td>Requirements specification</td>
<td>WP1</td>
<td>1</td>
<td>ASTS</td>
<td>10</td>
<td>M6</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D1.3</td>
<td>Overall architecture design</td>
<td>WP1</td>
<td>1</td>
<td>ASTS</td>
<td>2</td>
<td>M9</td>
<td>R</td>
<td>P/RE</td>
</tr>
<tr>
<td>D2.1</td>
<td>Resilient wireless communication architecture</td>
<td>WP2</td>
<td>2</td>
<td>FTW</td>
<td>8</td>
<td>M12</td>
<td>R</td>
<td>P</td>
</tr>
<tr>
<td>D2.2</td>
<td>Preliminary wireless communication solution</td>
<td>WP2</td>
<td>2</td>
<td>FTW</td>
<td>15</td>
<td>M18</td>
<td>R</td>
<td>P/RE</td>
</tr>
<tr>
<td>D2.3</td>
<td>Final wireless communication solutions</td>
<td>WP2</td>
<td>2</td>
<td>FTW</td>
<td>11</td>
<td>M30</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D3.1</td>
<td>MT architecture design</td>
<td>WP3</td>
<td>3</td>
<td>UNIFI</td>
<td>20</td>
<td>M12</td>
<td>R</td>
<td>P/RE</td>
</tr>
<tr>
<td>D3.2</td>
<td>Preliminary MT design</td>
<td>WP3</td>
<td>3</td>
<td>UNIFI</td>
<td>15</td>
<td>M18</td>
<td>R</td>
<td>P/RE</td>
</tr>
<tr>
<td>D3.3</td>
<td>Final MT design</td>
<td>WP3</td>
<td>3</td>
<td>UNIFI</td>
<td>15</td>
<td>M30</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D3.4</td>
<td>MT SW modules</td>
<td>WP3</td>
<td>3</td>
<td>UNIFI</td>
<td>46</td>
<td>M30</td>
<td>O</td>
<td>RE</td>
</tr>
<tr>
<td>D4.1</td>
<td>TPAD architecture design</td>
<td>WP4</td>
<td>5</td>
<td>ESL</td>
<td>6</td>
<td>M12</td>
<td>R</td>
<td>P/RE</td>
</tr>
<tr>
<td>D4.2</td>
<td>Preliminary TPAD design</td>
<td>WP4</td>
<td>5</td>
<td>ESL</td>
<td>6</td>
<td>M18</td>
<td>R</td>
<td>P/RE</td>
</tr>
</tbody>
</table>

* R - Report; PR - Prototype; O - Other; ME - Methodology

¹⁰ P - Public; RE - Restricted to a group specified by the Consortium (including the Commission Services); P/RE document with a P part and a RE part; CO - Confidential, only for members of the consortium
<table>
<thead>
<tr>
<th>Deliverable No</th>
<th>Deliverable name</th>
<th>WP no.</th>
<th>Lead beneficiary no.</th>
<th>Lead beneficiary short name</th>
<th>Estimated indicative person-months</th>
<th>Delivery date(s)</th>
<th>Nature*</th>
<th>Dissemination level¹⁰</th>
</tr>
</thead>
<tbody>
<tr>
<td>D4.3</td>
<td>Final TPAD design</td>
<td>5</td>
<td>ESL</td>
<td>11</td>
<td>M30</td>
<td>R</td>
<td>RE</td>
<td></td>
</tr>
<tr>
<td>D4.4</td>
<td>TPAD HW units and application SW</td>
<td>WP4</td>
<td>5</td>
<td>ESL</td>
<td>29</td>
<td>M30</td>
<td>O</td>
<td>RE</td>
</tr>
<tr>
<td>D5.1</td>
<td>MT integration procedure</td>
<td>WP5</td>
<td>5</td>
<td>ESL</td>
<td>2</td>
<td>M18</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D5.2</td>
<td>MT prototype</td>
<td>WP5</td>
<td>5</td>
<td>ESL</td>
<td>15</td>
<td>M18</td>
<td>PR</td>
<td>RE</td>
</tr>
<tr>
<td>D5.3</td>
<td>TPAD integration procedure</td>
<td>WP5</td>
<td>5</td>
<td>ESL</td>
<td>2</td>
<td>M18</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D5.4</td>
<td>TPAD prototype</td>
<td>WP5</td>
<td>5</td>
<td>ESL</td>
<td>15</td>
<td>M18</td>
<td>PR</td>
<td>RE</td>
</tr>
<tr>
<td>D5.5</td>
<td>ALARP System Integration Procedure</td>
<td>WP5</td>
<td>5</td>
<td>ESL</td>
<td>2</td>
<td>M24</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D5.6</td>
<td>ALARP PH2 integrated prototype</td>
<td>WP5</td>
<td>5</td>
<td>ESL</td>
<td>15</td>
<td>M24</td>
<td>PR</td>
<td>RE</td>
</tr>
<tr>
<td>D5.7</td>
<td>ALARP PH3 integrated prototype</td>
<td>WP5</td>
<td>5</td>
<td>ESL</td>
<td>15</td>
<td>M30</td>
<td>PR</td>
<td>RE</td>
</tr>
<tr>
<td>D5.8</td>
<td>ALARP System Integration Report</td>
<td>WP5</td>
<td>5</td>
<td>ESL</td>
<td>4</td>
<td>M32</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D6.1</td>
<td>Quantitative modelling of ALARP solutions</td>
<td>WP6</td>
<td>4</td>
<td>RT</td>
<td>16</td>
<td>M24</td>
<td>R</td>
<td>P/RE</td>
</tr>
<tr>
<td>D6.2</td>
<td>Verification and Validation Plan</td>
<td>WP6</td>
<td>4</td>
<td>RT</td>
<td>4</td>
<td>M12</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D6.3</td>
<td>PH1 testing and evaluation report</td>
<td>WP6</td>
<td>4</td>
<td>RT</td>
<td>12</td>
<td>M24</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D6.4</td>
<td>PH2 testing and evaluation report</td>
<td>WP6</td>
<td>4</td>
<td>RT</td>
<td>12</td>
<td>M30</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D6.5</td>
<td>PH3 testing and evaluation report</td>
<td>WP6</td>
<td>4</td>
<td>RT</td>
<td>12</td>
<td>M36</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D6.6</td>
<td>Final assessment and guidelines</td>
<td>WP6</td>
<td>4</td>
<td>RT</td>
<td>4</td>
<td>M36</td>
<td>R</td>
<td>P</td>
</tr>
<tr>
<td>D7.1.n</td>
<td>Periodic dissemination and exploitation plans (n = 1,2,3)</td>
<td>WP7</td>
<td>1</td>
<td>ASTS</td>
<td>14</td>
<td>M6, M12, M24</td>
<td>R</td>
<td>RE</td>
</tr>
<tr>
<td>D7.2</td>
<td>Collection of the dissemination material</td>
<td>WP7</td>
<td>1</td>
<td>ASTS</td>
<td>1</td>
<td>M36</td>
<td>O</td>
<td>P</td>
</tr>
</tbody>
</table>

Table 5 - Deliverables list
B1.3.5 Work package descriptions

The 7 ALARP Work-Packages (WP) are described in the following tables: the WP leader is bold squared.

<table>
<thead>
<tr>
<th>Work-package number</th>
<th>WP0</th>
<th>Start date</th>
<th>M1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work-package title</td>
<td>Project management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Participant ID</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Participant short name</td>
<td>ASTS</td>
<td>FTW</td>
<td>UNIFI</td>
</tr>
<tr>
<td>Person-months per participant:</td>
<td>20</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Objectives

This work package deals with both the co-ordination of the whole project and management of project coordinator activities. It will include establishment of procedures for project management and Quality Assurance (QA); i.e. establishing project structure, working procedures, detailed timetables, and communications. All systems for project control and monitoring will be set up to ensure a successful completion of the project on time and within budget.

Description of work

The project management WP will include the following activities:

- Management of the Consortium for administrative aspects, including the administration of Community financial contribution and distribution of Community funds.
- Monitoring of compliance of beneficiaries with their obligations under the Grant Agreement
- Review of reports to verify consistency with the project tasks.
- Designing and maintaining partner specific templates for collecting input to the required EC documents,
- Implementing and maintaining of a project-specific database for reporting and controlling, including the adaptation of the structure after changes in the work-plan and the consortium.
- Drafting and maintaining the dissemination and exploitation plan following the EC’s requirements,
- Preparing and post-processing of EC reviews from the consortium-side including support in the implementation of recommendations from the EC and reviewers,
- Preparing, executing and post-processing of major project meetings such as Executive Board meetings, General Assemblies and meetings with the advisory board (tasks: agendas, invitations, location of meeting places, organization of rooms and equipment, preparation and distribution of materials, minutes and action lists),
- Implementing and maintaining the project infrastructure, e.g., the internal platform for information exchange and email lists, etc.
- Handling of legal issues, IPR issues and maintenance of the consortium agreement.
- Handling of the project correspondence and the day-to-day requests from partners and external bodies.

A quality assurance plan will prepared at the outset of the project, and will be maintained throughout the project. It will define the procedures to be used by all partners in order to ensure that all the project developments can be used with confidence. These procedures will be used to establish a common way of working and efficient channels of communication between partners.

Modern electronic means will be used to maintain rapid and efficient communication between the partners, including the use of project specific intranet, bulletin boards and e-mail. Partners will be encouraged to share progress and problems with other partners, to avoid the possibility of divergence of approach.
### Deliverables

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D0.1.n</td>
<td>Six-monthly management reports (n = 1 ... 6)</td>
</tr>
<tr>
<td>D0.2</td>
<td>Quality Assurance Plan</td>
</tr>
<tr>
<td>D0.3</td>
<td>Final report</td>
</tr>
<tr>
<td>D0.4</td>
<td>Interim Periodic Management Report</td>
</tr>
<tr>
<td>D0.5</td>
<td>Final Periodic Management Report</td>
</tr>
<tr>
<td>D0.6</td>
<td>Report on the distribution of the Community financial contribution between beneficiaries</td>
</tr>
</tbody>
</table>

### Milestones and expected results

-
## Work-package number

<table>
<thead>
<tr>
<th></th>
<th>WP1</th>
<th>Start date</th>
<th>M1</th>
</tr>
</thead>
</table>

## Work-package title

System foundations

## Participant ID

<table>
<thead>
<tr>
<th>ID</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
</table>

## Participant short name

<table>
<thead>
<tr>
<th>Name</th>
<th>ASTS</th>
<th>FTW</th>
<th>UNIFI</th>
<th>RT</th>
<th>ESL</th>
<th>PRO</th>
<th>IAD</th>
</tr>
</thead>
</table>

## Person-months per participant

<table>
<thead>
<tr>
<th>Month</th>
<th>12</th>
<th>5</th>
<th>9</th>
<th>6</th>
<th>2</th>
<th>8</th>
<th>4</th>
</tr>
</thead>
</table>

## Objectives

The objective of WP1 is to pose the foundations for the entire ALARP project by implementing:

- the risk analysis;
- the requirements specification;
- the design of the overall ALARP architecture.

## Description of work

### WP1.1 Risk analysis and requirements and scenarios specification

The risk analysis will be based on the following steps:

- definition of system boundaries,
- definition of risk criteria,
- hazards identification using HAZOP and/or FMEA,
- assessment of probabilities,
- assessment of consequences,
- assessment of risks
- assessment against criteria,
- risk reduction measure/ modification.

The risk analysis will serve as a source of requirements for the project, identifying the technical challenges, threats, and resilience requirements that will be addressed by the design, evaluation, and testing solutions and scenarios to be developed in the project.

### WP1.2 Design of the overall architecture

The main goal is to design the overall architecture of the ALARP system, which consists of a set of Train Presence Alert Device (the “sensors”) and a set of Mobile Terminals (the distributed mobile nodes, using the information provided by the sensors). In ALARP we will adopt a hybrid architecture, subdividing the system in two parts, one “simple and trusted” and one “complex”, having different sets of properties and relying on different sets of assumptions, namely in terms of faults and synchronism. This approach will allow to reconcile the needs for predictability and timeliness with the uncertainty of the environment, to improve reliability and availability despite the unreliability of the communication and of the system components, and to ensure secure and trustworthy operation in the presence of non-trusted parties.

## Deliverables

- D1.1 Risk analysis
- D1.2 Requirements specification
- D1.3 Overall architecture design (public version)
- D1.4 Overall architecture design

## Milestones and expected results

MIL1
Work-package number | WP2 | Start date | M4
---|---|---|---
Work-package title | Resilient wireless communication design
Participant ID | 1 | 2 | 3 | 4 | 5 | 6 | 7
Participant short name | ASTS | FTW | UNIFI | RT | ESL | PRO | IAD
Person-months per participant: | 4 | 22 | 6 | - | 2 | - | -

Objectives

This WP will design the architecture and develop the necessary communication protocols to achieve a timely and resilient inter-device communication between personal devices, track-side monitoring device, and (if present) remote mission control centre. The solutions will thereby use off-the-shelf wireless technologies, with protocol extensions mainly on Network and Transport Layer to achieve resilience and meet the timeliness and safety requirements of ALARP.

Description of work

The work will be performed in the following steps:

**WP2.1 Definition of the overall communication architecture**

WP2.1 will define the overall communication architecture and select off-the-shelf wireless technologies. This will be performed in close collaboration to the platform selection in WP3.2. In order to allow resilience, multiple interfaces with potentially different wireless technology are envisioned to be utilized. Furthermore, off-the-shelf protocols (e.g. IPsec or TLS) will be selected to meet security requirements.

**WP2.2 Development of adaptive protocols for enhanced resilience**

WP2.2 will develop the adaptive protocols for enhanced resilience to meet the safety and timing requirements of ALARP. The functionalities that will be considered include:

- Neighbour discovery mechanisms and (remote) monitoring of device connectivity and activity status.
- Algorithms and protocols to increase resilience via multi-homing
- Reliable Broadcast and multi-hop forwarding
- Architecture and protocols for safe management of context information

**WP2.3 Iterations on solution approaches**

Enhancements of the solutions taking into account the feedback from the evaluation through quantitative models and on early prototype versions. Furthermore, a feasibility study of more advanced concepts will be performed on two aspects

- to obtain information from the signalling system in a non-intrusive way (e.g. via eavesdropping GSM-R communication);
- general safe context management solutions, i.e. approaches to access, store, and pre-process general, extensible context information within a dynamic ad-hoc network as formed by the MTs.

Deliverables

D2.1 Resilient wireless communication architecture
D2.2 Preliminary wireless communication solution
D2.3 Final wireless communication solutions

Milestones and expected results

MIL2, MIL3, MIL4
Objectives

WP3 objective is to design the Mobile Terminal component, according to the following phases:

- design of the safe and resilient architecture and development of the resilient core and the middleware (WP3.1);
- selection of the COTS platform (WP3.2);
- design and development of the methodology for the self-localisation in harsh environments (WP3.3);
- design and development of the application logic (WP3.4);
- design of the ergonomics and development of the Human Machine Interface (WP3.5).

Envisioned safeguards to ensure privacy (limited storage of data, anonymisation of individual devices, turn-off options) will be included in the final devices and their activation will not be controllable by the employer.

Description of work

WP3.1 Safe and resilient architecture design and development

We will propose middleware solutions for enhancing resilience, availability and security in the wireless domain. The solutions, ranging from algorithms and higher layer protocols to actual services, have to accommodate a balanced harmonization among security/trustworthiness, availability/performance and reliability/safety aspects. For this reason we plan to apply principles like architectural hybridisation, which allow to painlessly enhancing a given original architecture, in its timeliness, security, quality of service, etc.

WP3.2 COTS platform selection

The COTS platform selection will be based on the architecture chosen for the MT subsystem. The main aspects that are to be defined by the Human Machine Interface and Ergonomics and will include mainly the MT position on the human body, display and interface mechanism and alert options. In addition to the above, we will define as part of the requirements additional factors as communication channels, applications and required resources (CPU, memory, operating system), usage time (power), GPS, IMU, size (accelerometers and gyro), weight, environmental requirements, and others.

WP3.3 Design and development of the self-localisation solution

This task will develop the enhanced positioning solutions in ALARP following these steps:

- Selection of suitable algorithms which act as baseline of the positioning methods. These are influenced by decisions of the wireless technologies that are used and platform choices
- Definition of a set of (stochastic) mobility models matching the different ALARP scenarios.
- Enhancements of the algorithm to achieve enhanced accuracy, timeliness, and accuracy bounds, using fusion of information from satellite systems, communication links, and movement sensors on the device.
- Development of the protocols for information exchange between devices for positioning purposes.
- Analysis of the accuracy, timeliness, and communication overhead of the solutions. Iteration on the mechanisms.

WP3.4 Application logic design and development

The application logic for the operation of alarms for the safety of line workers will be assessed and the level set by considering the results of the risk assessment and recommendation from human factor analysis. The analysis will be specific to a type of alarm incorporated into ALARP devices which could be based on visual, sound or vibration modes or combination of these. The application logic will be incorporated into the ALARP MT using a real-time expert system. The expert system will be able to operate in two modes of operation: a) training mode and b) operational mode.

In training mode the device will be used as a training tool in which the trainee will be able to study about
alarms level, the action to be taken including evacuation modes.
In the operational mode - monitoring scope, the expert system will operate in an advisory capacity. The system will be updated to assess any new site or incorporation of any new devices into an ALARP system.

WP3.5 Ergonomics and Human Machine Interface design and development
MT will be developed in four main steps from context analysis threw requirements and solution analysis until design evaluation. Basic ergonomic knowledge as well the knowledge to ergonomic design process will be applied. The human centred process involves iterating until the objectives will be satisfied. Different user groups will test MT Interface. MT will have ergonomic design and interface easy for different users.

The aim is to have wearable, wireless robust, context-aware, ergonomic, trustable and highly reliable MT to inform the user/worker about hazardous conditions during work.

Main functional characteristics of the MT component will be tested from ergonomic point of view: like abilities to generate alarm signal perceivable in complex environmental conditions (e.g. noise, vibration, darkness, raining or snowing) or to identify the position of workers and the direction of his movement in emergencies. Accordingly the multilingual and / or mimics interface of the MT will design using ergonomic principles in order to have interface suitable to be used in interoperable cross-border services. Important HMI functions will be realised: e.g. visualizing the processes, supporting the human understanding by providing adequate explanation and justification as well as avoiding or compensating for user errors.

The concept will be realised in four main steps from context analysis threw requirements and solution analysis until design evaluation. Ergonomic and HMI methodology as well the knowledge to ergonomic design process will be applied. Usability testing has been planned in lab. The human centred process involves iterating until the objectives will be satisfied.

Different user groups with different characteristics (e.g. age, nationalities, experiences) will test the MT in selected phases.

Deliverables

D3.1 MT architecture design
D3.2 Preliminary MT design
D3.3 Final MT design
D3.4 MT SW modules

Milestones and expected results

MIL2, MIL3, MIL4
<table>
<thead>
<tr>
<th>Work-package number</th>
<th>WP4</th>
<th>Start date</th>
<th>M4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work-package title</td>
<td>Train Presence Alert Device (TPAD) design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Participant ID</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Participant short name</td>
<td>ASTS</td>
<td>FTW</td>
<td>UNIFI</td>
</tr>
<tr>
<td>Person-months per participant:</td>
<td>6</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Objectives**

- Definition of the TPAD specific system requirements based on definitions of the overall ALARP system requirements (WP1)
- Perform a analytical hazard analysis in order to verify the performance of the virtual gate in all environments
- Design of the overall TPAD detailed system architecture
- Development of the TPAD subunits including COTS sensors, central processing and storage unit, power, display and UI, housing, and COTS wireless communication (as defined in WP2)
- Development of TPAD application software and firmware

**Description of work**

**WP4.1 TPAD System Requirement Definition**

The TPAD System Requirement Definition will be based on the overall ALARP system requirements. In addition, the requirement definitions will be based on inputs from the hazard analysis (WP4.2), resilient wireless communication design (WP2), and the MT Design (WP3).

**WP4.2 TPAD Analytical Hazard Analysis**

In any development and especially when developing a safety system it is crucial that we analyze its performance during the architecture definition stages. In WP4.2 we are going to analytically verify that performance of key parameters including the TPAD’s detection capability (probability/false alarm rates) in all weather conditions and in various scenarios (noisy environment, multiple train passes, etc.), communication and latency, power analysis, sub-unit critical failures (including BIT), SW malfunctions.

**WP4.3 TPAD Detailed Architecture Design**

After definition of the TPAD system requirements (WP4.1), performing the hazard analysis (WP4.2), and passing the System Requirements Review gate we will continue to the TPAD detailed architecture design stage. Within this work package we will define the overall TPAD architecture and its sub-units including the sensor units (Day CMOS camera, uncooled FLIR, and acoustic sensors), the central processing unit (including the storage unit), the display and control unit, communication unit (derived from WP2), and power unit. The interfaces between modules will also be defined within this sub WP. Moreover, the SW architecture will also be defined and will include the detection algorithms, communication, three BIT modes, power management, video compression, user interface, and setup mode. WP4.3 will conclude with a Design Review that will define the TPAD Architecture Design.

**WP4.4 HW Units Development**

This WP will materialize the development process and build the HW sub-units. The inputs of this WP are the detailed design WP4.3. This development effort of the TPAD sub-units will include COTS sensors (CMOS day sensor, uncooled FLIR, and acoustic), central processing and storage unit, power unit, display and UI unit, mechanical housing, and COTS wireless communication (as defined in WP2).

**WP4.5 SW Application Development**

The SW layers will be coded and tested within this WP. The application SW will be hosted within a FPGA HW module if an embedded solution is selected or as an executable file if an operating based HW. The algorithm development methodology will be based on Matlab (or similar) coding, later transferred to higher coding language (C, C++, other). Other SW packages will be coded and simulated separately before being simulated as a full SW package. The final stage includes the integration with the targeted HW host. The main SW modules will include the detection algorithms, communication, three BIT modes, power management, video compression, user interface, and setup mode.
<table>
<thead>
<tr>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>D4.1    TPAD architecture design</td>
</tr>
<tr>
<td>D4.2    Preliminary TPAD design</td>
</tr>
<tr>
<td>D4.3    Final TPAD design</td>
</tr>
<tr>
<td>D4.4    TPAD HW units and application SW</td>
</tr>
</tbody>
</table>

**Milestones and expected results**

MIL2, MIL3, MIL4
**Objective**

- Definition of the MT integration process and success criteria
- MT sub-modules integration and testing
- Definition of the TPAD integration process and success criteria
- TPAD sub-modules integration and testing
- Full ALARP system integration definition process and success criteria
- Full ALARP system integration and testing

## Description of work

### WP5.1 MT integration

The MT integration effort will include MT integration and test plan definition, actual integration and testing, and additional system fixes (if required).

The MT integration effort will include among others:

- Hardware-Software Integration – which will checkout the integrity of the safe resilient middleware and algorithms and verify proper functionality. In addition we will checkout the functionality of the higher level applications including the Application Logic: Training and Operational Modes, User Interface, Situational Awareness Program, MT/TPAD communication software, and others
- Self Localisation – The self localization system provides the positioning data of each and every one of the MTs and TPADs. In addition, it also verifies that the user is "alive" i.e. moving with the MT. The integration effort will verify the functionality both outdoor and indoor and also in poor weather environments.
- Wireless Communication - During the MT integration phase we will verify proper functionality of the Wireless Communication Link, including neighbour discovery and remote device monitoring, multi-hop forwarding, and data authentication / security protocols.
- Human Machine Interface - This effort will include integration and testing of the various modes of operation on the user on the correct position of the MT. This will include initial tests that will verify proper ability to function with the system thus minimizing disturbance to the ongoing site activities. Further and more enhanced testing will be done in WP6 (evaluation phase).
- During the MT integration phase we will verify the functionality of the entire unit in different environmental situations including various temperature ranges, humidity, random vibration, and shock. In addition we will test the power management scheme and verify that it meets the MTs requirement specifications.

### WP5.2 TPAD integration

This effort will verify that the developed architecture of the TPAD are properly harmonized and that the overall functionality meets the requirements. This effort follows an initial TPAD integration task (within WP 4.4 and WP4.5) but will actually cover a more comprehensive system integration and acceptance tests prior to the actual field tests in WP6. This sub WP will include:

- Sensors Integration (day, FLIR, acoustic) - verifying the interface channel between the three sensors and the Central Processing and Storage Unit. During the integration we will verify the sensors performance, the readout mechanisms, latency, synchronization, throughput, and more.
- Wireless Communication - The chosen wireless communication module (WP2) will be integrated into the TPAD system through a dedicated interface with the Central Processing unit. Among the important tasks of the integration is to verify EMI-wise that the communication channel does not affect the functionality of the overall system, especially the sensors.
- Central Processing and Storage Unit - Is the heart of the system and actually hosts the
software/firmware that drives the system. The integration effort will initially verify that all the interfaces between the other sub-models and the central processing and storage unit function properly. Afterwards we will start loading the applications one by one, starting with the basic functions, thus verifying performances of all the unit including functionality, resources, power, and other. The SW applications will include the detection, communication, BIT, power management, video compression, UI, Setup applications.

- Display Unit - Similar to the sensor integration we will verify the interface between the display and the central processing and storage unit. This will include the display interface and the controls i.e. touch screen or near screen push-buttons.
- Power Unit - The power unit interface will verify the power sub-model HW including DC to DC regulators, power safety, interfaces to the secondary battery and to all the other sub-models.

WP 5.3 will be responsible for integrating the whole ALARP system. This effort will follow the successful completion of WP 5.1 and WP 5.2 (Integration of MT and TPAD accordingly). The system integration effort will concentrate on the connectivity and functionality of the whole system both between multiple MTs and between MTs and TPAD(s).

### Deliverables

<table>
<thead>
<tr>
<th>D5.1</th>
<th>MT integration procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>D5.2</td>
<td>MT prototype</td>
</tr>
<tr>
<td>D5.3</td>
<td>TPAD integration procedure</td>
</tr>
<tr>
<td>D5.4</td>
<td>TPAD prototype</td>
</tr>
<tr>
<td>D5.5</td>
<td>ALARP System Integration Procedure</td>
</tr>
<tr>
<td>D5.6</td>
<td>ALARP PH2 integrated prototype</td>
</tr>
<tr>
<td>D5.7</td>
<td>ALARP PH3 integrated prototype</td>
</tr>
<tr>
<td>D5.8</td>
<td>ALARP System Integration Report</td>
</tr>
</tbody>
</table>

### Milestones and expected results

MIL2, MIL3, MIL4
Objectives

Objectives of WP6 are to thoroughly model, verify, validate and evaluate ALARP project results during the entire project's life.

Description of work

WP6.1 Quantitative modelling
In this task we will first of all identify the appropriate modeling construction and solution approaches capable to address the significant challenges raising from the ALARP characteristics, like the varying operational conditions (e.g., in terms of involved users and available wireless connections) and the presence of both accidental and malicious faults.

Then, the following research activities will be investigated: i) quantitative model-based evaluations for early validation of components, mechanisms and design of the overall architecture; ii) modeling as support for experimentation and iii) experimentation as a support for modeling.

WP6.2 Verification and validation
Verification and Validation activities performed in WP5.2 will be highly integrated with the design and implementation processes; V&V will be practiced over the entire system life cycle. We will develop early in the project a V&V plan that will guide these processes. The requirements will be early defined in order to plan as soon as possible verification and validation activities and to guarantee traceability of the requirements in the project. In the task we firstly will develop a first V&V Plan, that will describe approaches and methods for single components verification, integration verification, qualification testing, and overall system verification. V&V techniques that we plan to use in ALARP include: dynamic testing, measurement techniques, dependability analysis and hazard analysis.

WP6.3 Testing and evaluation
Testing and evaluation will be carried out according to the following phases:

- A first phase (PH1) that will be carried out in laboratory, to test and evaluate the single ALARP components in a controlled environment.
- A second phase (PH2) that will be carried out in the field (most likely in one of the ASTS installations) to test and evaluate the basic functionalities of the integrated ALARP system.
- Finally, a third phase (PH3) in which the entire ALARP system will be tested and evaluated in the field against requirements covering all planned characteristics.

WP6.4 Final assessment and guidelines
The final assessment will assess and consolidate the results of PH3 tests. Then guidelines on how to utilize the new technical solutions, the modelling, verification, validation and evaluation methodologies and the proof-of-concept framework will be prepared.

Deliverables

D6.1 Quantitative modelling of ALARP solutions
D6.2 Verification and Validation Plan
D6.3 PH1 testing and evaluation report
D6.4 PH2 testing and evaluation report
D6.5 PH3 testing and evaluation report
D6.6 Final assessment and guidelines
<table>
<thead>
<tr>
<th>Milestones and expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL2, MIL3, MIL4</td>
</tr>
</tbody>
</table>
**Work-package number**: WP7  
**Start date**: M1

<table>
<thead>
<tr>
<th>Participant ID</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant short name</td>
<td>ASTS</td>
<td>FTW</td>
<td>UNIFI</td>
<td>RT</td>
<td>ESL</td>
<td>PRO</td>
<td>IAD</td>
</tr>
<tr>
<td>Person-months per participant:</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

**Objectives**

Dissemination and exploitation of experience, results, and IPRs gained in ALARP

**Description of work**

**WP7.1 Dissemination**  
The dissemination task will include the following activities:

- A plan for dissemination of ALARP results will be prepared at the start of the project to decide which strategies are most likely to be effective considering the peculiarities of the railway workers safety market.
- Preparation of dissemination material (leaflets, newsletters, etc.) including a demonstration disk that will include the presentation information prepared for the project and a demo of the main characteristics of the ALARP approach.
- Set-up, population and maintenance of the project web site.
- A budget is included to allow team members to attend conferences at which they will be able either formally or informally to promote the ALARP results.

**WP7.2 Exploitation**  
The exploitation task will include the following activities:

- Analysis of the railway workers safety market and of potential spin-off markets for the methodologies and approaches that are considered in ALARP.
- Preparation of an exploitation plan that will be revised and updated at months M12 and M24 to provide a guide for future exploitation of ALARP and related methodologies and approaches.

**Deliverables**

D7.1.n Periodic dissemination and exploitation plans  
D7.2 Collection of the dissemination material

**Milestones and expected results**

-
### B1.3.6 Efforts for the full duration of the project

#### B1.3.6.1 Indicative efforts per beneficiary per WP

<table>
<thead>
<tr>
<th>Beneficiary no</th>
<th>Beneficiary short name</th>
<th>WP0</th>
<th>WP1</th>
<th>WP2</th>
<th>WP3</th>
<th>WP4</th>
<th>WP5</th>
<th>WP6</th>
<th>WP7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ASTS</td>
<td>20</td>
<td>12</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>9</td>
<td>10</td>
<td>4</td>
<td>74</td>
</tr>
<tr>
<td>2</td>
<td>FTW</td>
<td>-</td>
<td>5</td>
<td>22</td>
<td>12</td>
<td>-</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>57</td>
</tr>
<tr>
<td>3</td>
<td>UNIFI</td>
<td>-</td>
<td>9</td>
<td>6</td>
<td>18</td>
<td>-</td>
<td>4</td>
<td>10</td>
<td>2</td>
<td>49</td>
</tr>
<tr>
<td>4</td>
<td>RT</td>
<td>-</td>
<td>6</td>
<td>-</td>
<td>12</td>
<td>6</td>
<td>12</td>
<td>18</td>
<td>2</td>
<td>56</td>
</tr>
<tr>
<td>5</td>
<td>ESL</td>
<td>-</td>
<td>2</td>
<td>2</td>
<td>12</td>
<td>40</td>
<td>35</td>
<td>5</td>
<td>2</td>
<td>98</td>
</tr>
<tr>
<td>6</td>
<td>PRO</td>
<td>-</td>
<td>8</td>
<td>-</td>
<td>18</td>
<td>-</td>
<td>-</td>
<td>8</td>
<td>2</td>
<td>36</td>
</tr>
<tr>
<td>7</td>
<td>IAD</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>18</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>1</td>
<td>26</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td></td>
<td>20</td>
<td>46</td>
<td>34</td>
<td>96</td>
<td>52</td>
<td>70</td>
<td>60</td>
<td>15</td>
<td>393</td>
</tr>
</tbody>
</table>

Table 6 - Indicative effort per beneficiary per WP

#### B1.3.6.2 Indicative efforts per activity type per beneficiary

<table>
<thead>
<tr>
<th>Activity type</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASTS</td>
<td>20</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>20</td>
</tr>
<tr>
<td>FTW</td>
<td>5</td>
<td>22</td>
<td>6</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>34</td>
</tr>
<tr>
<td>UNIFI</td>
<td>12</td>
<td>18</td>
<td>18</td>
<td>12</td>
<td>18</td>
<td>18</td>
<td>96</td>
<td>373</td>
</tr>
<tr>
<td>RT</td>
<td>6</td>
<td>-</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>15</td>
<td>373</td>
</tr>
<tr>
<td>ESL</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>12</td>
<td>35</td>
<td>-</td>
<td>-</td>
<td>70</td>
</tr>
<tr>
<td>PRO</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>373</td>
</tr>
<tr>
<td>IAD</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>15</td>
</tr>
</tbody>
</table>

Table 7 - Indicative effort per activity type per beneficiary
B1.3.6.3  INDICATIVE DISTRIBUTION PER BENEFICIARY PER TASK

<table>
<thead>
<tr>
<th>WP</th>
<th>Project management</th>
<th>ASTS</th>
<th>FTW</th>
<th>UNIFI</th>
<th>RT</th>
<th>ESL</th>
<th>PRO</th>
<th>IAD</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP0</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>20</td>
</tr>
</tbody>
</table>

| WP1 | System foundations | 12   | 5   | 9     | 6  | 2   | 8   | 4   | 46    |
| WP1.1 Risk analysis and requirements specifications | 3    | 2   | 3   | 3   | 1   | 5   | 2   | 19    |
| WP1.2 Design of the overall architecture | 9    | 3   | 6   | 3   | 1   | 3   | 2   | 27    |

| WP2 | Resilient wireless architecture design | 4    | 22  | 6     | 0  | 2   | 0   | 0   | 34    |
| WP2.1 Definition of the overall communication architecture | 2    | 6   | 2   | 0   | 0.5 | 0   | 0   | 10.5  |
| WP2.2 Development adaptive protocols for enhanced resilience | 0    | 10  | 3   | 0   | 1   | 0   | 0   | 14    |
| WP2.3 Iterations on solution approaches | 2    | 6   | 1   | 0   | 0.5 | 0   | 0   | 9.5   |

| WP3 | MT design | 6    | 12  | 18    | 12 | 12  | 18  | 12  | 96    |
| WP3.1 Safe and resilient architecture design | 2    | 2   | 12  | 10  | 0.5 | 2   | 1   | 29.5  |
| WP3.2 COTS platform selection | 1    | 0   | 1   | 2   | 0.5 | 2   | 1   | 7.5   |
| WP3.3 Design of the self-localisation solution | 0    | 10  | 3   | 0   | 2   | 0   | 1   | 16    |
| WP3.4 Application logic design | 1    | 0   | 1   | 0   | 4   | 12  | 2   | 20    |
| WP3.5 Ergonomics and Human Machine Interface design | 2    | 0   | 1   | 0   | 5   | 2   | 13  | 23    |

| WP4 | TPAD design | 6    | 0   | 0     | 6  | 40  | 0   | 0   | 52    |
| WP4.1 TPAD system requirement definition | 1    | 0   | 0   | 2   | 3   | 0   | 0   | 6     |
| WP4.2 TPAD analytical hazard analysis | 1    | 0   | 0   | 2   | 3   | 0   | 0   | 6     |
| WP4.3 TPAD detailed architecture design | 2    | 0   | 0   | 2   | 7   | 0   | 1   | 11    |
| WP4.4 HW units development | 1    | 0   | 0   | 0   | 11  | 0   | 0   | 12    |
| WP4.5 SW application development | 1    | 0   | 0   | 0   | 16  | 0   | 0   | 17    |

| WP5 | Integration and proof-of-concept | 9    | 10  | 4     | 12 | 35  | 0   | 0   | 70    |
| WP5.1 MT integration | 0    | 7   | 2   | 4   | 10  | 0   | 0   | 23    |
| WP5.2 TPAD integration | 0    | 0   | 0   | 2   | 15  | 0   | 0   | 17    |
| WP5.3 System integration and proof-of-concept implementation | 9    | 3   | 2   | 6   | 10  | 0   | 0   | 30    |

| WP6 | Modelling, verification, validation and evaluation | 10   | 6   | 10    | 18 | 5   | 8   | 3   | 60    |
| WP6.1 Quantitative modelling | 0    | 5   | 8   | 0   | 1   | 1   | 1   | 16    |
| WP6.2 Verification and validation | 2    | 0   | 0   | 9   | 0.5 | 2   | 0   | 13.5  |
| WP6.3 Testing and evaluation | 6    | 0   | 0   | 3   | 1.5 | 4   | 1   | 15.5  |
| WP6.4 Final assessment and guidelines | 2    | 1   | 2   | 6   | 2   | 1   | 1   | 15    |

| WP7 | Dissemination and exploitation | 4    | 2   | 2     | 2  | 2   | 2   | 1   | 15    |
| WP7.1 Dissemination | 2    | 2   | 1   | 1   | 1   | 1   | 1   | 9     |
| WP7.2 Exploitation | 2    | 0   | 1   | 1   | 1   | 0   | 0   | 6     |

Table 8 - Indicative distribution per beneficiary per task

B1.3.7  List of milestones and planning of reviews

B1.3.7.1  LIST OF MILESTONES

<table>
<thead>
<tr>
<th>Milestone No</th>
<th>Milestone name</th>
<th>WPs involved</th>
<th>Delivery date</th>
<th>Deliverables included</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL1</td>
<td>System foundations. The project has completed the risk analysis, defined all the requirements and constraints to be considered for the ALARP system and the overall system architecture and has therefore completed the basis for the scientific and technical development.</td>
<td>WP1</td>
<td>M9</td>
<td>D1.1, D1.2, D1.3</td>
</tr>
<tr>
<td>MIL2</td>
<td>Phase 1 (PH1) prototypes. The project has completed the design and the first stage integration of the TPAD and MT prototypes. These components will start to be tested in PH1 testing phase</td>
<td>WP2, WP3, WP4, WP5, WP6</td>
<td>M18</td>
<td>D2.2, D3.2, D4.2, D5.1, D5.2, D5.3, D5.4, D6.2</td>
</tr>
</tbody>
</table>
### Table 9 - Milestones list

<table>
<thead>
<tr>
<th>Milestone No</th>
<th>Milestone name</th>
<th>WPs involved</th>
<th>Delivery date</th>
<th>Deliverables included</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL3</td>
<td>Phase 2 (PH2) prototypes. The project has completed the test of the single components in PH1, has used the experience gained to tune and modify the prototypes and has produced the first integrated ALARP prototype to be tested in PH2 testing phase.</td>
<td>WP2, WP3, WP4, WP5, WP6</td>
<td>M24</td>
<td>D5.5, D5.6, D6.1, D6.3</td>
</tr>
<tr>
<td>MIL4</td>
<td>Phase 3 (PH3) prototypes. The project has completed the test of the first integrated ALARP prototype in PH1, has used the experience gained to tune and modify the TPAD and MT prototypes and has produced the final integrated prototype to be tested in PH3 testing phase.</td>
<td>WP2, WP3, WP4, WP5, WP6</td>
<td>M30</td>
<td>D5.7, D6.4</td>
</tr>
</tbody>
</table>

### B1.3.7.2 PLANNING OF REVIEWS

<table>
<thead>
<tr>
<th>Review No</th>
<th>Tentative timing</th>
<th>Planned venue</th>
<th>Comments (if any)</th>
</tr>
</thead>
<tbody>
<tr>
<td>REV1</td>
<td>M18</td>
<td>ASTS premises</td>
<td>The review is aimed at verifying if the project is on rail, using the completed System Foundations (MIL1) as well as the design and the first stage integration of the TPAD and MT prototypes (MIL2).</td>
</tr>
<tr>
<td>REV2</td>
<td>M36</td>
<td>ELBIT premises</td>
<td>The review is aimed at verifying the achievements of the project.</td>
</tr>
</tbody>
</table>

### Table 10 - List of review
B2 IMPLEMENTATION

B2.1 MANAGEMENT STRUCTURE AND PROCEDURES

B2.1.1 Introduction

The proposed project management structure has been already adopted and consolidated by Ansaldo STS in many projects of similar size and has always led to a successful completion of the projects. Moreover, this approach has been already shared and agreed with many of the ALARP partners in previous successful projects.

B2.1.2 The project management structure

Due to the small size of the consortium, the project management structure is kept as simple and effective as possible, yet following best practices and methodologies in R&D consortium management. The management of the project is structured as follows:

- an Executive Board (EB);
- a Project Manager (PM);
- an Administrative Coordinator (AC).

The Project will be supervised by an *Executive Board (EB)* that has full executive responsibility for the project. Membership of the Executive Board will consist of one senior representative for each partner of the Consortium (*Team Leader*), though other individuals may be co-opted as appropriate. In any case, only one member per partner will take part in EB decisions. The Team Leader is a person with the authority of making decisions on behalf of her/his organization and is responsible for the technical management of the partner’s activity in the project. The Executive Board will be responsible for the overall conducting of the project, setting overall goals, co-ordinating and reviewing progress, revising the project plan as necessary, and ensuring the timeliness and quality of the deliverables.

The ALARP project will be coordinated by Mr. Vito Siciliano, *Project Manager (PM)*, from ASTS. He is in charge of project management, and this includes day-to-day management of the project evolution and monitoring of technical progress with respect to the work plan, co-ordination of project resources, control of dependencies among work packages, production and distribution of meeting minutes, approval and distribution of deliverables. The PM will be assisted by an *Administrative Coordinator (AC)*, from ASTS. The Administrative Coordinator is the contract manager responsible for the administrative aspects of the Project, and has primary responsibility for managing the budget, supporting the project committees, maintaining an information service, assisting the PM in the above-mentioned tasks.

The Project Manager is the single point of interface with the European Commission. In this function he shall in particular perform the following tasks:

(a) manage the signature of the Contract with the European Commission;

(b) collect from all Parties the cost and other statements for submission to the European Commission;

(c) prepare the reports and project documents required by the European Commission;

(d) ensure delivery of all the items identified as deliverable items in the Contract or requested by the European Commission for reviews and audits;

(e) manage the transfer of sums allocated among the Contractors as per the budget agreed and keep related records;

(f) set up a mechanism to assure the quality of the project.

In order to ensure the timely progress of the work, each work package is assigned a responsible partner that appoints a *Work-Package (WP) Leader*. The WP Leader, in cooperation with the partners involved in the WP, sees to it that each task is assigned a responsible partner.
It is the responsibility of the WP Leader that the tasks progress according to the schedule defined for the project, and that the needed co-ordination with other work packages is carried out. The progress of the work package is monitored by the WP Leader with respect to the defined goals of each task and the schedule of Milestones. Any deviation from the schedule shall be reported to the Executive Board and the Project Manager.

This management structure is aimed at ensuring and controlling the quality of the project.

**B2.1.3 Meetings**

The Executive Board will meet regularly, at least twice per year, either in person (typically on the occasion of Project plenary meetings), or by teleconference. Additional meetings will be called as and when necessary.

**B2.1.4 Conflict resolution**

The Project Manager is in charge of driving the possible conflicts arising on technical issues towards solutions which are of benefit for the Consortium and which aim at the successful completion of the project, involving the Executive Board as appropriate for the concerned issues. A disagreeing contractor has, however, the right of appeal to the Executive Board.

In normal operation, conflicts will be resolved in discussions at the appropriate work package level or, in case of non-technical matters, by the Project Manager.

Where a conflict is not amenable to solution through such discussions, the matter will be raised at the next scheduled Executive Board meeting or, if requested by any partner, at a specially convened meeting. Any conflict that is amenable to resolution through discussion in the Executive Board will be resolved by means of a majority voting. Each of the partners of the project will be eligible to cast a single vote. The decisions of the Executive Board, whether taken by discussion or voting, will be binding on all partners of the project.

**B2.1.5 Quality Assurance (QA)**

The project management system will be defined in a Quality Assurance (QA) Plan which will be the top tier document for project management purposes following the ISO 9001 criteria. This QA Plan will be supported by a Project Standards Document and Project Procedures. The QA Plan will set out the organisation for project management and define the key criteria for planning and control of the technical work, the budget and the programme.

The Project Standards document will define the relevant standards which all work done on the project must satisfy. As the project progresses and the specifications become more clearly defined, the Project Standards document will be reviewed and updated as necessary.

There will be a number of Project Procedures setting out the arrangements for controlling the project and ensuring good communications, co-operations and understanding between the partners.

Project progress will be monitored and reviewed against the timely delivery of the project deliverables to an acceptable quality, and also against the indicators of success.

**B2.1.6 Communication Strategy**

Documents received from the Commission or other projects will be circulated as appropriate. For all matters within the scope of the Project, there will be no limitations on the flow of information among partners.

The participants (partners, Executive Board, and Project Manager) will communicate using electronic means, such as electronic mail, e-mail archives, document repositories, web servers, audio and video conferences. In particular, the Consortium will make extensive use of the open web portal to exchange all the information related to ALARP activities.

**B2.1.7 Project risk management**

Most of the risks in running the Project activities have been eliminated by:
• building a balanced consortium, where: there are no unnecessary redundancies; partners complement each other in know-how; the union of partners’ know-how covers all of the fields to be researched;

• establishing a Consortium Agreement to be agreed by all Partners in order to avoid any conflict.

• creating a realistic schedule for producing tangible results, like deliverables and milestones.

Technical risks (see section B1.3.1.7B1.3.1.7) are minimised by the expertise of partners. Any of the partners have a previous record of prototypes, systems and publications that demonstrate their high qualification and their aptitude to work at international level, in a cooperative way. The fact that the key personnel from partners have an already extensive track record of successful participations in previous EU funded projects also decreases the risk inherent to international consortia.

An approach to formally identify, assess, and mitigate residual technical risks throughout the life of the program is chosen. Risks will be actively monitored, ranked (from 1 - high to 5 - low) and reported. For all identified risks, efficient contingency plans (resource reallocation, fall-back, contingency measures) will be implemented immediately at the appropriate work package level or at the level of the Executive Board.

**B2.2 BENEFICIARIES**

**B2.2.1 ANSALDO STS S.p.A. (ASTS)**

**B2.2.1.1 BRIEF DESCRIPTION OF THE ORGANIZATION**

ANSALDO STS is the leading technology group operating in the railway and underground transportation sector. In particular, it controls Ansaldo Signal N.V., a Dutch holding company which is the largest of a group of companies operating in the field of railway and underground signalling as well as Ansaldo Trasporti-Sistemi Ferroviari S.p.A., an Italian company, expert in IT systems integration in the area of "turnkey" railway and underground transport systems.

The activities of the ANSALDO STS Group are organized into two business units:

• the **Signalling Unit** which works in design, realization, management and maintenance of systems, subsystems and components for signalling and monitoring railway and subway traffic systems, aimed at increasing the safety and efficiency of railway and underground transport systems

• the **Transport System Unit** which operates in the design, realization, installation, integration, management and maintenance of "turnkey" railway and underground transport systems among which signalling systems are an essential part

The Ansaldo STS Group designs, produces, distributes and manages systems and components for signalling and monitoring railways and underground transit systems. Concerning underground transit systems, Ansaldo provides both traditional and automatic driverless networks with signalling systems, while in the area of railway transit systems the group's signalling systems range from conventional to high-speed networks.

The Group's head office is in Genova, and Ansaldo STS has company branches located in 18 countries with over 3,600 employees. In 2005, the group realized profits amounting to 840 million Euros with a gross operating margin of 89 million Euros and a net profit of 44 million Euros.

**B2.2.1.2 MAIN TASK(S) IN THE PROJECT**

ASTS’s role in ALARP will be:

• project coordinator and therefore leader of WP0;

• leader of WP1 to coordinate the definition of the system foundations;
- participation in WP2 to contribute to the definition of the overall communication architecture (WP2.1) and to the iterations on solution approaches (WP2.3);
- participation in WP3 to contribute to the MT design with particular emphasis on the COTS platform selection, the application logic design and the ergonomics and HMI design;
- participation in WP4 to mainly contribute to the TPAD system requirements definition (WP4.1) and the analytical hazard analysis (WP4.2);
- participation in WP5 to mainly contribute to proof-of-concept implementation (WP5.3);
- participation in WP6 to mainly contribute to the testing and evaluation (WP6.3) and the final assessment (WP6.4) tasks;
- leader of WP7 to manage the knowledge dissemination and the IPRs (WP7.1) and to drive the exploitation strategy (WP7.2).

B2.2.1.3 SHORT PROFILE(S) OF THE STAFF MEMBERS

Mr. Vito Siciliano
He will steer the ALARP project and coordinate the technical contribution of its company. He has more than ten years of experience in R&D and system engineering on transportation systems of the company. He has been the project leader of the Project TRIPS “Transport Infrastructure Protection System” (DG ENT - PASR).

Ms. Nadia Mazzino
Laurea degree in mathematics. In ASTS group since 1993, she has been working in signaling and railway control automation and she is now responsible for design and development projects in the Business Innovation Unit.

B2.2.2 Forschungszentrum Telekommunikation Wien (FTW)

B2.2.2.1 BRIEF DESCRIPTION OF THE ORGANIZATION

The Telecommunications Research Center Vienna (FTW) is the joint research centre of leading players in telecom business and science in Austria, including major telecom equipment manufacturers, network operators, and the Universities of Technology in Vienna and Graz.

Established in 1998 within the Austrian government’s Kplus Competence Centres Program, FTW conducts co-operative research in the following core research areas:

- Signal & Information Processing,
- Packet Networking,
- Networked Services & Distributed Systems,
- Digital Content & User Interaction,
- Security & Privacy.

The research group of FTW is an international and multi-disciplinary team of more than 60 full-time researchers. Research work is supported by appropriate organizational structures and an efficient management and administration team.

FTW has strong experience in managing multi-lateral collaboration and a significant track record of participation in European co-operation projects. This includes FP5 projects (Moby Dick, M3I, FLOWS, HIMM, and INCA), FP6 projects (TARGET, E-Next, NEWCOM, MAGNET-Beyond, MASCOT, and CRUISE), CELTIC/Eureka project BANITS2, and COST actions (273, 278, and 279, and recently IS0605) ) and the FP7 STREPS PRISM and mCIUDAD. In addition to European
projects, strong expertise on network monitoring and routing has been built up in previous close collaborations in industrial projects with Austrian operators.

B2.2.2.2 MAIN TASK(S) IN THE PROJECT

FTW role in the project will be:

- WP leader and strongest contributor of WP2
- contributions to the architecture definition in WP1
- development of localization solutions in WP3
- contribution to the integration of the resilient communication system into the MT (WP51.), the TPAD (WP5.2) and the overall ALARP system (WP5.2)
- contribution to the modelling (WP6.1), verification, validation (WP6.2) and testing WP6.3) of the resilient communication solution
- dissemination of projects results (WP7)

B2.2.2.3 SHORT PROFILE(S) OF THE STAFF MEMBERS

Hans-Peter Schwefel is coordinating the ‘Networked Services’ Research Area at FTW. The Area currently consists of 9 research staff members, and is actively involved in several FP6 and FP7 research projects. Core research goals of the group are middleware and communication solutions for future context-sensitive, intelligent applications with particular interest in Intelligent Transport Systems. In addition, Hans is Associate Professor and leading the research group at Aalborg University/CTIF that focuses on network architectures, communication protocols and evaluation methodologies for future IP-based wireless networks. He is actively involved in research and coordination activities for several projects in that area, including the coordination of the EU FP6 STREP HIDENETS, in which end-to-end dependability solutions for mobile services in car-to-car and car-to-infrastructure scenarios are being developed, as well as the EU FP6 projects SafeDMI and MAGNET, in which safe communication solutions for railway transport systems and context-aware communication architectures for Personal Networks are developed. He is also leading several industrial cooperation including in particular projects on Quality of Service and Mobility Support in future mobile networks. Hans has a strong background in coordination of research activities, also in industrial environments, since he was coordinating external research cooperation at Siemens Mobile Networks before he joined Aalborg University. These research cooperations were directed at innovative technological concepts for future mobile networks. While working at Siemens he obtained extensive training on modern industrial management and leadership methods as part of a special management preparation program. Hans obtained his doctoral degree (Dr. rer. nat.) in the area of IP traffic and performance modelling from the Technical University in Munich, Germany. For his research activities, he also spent extended periods of time at the University of Connecticut, USA, and at AT&T Labs, USA, and, more recently, at University of Florence and CNR-ISTI in Pisa, Italy.

Slobodanka Tomic received her Ph.D. degree in Electrical and Computer Engineering from the Vienna University of Technology (TU Wien), Austria. Since 2005 Mrs. Tomic is with The Telecommunications Research Centre Vienna (FTW), where she works on topics dealing with the service and communication aspects of NGN networks, including wireless ad-hoc and sensor networks and vehicular scenarios. Previous to that, Ms. Tomic was working with the industry and at the TU Wien, in several research projects. Within nationally funded research project “AD-HOC Networks” (2002-2004) she was working on energy efficient protocols for ad-hoc and sensor networks*. Within FP6 Project CRUISE (2006-2007) (Creating Ubiquitous Sensing Environments, NoE on Communication and Application Aspects of wireless sensor networks) she was contributing to topics including topology control and re-configuration in IEEE 802.15.4/Zig-Bee networks, mobility aspects of wireless sensor networks, opportunistic ad-hoc routing, data-aggregation concepts, and inter-working architectures.
B2.2.3 Università degli Studi di Firenze (UNIFI)

B2.2.3.1 **BRIEF DESCRIPTION OF THE ORGANIZATION**

The Università degli studi di Firenze (UNIFI) is a University with approximately 25,000 students, and research activities in several domains, from engineering to human sciences, natural sciences, architectures, medicine and computer science. The Resilient Computing Lab (RCL) research group at the Dept. of “Sistemi e Informatica” (Systems and Informatics) has its main research focus in research and experimentation of dependable architectures and systems. The group is currently involved in research spanning two areas: i) Architectures and Techniques for Resilient Systems and Infrastructures, and ii) Quantitative Dependability and QoS Evaluation. Members of the group have been involved in many cooperative projects: ESPRIT BRA PDCS and PDCS-2, the 20716 GUARDS RTD, the ESPRIT LTR 27439 HIDE and the IST-2001-38229 CAUTION++. RCL is currently involved in the following European projects: FP6-IST-STREP-26979 HIDENETS, FP6-IST-STREP-027513 CRUTIAL, FP6-SUSTDEV-STREP-031413 SAFEDMI, in the FP6-IST-026764 RESIST Network of Excellence and in the FP7-ICT-216295 AMBER Coordination Action. Contributions made are on fault tolerance (design and validation), evaluation of ultra-high dependability and real-time, the identification and definition of fault tolerance mechanisms, dependability modelling and evaluation of complex systems, issues of validation of systems designed using UML. Further experience has been gained through interaction with industries.

The Resilient Computing Lab (RCL) has previous deep experience in the in design and architecture area, with a rich expertise in the development of dependable architectures for distributed and real-time critical systems. People of the group worked on this area in several European projects, like FP6-IST-STREP-26979 HIDENETS, FP6-IST-STREP-027513 CRUTIAL and IST-2001-38229 CAUTION++.

In addition, the RCL has previous experience in the field of assessment and measurement of dependability attributes of critical systems. Among others, it has contributed and taken the leadership of the evaluation-related work packages of many European projects (UNIFI is currently leader of the WP on evaluations in FP6-IST-STREP-26979 HIDENETS). Its experience spans from analytical models to experimental evaluations and their mutual relationships. Moreover, it has recently started an activity for understanding metrology principles applied to the measurement, evaluation and assessment of computer performance and dependability.

B2.2.3.2 **MAIN TASK(S) IN THE PROJECT**

UNIFI’s role in ALARP will be:

- Leadership in WP3, to propose middleware solutions for enhancing resilience, availability and security in the wireless domain. Besides the WP3 coordinator’s role, UNIFI will contribute in the definition of consistency mechanisms, through a work on timing abstractions, and resilience mechanisms, with investigation on a framework for diagnosis activities.

- Participation in WP1, to contribute to the design of the overall architecture applying principles like architectural hybridisation.

- Participation in WP2, to help the design of resilient wireless communication solutions.

- Participation in WP5, to help the instrumentation of the proof-of-concept demonstrator for experimental evaluation in a realistic scenario.

- Participation in WP6, to conduct activities on model-based quantitative evaluation, both for an early system validation and as support for experimentation.

- Participation in WP7, on dissemination activities.

B2.2.3.3 **SHORT PROFILE(S) OF THE STAFF MEMBERS**

Andrea Bondavalli is an Associate Professor at the Faculty of Science at the Università degli Studi di Firenze, Italy. Previously he was a researcher of the Italian National Research Council, working at the CNUCE Institute at Pisa where he was responsible for the Dependable Computing Group. He has a long experience in participating to European funded projects: 3092 PDCS, 6362...
Andrea Bondavalli has authored or co-authored more than 110 papers appeared in International Journals and proceedings of International Conferences. He served as reviewer and as member of the PC in several International Conferences such as IEEE FTCS, IEEE SRDS, EDCC, IEEE HASE, IEEE ISORC, IEEE ISADS, IEEE DSN, SAFECOMP. He also served as Program Co-Chair of IEEE SRDS 2000, of IEEE HASE 2001, LADC 2007, as Program Chair of EDCC 2002, of IEEE ISADS 2003, IEEE/IFIP DCCS-DSN 2005. He served as the General Chair of IEEE SRDS 2003, and vice General Chair of IEEE/IFIP DSN 2004 and IEEE ISADS 2005. His current research interests include the design of dependable computing systems, software and system fault tolerance and the modelling and evaluation of dependability attributes like reliability and performability. Andrea Bondavalli is a member of the IEEE Computer Society, and the IFIP WG 10.4 “Dependable Computing and Fault-Tolerance”.

Paolo Lollini is Associate Researcher at the Faculty of Science at the Università degli Studi di Firenze, Italy. He received the laurea degree and the PhD degree in Computer Science from the same University in 2001 and 2006, respectively. He has participated in the European funded project IST-2001-38229 CAUTION++, and he is presently participating in FP6-IST-STREP-26979 Hidenets, FP6-IST-STREP-027513 CRUTIAL, FP6-SUSTDEV-STREP-031413 SAFEDMI, FP6-IST-NoE-026764 RESIST and FP7-ICT-CA-216295 AMBER. He served as reviewer in several International Conferences such as IEEE SRDS and IEEE DSN. He has authored/co-authored papers appeared in proceedings of International Conferences, journals and books. His current research interests include the modelling and evaluation of dependability attributes, with reference to a variety of application fields including telecommunications systems, railway control systems and electric power.

B2.2.4 ResilTech S.r.l. (RT)

B2.2.4.1 BRIEF DESCRIPTION OF THE ORGANIZATION

ResilTech is a recently created spin-off company (SME) that integrates the experiences of research and development in resilient computing with specific skills in industrial verification and validation of critical systems.

ResilTech founders team is composed by engineers with PhD degree in ICT with leading-edge research and development skills in resilient computing, electronic engineers with long-standing expertise in the design, verification and validation of critical systems and senior engineers with more than 10 years experience in project management.

ResilTech has a leading-edge expertise in both basic and applied ICT research and technological development, in particular in the field of the theory and practice of resilient systems. The expertise is mainly in two macro areas:

i) Architectures and Methodologies for Resilient Systems and

ii) Dependability and Quality of Service (QoS) Quantitative Evaluation.

Resiltech is currently participating as a partner in FP7 funded AMBER (Assessing, Measuring, and Benchmarking Resilience) - Coordination Action (CA)

B2.2.4.2 MAIN TASK(S) IN THE PROJECT

ResilTech’s role in ALARP will be:

- Leadership in WP6, to propose the methodology of modelling, verification, validation and evaluation of middleware solutions and the proof-of-concept prototype and to led the activities performed in the WP.
- Participation in WP1, to help in the definition of of the overall architecture of the system.
• Participation in WP3, to help in the definition and to support the implementation of middleware solutions for enhancing resilience, availability and security in the wireless domain.
• Participation in WP4, to help in the definition and the implementation of train presence alert device.
• Participation in WP5, to participate in the integration of the proof-of-concept demonstrator and to support instrumentation of it for experimental evaluation in a realistic scenario.
• Participation in WP7, on dissemination activities.

B2.2.4.3 SHORT PROFILE(S) OF THE STAFF MEMBERS

Lorenzo Falai is the Vice President of ResilTech. Dr. Falai took his Master degree in Computer Science at the University of Firenze in 2004 and his PhD degree in Computer Engineering at the Resilient Computing Lab - University of Firenze in 2008. During his PhD he participated in national and European funded projects (IST-2004-26979 HIDENETS) where he led UNIFI participation in several Wps. Currently he led ResilTech participation in FP7-ICT-CA-216295 AMBER project. He has authored and co-authored papers appeared in Proceedings of International Conferences and books. He served as reviewer in many International Conferences such as IEEE SRDS, IEEE DSN, LADC, QEST. His current research interests include the design of dependable computing systems and the experimental evaluation of dependability attributes.

Rosaria Esposito is the CEO (Chief Executive Officer) of ResilTech. She took his Master degree in Computer Science at the University of Salerno. After the Master she started working in Ansaldo Segnalamento Ferroviario S.p.A. where she worked until mid 2007. She has relevant experience in the analysis, design, verification and validation of IT critical systems including Italian (SCMT - Sistema di Controllo Marcia Treno) and European (ERTMS - European Railways Train Management Systems) railway systems. She has authored and co-authored papers appeared in Proceedings of International Conferences. She served as reviewer in several International Conferences.

B2.2.5 ELBIT Systems Ltd. (ESL)

B2.2.5.1 BRIEF DESCRIPTION OF THE ORGANIZATION

Elbit Systems Ltd. is the largest defence company in Israel with approximately 2Billion US$ turnover per year. The company has above 8000 employees worldwide, half of them engineers and technicians. The company is one of the main contractors for the local security programs issued by the government of Israel with vast experience in the field. Our systems include border control and management systems, border and site security systems, Command and Control Systems, Long Range Observation Systems, Communication Systems, Smart Fences, and others. We are also involved with local Israeli Railway Company in which we are testing our surveillance systems as part of their new security initiative.

B2.2.5.2 MAIN TASK(S) IN THE PROJECT

Elbit's role in ALARP will be:
• Leadership in WP4, Train Presence Alert Device design.
• Leadership in WP5, Integration and Proof Of Concept. The main task is to integrate all the developed parts into one system.
• Participation in WP1, to help in the definition of the overall System.
• Participation in WP2, to help in the definition of the long range wireless network.
• Participation in WP3, responsible for Mobile Terminal COTS selection. In addition we will support the requirement definition phase, the self localization WP, and the human machine interface design.
- Participation in WP6, on modelling, verification, validation and evaluation.
- Participation in WP7, on dissemination and exploitation activities.

B2.2.5.3 SHORT PROFILE(S) OF THE STAFF MEMBERS

Asaf ASHKENAZI received his IMBA from Northwestern University (Kellogg) and Tel-Aviv University in 2002. In addition he received his Bsc in Electrical Engineering from Tel-Aviv University in 1995. Asaf is Senior Director of Business Technology Development in the Aerospace division. Among his duties is the overall group’s R&D effort responsibility, leading several development programs in the area of advanced day and night vision displays, and looking for business/technological opportunities including partnerships, investments, and other. Since joining ESL in 1995, Asaf has gained massive experience in both the technical area as an HMD System engineer and Technical manager, as well as in the management area as Program manager in day/night sensor imaging, reconnaissance systems, and other real-time platforms.

Dr. Ofer DAVID Received his B.Sc and M.Sc. from the Technion Haifa, Israel. PhD in electro-optics from Ben Gurion University, limitation of active imaging. He is the head of the Electro-Optic group at Elbit Systems with more than 20 years in the field. Ofer has various publications and patents in the area of active imaging systems. Other areas in which Ofer is involved include Long range active imaging systems, Fog penetrating day/night imaging systems, Visibility measurement systems, Automotive night vision systems, Laser warning systems and Optical detection systems.

B2.2.6 PROPRS Ltd. (PROPRS)

B2.2.6.1 BRIEF DESCRIPTION OF THE ORGANIZATION

PROPRS is an independent, British company providing a range of consultancy services in risk management. The Company’s main area of expertise is in assessing and quantifying risks to the public, the workforce and the environment associated with the design, construction, operation and management of industrial plant and processes, transport operations and infrastructure. PROPRS has considerable experience in the development of computer software for clients and in-house use, including stochastic systems, hazard and safety analysis, decision support and expert systems.

PROPRS software covers technical and decision support requirements within the following disciplines: fluid flow and heat transfer, atmospheric dispersion, groundwater and solute transport, consequence analysis, simulation (deterministic and Monte Carlo) and risk.

The directors have extensive experience of participating in Framework projects. They have participated in FORFAIT, HUMICS, JETDEM, CARES, Destiny, ERTMS and in the following railway-related projects:
- GLEER – development of general loss estimation engine for the rail industry;
- Railtrack plc - Risk profiling of railway industry. Hazards caused (future and consequence analysis);
- Train accident modelling together with City University and TRL Limited;
- ERTMS study – case consequence analysis for several Core Hazards;
- Railtrack - Software development for holistic risk assessment.

B2.2.6.2 MAIN TASK(S) IN THE PROJECT

PROPRS role in ALARP will be as follows:
- Participation in WP1 with the main role of defining the risk assessment and the requirements specification.
- Participation in WP4, with the responsibility of the development of the application logic for the Mobile Terminal.
• Participation in WP6, on modelling, verification, validation and evaluation of the application logic.
• Participation in WP7, on dissemination and exploitation activities

B2.2.6.3  SHORT PROFILE(S) OF THE STAFF MEMBERS

DR Z.A. GRALEWSKI, PhD, MSc, BSc, DIC, ACGI, CEng, MBCS CITP, FRSS

He is currently Managing Director of PROPRS Ltd. He has over thirty years' experience in risk management, safety, engineering consultancy and international research. He has wide experience in environmental engineering, risk, safety and mathematical modelling including software development for a variety of industries including: railways, aviation, ports, oil & gas and nuclear industries, as well as regulatory bodies and Government departments.

Dr. Gralewski has had overall responsibility for numerous projects including multidisciplinary and international teams. His experience covers all forms of risk, including safety, environmental, commercial, financial and project risk. He has been involved in the development of risk assessment methodologies using expert systems, fuzzy logic, matrix methods and various statistical sampling techniques. He is regularly consulted by European and national government bodies for peer review and research evaluation in IT applications fields (e.g. under the EC Telematics programme). He was heavily involved in the development of codes for risk assessment using Monte Carlo simulations for fires and explosions and for groundwater and solute transport. In the latter case he was instrumental in the development of formal techniques for taking account of uncertainty and bias, and for the introduction of parallel processing to speed up complex stochastic modelling. These techniques were used in the assessment of proposals for the underground burial of nuclear waste at Sellafield in Cumbria (England), on behalf of the UK Environment Agency. He was also involved in the ATMOSPHERE project under EUREKA and in the EC FORFAIT, DESTINY, CARES, JETDEM, HUMICS projects.

Dr. Carlo Dambra, PhD, MSc

Carlo Dambra, R&D Director of PROPRS Ltd. He received his PhD in Computer Science and Electronic Engineering in 1993 from the University of Genova (Italy). He has a long-standing expertise in RTD project management on both nationally- and EC-funded projects (ICT, RTD Transport, RTD Environment). He has been also invited as expert in RTD DG ICT and DG Research proposals evaluation and in support to negotiation.

B2.2.7  Institute of Ergonomics at Darmstadt University of Technology (IAD)

B2.2.7.1  BRIEF DESCRIPTION OF THE ORGANIZATION

The Institute of Ergonomics (IAD) at Darmstadt University of Technology is national and international noted institute. Under the direction of Professor Dr.-Ing. Walter Rohmert (1963 - 1995) and Professor Dr.-Ing. Kurt Landau (1995 - 2005) emerges one of the leading institutes for Ergonomics in Germany. The institute (IAD) as part of the department of mechanical engineering of Darmstadt University of Technology enjoys a worldwide established reputation. One of its main characteristics is their broad subject orientation.

Thank to this diversity and our experience for more than 40 years, the institute could always react appropriate to new problems, and influence entrepreneurial and social development through relevant research topics. The claim of IAD to be a "universal institute" will continue with Professor Dr.-Ing. Ralph Bruder as head of the institute since January 1, 2006.

The multidisciplinary and international character of the institute warrants for the quality of research. More than 25 researchers of IAD qualify with their degrees in ergonomics, engineering, occupational medicine, industrial engineering & safety and psychology.

Main IAD-competences and applied research areas are:
- **Product ergonomics**: Product development and evaluation, usability testing, prototype simulation, product design;

- **Work design/work organization**: Work process organization and management, industrial engineering & safety, shift work, group work;

- **Production ergonomics**: Workplace analysis & design, risk analysis and management, ergonomics in VDP (Vehicle Development Process), musculo-skeletal injury reduction tools for health and safety;

- **Vehicle ergonomics**: Driver assistance systems, ergonomic applications for: steering and brake systems, vehicle seating, virtual environment and testing of vehicles;

IAD has been participated in numerous EU-projects since 1996. Some of them are: EUROHANDTOOL, VIRTUAL, IRMA, MIRTH (coordinator), ERGOMACH;

**B2.2.7.2 MAIN TASK(S) IN THE PROJECT**

IAD’s role in ALARP-project will be:

- Participation in WP1, to contribute to the “Mobile Terminal “work system analysis in order to have requirements for ergonomic design.

- Participation in WP3, to give input for ergonomic user centred design process and human-Mobile Terminal interface solutions.

- Participation in WP6, to conduct activities on quantitative/qualitative evaluation of working systems for an early system validation and as support for experimentation.

- Participation in WP7, to perform dissemination and exploitation activities to prepare some articles in magazine and conference papers.

**B2.2.7.3 SHORT PROFILE(S) OF THE STAFF MEMBERS**

**Prof. Dr.-Ing. Ralph Bruder**

Since January 2006 he is professor at the TU Darmstadt in the Faculty of Mechanical Engineering and Head of the Institute of Ergonomics at the TU Darmstadt. The Institute of Ergonomics at TU Darmstadt is one of the worldwide leading academic institutes in Ergonomics having more than 40 years of experience.

From 2002 until 2006 Professor Bruder has been President and Managing Director of the Zollverein School of Management and Design. He was organizer of several scientific conferences in Ergonomics, Design and Management and is a member of the Scientific Board of several conferences in Ergonomics. Currently he is also a Member of the EQUID (Ergonomics Quality in Design) Committee of International Ergonomics Association (IEA).

Professor Bruder has a lot of experience in leading projects with public and/or private partners. His main research interest in the field of product ergonomics are the development of an User-centred design process, the definition of user characteristics for product development, the development of new product and service concepts and finally the evaluation of product and service concepts.

**Dr.-Ing. Jurij Wakula,**

From 1992 until 1996 Dr. Wakula was researcher and since 1997 he is senior researcher on the Institute of Ergonomics at the TU Darmstadt. Dr. Wakula has a lot of experience in leading projects with public and/or industrial partners. His main research fields are: ergonomic work place design and product design. He has a long experience in participation and leading of European Commission funded projects: Euro-Handtool (Euro-BRITE III), VIRTUAL, (FP5), MIRTH (as coordinator, FP6), ERGOMACH.

He participated in several scientific conferences in Ergonomics, Human Factors, and Industrial Ergonomics & Safety. He has prepared more that 70 publications in scientific and applied magazines. He is a member of German Ergonomic Society since 1996 and European Technology and Safety plattform since 2007.
### B3 IMPACT

#### B3.1 STRATEGIC IMPACT

**B3.1.1 Impacts listed in the work programme**

The expected impacts of ALARP on the Transport 2008 work programme (area 7.2.4.1, topic SST.2008.4.1.2) are listed in the table below together with the ALARP potential contribution.

<table>
<thead>
<tr>
<th>Transport work programme impacts for area 7.2.4.1 “Integrated safety and security for surface transport systems”</th>
<th>ALARP contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>All proposals submitted to every topic would have to ensure at least a neutral impact on climate change.</td>
<td>ALARP has a fully neutral impact on climate change since it does not plan to use any technology/material that may adversely impact on the environment.</td>
</tr>
<tr>
<td>Increase the level of safety and security of both the whole transport system and its components, thus contributing to the overall scope of reducing the number of fatalities and the severity of injuries caused by transport accidents.</td>
<td>The ALARP is directly contributing to the safety of the rail transport system by developing an innovative Automatic Track Warning System (ATWS), thus reducing the number of casualties and the number and severity of injuries to the workers. The ALARP system, being independent from the signalling systems, does not impact on its Safety Integrity Level (SIL).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transport work programme impacts for topic SST.2008.4.1.2</th>
<th>ALARP contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems, technologies and their integration and evaluation aimed at increasing the level of protection of the transport system’s users (pilot/drivers, passengers, motorcyclists, workers, pedestrians) with special attention to the most vulnerable ones. Contributions may also include methodological aspects, aiming at the evaluation of social benefits associated to investments in technology for the protection of vulnerable users such as pedestrians and cyclists.</td>
<td>By developing an innovative ATWS, ALARP directly contributes to the protection and the safety of track workers, that in railway are the workers that are more prone to injuries and fatalities.</td>
</tr>
<tr>
<td>Enhance safety relevant behaviour of railway workers and road and railway construction workers. Technical and organisational applications to increase workers’ safety in these areas.</td>
<td></td>
</tr>
</tbody>
</table>
B3.1.2 RIMINI Standard
ALARP is fully in line with the prescriptions of the UK Network Rail’s RIMINI (risk minimisation) standard, one of the most advanced standard available in Europe for the improvement of the way in which track work is planned and carried out.

B3.1.3 Interactions with the European Railway Agency (ERA)
The main objective of the ERA is to provide the Commission and the Member States with technical assistance in order to enhance the level of interoperability and safety of the European rail system.

The interactions between ALARP and the ERA can be bidirectional:
- ALARP can exploit the information stored in the “Accident Investigation notification and reports Database” of the ERA to complete the risk analysis planned in WP1.1;
- ALARP can contribute to the ERA work related to Common Safety Targets\(^{11}\) (CSTs) by evaluating how the proposed ALARP ATWS can contribute to improve safety level performances.

B3.1.4 Market opportunities for European industry
Measures to reduce the consequences of a wide variety of accidents and incidents in railway caused by technical or human failure, calling for a swift and sure response, will be in the years to come a growing market.

Companies with new, innovative products are able to gain a large share of the market rapidly.

Sustainable costs and high quality are the most important factors in determining the success for safety-related products and services in the global market.

Advanced technological features, offered in innovative products and services, will become an important factor in establishing market penetration.

Marketing EU safety-related products and services can be successful if:
- there is a high technological content;
- they contain a high level of flexibility and ability to be used in different context conditions;
- they meet end user requirement;
- they can take profit from past experience in other field (e.g. military or space).

The goal of ALARP project are limited but no restricted to transport infrastructure: the complexity of context is particularly difficult and the level of activities needed in research and development will embrace many aspects of workers safety, quite similar in more generic situation.

The benefit of results of the project will be in qualification of companies that take part into in domestic market as well in the international market.

The potential client of products and technologies developed inside the ALARP project will include not only the owner of railway infrastructures and national and regional train operators but also underground managers and contractors for railway lines maintenance and renewal.

\(^{11}\) Development of common safety targets which represent the safety levels and safety performance that must at least be reached by the system as a whole in the different Member States, expressed in risk acceptance criteria.
**B3.2 PLAN FOR THE USE AND DISSEMINATION OF FOREGROUND**

### B3.2.1 Dissemination of project results

#### B3.2.1.1 Dissemination to the public

Apart from the core restricted and protected knowledge, ALARP is expected to create also added value know-how knowledge not to be protected by patents but necessary to carry out the tasks within the project.

A specific not restricted area in the ALARP website is foreseen and links with other web-sites of stakeholders directly or indirectly dealing with rail track workers safety. A major press conference for the media will be organised in parallel with the first publication or conference presentation of the results. Special efforts will be made to ensure the widest possible dissemination of the results in both the specialist and general media.

#### B3.2.1.2 Dissemination among the consortium and to the scientific community

Knowledge dissemination and sharing among the Consortium members is a crucial step to foster mutual trust and cooperative capacity building as well as to create an environment in which potential barriers and fears can be overcome and in which sustainable long-term cooperation can be established.

There will be two main groups of target users; the members of the Consortium and the stakeholders and organisations outside the Consortium at regional, national and European levels.

A knowledge dissemination plan will ensure the appropriate exploitation of some deliverables coming from the consortium activities such as scientific papers, consensus reports, position papers. The aim of this process will be to meet criteria of credibility, relevance and comprehensiveness of information content as well as the accessibility, user friendliness, transparency and attractiveness of the information release. The knowledge dissemination plan will ensure that exchange and sharing of existing knowledge.

The technology for knowledge management will be developed and implemented according to the activities described in the work plan - the likely technology being a web portal with a public, free access section and a restricted password-protected access section that will also include a groupware application.

To protect the confidentiality of information, appropriate measures will be taken, whenever relevant.

Specific meetings (conferences, courses, congresses, etc.) will be approached in order to disseminate and promote the ALARP project.

#### B3.2.1.3 Dissemination to stakeholders and the stakeholder group

Dissemination outside the Consortium will also made by sending specific reports to stakeholders, including railway infrastructure owners (e.g. through the UIC, the International Union of Railways), rail research organisations (e.g. through ERRAC, the European Rail Research Advisory Council), railway workers organisations (e.g. EFRTC, the European Foundation of Railway Trackside Contractors), unions of railway workers, in addition to publication on the ALARP web portal, dissemination of knowledge will involve the submission of papers to relevant railway-related journals and presentations of results at international conferences.

It is planned to create a **Stakeholder Group**, where members of relevant organisations (see above paragraph) will be invited to provide their contribution and feedback on the ALARP results.

Decision makers will be reached, both for dissemination and exploitation purposes, also through the following actions:

- organisation of regular thematic workshops involving selected panels of stakeholders/decision makers;
• organization of a public events during phase 3 demonstration with the presence of decision makers and opinion makers;
• production of dissemination material: newsletter, posters, flyers, etc.

B3.2.1.4 COMMUNICATION MATRIX
ALARP will generate five categories of knowledge: scientific, technological, societal, economical, and ethical. The matrix below summarises the communication policies and the targeted communities.

<table>
<thead>
<tr>
<th>Targeted communities</th>
<th>Knowledge</th>
<th>Scientific</th>
<th>Technological</th>
<th>Economical</th>
<th>Ethical</th>
<th>Societal</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALARP Partners</td>
<td>Daily exchange by electronic means, annual meeting and reports, topical intermediate meetings, internal reports, exchange of personnel, technology implementation plan.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academics</td>
<td>Articles, patents, conferences</td>
<td>Conferences, patents, project showcases</td>
<td>Articles, conferences, websites</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industries and SMEs</td>
<td>Articles, conferences, patents, consultancy</td>
<td>Demonstration activities, project showcases, patents, consultancy</td>
<td>Articles, conferences, websites</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td>Project showcases</td>
<td>Demonstration activities, project showcases</td>
<td>Reports, websites</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>National contact points</td>
<td></td>
<td>Reports, website, project showcases</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Journalists</td>
<td></td>
<td>Reports, website, interviews, project showcases</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td></td>
<td>Reports, website, expertise, project showcases</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citizens</td>
<td></td>
<td>Website, concrete approach with a clear connection to daily life.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B3.2.2 Knowledge Management, IPR and exploitation

B3.2.2.1 KNOWLEDGE MANAGEMENT
All knowledge will be managed in accordance with the signed Consortium Agreement (CA). Relevant discoveries will be possibly patented for the use of the partners, and relevant licensees and spin-offs transferred, so that both established companies and emerging companies can benefit from the project’s research result.

Knowledge Management and communication in the project will be based on a web system, which condenses all information and allows cooperative work on “living” documents.

B3.2.2.2 INTELLECTUAL PROPERTY RIGHTS (IPR) MANAGEMENT
The IPR regulations are defined in the Consortium Agreement. The rules deal with the management of knowledge related to joint invention, application for patents and its further use.
Additionally, rules are defined for the access-rights to knowledge, mainly based on the document on the provisions for implementing STREP. The legally binding IPR agreement in the CA deals with: (i) the protection of individual partners pre-existing know-how, (ii) protection of IPR gained in the project, (iii) the exploitation strategy (patents, licensing etc.), (iv) a contingency plan that ensures the access to knowledge (project-critical IPR), if a partner leaves the consortium.

Partners, who own knowledge developed in the project, are encouraged to exploit these results or to transfer their rights in exchange for an appropriate financial compensation to partners willing to exploit these.

The wish and responsibility to publish research results and carry out Technology Transfer will be carefully weighed against the necessity not to endanger future exploitation. If plans for patents will be committed in the consortium, publications can be delayed until patents applications etc. have been filled. Generated knowledge will (according to the CA) be integrated in relevant education, including lifelong learning. At every opportunity, dissemination of the knowledge generated from ALARP activities will occur through international events, such as conferences, symposia, etc.

B3.2.2.3 EXPLOITATION STRATEGY

B3.2.2.3.1 Exploitable products
The main exploitable products expected at the end of the ALARP project are:

- the overall ALARP system that has its natural market in the railway infrastructure managers and contractors where ASTS has a long standing presence all over the world;
- the Mobile Terminals that can also be exploited in many other industrial areas where the safety of workers is a major issue by replacing the current TPAD with other sensing devices e.g.
  - mining where, for example, the TPAD can be replaced by gas and seismic sensors;
  - in harbours, where different transport systems are interconnected putting often at risk workers’ safety;
- the Train Presence Alert Device that can have spin-off applications including:
  - advanced detection systems for homeland security;
  - multi-spectral sensing for infrastructure protection;
  - short range port security;
- the safe wireless communication system that can be applied in many other safety-critical applications.

B3.2.2.3.2 Overall exploitation strategy
During the ALARP project, a detailed exploitation plan will be created. It will specify the objectives and strategy (based on a market survey), creation of mechanisms, plans of action (including costing and timetables of future activities), and incorporate an assessment of the impacts of dissemination opportunities on future exploitation.

During the early phase of the project, drafts of these plans will be written for discussion and approval by the consortium.

The exploitation plan and the scientific and technological prospects plan will be co-ordinated by a the Executive Board (see §B2.1.1).

The responsibilities of the Executive Board with regard to exploitation are:

- monitoring the project to guarantee consistency between technical and marketing choices;
- alerting the management committee in cases of inconsistencies between the technical choices and the marketing goals;
- planning exploitation initiatives throughout the project;
• monitoring of the railway market and potential spin-off markets for the whole duration of the project;
• co-ordinating the preparation of the detailed dissemination plan for the final product;
• preparing an outline business plan for the future exploitation of the study.

The commercial exploitation potential of the ALARP results is guaranteed by the worldwide presence of both Ansaldo STS and Elbit Systems in the railway and safety markets.

B3.2.2.3.3 Individual exploitation strategy

<table>
<thead>
<tr>
<th>Beneficiary no.</th>
<th>Beneficiary short name</th>
<th>Exploitation strategy</th>
</tr>
</thead>
</table>
| 1              | ASTS                   | ASTS will directly exploit the ALARP results:  
                 |                        | • by offering it as device in support of maintenance for the new transport systems;  
                 |                        | • by selling it as standalone system to railway contractors, railway infrastructure managers.  
                 |                        | ASTS, with company branches located in 18 countries, can guarantee a worldwide coverage of the market for the ALARP products. |
| 2              | FTW                    | As an Austrian centre of competence in ICT, with a unique mission to provide a platform for joint academic and industrial research, FTW will exploit the results of the ALARP project, on the one hand, by strengthening its strategic research, and the links with its academic partners, and on the other hand, in a co-operation with the industrial partners, within nationally funded application-oriented projects, within which it will examine the commercial applicability of the developed technology in a pre-product developments. FTW will also put effort in publication of results in relevant scientific publications. In order to disseminate results of the project. FTW will also use its established practice and organize tutorials for its industrial and academic members. |
| 3              | UNIFI                  | The dissemination activities of the RCL, Resilient Computing Lab, the research group of the University of Florence (UNIFI) participating in ALARP, will be along three lines:  
                 |                        | • presentations, participation to panels and organization of workshops in international conferences;  
                 |                        | • publications in international journals and conference proceedings;  
                 |                        | • dissemination in advanced courses and seminars, both at university level and in training courses that members of the group are regularly giving to Italian companies.  
<pre><code>             |                        | UNIFI also has a tradition for exploitation of research results through technology transfer. In particular RCL in last years participated to several collaborative projects with companies in several business segments, both in national and European research projects. The results of ALARP will contribute in increasing collaborative development and technology transfer actions with companies working in the area. |
</code></pre>
<table>
<thead>
<tr>
<th>Beneficiary no.</th>
<th>Beneficiary short name</th>
<th>Exploitation strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>RT</td>
<td>RT will be in charge of proposing methodology of modelling, verification, validation and evaluation of middleware solutions and the proof-of-concept prototype and to led the activities performed in the WP6. This roles is in line with consultancy activities of RT and thus RT will benefit from the involvement in the new market segment of workers’ safety. RT will also support the implementation of middleware solutions for enhancing resilience, availability and security in the mobile domain. This is in line with current RT interest in the development of software for resilient systems: the exploitation potential for RT lies in the design of SW for safety critical applications and on resilient platforms. This will allow to increase the marketing potential of RT</td>
</tr>
</tbody>
</table>
| 5              | ESL                    | ESL’s exploitation and dissemination strategy will be twofold:  
  - publications, presentations and demonstrations within international conferences and workshops;  
  - within marketing efforts to our transport business customers. ESL through its large organization has a well established group of workers that collaborate in various areas in programs within the EU and the rest of the world. Our one company philosophy enables not only to exploit the technologies developed in various projects but also to disseminate the knowledge in various interactions with customers worldwide. |
| 6              | PRO                    | In ALARP PROPRS will be in charge of developing the risk assessment methodology, support the requirement definition phase and the development of the application logic for the Mobile Terminal. The former tasks are in line with its consultancy activities and PROPRS will benefit from the involvement in the new market segment of workers’ safety. The latter task is in line with current PROPRS development of SW for risk assessment and decision support: the exploitation potential for PROPRS lies in the design of SW for safety critical applications and on resilient platforms. This will allow to broaden PROPRS SW offer and therefore increase the marketing potential. |
| 7              | IAD                    | The dissemination and exploitation activities includes:  
  - presentations, of workshops in international conferences;  
  - publications in international journals and conference proceedings;  
  Dissemination and exploitation of project results and usability testing experiences in seminars / workshops at academic level (universities) and in training courses for industry and companies. |
B4  ETHICAL ISSUES

B4.1  PRIVACY OF WORKERS

The ALARP consortium is aware that an improper use of the developed devices could potentially have an impact on the privacy of workers using them.

However, the ALARP device:

- is NEITHER using NOR storing any worker’s personal data (health, religion, sex, race, ...);
- the only “personal” information MONITORED but NOT stored is:
  - the location of the worker in the working site,
  - its status: “life or dead”,
  - if he is using or not the Mobile Terminal (coupling);
- is not using the worker’s identity but only a code that can be by design totally independent from the worker’s identity;
- during the project the most appropriate technological solution will be selected and implemented.

Moreover, the ALARP approach is the following:

- the system will be designed to grant safety and not to track workers to identify misbehaviours;
- therefore the system will be totally anonymous, i.e. without coupling Mobile Terminal ID codes to personal identity of the worker using currently available and well established technologies;
- the tracking system will therefore display position and code but not the personal identity and therefore it will be made impossible to infringe on the worker’s privacy using the ALARP system;
- envisioned safeguards to ensure privacy (limited storage of data, anonymisation of individual devices, turn-off options) will be included in the final devices and their activation will not be controllable by the employer;

In any case, the workers participating into the project trials will fill an informed consent form. A copy of the informed consent will be submitted to the European Commission.

Finally, the Consortium as a whole will comply to all relevant national and European data protection and privacy norms. Approvals and/or notifications to national data protection authorities, if any, will be provided to the European Commission.

As a reference, the consortium will follow the best practices described in the following documents:

- “Protection of workers’ personal data” published by the International Labour Office in Geneva (affiliated to United Nations);
- the studies funded by European Commission, DG for Employment and Social Affairs:
  - “Study on the protection of workers’ personal data in the European Union: general issues and sensitive data”,
  - “Study on the protection of workers’ personal data in the European Union: surveillance and monitoring at work”.

The consortium will constantly monitor possible new regulations/best practices either emerging in literature during project execution or suggested by the European Commission.
**B4.2 DUAL USE**

ALARP will not develop neither directly nor indirectly any technology that could have any dual use implication, according the definition of dual use as provided by the European Commission in CORDIS 7th FP (ftp://ftp.cordis.europa.eu/pub/fp7/docs/dual-use.doc):

“... omissis ... technology which can be used for both peaceful and military aims, usually in regard to the proliferation of nuclear weapons.

*Ethical issues of dual use might arise in cases where:*-

- Classified information, materials or techniques are used in research
- Dangerous or restricted materials e.g. explosives are used in research
- The specific results of the research could present a danger to participants, or to society as a whole, if they were improperly disseminated

... omissis ..."
REFERENCES


[33] ISO 13407:1999 - “Human-centred design processes for interactive systems"