



Company Profile

03.00 - 01/01/2011

Table of Contents

Short presentation	3
Mission and Vision	4
ResilTech Role	5
Projects - Industrial Consultancy	6
Projects - R&D	8
AMBER	8
SILFI	9
ALARP	9
Expertise	11
a) Professional Technical Expertise in Industrial Field	11
Methodologies and tools	13
Knowledge of SW packages and programming languages	13
b) Experiences and Expertise in Scientific Research	14
Main Customers	17

Short presentation

The company founded in 2007 was born from the experience of ICT experts specialized in the field of the *critical systems*. Such an expertise has been gained from projects in the industrial and academic research fields. With such a background the company can provide a competitive added value for:

- *analysis, verification and validation* of existing systems,
- *design* of new systems,
- *research projects* with a strong orientation to industrial applications.

In the following sections the mission and the vision of the company are described together with the experiences and expertise in both industrial and academic research fields. These two sectors perfectly integrated inside the company makes of *ResilTech* an ICT consulting company always aware of leading edge technologies and open to innovation

Mission and Vision

ResilTech first of all focuses on the definition of *RAMS* (*Reliability, Availability, Maintainability and Safety*) requirements and the verification that the system under test fulfills the target *RAMS* requirements. In such activities, all V&V activities are included.

In this context, *ResilTech* is willing to collaborate:

- with companies to perform *RAMS* analysis, or as an independent V&V partner;
- with certification bodies for certification and safety assessment activities of critical systems.

These activities are performed according to a rigorous scientific methodological approach. *ResilTech* aim is also to collaborate in national and international *research projects* in ICT. The research activities are carried on within the scope of both national and international research projects, both for a specific customer or in the context of collaborative projects. In particular, *ResilTech* gives high priority to the participation to EU's research programs, since joining multinational knowledge-generation efforts is key to keep the company innovative and near to the leading edge technologies. Additionally participation to such projects grants access to interesting collaboration networks.

ResilTech provides moreover *training programs*, both to industries and to public institutions. Indeed *ResilTech* proposes high-quality professional courses on: *Safety Critical Systems; V&V Processes; Fundamentals of Dependability of Computing Systems; Quantitative Evaluation of Computing Systems*. All courses are held by highly professional experts in the field.

ResilTech vision can then be summarized as follows:

**«To develop and promote, with the support of a rigorous scientific approach,
Techniques and Technologies for Resilience»**

ResilTech Role

ResilTech role is to perform activities in the following areas:

a) Technical activities

- to specify/to verify system safety requirements;
- to support companies in the definition of the mechanisms which assure specified safety levels;
- to execute analyses and tests.

b) Formal activities

- Projects Review;
- Technical inspection of source code and project documentation.

c) Research activities

- Definition and application of validation strategies;
- Definition of methods and tools for V&V processes and acceptance criteria;
- Definition of innovative architecture and mechanisms for highly dependable (available, safe, reliable) systems.

d) Training activities

- Providing high-quality professional courses both to industries and to public institutions on:
 - *Safety Critical Systems*;
 - *Verification & Validation Processes*;
 - *Fundamentals of Dependability of Computing Systems*;
 - *Quantitative Evaluation of Computing Systems*;
 - National and International safety standard specific courses.

Projects - Industrial Consultancy

ResilTech is experienced in consulting projects in the field of industrial critical systems, mainly in the field of railway signaling.

A summary of the major projects is reported in this section.

1. Activities of V&V and Safety Analysis of on-board train subsystems (Fire Detection): activity of Verification, Validation and Safety Analysis of Fire detection systems for rail vehicles.

2. Verification of interoperability properties of RBC (in High-speed lines context)

3. Feasibility study and definition of the architecture of the system of CTC-Centralized Traffic Control System (SIL2)

4. Definition of a SIL2 quality standard for C++

5. ATP: static and dynamic tests (SCMT on TGV)

6. Activities of V&V and Safety Analysis of railway signaling system (in high speed lines and SCMT context)

Support in the activities of Verification and Validation and Safety Analysis of railways systems for the following systems:

- i) Encoder Subsystem
- ii) Infill Subsystem
- iii) ATP Subsystem

7. Activity of Safety Assessment

Verification of compliance of CENELEC norms regarding the following critical systems:

- i) Radio Block Center for High Speed System
- ii) Alifana Inferiore
- iii) Circumvesuviana (Supervision System)

- iv) SSC Subsystem (BL3)
- v) Braking Subsystems (Delhi Metro, LocoVossloh, NTV)
- vi) Vinkovci to Tovarnik to State border Railway Signalling Rehabilitation (project currently on going)

8. Low (LED) Signal: RAMS and V&V activities (project currently on going)

9. Advanced Cooperative Info-mobility Systems: Specification, prototypal definition, and evaluation/validation of a distributed approach to the problem of transportation movement

10. Specification, development and V&V of a Distributed Metadata Model Repository

Projects - R&D

ResilTech participated and is currently participating in several R&D projects in the field of critical systems, V&V and Safety.

Most important projects are reported hereafter in this section.

AMBER

Project name: Assessing, Measuring and Benchmarking Resilience

Status: project closed

Duration: 01/01/2008-31/12/2009

Project type: CE FP7 ICT (Coordination Action) [IST-216295]

Project description

AMBER brings together leading research teams on assessment, measurement, and benchmarking of resilience in computer systems in order to coordinate the effort of defining metrics and benchmarks for comparative evaluation of the resilience of computer systems and components. The consortium includes seven partners (universities of Coimbra, Budapest, City, Chalmers, Florence, and Newcastle and the company ResilTech) from five EU countries, which constitute core research groups on resilience assessment, and relies on a large and representative Advisory Board that constitutes the necessary link between the coordination action and the influential parties in industry and government, thus ensuring that the views of major stake-holders are being taken into account by the AMBER Consortium.

AMBER aims to coordinate the study of resilience measuring and benchmarking in computer systems and components, fostering European research in order to address the big challenges on resilience assessment posed by current and forthcoming computer systems and computer-based infrastructures. Key objectives of AMBER are:

- build consensus on common understanding, methodologies and practices for resilience assessment;
- integrate and coordinate European research and practice on resilience assessment;
- establish a resilience assessment and benchmarking research forum through AMBER web portal;

- build and maintain a repository to analyse and share resilience measurement data, including field data on failures in real systems and experiment results;
- foster the effective transfer of resilience assessment best practices to European industry, namely contribute to the acceptance and adoption of resilience benchmarks by industry;
- promote the proposal of standards for resilience assessment and benchmarking;
- define a research agenda on the key topics for enhancing and advancing European research and industry on assessing resilience and benchmarking resiliency of systems and infrastructures.

SILFI

Project name: Sistema Intelligente per la Lotta al Fuoco Integrata (Innovative System for an Integrate Fire Detection and Extinction)

Status: on-going

Duration: 01/01/2010-31/12/2011

Project type: Regione Toscana - POR CREO, Attività numero 1.5 (Tuscany Region – Activity 1.5 of the POR CREO project).

ALARP

Project name: A railway automatic track warning system based on distributed personal mobile terminals

Status: on-going

Duration: 01/01/2010-31/12/2012

Project type: FP7 Project, contract 234088

Project description

The objective of the ALARP project is 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 localization of the workers (and especially those at risk, not responding) and of the operating conditions of devices.

The proposed ALARP concept 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.

Expertise

ResilTech expertise is twofold, from one side is made up by people with a long term experience in the sector of validation and support to certification activities of critical systems (mainly railway), from the other is made up by people with a large and internationally recognized experience in academic research in the field of dependable computing systems.

a) Professional Technical Expertise in Industrial Field

In more details the technical knowhow available in *ResilTech* is summarized in the below points:

- **Modeling, specification, validation and verification of safety critical systems,**
- **Analysis of the Specifications and Hazard Analysis of critical systems,**
- **Analysis of Mean Time Between Hazardous Events (MTBHE) ,Analysis of mean time to failure (MMTF) and mean time to repair (MTTR),**
- **Fault tree Analysis (FTA),**
- **Quantitative analysis through Modelling and Simulation,**
- **Failure Mode and Effect analysis (FMEA),**
- **Planning and Management of Safety Cases,**
- **Verification and Validation activities planning (V&V Plan),**
- **Planning of activities for the safety (Safety Plan),**
- **Software Quality verification,**
- **Software tool development,**
- **Safety Analysis of HW microarchitectures: Systems on Chip and MCUs.**

All the activities are performed in accordance with the most important international standards, the most relevant of which are reported below.

1) Generic functional safety standard:

- **IEC61508** – "Functional safety of electrical/electronic/programmable electronic safety-related systems".

2) Specific standards in the railway transport sector

- **CENELEC EN 50126** - "Railway Applications - The Specification and Demonstration of Dependability: Reliability, Availability, Maintainability and Safety (RAMS)";
- **CENELEC EN 50128** - "Railway Applications: software for Railway Control and Protection Systems";
- **CENELEC EN 50129** - "Railway Applications-Safety-related Electronic Railway Control and Protection Systems";
- **CENELEC EN 50159-1 e 2** - "Railway Applications - Communication, Signalling and Processing Systems - Safety Related Communication in Closed Transmission Systems".

3) Specific standard in the automotive sector

- **ISO26262 FDIS** – "Road vehicles - Functional safety".

4) Generic standards for the software quality:

- **ISO/IEC 9126**: Software Engineering - Product Quality;
- **ISO/IEC JTC1/SC7 IS 14598-1**: Information Technology - Software Product Evaluation.

One of the person part of the company is author of company standards in the following fields:

- Methodology for **Hazard and Risk Analysis**;
- Analysis for **Evaluation of Software Quality**;
- Rules for **Code Development (Programming and Coding)**.

People collaborating with the company have expertise in full RAMS analysis (e.g.: to derive MTBF or MTBHE), adopting Quantitative Analysis that makes use of both model based and simulation based approaches. In this context MIL Handbook 217F can be used as source of data such calculations.

Acquired experience and expertise in the railway field originate from activities made in several railway systems, as:

- **ATC (Automatic Train Control) of on-board railway control system,**

- **ACS (Apparato Centrale Statico – Central Static Equipment),**
- **ACS (Apparato Centrale Statico – Central Static Equipment) – Manchester Control,**
- **Copenhagen Metro System (Ansaldo STS - USA),**
- **BTM (Module for Data Transmission from balise to board),**
- **ENCODER subsystem for ACEI/ACS (ground subsystem),**
- **High Speed Railway Project (Italy),**
- **SCMT (Sistema di controllo della Marcia Treno - Control system of train gear) project (both ground and on-board subsystems).**

Methodologies and tools

Main used methodology for modeling, capturing specification, verification and validation of safety critical systems is **OO** (Object Oriented), through the languages SDL and UML and the tools available for them (in particular Verilog ObjectGeode, Telelogic TAU Rational Rose Real Time Studio).

With regards to quantitative analysis, methodologies of analysis are: Fault Trees, Reliability Block Diagrams, Petri Nets, etc, with supporting tools (in particular the DEEM tool is used).

Knowledge of SW packages and programming languages

Operating Systems: Unix/Linux, Windows, MacOS, Dos.

Applications: Microsoft Office, ObjectGeode, Greatspn, UML RT Rose, TAU Logiscope, DOORS, RequisitePro.

Programming Languages: C, C++, Java, C#, Assembler Motorola HC11.

HW Description Languages: VHDL, Verilog.

Modeling Languages: UML, SDL, MSC.

b) Experiences and Expertise in Scientific Research

Persons working for the *ResilTech* Company have a deep expertise in academic research in ICT, in particular in the field of the ***theory and practice of dependable systems***, both in basic and in applied research.

The expertise is mainly in two macro-areas:

- *Architectures and Techniques for Dependable Systems*;
- *V&V Processes*, in particular *Quantitative Evaluation of Dependability and QoS*.

Main topics of this research expertise are described in the following in more details, with a brief description of the context of research projects in which they were studied and used.

- **Mechanisms for fault-tolerant systems**

Research made by people in *ResilTech* in this field is long-dated. Important activities in this sector focused on i) management of transient faults through a threshold based approach, with the aim at improving the availability of a system as well as its efficiency; and ii) on-line restoration of a correct state in a component belonging to an N-modular structure. Both these studies have produced solutions, implemented in the GUARDS prototyping architecture (developed in the framework of the homonym research project, *GUARDS*¹). Recently *diagnosis* and *failure detection*, both from a theoretical viewpoint and from a more practical one, are under study i) in the field of protection of critical infrastructures (in the context of FP6 European project *CRUTIAL*²) and ii) in the field of mobility-aware services in ubiquitous communication scenarios (in the context of FP6 European project *HIDENETS*³).

¹ *Generic Upgradable Architecture for Real-time Dependable Systems*. ESPRIT Project 20716.

² *CRITICAL UTILITY InfrastructurAL Resilience*. European IST research project, Sixth Framework Programme (FP6).

³ *Highly DEpendable IP-based NETworks and Services*. European IST research project, Sixth Framework Programme (FP6).

- Development of generic architectures for fault-tolerant (real-time) systems**

Generic architectures are very appealing, because of their ability to be configured to meet a variety of different application requirements, thus significantly decreasing the lifecycle costs. People in *ResilTech* has contributed to the development of a generic architecture for dependable real-time embedded systems, largely based on commercial off-the-shelf (COTS) components, in the context of the European project GUARDS. Research activities in this field is going to continue, with a special focus on railway applications and in the context of the build of IP (Internet Protocol)-based dependable applications for wireless/mobile environments (in the context of FP6 European project HIDENETS).
- Multiple Phased Systems (MPS)**

Multiple Phased Systems (MPS) constitute a quite general class of systems including Phased Mission Systems (PMS) and Scheduled Maintenance Systems (SMS). Research on modeling and evaluation of MPSs is going on from several years, with output both in theoretical results and in the development of a specific tool. We started proposing a hierarchical, modular methodology for the modeling & evaluation of phased-mission systems, characterized by separate modeling & resolution of phases & of dependencies among phases. By taking advantage of the special structure of phased mission systems, we developed an analytical solution technique, based on Markov Regenerative Stochastic Petri Nets, having a low computational complexity, basically dominated by the cost of the separate analysis of each phase. These theoretical results are being applied in the *DEEM software package*, a computational efficient tool for model-based evaluation of dependability attributes of MPSs. The current version of DEEM has been successfully employed in support to the definition and evaluation of maintenance policies of management data bases in commercial wireless communications systems, and of control systems of nuclear power plants. Further activity is planned on both extending the features of the DEEM tool, and on applying DEEM to dependability evaluation in pertinent application fields.

- **Quality of Service in Network Systems and Protocols**

The definition of QoS, originally quite narrowly given in terms of message delay and jitter in telecom applications, has been recently given the wider meaning of the set of qualitative and quantitative characteristics of a distributed system which are necessary for obtaining the required functionality of an application. Therefore the term QoS encompasses many aspects such as reliability, availability, fault tolerance and even properties such as atomicity or reliability of broadcast/multicast. Current activities go into two directions: *QoS evaluation of Protocols* and *QoS evaluation of network systems*. Following a modeling approach, protocols behavior is analysed and quantitatively evaluated under both typical performance indicators and the coverage of the assumptions the correctness of the protocols is based on. This is a novel evaluation method for protocols, typically evaluated through classical performance measures only, like throughput and execution time. Experience has been gained on analysis of wireless group communication protocols and consensus protocols. Currently, communication protocols to coordinate activities among vital subsystems in the railway field are under study.

- **Experimental Quantitative Evaluation and Monitoring of Computing Systems**

Recently basic research work was made in the characterization of tools for quantitative experimental evaluation of computing systems. People in ResilTech are currently working in this field. Some preliminary studies were done in the characterization of tools for quantitative experimental evaluation seen from a *metrological* perspective. Metrology is the science of measurement; it includes theoretical and practical aspects of measurement. This science offers a conceptual framework that was never used in ICT and that, to our view, could be really useful, both for computing systems experimental evaluation and for monitoring of computing systems (in particular, for monitoring of distributed system). ResilTech is willing to continue such work, also in the context of EU research projects (FP7).

Main Customers

ResilTech provided its services to several companies, both in the railway market and in more general ICT markets:

- Ansaldo STS SpA
- ISE Srl
- Polaris SpA
- RFI SpA
- Engineering Informatica SpA

ResilTech also collaborates with RINA Services SpA offering support in safety assessment activities.