| | |
|---|---|
| **Soggetto coordinatore** | Dipartimento di Sistemi e Informatica<br>Università di Firenze |
| **Titolo del progetto** | Safe Driver Machine Interface (DMI) for ERTMS trains. |
| **Acronimo** | SAFEDMI |
| **Descrizione del progetto** | The objective of the SAFEDMI project is to design and develop a DMI system that distinguishes itself from other trainborne DMIs currently available on the market by being able to satisfy at least SIL 2 (Safety Integrity Level 2) according to CENELEC specifications (with all the related implications) and to integrate in such safe DMI safe wireless communication interfaces for configuration, SW and firmware downloading and diagnostic purposes.<br>The detailed proposed objectives are to design and develop:<br>• a safe DMI integrated with the current on-board ERTMS systems;<br>• all the HW and SW solutions to properly address the safety and fault tolerance issues generated by the SIL 2 requirements;<br>• a safe wireless communication interfaces for configuration and diagnostic purposes;<br>• a HW and SW tool infrastructure to support automatic test execution, simulating driver's action. |
| **TA/SG** | |
| **Riferimento Bando** | FP6-2005-TRANSPORT-4 |
| **Valore del progetto** | **€** 2.022.666,00 |
| **Pubblicazioni** | **Capability: TA2.10 Sicurezza di rete**<br>**TA: Comunicazioni/SG: ICT per la sicurezza**<br><br>- J. Gronbaek, H. -. Schwefel, A. Ceccarelli and A. Bondavalli. "Improving Robustness of Network Fault Diagnosis to Uncertainty in Observations". *Network Computing and Applications (NCA), 2010 9th IEEE International Symposium on*. 2010. pp. 229 -232.<br><br>- P. Ferrari, A. Flammini, S. Rinaldi, A. Bondavalli and F. Brancati. "Experimental Characterization of Uncertainty Sources in a Software-Only Synchronization System", *Instrumentation and Measurement, IEEE Transactions on*, Vol. 61, May, 2012, pp. 1512-1521. |

| | |
|---|---|
| | - A. Bondavalli, F. Brancati, A. Flammini and S. Rinaldi. "A Reliable and Self-Aware Clock for Reference Time Failure Detection in Internal Synchronization Environment". *IEEE International Workshop on Measurements and Networking (M&N 2011)*. 2011.<br><br>- P. Ferrari, A. Flammini, S. Rinaldi, A. Bondavalli and F. Brancati. "Evaluation of Timestamping Uncertainty in a Software-based IEEE1588 Implementation". *2011 IEEE Instrumentation and Measurement Technology Conference (I2MTC)*. 2011.<br><br>**Capability: TA5.2 Sistemi ICT sicuri e resistenti agli attacchi (sicurezza del dato)**<br><br>**TA: Information processing and management/SG: ICT per la sicurezza**<br><br>- M. Dixit, A. Casimiro, P. Veríssimo, P. Lollini and A. Bondavalli. "Adaptare: Supporting automatic and dependable adaptation in dynamic environments", *To appear in ACM Transactions on Autonomous and Adaptive Systems*. 2012.<br><br>- P. Ferrari, A. Flammini, S. Rinaldi, A. Bondavalli and F. Brancati. "Improving robustness of the synchronization quality of IEEE1588 nodes". *Precision Clock Synchronization for Measurement Control and Communication (ISPCS), 2010 International IEEE Symposium on*. 2010. pp. 36 -41.<br><br>**Capability: TA5.3 Piattaforme, architetture ed algoritmi per l'analisi in tempo reale di grandi volumi di dati (high performance computing)**<br>**TA: Information processing and management/SG: ICT per la sicurezza**<br>- F. Brancati and A. Bondavalli. "Practical Aspects in Analyzing and Sharing the Results of Experimental Evaluation". *Reliable Distributed Systems, 2010 29th IEEE Symposium on*. 2010. pp. 328 -332.<br><br>- A. Ceccarelli, L. Vinerbi, L. Falai and A. Bondavalli. "RACME: a framework to support V&V and certification". In Proc. of the 5th Latin-American Symposium on Dependable Computing (LADC 2011), Page(s): 116 – 125, São José dos Campos, Brazil, 25-29 April, 2011.<br><br>**Capability: TA5.4 Metodologie e sistemi per il monitoraggio di grandi architetture di rete ICT al fine di detettare anomalie, tentativi di accesso non autorizzato, incidenti**<br>**TA: Information processing and management/SG: ICT per la sicurezza**<br><br>- A. Bondavalli, A. Ceccarelli and P. Lollini. "Architecting and Validating Dependable Systems: Experiences and Visions". *Architecting Dependable Systems VII*. 2010.<br><br>- L. Vinerbi, A. Bondavalli and P. Lollini. "Emergence: a new source of failures in complex systems". *Third International Conference on* |

| | |
|---|---|
| | *Dependability (DEPEND 2010)*. 2010.<br><br>- A. Bondavalli, A. Ceccarelli, L. Falai and M. Vadursi. "A New Approach and a Related Tool For Dependability Measurements on Distributed Systems", *IEEE Tran. on Instr. and Meas.*, Vol. 59. 2010, pp. 820-831.<br><br>- A. Bovenzi, F. Brancati, S. Russo and A. Bondavalli. "Towards identifying OS-level anomalies to detect Application Software Failures". *IEEE International Workshop on Measurements and Networking (M&N 2011)*. 2011.<br><br>- A. Bovenzi, F. Brancati, S. Russo and A. Bondavalli. "A Statistical Anomaly-Based Algorithm for On-line Fault Detection in Complex Software Critical Systems". *Computer Safety, Reliability, and Security*. Flammini et al eds. 2011. pp. 128-142.<br><br>- A. Bondavalli, F. Brancati, A. Ceccarelli and M. Vadursi. "Experimental Validation of a Synchronization Uncertainty-Aware Software Clock". *SRDS 2010*. 2010. pp. 245-254.<br><br>- M. Ficco, A. Daidone, L. Coppolino, L. Romano, A. Bondavalli. An event correlation approach for fault diagnosis in SCADA infrastructures. In Proceedings of the 13th European Workshop on Dependable Computing (EWDC '11), pages 15-20, Pisa, Italy, 2011.<br><br>**Capability: TA2.6 Middleware, architetture di rete e comunicazione (Network Centric Communication), per l'integrazione di reti e sistemi eterogenei**<br><br>**TA: Comunicazioni/SG: Protezione dell'approvvigionamento, della generazione e della distribuzione di energia elettrica**<br>**TA: Comunicazioni/SG: Sicurezza del trasporto multimodale**<br><br>- A. Ceccarelli, J. Gronbaek, L. Montecchi, H. P. Schwefel and A. Bondavalli. "Towards a Framework for Self-Adaptive Reliable Network Services in Highly-Uncertain Environments". *13th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW 2010)*. 2010. pp. 184 -193.<br><br>**Capability: TA2.9 Architetture di rete orientate al fast deployment**<br>**TA: Comunicazioni/SG: Sicurezza dei confini**<br><br>- A. Ceccarelli, A. Bondavalli and M. Vieira. "A Testing Service for Lifelong Validation of Dynamic SOA." In *IEEE HASE 2011*. 2011.<br><br>- A. Ceccarelli, M. Vieira and A. Bondavalli. "A Service Discovery |

| | |
|---|---|
| | Approach for Testing Dynamic SOAs". *Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2011 14th IEEE International Symposium on*. 2011. pp. 133-142.<br><br>**Capability: TA4.7 Metodologie e strumenti per l'analisi del rischio e l'ottimizzazione costo/benefici basati su simulazione e modellistica analitica**<br><br>**TA: Tecnologie per Crisis Management e per la Protezione di Persone, Asset e Infrastrutture/SG: Sicurezza Ferroviaria/SG: Protezione dell'approvvigionamento, della generazione e della distribuzione di energia elettrica**<br><br>- L. Montecchi, P. Lollini and A. Bondavalli. "Towards a MDE Transformation Workflow for Dependability Analysis". *16th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2011)*. 2011.<br><br>- L. Montecchi, P. Lollini and A. Bondavalli. "Dependability Concerns in Model-Driven Engineering". *14th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW 2011)*. 2011.<br><br>- Bondavalli, P. Lollini and L. Montecchi. "Graphical formalisms for modeling critical infrastructures". In F. Flammini (ed), *Critical Infrastructure Security: Assessment, Prevention, Detection, Response*. Ashurst Lodge, Ashurst, Southampton, UK : WIT Press. 2012. pp. 57-73.<br><br>- A. Bondavalli, O. Hamouda, M. Kaâniche, P. Lollini, I. Majzik and H. -. Schwefel. "The HIDENETS Holistic Approach for the Analysis of Large Critical Mobile Systems", *IEEE Transactions on Mobile Computing*, Vol. 10, June, 2011, pp. 783 - 796.<br><br>**Capability: TA1.6 Sistemi di localizzazione, navigazione e guida assistita TA: Sorveglianza & Situation Awareness/SG: Sicurezza dei confini**<br><br>- A. Bondavalli, A. Ceccarelli, F. Gogaj, A. Seminatore and M. Vadursi. "Localization errors of low-cost GPS devices in railway worksite-like scenario". *M&N 2011*. 2011. |
| **Curriculum** | |