



[www.etfa2007.org](http://www.etfa2007.org)



Welcome

Committees

Table of Contents

Keynotes

Technical Program

Author Index

Help

Search

© 2007 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.



## TECHNICAL PROGRAM

<b>Session: T1.1</b>		<b>Room: I4</b>	<b>Wednesday, Sep. 26, 11:30 - 13:00</b>
<b>Communication in Automation Systems: Possibilities and Limitations</b>			
<b>Chairing: Juergen Jasperneite, Alexander Fay</b>			
<i>Life-cycle Oriented Data Access for a Maintenance Framework</i>			
<i>Andreas Gössling, Martin Wollschlaeger</i>			1
<i>OWL Based Information Agent Services for Process Monitoring</i>			
<i>Antti Pakonen, Teppo Pirttioja, Ilkka Seilonen, Teemu Tommila</i>			9
<i>Limits of Increasing the Performance of Industrial Ethernet Protocols</i>			
<i>Juergen Jasperneite, Markus Schumacher, Karl Weber</i>			17
<i>Prediction of End-to-End Deadline Missing in Distributed Threads Systems</i>			
<i>Patricia Della M�ea Plentz, Carlos Montez, R�omulo Silva de Oliveira</i>			25
<i>Performance Evaluation and Prediction of a Bluetooth Based Real-Time Sensor Actuator System in Harsh Industrial Environments</i>			
<i>Uwe Meier, Stefan Witte, Kai Helmig, Michael Hoeing, Markus Schnueckel, Hermann Krause</i>			33
<i>Formalised specification of a test tool for safety related communication</i>			
<i>Mathias M�uhlhause, Christian Diedrich, Matthias Riedl, Daniel Schmidt</i>			38
<b>Session: T6.1</b>		<b>Room: I 10</b>	<b>Wednesday, Sep. 26, 11:30 - 13:00</b>
<b>Embedded Model Control and Emerging Ttechnologies</b>			
<b>Chairing: E. Canuto, J. Ospina</b>			
<i>Embedded Model Control: principles and applications. Part I</i>			
<i>Enrico Canuto, Luis David Prieto</i>			45
<i>Embedded Model Control: principles and applications. Part II</i>			
<i>Enrico Canuto, Luis David Prieto</i>			53
<i>Embedded Model Control: sub-microradian horizontality of the Nanobalance thrust-stand</i>			
<i>Enrico Canuto, Fabio Musso, Luca Massotti</i>			61
<i>Emerging technologies in the ESA Science and Earth Observation Programme</i>			
<i>Luca Massotti, Enrico Canuto</i>			69
<i>Multilayer control of an optical reference cavity for space applications</i>			
<i>Enrico Canuto, Jos�e Ospina, Angelo Ripa, Fabio Musso, Franco Alasia, Fabrizio Bertinetto, Marco Bisi, Paolo Cordiale</i>			77
<b>Session: T3.1</b>		<b>Room: I 11</b>	<b>Wednesday, Sep. 26, 11:30 - 13:00</b>
<b>Scheduling and Resource Management</b>			
<b>Chairing: Bjorn Anderson, Luigi Sassoli</b>			
<i>Sensitization of Symbolic Runs in Real-Time Testing Using the ORIS Tool</i>			
<i>Enrico Vicario, Luigi Sassoli, Laura Carnevali</i>			85
<i>Virtual Execution Environment for Real-Time TDL Components</i>			
<i>Claudiu Farcas, Wolfgang Pree</i>			93
<i>Deriving Exact Stochastic Response Times of Periodic Tasks in Hybrid Priority-driven Soft Real-time Systems</i>			
<i>Giordano Kaczynski, Lucia Lo Bello, Thomas Nolte</i>			101
<i>Uniprocessor Scheduling Under Time-Interval Constraints</i>			
<i>F�abio Rodrigues de la Rocha, R�omulo Silva de Oliveira, Carlos Montez</i>			111
<i>Resource Management for Dynamically-Challenged Reconfigurable Systems</i>			
<i>Muhammad Hasan, Sotirios Ziavras</i>			119
<i>Reliable Scheduling of a Distributed Real-time Embedded Application Considering Common Cause Failures</i>			
<i>Thanikesavan Sivanthi</i>			127

**Session: SS2.1**                      **Room: I 12**                      **Wednesday, Sep. 26, 11:30 - 13:00**

**Emerging Technologies to Enable Integrated Manufacturing and Service Systems (IMSS)**

**Chairing: Goh Kiah Mok, Cristian Vasar**

- A Rapid Configurable Embedded Development Framework***  
Kiah Mok Goh, Benny Tjahjono, Anton J.R. Aendenroomer 135
- The Wireless Sensor Networks for Factory Automation: Issues and Challenges***  
L.Q. Zhuang, K.M. Goh, J.B. Zhang 141
- A Service Based Multi-Agent System Design Tool for Modeling Integrated Manufacturing and Service Systems***  
Han Yu, Zhiqi Shen, Chunyan Miao, Jing Wen, Qizhen Yang 149
- Model-based Monitoring and Failure Detection Methodology for Ball-nose End Milling***  
Sheng Huang, Kiah Mok Goh, Yoke San Wong, Geok Soon Hong, Kah Chuan Shaw 155
- Fault Detection Methods for Frequency Converters Fed Induction Machines***  
Lucian Mihet, Octavian Prosteian, Ioan Filip, Iosif Szeidert, Cristian Vasar 161
- Semantic Enhancement and Ontology for Interoperability in Integration of Design Information Systems***  
Qizhen Yang, Chunyan Miao 169

**Session: T2.1**                      **Room: I4**                      **Wednesday, Sep. 26, 14:30 - 16:00**

**Wireless Industrial Communications**

**Chairing: Christos Koulamas, Julian Proenza**

- Development and Performance Evaluation of an Antenna Diversity Module for Industrial Communication based on IEEE 802.15.4***  
Andreas Vedral, Thomas Kruse, Jörg Wollert 177
- Reasoning about communication latencies in real WLANs***  
Claudio Zunino, Gianluca Cena, Ivan Cibrario Bertolotti, Adriano Valenzano 187
- Monitoring, Controlling and Configuring of ZigBee Wireless Household-Electric Network through Remote Virtual Interface***  
Antonio Heronaldo de Sousa, Ana Teruko Yokomizo Watanabe, Luiz Ricardo Lima, Bruno Henrique Kikumoto de Paula 195
- Fast Hand Off for Mobile Wireless Process Control***  
Orazio Mirabella, Lucia Lo Bello, Antonino Raucea, Michele Brischetto 202
- The Use of Clustered Wireless Mesh Networks in Industrial Settings***  
Urban Bilstrup, Katrin Bilstrup, Bertil Svensson, Per-Arne Wiberg 211
- Requirements, Drivers and Analysis of Wireless Sensor Network Solutions for the Oil & Gas Industry***  
Stig Petersen, Paula Doyle, Christian Salbu Aasland, Svein Vatland, Trond Michael Andersen, Dag Sjong 219

**Session: T8**                      **Room: I 10**                      **Wednesday, Sep. 26, 14:30 - 16:00**

**Computational Intelligence in Automation**

**Chairing: E. Man, J. Tar**

- Texture Recognition for Frog Identification***  
Flavio Cannavo', Boray Tek, Izzet Kale, Giuseppe Nunnari 227
- Modeling Supply Chain's Reconfigurability using Fuzzy Logic***  
Bin Ma, Laura Xu, Roland Lim 234
- On the Application of Recurrent Neural Network Techniques for Detecting Instability Trends in an Industrial Process***  
Eva Portillo, Itziar Cabanes, Marga Marcos, Asier Zubizarreta 242
- Intelligent Control in Automation Based on Wireless Traffic Analysis***  
Kurt W. Derr, Milos Manic 249

<i>On-line Identification of Hybrid Systems Using an Adaptive Growing and Pruning RBF Neural Network</i>	257
Tohid Alizadeh, Karim Salahshoor, Mohammad Reza Jafari, Abdollah Alizadeh, Mehdi Gholami	
<i>Fault diagnosis and fuzzy logic decision for stochastic timed automata</i>	265
Ghada Beydoun, Zemouri Ryad	

<b>Session: T5.1</b>	<b>Room: I 11</b>	<b>Wednesday, Sep. 26, 14:30 - 16:00</b>
<b>Architectures, Methods and Technologies for Enterprise Integration</b>		
<b>Chairing: Rei Itsuki, Jose Lastra</b>		

<i>Impact of the Delay of Subcontracting in a Context of Integrated Maintenance: Analytical Approach</i>	273
Mohammed Dahane, Christian Clementz, Nidhal Rezg	
<i>Development of Communications Protocols between Manufacturing Execution System and Production Equipment</i>	280
Satoshi Iwatsu, Yuji Watanabe, Kiminobu Kodama	
<i>On Ontology Mapping in Factory Automation Domain</i>	288
Corina Popescu, Jose L. Martinez Lastra	
<i>Integration of SOA-ready Networked Embedded Devices in Enterprise Systems via a Cross-Layered Web Service Infrastructure</i>	293
Stamatis Karnouskos, Oliver Baecker, Luciana Moreira Sa de Souza, Patrik Spiess	
<i>An Information Management System in Inter-organization Supply Chain by Secure RFID Tag</i>	301
Kazuhiro Kawashima, Norihisa Komoda	
<i>An Approach for Integrating Real and Virtual Production Automation Devices Applying the Service-oriented Architecture Paradigm</i>	309
Daniel Cachapa, Armando Colombo, Martin Feike, Axel Bepperling	

<b>Session: SS2.2</b>	<b>Room: I 12</b>	<b>Wednesday, Sep. 26, 14:30 - 16:00</b>
<b>Planning and Integration Technologies for Manufacturing and Service Systems</b>		
<b>Chairing: Angle Goh, He Wei</b>		

<i>Web 2.0 Concepts and Technologies for Dynamic B2B Integration</i>	315
Chong Minsk Goh, Siew Poh Lee, Wei He, Puay Siew Tan	
<i>Composing OWL-S Web Services</i>	322
B.D. Tran, P.S. Tan, A. Goh	
<i>An Investigative Approach on Improving B2B Interactions and Communication Capabilities for Enterprise Integration using Web 2.0 Technologies</i>	330
Wei He, Puay Siew Tan, Chong Minsk Goh, Siew Poh Lee, Eng Wah Lee	
<i>Common Capacity Modelling for Multi-site Planning: Case Studies</i>	336
F.Y. Wang, T.J. Chua, T.X. Cai, L.S Chai	

<b>Session: T1.2</b>	<b>Room: I4</b>	<b>Wednesday, Sep. 26, 16:30 - 18:00</b>
<b>IT in the Design Process of Automation Systems</b>		
<b>Chairing: Alexander Fay, Juergen Jasperneite</b>		

<i>Introducing the Modeling and Verification process in SysML</i>	344
Marcos Vinicius Linhares, Rômulo Silva de Oliveira, Jean-Marie Farines, François Vernadat	
<i>Automated PLC Software Generation Based on Standardized Digital Process Elements</i>	352
Martin Bergert, Jens Kiefer, Christian Diedrich, Thomas Bär	
<i>A rule format for industrial plant information reasoning</i>	360
Till Schmidberger, Alexander Fay	
<i>Software Quality Measures to determine the Diagnosability of PLC Applications</i>	368
Mohammed Bani Younis, Georg Frey	

<i>Engineering Components for Flexible and Interoperable Real-Time Distributed Supervision and Control Systems</i>	376
<i>Sandro Andrade, Raimundo Macêdo</i>	
<i>Interactively Configurable Framework for Industrial Agents</i>	384
<i>Sebastian Theiss, Joern Ploennigs, Volodymyr Vasyutynskyy, Jens Naake, Klaus Kabitzsch</i>	
<i>A Linear Programming Based Heuristic for Solving a Two-Stage Flowshop Scheduling Problem</i>	392
<i>Ewa Figielska</i>	

**Session: T6.2                      Room: I 10                      Wednesday, Sep. 26, 16:30 - 18:00**

**Industry/Bank Automation**

**Chairing: R. Vilanova, F. Koumboulis**

<i>A Survey on Automata-based Methods for Modelling and Simulation of Industrial Systems</i>	398
<i>Vasilis Deligiannis, Stamatis Manesis</i>	
<i>On the automatic generation of timed automata models from ISA 5.2 diagrams</i>	406
<i>Luiz Paulo Barbosa, Kyller Gorgônio, Antonio Marcus Lima, Angelo Perkusich, Leandro Silva</i>	
<i>Bank Note Classification Using Neural Networks</i>	413
<i>Sigeru Omatu, Michifumi Yoshioka, Toshihisa Kosaka</i>	
<i>Feedforward Control for uncertain systems. Internal Model Control approach</i>	418
<i>Ramon Vilanova</i>	

**Session: T4                              Room: I 11                              Wednesday, Sep. 26, 16:30 - 18:00**

**Intelligent Sensors and Sensor Networks**

**Chairing: Pedro M. Ruiz Martinez, Paul M. Havinga**

<i>Utilising Noise Effects on Infrared Pattern Reception for Position Estimation on a Grid Plane</i>	426
<i>Nikos Petrellis, Nikos Konofaos, George Alexiou</i>	
<i>A Tight Lower Bound for Art Gallery Sensor Location Algorithms</i>	434
<i>Andrea Bottino, Aldo Laurentini, Luisa Rosano</i>	
<i>Implementation and Evaluation of a Hybrid Network utilizing TinyOS-based systems and Ethernet</i>	441
<i>Angelos Anastasopoulos, Dimitrios Tsitsipis, Spilios Giannoulis, Stavros Koubias</i>	
<i>SensorScheme: Supply Chain Management Automation using Wireless Sensor Networks</i>	448
<i>Leon Evers, Paul Havinga, Jan Kuper, Maria Lijding, Nirvana Meratnia</i>	
<i>METATRO: A Real Time RFID enabled haulage monitoring system for perishable comestibles</i>	456
<i>George Asimakopoulos, Spiros Loubros, Vassilis Triantafillou</i>	
<i>Performance Evaluation of Instrumentation Sensor Network Design Using a Data Reconciliation Technique Based on the Unscented Kalman Filter</i>	460
<i>Karim Salahshoor, Mohammad Reza Bayat, Mohsen Mosallaei</i>	
<i>50 Ways to Build your Application: A Survey of Middleware and Systems for Wireless Sensor Networks</i>	466
<i>Ioannis Chatzigiannakis, Georgios Mylonas, Sotiris Nikolettseas</i>	

**Session: SS1.1                      Room: I 12                      Wednesday, Sep. 26, 16:30 - 18:00**

**The IEC 61499 Function Block Model in Control and Automation**

**Chairing: Kleanthis Thramboulidis, Georg Frey**

<i>Benchmarking of IEC 61499 runtime environments</i>	474
<i>Christoph Sünder, Alois Zoitl, Hermann Rofner, Thomas Strasser, Jeroen Brunnenkreef</i>	
<i>Educational Approaches for the Industrial Acceptance of IEC 61499</i>	482
<i>Seppo A Sierla, James H Christensen, Kari O Koskinen, Jukka P Peltola</i>	
<i>Incorporating Industrial Experience to IEC 61499 Based Development Methodologies and Toolsets</i>	490
<i>Mika P. Strömman, Kleanthis C. Thramboulidis, Seppo A. Sierla, Nikolaos Papakonstantinou, Kari O. Koskinen</i>	

<i>Implementing IEC 61499 Communication with the CIP Protocol</i> Frans Weehuizen, Aidan Brown, Christoph Sünder, Oliver Hummer	498
<i>Deployment of IEC 61499 Compliant Distributed Control Applications</i> Tanvir Hussain, Georg Frey	502
<i>Integrating CNet and IEC 61499 function blocks</i> Nils Hagge	506

**Session: SS3                      Room: I4                      Thursday, Sep. 27, 11:00 - 12:30**

**Methods and Instrumentation for Performance Measurement in Real-time Networks**

**Chairing: Alessandra Flammini, José A. Fonseca**

<i>Precision of Ethernet Measurements based on Software Tools</i> Iwan Schafer, Max Felser	510
<i>Delay Measurement System for Real-Time Serial Data Streams</i> Paulo Bartolomeu, Valter Silva, José Fonseca	516
<i>A new distributed instrument for Real Time Ethernet networks: experimental tests and characterization</i> Paolo Ferrari, Alessandra Flammini, Daniele Marioli, Andrea Taroni	524
<i>Measuring the impact of vertical integration on response times in Ethernet fieldbuses</i> Bruno Denis, Silvain Ruel, Jean-Marc Faure, Gaëlle Marsal, Georg Frey	532
<i>Measuring Real Time Performances of PC-based Industrial Control Systems</i> Micaela Caserza Magro, Paolo Pinceti	540

**Session: T6.3                      Room: I 10                      Thursday, Sep. 27, 11:00 - 12:30**

**Control Theory and Applications**

**Chairing: A. Tzes, L. Massotti**

<i>Stability margins characterization of a combined Servo/Regulation tuning for PID controllers</i> Orlando Arrieta, Ramón Vilanova	548
<i>I/O Decoupling And Disturbance Rejection For General Linear Time Delay Systems Via Measurement Output Feedback</i> Fotis N. Koumboulis, George E. Panagiotakis	555
<i>An Adaptive Input Shaping Technique for the Suppression of Payload Swing in Three-Dimensional Overhead Cranes with Hoisting Mechanism</i> John Stergiopoulos, Anthony Tzes	565
<i>Dynamic modeling of Proton Exchange Membrane Fuel Cell: The effect of temperature and membrane humidity</i> Ahmad Haddad, Rachid Bouyekhf, Abdellah El Moudni, Maxime Wack	569
<i>Automation of diagnosis of electric power transformers in Itaipu Hydroelectric Plant with a Fuzzy Expert System</i> Jovelino Falqueto, Matheus Telles	577

**Session: T5.2                      Room: I 11                      Thursday, Sep. 27, 11:00 - 12:30**

**Emerging Issues and Solutions**

**Chairing: Masanori Akiyoshi, Jose Lastra**

<i>Towards Biologically Inspired Control of Distributed Manufacturing Systems</i> Dania A. El Kebbe, Nils Kretzschmar	585
<i>An Alert Management System for Concrete Batching Plant</i> Jason C.S. Chung, Dickson K.W. Chiu, Eleanna Kafeza	591
<i>Electric power service selection considered flexibility of contract</i> Shigeyuki Tani, Masaharu Akatsu, Norihisa Komoda	599
<i>Enforcing Transition Deadlines in Time Petri Nets</i> Haisheng Wang, Liviu Grigore, Ugo Buy, Houshang Darabi	604



<i>Development of Web-Based Software for a Multi-Fieldbus Diagnosis Tool</i> Scott Warner, Hassan Kaghazchi	720
<i>Assessment of the Ontological Approach in Factory Automation from the Perspectives of Connectionism</i> Aleksandra Dvorynachikova, Jose Lastra	724
<i>OPC server implementation with MMS over Ethernet</i> Hubert Kirmann, Sébastien Chatelanat, Michael Obrist	728
<i>Modeling Logical and Temporal Conditions to Formally Validate Factory Automation Web Services</i> Corina Popescu, Jose L. Martinez Lastra	732
<i>Message-Oriented Middleware for Automated Piezomotor Manufacturing</i> Patrick Otto, Bernd Lindner, Martin Wollschlaeger	736
<i>A Simulation Study of Ethernet Powerlink Networks</i> Stefano Vitturi, Lucia Seno	740
<i>Using a Packet Manipulation Tool for Security Analysis of Industrial Network Protocols</i> Tiago H. Kobayashi, Aginaldo B. Batista Jr., Agostinho M. Brito Jr., Paulo S. Motta Pires	744

**Session: WIP 2                      Room: I 10                      Thursday, Sep. 27, 16:00 - 17:00**

**Embedded Systems and Tools**

**Chairing: Thilo Sauter**

<i>A Power Manager for Deeply Embedded Systems</i> Geovani R. Wiedenhof, Arliones Hoeller Jr., Antônio A. Fröhlich	748
<i>Coprime factorization based strong stabilizing controller design</i> Salva Alcántara, Carles Pedret, Ramon Vilanova, Romualdo Moreno	752
<i>A Constraint Logic Programming Framework for the Synthesis of Fault-Tolerant Schedules for Distributed Embedded Systems</i> Kåre Harbo Poulsen, Paul Pop, Viacheslav Izosimov	756
<i>Embedded linux scheduler monitoring</i> Zdenek Slanina, Vilem Srovnal	760
<i>Enhanced Engineering of Downtimeless System Evolution by use of Hardware Capability Descriptions within the eCEDAC Approach</i> Christoph Sünder, Oliver Hummer, Bernard Favre-Bulle	764
<i>Security in Agent-based Automation Systems</i> Basit Ahmed Khan, Jörgen Mad, Albert Treytl	768
<i>Automating Security Tests For Industrial Automation Devices Using Neural Networks</i> Joao Paulo S. Medeiros, Allison C. da Cunha, Agostinho M. Brito Jr., Paulo S. Motta Pires	772
<i>New Developments in EPOS Tools for Configuring and Generating Embedded Systems</i> Rafael Luiz Cancian, Marcelo Ricardo Stemmer, Antônio Augusto Fröhlich	776
<i>Genetic Algorithms Multiobjective Optimization of a 2 DOF Micro Parallel Robot</i> Dan Stan, Vistrian Maties, Radu Balan	780
<i>A Hidden Markov Models Tool for Estimating the Deterioration Level of a Power Transformer</i> Fotios Sotiropoulos, Panayiotis Alefragis, Efthymios Housos	784
<i>A Graphical Editor for the Input-Output Place-Transition Petri Net Class</i> Ricardo Nunes, Luis Gomes, Joao Paulo Barros	788
<i>Feasibility Conditions with Kernel Overheads for Mixed Preemptive FP/FIFO Scheduling with Priority Ceiling Protocol on an Event Driven OSEK System</i> Franck Bimbard, Laurent George	792

**Session: SS9**                      **Room: I 11**                      **Thursday, Sep. 27, 16:00 - 17:30**  
**Business Intelligence and its Applications in Industrial Ecosystems**  
**Chairing: Elizabeth Chang, Tharam Dillon**

<i>An FCA-based mapping generator</i> Paolo Ceravolo, Zhan Cui, Alex Gusmini, Marcello Leida	796
<i>Addressing The Challenges Of Enetwork Cyberengineering</i> Miheala Ulieru, Mohsin Sohail	804
<i>Trust based Decision Making Approach for Protein Ontology</i> Amandeep Sidhu, Farookh Hussain, Tharam Dillon, Elizabeth Chang	810
<i>Application of SPARQL in Semantic Search</i> Hai Dong, Farookh Hussain, Elizabeth Chang	816
<i>Quantifying the Level of Failure in a Digital Business Ecosystem Interactions</i> Omar Hussain, Elizabeth Chang, Farookh Hussain, Tharam Dillon	820
<i>An Overview of the interpretations of trust and reputation</i> Omar Hussain	826
<i>Ontology Engineering and (Digital) Business Ecosystems: a case for a Pragmatic Web</i> Peter Spyns, Robert Meersman	831

**Session: SS6.1**                      **Room: I 12**                      **Thursday, Sep. 27, 16:00 - 17:30**  
**Interoperability Issues and Research Work in Progress**  
**Chairing: Vincent Chapurlat, Athanasios Kalogeras**

<i>Enterprise modelling and verification approach for characterizing and checking organizational interoperability</i> Vallespir Bruno, Chapurlat Vincent	839
<i>Enterprise Semantic Modelling for Interoperability</i> Nacer Boudjlida, Hervé Panetto	847
<i>An Ontology-based Interoperability Framework for Distributed Manufacturing Control</i> Daniel Diep, Christos Alexakos, Thomas Wagner	855
<i>Interoperable Language Family for Agent Communication in Industrial Applications</i> Thomas Wagner, Albert Treytl, Basit Ahmed Khan	863
<i>Multilevel Order Decomposition in Distributed Production</i> Daniela Wuensch, Aleksey Bratukhin	872

**Session: WIP 3**                      **Room: I 13**                      **Thursday, Sep. 27, 16:00 - 17:00**  
**Sensors and Actuators**  
**Chairing: Thilo Sauter**

<i>Accuracy analysis of a 3D measurement system based on a laser profile scanner mounted on an industrial robot with a turntable</i> Mohamed Rahayem, J.A.P Kjellander, Sören Larsson	880
<i>Group Management System of RFID Passwords for Item Life Cycle</i> Yuichi Kobayashi, Toshiyuki Kuwana, Yoji Taniguchi, Norihisa Komoda	884
<i>Service Oriented Architecture for Mobile Robot Localization</i> Camilo Christo, Carlos Cardeira	888
<i>Active Beacon System with the fast processing architecture for Indoor Localization</i> Byoung-hoon Kim, Jong-suk Choi	892
<i>Line based robot localization using a rotary sonar</i> Danilo Navarro, Ginés Benet, Milagros Martínez	896
<i>Surveillance of Mobile Objects using Coordinated Wireless Sensor Nodes</i> Tony Larsson	900

<i><b>RAVEN: A Maritime Surveillance Project Using Small UAV</b></i> <i>Siu O'Young, Paul Hubbard</i>	904
<i><b>Intelligent Multisensorsystem for In-line Process- and Quality Monitoring of Welding Seams using Methods of Pattern Recognition</b></i> <i>Michael Kuhl, Reimund Neugebauer, Paul-Michael Mickel</i>	908
<i><b>Sensor Enabled Rule Based Alarm System for the Agricultural Industry</b></i> <i>Christos Gogos, Panayiotis Alefragis, Efthymios Housos</i>	912
<i><b>Matching Images of Imprinted Tablets</b></i> <i>Ziga Spiclin, Marko Bukovec, Franjo Pernus, Bostjan Likar</i>	916
<i><b>Wireless Vibrating Monitoring (WiVib) An industrial case study</b></i> <i>Jonas Neander, Stefan Svensson, Tomas Lennvall, Mats Björkman, Mikael Nolin</i>	920

**Session: T3.2                      Room: I 10                      Thursday, Sep. 27, 17:00 - 18:00**

**Real-Time and Control**

**Chairing: José A. Fonseca**

<i><b>Optimal Flow Routing in Multi-hop Sensor Networks with Real-Time Constraints through Linear Programming</b></i> <i>Jiri Trdlicka, Zdenek Hanzalek, Mikael Johansson</i>	924
<i><b>Simple PID Control Algorithm adapted to Deadband Sampling</b></i> <i>Volodymyr Vasyutynskyy, Klaus Kabitzsch</i>	932
<i><b>Second order sliding mode real-time network control of a robotic manipulator</b></i> <i>Luca Capisani, Tullio Facchinetti, Antonella Ferrara</i>	941
<i><b>On the practical issues of implementing the VTPE-hBEB protocol in small processing power controllers</b></i> <i>Jose Fonseca, Paulo Bartolomeu, Valter Silva, Francisco Carreiro</i>	949

**Session: T9.1                      Room: I4                      Friday, Sep. 28, 10:00 - 11:30**

**Intelligent Robots I**

**Chairing: Josep M. Mirats, Yolanda Bolea**

<i><b>A New Time-Independent Image Path Tracker to Guide Robots Using Visual Servoing</b></i> <i>Gabriel J. García, Jorge Pomares, Fernando Torres</i>	957
<i><b>Real-Time Architecture for Mobile Assistant Robots</b></i> <i>Pedro Sousa, Rui Araújo, Urbano Nunes, Luis Alves, Ana Lopes</i>	965
<i><b>Hierarchical Distributed Architectures for Autonomous Mobile Robots: a Case Study</b></i> <i>Jose Azevedo, Bernardo Cunha, Luis Almeida</i>	973
<i><b>Camera Localization and Mapping using Delayed Feature Initialization and Inverse Depth Parametrization</b></i> <i>Rodrigo Munguia, Antoni Grau</i>	981
<i><b>An Outdoor Guidepath Navigation System for AMRs Based on Robust Detection of Magnetic Markers</b></i> <i>Ana Lopes, Fernando Moita, Urbano Nunes, Razvan Solea</i>	989
<i><b>Decision Making among Alternative Routes for UAVs in Dynamic Environments</b></i> <i>Jose J. Ruz, Orlando J. Arevalo, Gonzalo Pajares, Jesus M. de la Cruz</i>	997

**Session: T5.3                      Room: I 11                      Friday, Sep. 28, 10:00 - 11:30**

**Automated Manufacturing Systems**

**Chairing: Toshiya Kaihara, Jose Lastra**

<i><b>Development of a holistic Guidance System for the NC Process Chain for benchmarking Machining Operations</b></i> <i>Ulrich Berger, Ralf Kretzschmann, Matthias Aner</i>	1005
<i><b>Design and Realization of a STEP-NC Compliant CNC Embedded Controller</b></i> <i>Francesco Calabrese, Giovanni Celentano</i>	1010

<i>A Study on Automated Scheduling Methodology for Machining Job Shop</i> Yoshihiro Yao, Toshiya Kaihara, Kentaro Sashio, Susumu Fujii	1018
<i>A Heuristic Approach For Scheduling Multi-Chip Packages For Semiconductor Backend Assembly</i> Tay Jin Chua, Tian Xiang Cai, Xiao Feng Yin	1024
<i>A Formal Approach for the Specification, Verification and Control of Flexible Manufacturing Systems</i> Sajeh Zairi, Belhassen Zouari, Laurent Piétrac	1031
<i>Design and Implementation of Petrinet Based Distributed Control Architecture for Robotic Manufacturing Systems</i> G. Yasuda	1039

**Session: SS8 Room: I 12 Friday, Sep. 28, 10:00 - 11:30**

**Design and Analysis of Distributed Automation Systems**

**Chairing: Georg Frey, Alexander Fay**

<i>Formal verification of redundant media extension of Ethernet PowerLink</i> Steve Limal, Bruno Denis, Jean-Jacques Lesage, Stéphane Potier	1045
<i>DesLaNAS – a language for describing Networked Automation Systems</i> Jürgen Greifeneder, Georg Frey	1053
<i>Simulation Approach for Evaluating Response Times in Networked Automation Systems</i> Liu Liu, Georg Frey	1061
<i>UML-based safety analysis of distributed automation systems</i> Sebastian Schreiber, Till Schmidberger, Alexander Fay, Jörg May, Jörn Drewes, Eckehard Schnieder	1069
<i>Incremental design of distributed control systems using GAIA-UML</i> Arndt Lüder, Jörn Peschke	1076
<i>Distributed control programming in Java - The JAKOBI system</i> Michael Heinze, Joern Peschke	1084

**Session: T3.3 Room: I 13 Friday, Sep. 28, 10:00 - 11:30**

**Distributed Real-time Systems**

**Chairing: Thomas Nolte, Orazio Mirabella**

<i>Simulation for end-to-end delays distribution on a switched Ethernet</i> Jean-Luc Scharbarg, Christian Fraboul	1092
<i>Exploiting a Prioritized MAC Protocol to Efficiently Compute Interpolations</i> Björn Andersson, Nuno Pereira, Eduardo Tovar	1100
<i>Master Replication and Bus Error Detection in FTT-CAN with Multiple Buses</i> Valter Silva, Joaquim Ferreira, José Fonseca	1107
<i>Embedded Web Services for Industrial TCP/IP Services Monitoring</i> Francisco Maciá-Pérez, Diego Marcos-Jorquera, Virgilio Gilart-Iglesias	1115

**Session: T10 Room: I4 Friday, Sep. 28, 12:00 - 13:30**

**Emerging Issues**

**Chairing: Gianluca Cena, Dacfez Dzung**

<i>The Effect of Quartz Drift on Convergence-Average based Clock Synchronization</i> Eric Armengaud, Andreas Steininger, Alexander Hanzlik	1123
<i>Supply Chain Performance Evaluation from Structural and Operational Levels</i> Zhengping Li, Arun Kumar, Xiaoxia Xu	1131
<i>Common Approach to Functional Safety and System Security in Building Automation and Control Systems</i> Thomas Novak, Albert Treytl, Peter Palensky	1141

<i>A Development Process for Mechatronic Products: Integrating Software Engineering and Product Engineering</i>	1149
<i>Ana Patricia Magalhães, Aline Andrade, Leila Silva, Herman Lepikson</i>	
<i>A Novel Class of Multi-Agent Algorithms for Highly Dynamic Transport Planning Inspired by Honey Bee Behavior</i>	1157
<i>Horst F. Wedde, Sebastian Lehnhoff, Bernhard van Bonn</i>	
<i>Introducing and Evaluating a Relaying Concept for the IEEE 802.16 Wireless Metropolitan Networks</i>	1165
<i>Christos Antonopoulos, Kostas Stamatis</i>	

**Session: SS4 Room: I 10 Friday, Sep. 28, 12:00 - 13:00**

**Innovative E-Learning Experiences**

**Chairing: Luis Gomes, Orazio Mirabella**

<i>Synchronous Multipoint E-Learning Realized on an Intelligent Software-Router Platform over Unicast Networks: Design and Performance Issues</i>	1172
<i>Giuseppe Maraviglia, Marina Masi, Vincenzo Merlo, Francesco Licandro, Alessandra Russo, Giovanni Schembra</i>	
<i>A Proposal of Remote Laboratory for Distance Training in Robotic Applications</i>	1180
<i>Marc Murtra, Gloria Jansa, Herminio Martinez, Joan Domingo, Juan Gamiz, Antoni Grau</i>	
<i>Remote Laboratory for Control Engineering Degree</i>	1188
<i>Yolanda Bolea, Antoni Grau</i>	

**Session: SS7 Room: I 10 Friday, Sep. 28, 13:00 - 13:30**

**Grouping and Cooperating of Services**

**Chairing: Carsten Buschmann, Reinhardt Karnapke**

<i>In-network Processing and Collective Operations using the Cocos-Framework</i>	1194
<i>Maik Krüger, Reinhardt Karnapke, Jörg Nolte</i>	
<i>Lean and Robust Phenomenon Boundary Approximation</i>	1202
<i>Carsten Buschmann, Daniela Krueger, Stefan Fischer</i>	

**Session: T5.4 Room: I 11 Friday, Sep. 28, 12:00 - 13:30**

**Multi-agent Systems for Manufacturing Control**

**Chairing: Masanori Akiyoshi, Jose Lastra**

<i>Methodology for the efficient distribution a manufacturing ontology to a multi-agent system utilizing a relevant Meta-Ontology</i>	1210
<i>Manos Georgoudakis, Christos Alexakos, Athanasios Kalogeras, John Gialelis, Stavros Koubias</i>	
<i>Agent-based Control of Rapidly Reconfigurable Material Handling System</i>	1217
<i>Jani Jokinen, Jose L. Martinez Lastra</i>	
<i>Agent Based Prototype for Interoperation of Production Planning and Control and Manufacturing Automation</i>	1225
<i>Rui M. Lima, Rui M. Sousa</i>	
<i>Agent-Based Control Model for Reconfigurable Manufacturing Systems</i>	1233
<i>Omar López, Jose Lastra</i>	
<i>A holonic approach for manufacturing execution system design: an industrial application</i>	1239
<i>Blanc Pascal, Demongodin Isabel, Castagna Pierre, Hennet Jean-Claude</i>	

**Session: T2.2 Room: I 12 Friday, Sep. 28, 12:00 - 13:30**

**Scheduling, Safety and Response Times of Industrial Communication Networks**

**Chairing: Julian Proenza, Thomas Nolte**

<i>Network Recovery Time Measurements of RSTP in an Ethernet Ring Topology</i>	1247
<i>Gunnar Prytz</i>	

<i>Evaluation of timing characteristics of a prototype system based on PROFINET IO RT_Class 3</i>	1254
<i>Paolo Ferrari, Alessandra Flammini, Daniele Marioli, Andrea Taroni, Francesco Venturini</i>	
<i>Hyperperiod Bus Scheduling and Optimizations for TDL Components</i>	1262
<i>Emilia Farcas, Wolfgang Pree</i>	
<i>Testing Approach for Online Hardware Self Tests in Embedded Safety Related Systems</i>	1270
<i>Thomas Tamandl, Peter Preininger, Thomas Novak, Peter Palensky</i>	
<i>BuST: Budget Sharing Token Protocol for Hard Real-Time Communication</i>	1278
<i>Gianluca Franchino, Giorgio C. Buttazzo, Tullio Facchinetti</i>	

**Session: SS6.2 Room: I 13 Friday, Sep. 28, 12:00 - 13:30**

**Interoperability Applications**

**Chairing: Athanasios Kalogeras, Ioannis Gialelis**

<i>Semantically-Enabled Inter-Enterprise Integration in the Tourist Sector</i>	1286
<i>Christos Alexakos, Panagiotis Konstantinopoulos, Kostas Charatsis, Stavros Koubias</i>	
<i>Interoperability Issues in Virtual Organization – How to Proceed?</i>	1293
<i>Taivo Kangilaski</i>	
<i>Towards an ontology-based system for intelligent prediction of firms with fraudulent financial statements</i>	1300
<i>Dimitris Kanellopoulos, Sotiris Kotsiantis, Vasilis Tampakas</i>	
<i>AHP Based Supply Chain Performance Measurement System</i>	1308
<i>Laura Xiao Xia Xu</i>	

**Session: T9.2 Room: I4 Friday, Sep. 28, 13:30 - 15:00**

**Intelligent Robots II**

**Chairing: Antoni Grau, Gabriel J. Garcia**

<i>Accurate Range Image Registration: Eliminating or Modelling Outliers</i>	1316
<i>Yonghuai Liu, Honghai Liu, Longzhuang Li, Baogang Wei</i>	
<i>A Two Stage Robot Control for Liquid Transfer</i>	1324
<i>Maria P. Tzamtzi, Fotis N. Koumboulis, Nicholas D. Kouvakas</i>	
<i>Dynamic equations of motion for a 3-bar tensegrity based mobile robot</i>	1334
<i>Josep M. Mirats Tur, Sergi Hernandez Juan, Albert Graells Rovira</i>	
<i>Onto computing the Uncertainty for the Odometry Pose Estimate of a mobile robot</i>	1340
<i>Josep M. Mirats Tur</i>	
<i>Solving the Inverse Kinematics Problem Symbolically by Means of Knowledge-Based and Linear Algebra-Based Methods</i>	1346
<i>Michael Wenz, Heinz Wörn</i>	
<i>Multivariable Iterative Feedback Tuning – A Step-Wise Safe Switching Approach</i>	1354
<i>Fotis N. Koumboulis, Maria P. Tzamtzi, George E. Chamilothis</i>	
<i>Fuzzy Cooperative Control of Automated Ground Passenger Vehicles</i>	1364
<i>Francesco M. Raimondi, Maurizio Melluso</i>	

**Session: WIP 4 Room: I 10 Friday, Sep. 28, 13:30 - 14:30**

**Wireless and Dependable Networks**

**Chairing: Thilo Sauter**

<i>Implementation of Power Aware Features in AODV for Ad Hoc Sensor Networks. A Simulation Study</i>	1372
<i>Konstantina Pappa, Antonis Athanasopoulos, Evangelos Topalis, Stavros Koubias</i>	
<i>Integrating Building Automation Systems and Wireless Sensor Networks</i>	1376
<i>Erik Pramsten, Daniel Roberthson, Fredrik Österlind, Joakim Eriksson, Niclas Finne, Thiemo Voigt</i>	

<b><i>Multicast Communication in Wireless Home and Building Automation: ZigBee and DCMF</i></b>	1380
<i>Christian Reinisch, Wolfgang Kastner, Georg Neugschwandtner</i>	
<b><i>Using Time-Triggered Communications over IEEE 802.15.4</i></b>	1384
<i>Nuno Ferreira, José A. Fonseca</i>	
<b><i>On a IEEE 802.15.4/ZigBee to IEEE 802.11 Gateway for the ART-WiSe Architecture</i></b>	1388
<i>João Leal, André Cunha, Mário Alves, Anis Koubâa</i>	
<b><i>Performance measurements of 802.11 WLANs with burst background traffic</i></b>	1392
<i>Claudio Zunino</i>	
<b><i>IEC 62439 PRP: Bumpless Recovery for Highly Available, Hard Real-Time Industrial Networks</i></b>	1396
<i>Hubert Kirmann, Mats Hansson, Peter Müri</i>	
<b><i>A Two-Competitive Approximate Schedulability Analysis of CAN</i></b>	1400
<i>Björn Andersson, Nuno Pereira, Eduardo Tovar</i>	
<b><i>Modelling MajorCAN with UPPAAL</i></b>	1404
<i>Matias Bonet, Gabriel Donaire, Julian Proenza</i>	
<b><i>A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks</i></b>	1408
<i>Ioannis Chatzigiannakis, Andreas Strikos</i>	
<b><i>Energy Efficient Authentication in Wireless Sensor Networks - An industrial case</i></b>	1412
<i>Rickard Soderlund, Stefan Svensson, Tomas Lennvall</i>	

**Session: WIP 5                      Room: I 11                      Friday, Sep. 28, 13:30 - 14:30**

**Control**

**Chairing: Thilo Sauter**

<b><i>A Visual-Servoing System for a Humanlike Shape Memory Alloy Actuated Finger</i></b>	1417
<i>Konstantinos Andrianesis, Anthony Tzes, Efthymios Kolyvas, Yannis Koveos</i>	
<b><i>Optimization rules for mill cutter and cutting parameters selection incorporating a control algorithm</i></b>	1421
<i>Luis Rubio, Manuel De la Sen</i>	
<b><i>Ontology-driven Control Application Design Methodology</i></b>	1425
<i>Athanasios Kalogeras, Luca Ferrarini, Arndt Lueder, John Gialelis, Christos Alexakos, Joern Peschke, Carlo Veber</i>	
<b><i>A Metaheuristic Approach for Controller Design of Multivariable Processes</i></b>	1429
<i>Fotis N. Koumboulis, Maria P. Tzamtzi</i>	
<b><i>Robust Controller Design for Active Hydraulic Suspension</i></b>	1433
<i>Michael G. Skarpetis, Fotis N. Koumboulis, Achilleas S. Ntellis, Apostolis Sarris</i>	
<b><i>Robust Lane Keeping for a Tractor-Trailer</i></b>	1437
<i>Michael G. Skarpetis, Fotis N. Koumboulis, Achilleas S. Ntellis, Thomas E. Tsimos</i>	
<b><i>Fuzzy Control of Sparing in Disk Arrays</i></b>	1441
<i>Guillermo Navarro, Milos Manic</i>	
<b><i>CARUSO - Towards a Context-Sensitive Architecture for Unified Supervision and Control</i></b>	1445
<i>Rolf Kistler, Stefan Knauth, Daniel Käslin, Alexander Klapproth</i>	
<b><i>Smoothing out the Adaptive Variable Structure Control Law for Induction Motors</i></b>	1449
<i>Oscar Barambones, Patxi Alkorta, Izaskun Garrido, Aitor Garrido</i>	
<b><i>Industrial robot motion control with real-time Java and EtherCAT</i></b>	1453
<i>Sven Robertz, Klas Nilsson, Roger Henriksson, Anders Blomdell</i>	

**Session: T2.3                      Room: I 12                      Friday, Sep. 28, 13:30 - 14:30**

**Clock Synchronization and Multimedia Real-time Communications**

**Chairing: Thomas Nolte, Christos Koulamas**

<b><i>A PLL-Based Approach to Clock Synchronization for Trajectory Rebuilding in Event-Triggered Communication Systems</i></b>	1457
<i>Carlo Rossi, Manuel Spera</i>	

*A Simulation Framework for Fault-Tolerant Clock Synchronization in Industrial Automation Networks*  
Fritz Praus, Wolfgang Granzer, Georg Gaderer, Thilo Sauter 1465

*Dynamic QoS Management for Multimedia Real-Time Transmission in Industrial Environments*  
Javier Silvestre, Luis Almeida, Ricardo Marau, Paulo Pedreiras 1473

*Integration of a flexible time triggered network in the FRESCOR resource contracting framework*  
Ricardo Marau, Paulo Pedreiras, Luis Almeida, Michael Harbour, Daniel Sangorrin, Julio Medina 1481

**Session: SS1.2                      Room: I 13                      Friday, Sep. 28, 13:30 - 15:00**

**IEC61499 Implementations**

**Chairing: Kleanthis Thramboulidis, Georg Frey**

*RTAI-based Execution Environments for Function Block Based Control Applications*  
George Doukas, Alessandro Brusaferrri, Marco Colla, Kleanthis Thramboulidis 1489

# Common Approach to Functional Safety and System Security in Building Automation and Control Systems

Thomas Novak<sup>1</sup>, Albert Treytl<sup>1,2</sup>, Peter Palensky<sup>1</sup>

<sup>1</sup>) Vienna University of Technology,  
Institute of Computer Technology  
Gusshausstrasse 27-29  
1040 Vienna, Austria  
{novakt, treytl, palensky}@ict.tuwien.ac.at

<sup>2</sup>) Austrian Academy of Sciences  
Research Unit for Integrated Sensor Systems  
Viktor-Kaplan-Strasse 2  
2700 Wiener Neustadt, Austria  
Albert.Treytl@oeaw.ac.at

## Abstract

*Building automation and control systems (BACS) are an important part of modern automated buildings. More and more they are also responsible for functions affecting people's safety, security and health. Thus the respective technology is supposed to work reliably, securely, safely and efficiently. The two important features of such a BACS are functional safety and system security (short safety and security) of both the network nodes and the communication protocols. Up to now little effort has been made to specify a life cycle for a safe and secure BACS that defines requirements for the different stages of the product life of a BACS. Special focus is related to the commonalities between the development of safety and security systems to benefit from these commonalities in development.*

## 1. Introduction and Problem Statement

Building automation and control systems (BACS) are often integrated into modern buildings. More and more modern BACS go beyond trivial control or measurement tasks. Their importance for the processes of a building (climate, logistics, etc.) is constantly growing. They also become responsible for functions that affect people's safety and security. Due to social developments and personal safety desires it is absolutely necessary that modern BACS feature functional safety (short safety) and network and system security (short security) of the network nodes and the communication protocols.

Today's BACS typically lack real security features [1]. In fact, most of them are not considered secure at all although effort is made to integrate such features. A solution for a BACS is presented in [19]. Speaking of functional safety, first promising extensions of standard BACS are currently making their way to the market. Functional safety of these systems, however, is compromised by their intrinsic security flaws. There is no real safety without security: proper measures to grant

confidentiality, integrity, availability (CIA) of data as well as efficient access control. In fact, security must be seen as actually supporting safety, instead of hindering it and vice versa.

Harmonizing safety and security is not a new topic in literature. Eams [2] investigated safety and security requirements specification methods in the context of an air control system and problems relating to their independent development. Stavridou [3] and Simpson [4] discussed the relevance of the security concept of non-interference to safety related properties. Stoneburner [15] presented a unified security/safety risk framework.

The discipline called dependability pursues the idea of an unified approach. According to Laprie [5] dependability is an integrative concept. A dependable system is characterized by the following attributes: availability, reliability, safety, confidentiality, integrity and maintainability. Dewsbury [6] presented a dependability model for domestic systems.

Although a lot of research has been done on this topic, up to now there have not been any guidelines, technical specifications or standards for an open-standard BACS that give requirements for specifying a safe and secure BACS. It is not documented publicly how to benefit from the commonalities of safety and security during development of a BACS and how to deal with contradictions between both areas.

As a consequence an approach to specify a safe and secure system is being presented in the following that specifies different stages in the pre-design phase of a safe and secure BACS. It is the first phase of a safe and secure life cycle model. It harmonizes the safety and security disciplines by giving requirements for the various stages. The approach does not focus on particular applications, but concentrates on the properties of BACS to maintain their today's flexible utilization in a safe and secure way.

The remainder of the document is structured as follows: section 2 presents an approach to develop a safety related system according to the international

standard IEC 61508. Section 3 deals with security issues mentioned in Common Criteria. Section 4 points out the approach to develop a safe and secure system. Section 5 discusses the approach while section 6 outlines the usage of the presented approach by means of a practical application.

## 2. Safety – IEC 61508

In the last years the need for establishing a technology for safety related data communication with BACS has been increased due to recent political and technical developments. A new international standard IEC 61508 [6] was developed and published that gives requirements for programmable electronic safety related systems.

The standard IEC 61508 defines safety as “the absence of unacceptable risk of physical injury or damage to the health of people [...]” [6]. It standardizes a life cycle model for creating a safety related systems. It specifies requirements for every stage of the life of a system to avoid systematic failures and to handle stochastic failures. It guides the developer through the pre-design phase, the design and installation phase, and the operation phase of the system.

Safety related systems are developed to reduce the inherit risk of the equipment under control (EUC) below the maximum tolerable risk by applying a variety of measures. The EUC, for example, corresponds with the building automation and control system.

The amount and kind of measures are always specified on account of hazards and its associated risks. As a result developing a safety related systems always requires a hazard and risk analysis of the EUC. It consists of a specification of hazards causing a dangerous situation, a description of the reason of the hazards and an identification of risks associated with the different hazards.

Safety requirements that describe how to handle hazards in a safe way are derived from the hazard and risk analysis. Safety requirements define the behavior of the safety functions performed by the safety related system.

Beside safety requirements there are also safety integrity requirements, i.e. performance requirements for the safety functions, necessary to be defined in order to achieve functional safety with a safety related system.

**Table 1. Safety integrity level (IEC 61508)**

Safety integrity level (SIL)	High demand or continuous mode (Error probability per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

**Table 2. Safety integrity of deployed hardware (IEC 61508)**

Safe failure fraction	Hardware fault tolerance <sup>1</sup>		
	0	1	2
< 60%	not possible	SIL 1	SIL 2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 4
$\geq 99\%$	SIL 3	SIL 4	SIL 4

1) A hardware fault tolerance of N denotes that N+1 faults cause a loss of the safety status of the system.

Safety integrity requirements specify the possibility of a safety function being performed according to expectation. Safety integrity requirements are derived from the risk assessment where the risk of every hazard is determined. Risk can be decided either by means of qualitative or quantitative measures. Due to general uncertainties in determining the probability and the damage of hazards it is state of the art to use qualitative measuring such as a risk matrix [7] or a risk graph [6].

The performance of the safety functions is categorized by four safety integrity levels (SIL) defined in IEC 61508. Safety integrity level 1 (SIL 1) is the lowest and safety integrity 4 (SIL 4) is the highest level. Each level corresponds with a specific error probability per hour (see Table 1). The value of the error probability specifies the probability of a dangerous error per hour.

On account of the safety integrity level the likelihood for successfully performing the safety functions is defined. The lower the likelihood of dangerous failure the higher the performance of the safety functions must be and the more thorough are the safety integrity requirements.

After specifying the safety functions and the safety integrity level, designing a safety related systems additionally requires a consideration of the deployed hardware where the safety functions are executed. A defined safety integrity level of safety functions can only be reached by increasing the hardware fault tolerance (see Table 2 for an explanation) or the safe failure fraction. The safe failure fraction (SFF) specifies the quantity of failures that do not result in a dangerous situation. The standard IEC 61508 presents a couple of ways to reach a safety integrity level.

Safe failure fraction can be augmented by detecting failures with a high probability. These detected failures are handled by the safety related system properly. Another way is to deploy highly reliable hardware where per se failures occur with a very low probability.

An alternative way to reach a defined safety integrity level is to increase the hardware fault tolerance. That is, additional measures are taken (such as the use of redundant hardware) to avoid a dangerous situation although a hazard has occurred.

### 3. Security – Common Criteria

In 1993 the CC (Common criteria) project was started to harmonize US, Canadian and European security criteria and create a single set of IT security criteria. After some draft versions were published and extensive reviews were made, CC version 2.0 was finally standardized as ISO/IEC 15408 [9] in 1999. The standard (for historical purpose called CC) is a basis for evaluation of security properties of IT products and systems. CC specifies a set of requirements for the security functions of IT products and systems. Additionally, it gives requirements for assurance measures applied to the security functions during security evaluation. As a consequence CC permits to compare results of independent security evaluations.

Within this paper security is defined the following: “Security is concerned with the protection of assets from threats, where threats are categorized as the potential for abuse of protected assets” [9]. Assets are described as information or resources to be protected by security countermeasures. Security especially pays attention to those threats related to malicious or other intentional activities.

CC includes two basic concepts: a security concept and an evaluation concept. The idea of the first one is that owners of assets analyze the possible threats to the assets. They determine which threats apply to their environment. These threats result in risk to the assets. To reduce the risk to assets, countermeasures are required that themselves may possess vulnerabilities and lead to a risk to the assets.

The evaluation concept is based on the idea that evaluation gives evidence of assurance and assurance techniques produce assurance. Owner of assets require assurance because it gives confidence that countermeasures minimize risk to their assets.

The standard presents a framework in which an effective evaluation is possible by defining a way to derive requirements and a specification of the TOE (Target of evaluation; IT product or system that is subject of evaluation). It, however, does not mandate any life cycle model. To receive a TOE specification, four major stages must be run through.

1. Establish security environment: Investigate the

**Table 3. Functional Security Classes [9]**

Security audit	Privacy
Communications	Trusted path
Cryptographic support	Resource utilization
User data protection	TOE access
Identification and authentication	Protection of the trusted security functions
Security management	

**Table 4. Security Assurance Classes [9]**

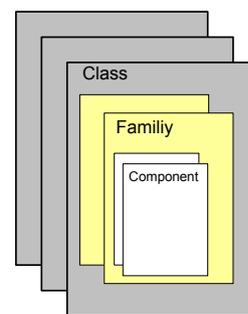
Configuration management	Tests
Delivery and operation	Vulnerability assessment
Development	Evaluation criteria
Guidance documents	Assurance maintenance
Life cycle support	

- physical environment, assets requiring protection, purpose of the TOE.
2. Establish security objectives: Identify assumptions, threats and security policies.
  3. Establish security requirements: Derive requirements from the security objectives by means of the CC requirements catalogue.
  4. Establish TOE summary specification: Functional and assurance requirements lead to the TOE summary specification.

Security function and security assurance requirements are specified in the CC catalogue.

- Security requirements describe the security behavior of a TOE.
- Assurance requirements define the scope, depth and rigor of evaluation of a TOE.

Both, security and assurance requirements, are categorized in classes. Security requirements of a class share a common focus. The name of an assurance class indicates the covered topics. Each class consists of different families of security requirements which share same security objectives. Families are finally divided into components that are the smallest set of requirements (Figure 1).



**Figure 1. Class, family, component hierarchy**

Security requirements from the different functional security classes (Table 3) are chosen depending on the security objectives. Security assurance requirements are selected from various assurance classes (Table 4) regarding the evaluation assurance level (EAL).

The philosophy of CC is to grant assurance based on an evaluation, i.e. active investigation of the IT product or system that is to be trusted. For that reason seven evaluation assurance levels (EAL) are specified that provide a uniformly increasing scale. A higher EAL reduces the likelihood of vulnerabilities and increase the

amount of confidence, but the effort is getting greater because a larger portion of the system is included in the evaluation process. In addition, more details of the design are covered and the evaluation process is carried out in a more structured and formal manner the higher the EAL is required.

#### 4. Integrated Pre-design of Safe and Secure BACS

Section 2 and section 3 outlined the basics specified independently in safety and security standards of getting requirements for a system to develop. Whereas the safety standard specifies a life cycle model, the security standard only describes a way of deriving requirements and specifications. Both safety and security standards define levels to categorize the system. Safety integrity level (SIL) specify the level of performance of safety functions. Evaluation assurance level (EAL) give information about the level of security evaluation.

The integrated pre-design of safe and secure BACS is the first phase of a safe and secure life cycle model. The idea proposed by the authors and in standardization of BACS (CEN/TC 247) is to use the safety life cycle from IEC 61508 and integrated the way of deriving security requirements from CC. Moreover activities are added to consider safety and security dependences.

A life cycle model is a general model of the life of a system, including all the activities needed to develop, maintain and dispose a system. The advantage of such a life cycle model is the structured and formal way of development and maintenance.

This paper focuses on the pre-design phase of the safety and security life cycle (see Figure 2). The pre-design phase summarizes activities of the first phase of the life cycle. Step 1 to 4 is following IEC 61508 [7], steps 5 to 8 are following the Common Criteria [9]. Note that the arrows in Figure 2 do not intend to symbolize a sequential development process such as the waterfall model [10] or V-model [11] does. They imply that activities of step  $n$  requires input from the preceding step  $n-1$ . The pre-design phase can/must be repeated in an iterative process to finally receive a complete set of safety/security requirements for the BACS.

The pre-design phase begins with “definition of the concept” and “safety scope definition”. During that steps the physical environment of the BACS, field of application and relevant laws are examined as well as typical hazards in BACS are identified. Next the scope of the BACS and the scope of the hazard and risk analysis is specified.

“Hazard and risk analysis” aims at identifying typical hazards in BACS. Additionally, it describes the reasons for the hazards and determines the risk associated with the hazards. In the following the safety requirement specification, used to define the safety related system, is



Figure 2. Pre-design of a safe and secure BACS

derived from the hazard and risk analysis.

The next step comprises the list of assets requiring protection, already including the safety related system functionality, the purpose of the target of evaluation (TOE) and the field of application. Next security objectives are derived from a list of threats and the associated risk to the BACS itself and the safety related system. Moreover security policies are investigated. The desired evaluation assurance level (EAL) is defined. Security objectives and the CC requirements catalogue are used to specify the security requirements, functional and assurance ones according to the EAL.

Step 9 “overall hazard and risk analysis” investigates safety and security requirements. It is checked whether security requirements lead to new hazards and risks to human health. I.e., are there new safety requirements necessary due to security needs and how they influence security.

In the end the common, overall safety/security requirements are specified. At this point the commonalities and contradictions between safety and security requirements are evaluated. In case of contradicting requirements safety is favored over security or vice versa depending on the field of application. Finally, requirements are allocated to the safety/security functions as well as the level of performance regarding safety (SIL) is chosen.

## 5. Discussion

The developed approach to integrated safety and security in building automation and control systems (BACS) is a life cycle model trying to harmonize the safety and security discipline. Based on well approved standards for safety and security the common concepts and methods (see section 2 and 3) are integrated.

Both, safety and security disciplines, deal with the problem of risk reduction. However, their objectives differ. Safety measures try to protect people, security measures aim at protecting resources or information. Risk reduction is achieved by safety and security functions respectively. They are derived from the respective requirements. IEC 61508 on the safety side and Common Criteria (CC) on the security side specify a big number of requirements to receive safety or security requirements by using the same concept(s) of requirements derivation.

Moreover, the standards define levels (safety integrity and evaluation assurance) to allow for a comparison of different system designs. Safety integrity levels are defined by different numbers of error probability per hour (Table 1). Evaluation assurance levels specify a set of requirements from the different assurance classes (Table 4). Although the measurands are different, both levels, however, have in common that the higher the level the more and stricter requirements must be met. A higher level results in a higher risk reduction. I.e., safety and security have the strikingly similar goals.

For that reason approaches to unify safety and security have already been published. In [15] an unified security/safety risk framework is presented. It combines the existing security and safety risk model. It specifies that the output of the existing security model, the “potential for harmful security event”, should be considered as a safety hazard. The common approach presented in this paper, however, starts with activities relating to safety and then analysis security.

This procedure was chosen because:

1. First of all because IEC 61508 specifies a very formal and strict way of receiving requirements. The IEC 61508 procedure is very well adopted and often a legal requirement
2. Depending on the safety integrity level a hardware fault tolerance different from zero is required (see Table 2). This requirement results in a specific physical system architecture (e.g., “two channel architecture”) that must be considered while establishing the security environment.
3. Moreover assets to be protected included safety requirements might be comprising the security environment. In most BACS safety is a key application functionality that cannot be readjusted.
4. [20] suggests to integrate security measures as monitoring functions that indicate failures in the

safety system. This will limit security functions to a passive subordinate role. In proposed approach security is an active part of the system.

After step 8 of the pre-design phase (Figure 2) safety requirements were specified that are part of the security environment. Additionally, a set of security requirements is available already considering safety requirements. What is still missing at this point is a cross-checking of both sets of requirements. Are there new hazards and are new risks imposed on the BACS due to security? Are the safety and security requirements complementary? Do security requirements contradict safety requirements and vice versa? Finally, what functions are necessary to meet safety and security requirements?

The “overall hazard and risk analysis” uses the hazards and threats already identified in step 3 and step 6 of the pre-design phase respectively. At this point attention is paid to the dependencies of safety and security. First security requirements are checked if they cause not yet identified hazards. If so, another cycle need to be started. New safety requirements are specified and step 5 to 8 in Figure 2 are repeated. In case the “overall hazard and risk analysis” reveals the same hazard due to security requirements at the end of an additional cycle, a clear contradiction between safety and security was identified. Next risk of the hazards and threats are evaluated with regard to the safe and secure BACS. At this stage of the pre-design phase a possibility is given to set the focus of the BACS either on safety or security. Risk allocation depends on the field of application: either safety or security has priority but in many cases safety is dominant.

Regarding safety and security requirements and hazards coming from the overall hazard and risk analysis, so called safety/security requirements are specified. Most of them are equal to the safety and the security requirements they are based on. In case some requirements are contradicting each other, the presented approach foresees that the one that impose a higher level of risk will be selected. This kind of methodology presents a clear and concise way of solving the problem of contradiction between safety and security requirements. To show a way how to deal with contradictions, the following example is given.

In the safety world it is common practice to send “alive messages”, so-called heartbeats, between a producer (actuator) and a consumer (sensor). They are sent periodically according to the chosen SIL (Table 1) to check whether the consumer is still running. In addition, the heartbeats must be generated within a defined time frame on a node. Since a consumer should just accept heartbeats from particular defined producers, authentication using a message authentication code (MAC) is applied. Let’s assume that generating a heartbeat must be performed within 30 ms due to the chosen SIL; moreover generating a 16-byte MAC

**Table 5. Typical reasons for network hazards in BACS [13]**

Cross talk	Aging
Broken cable	EMC Failure
Wiring failure	Human failure
Stochastic failure	Temperature
Stuck at failure	Transmission of non-authorized messages

requires 50 ms of time.

If heartbeats are sent in a fire alarm system in office buildings between a fire detector and fire damper, the following problem has to be solved: generating an authenticated heartbeat within 30 ms is impossible because processing a 16-byte MAC takes 50 ms. As in this scenario the risk of sending heartbeats less frequently is much higher (Risk of not detecting a defect sensor imposes a high risk to people in the building.), the safety requirement is preferred.

In case of an access control system to a vault the situation is different. Heartbeats are sent between an actuator to open door and the input screen. If we assume that the door of the vault can be opened manually from the inside – low risk level to people being inside the vault –, authentication (generating a MAC) has priority to avoid unauthorized access to the actuator.

The final step of the pre-design phase in Figure 2 specifies functions derived from the requirements. Methods from the safety or security world that form the functions are applied depending on the prioritization of safety or security.

The following section presents the usage of the integrated pre-design model. Special attention is paid to dependencies between safety and security. As an example for this, the usage of source addresses is taken.

## 6. Practical Application

Applications for safety use source addresses to prevent message insertion. Security access control can be based on entity identification by source addresses.

According to the developed pre-design model (Figure 2) steps 3 and 4 as well as steps 6 and 8 are the core parts of the joint analysis. Although based on general requirements, the definition of safety scope and security objectives needs to address specific issues of both areas. The different focal position in the pre-design model mainly stem from historical reasons. The security approach is to first check what harm can be done and then define the security measures. In safety a certain requirement is usually given in advance. In practical usage, both cases will have a (preliminary) definition of scope and objectives before the hazard/threat and risk analysis and a reconsideration or definition after this

**Table 7. Typical reasons for network threads in BACS [18]**

Trojan horse	Data forgery
Eavesdropping on the net	Address Spoofing
Flooding machines with bogus data	Human failure
Isolating machines by DNS attacks	Impersonation of illegitimate users
Viruses	Transmission of non-authorized messages

analysis.

Table 5 and Table 7 show typical reasons for hazards and threats for field level communication systems that effects the integrity of source addresses in a message. Data for this analysis have been take from the projects SafetyLON [16] and REMPLI [17].

At this stage little commonalities can be identified. Although similar tools (e.g. methods to identify risk with a risk matrix) and approaches for analysis are taken each area is investigated on its own.

Table 6 and Table 8 show the effects of hazards and threats. At this stage of the process the commonalities can already be identified. E.g., corruption of a message can stem from a stochastic failure, but also from an intentional manipulation by an attacker.

If safety and security measures are used jointly and not installed in parallel, a potential for synergies can be acquired. The measures and synergies gained can be classified in three groups:

1. There are measures that *directly match* such as time stamps or sequence numbers for delayed or repeated messages. Usually there will be no problem to commonly use them. High potential for synergies exists since measures are easily combinable.
2. There are measures that require *different efforts*, e.g. in terms of computational power or consumed bandwidth, such as CRC (Cyclic Redundancy Check) or MAC (Message Authentication Code).

**Table 6. Effect of network hazards and resulting safety requirements [8]**

Hazard	Safety requirements
Corruption of data	CRC, duplication of message
Loss of a message	Use of a watchdog
Insertion of a message	Use of safe source addresses
Repetition of a message	Use of a time stamp
Wrong sequence of messages	Use of a time stamp
Delay of a message	Use of a time stamp
Non safety related message	Use of a specific header, safe source addresses

**Table 8. Effect of network threats and resulting security requirements**

Hazard	Security requirements
Modification of data	MAC, Signature
Loss of a message	protocol timeout
Insertion of a message	sequence number (protected against modification)
Replay of a message	sequence number/time stamp
Wrong sequence of messages	sequence number
Eavesdropping	Message encryption
Spoofing of source address	Inclusion of source address in MAC or signature

Both of these measures protect the integrity of the message, but the execution time (e.g., 10-100µs for CRC and 8-15ms for MAC) and bandwidth (e.g., length 2 byte for CRC and 16 byte for MAC) differs. Gains need to be judged on application.

- There are measures that are unique for safety and security (such as a watchdog timer) and needs to be implemented separately. No synergies possible.

E.g., in a safety related system a source-addressing model is used to guarantee message exchange between safe nodes only and to avoid message insertion. Therefore each safe node is assigned an additional unique address, a so called *safe address*. The receiving nodes check this safe address against their access list and only allows reception of packets in the list. The safety is given by a CRC checking and the transfer of a safe address within the safe message that can only be generated by safe nodes.

In a secure system similar techniques are used. An access control is also based on the node address [17], but instead of the CRC a cryptographic message authentication code (MAC) is used that cannot be recalculated without the knowledge of the appropriate key.

A matching of the requirements and measures can lead to synergies in the design of an integrated safe and secure system. In our example the CRC is replaced by the MAC which allows to remove the safe address. Access control is now managed by normal addresses and the requirement to identify nodes belonging to the safe group is realized by a particular key only available to nodes in this (safe) group. Timestamps and replay counters are unchanged since they have equal tasks in both areas. In this case also the overall hazard and risk analysis will indicate no new risks, since all requirements are covered by the new solution.

In general, security measures will replace safety measures since measures designed for safety do not withstand intentional attacks. E.g., a CRC protects the integrity of a message, but can be recalculated online.

Hence stochastic failures are discovered, but an attacker is not impeded to manipulate the targeted information (asset) as well as the CRC.

Another important issue to consider is the resource consumption of the applied measures. Introducing safety and security measures will increase the overhead in computational resources as well as network bandwidth consumption to achieve. Selection and trade-off of different measures inside the fields of safety and security is set out of scope for this paper. E.g., if a CRC or a message duplication is used will not be analysed since this is included in the analysis of the individual security requirements and often demanded by normative regulations.

In particular the adding of security measures to a safe system should be analysed since this is a common case: Table 9 shows the overhead of typical security measures used in embedded systems. If there are no synergies this overhead is directly added and can even double, e.g., if messages are duplicated. In case of synergies such as the replacement of the CRC (typically 2, 4, or 8 byte) the network overhead is 6, 4 and 0 byte for the 8 byte MAC. Other typical MAC functions have a length of 16, 20 or 32 bytes. Concerning the computational power security measures will usually show no synergies since other types of checksums are much faster (factor 100) and/or can be implemented with a negligible effort in hard- or software.

## 7. Conclusion

The possibilities to gain synergies by taking an integrated approach towards safety and security in BACS is given in many areas. This fact is well known, e.g., "Safety and security [...] are closely related, and their similarities can be used to the advantage of both in terms of borrowing effective techniques from each to deal with the other." [12]. Yet little effort to combine these fields is given since applications are usually either safety or security.

**Table 9. Performance of key derivation and security functions [17]**

Description	Time [ms]
Derive key by 3-DES function	89
Cipher message using 3-DES in outer CBC mode stored in EEPROM/RAM	63/58
Decipher message using 3-DES in outer CBC mode stored in EEPROM/RAM	54/55
Authenticate message with 8-byte MAC using 3-DES in outer CBC mode in EEPROM/RAM	57/53
Verify 8-byte MAC using 3-DES in outer CBC mode stored in EEPROM/RAM	45/47

In building automation this situation changes since mainly for cost reasons a combination of formerly separated networks for safety, e.g., fire alarm system, security, e.g., access control, and operation, e.g. heating, ventilation and air condition, is desired. Combination on the one hand demands for a reliable system and also increase the need for security since systems formerly physically separated are now accessible for a bigger group of users.

This article proposed a common approach for the pre-design phase of such integrated safety and security systems. Techniques such as the risk analysis common in both areas are synchronized to figure out overall hazards that endanger safety or security of a BACS. Since various hazards even put in danger both safety and security of the system, a dual usage of counter measures seem feasible. The life cycle model presented specifies requirements for the different stages in development of a BACS. At the moment the work done focuses on the pre-design phase and the network communication. Inclusion of hardware integrity and the following stages of the life cycle are important topics for further research.

In the area of building automation a certain convergence of systems to safe and secure systems can be noticed, but finally it must be stated that the common approach will only show benefits when both security and safety functions are required by the application. Convergence seem more likely for applications with high security requirements since in this case the overhead given by security is not a hindrance rather a requirement. Moreover contradictions between both areas cannot be completely avoided. The final decision if security or safety is to be preferred within such conflicts is application and environment dependent.

## References

- [1] C. Schwaiger, A. Treytl, "Smart Card Based Security for Fieldbus Systems", *Proceedings of IEEE International Workshop on Factory Communication Systems*, Vol. 1, pp. 398-406, 2003.
- [2] D. P. Eames, J. Moffett, "The Integration of Safety and Security Requirements", *SAFECOMP'99, LNCS 1698*, Springer-Verlag, Berlin, Heidelberg, pp. 468-480, 1999.
- [3] V. Stavridou, B. Dutertre, "From Security to Safety and Back", *Proceedings of Computer Security, Dependability and Assurance: From needs to Solutions*, pp. 182-195, 1998.
- [4] A. Simpson, J. Woodcock, J. Davies, "Safety through Security", *Proceedings of the 9<sup>th</sup> International Workshop on Software Specification and Design*, pp. 18-24, 1998.
- [5] A. Avizienis, J-C. Laprie, B. Randel, "Fundamental Concepts of Dependability", 2001.
- [6] G. Dewsbury, I. Sommerville, K. Clarke, M. Rouncefield, "A Dependability Model for Domestic Systems", *SAFECOMP 2003, LNCS 2788*, Springer Verlag, Berlin, Heidelberg, pp. 103-115, 2003.
- [7] "IEC 61508 – Functional safety of electric/electronic/programmable electronic safety-related systems", 1999.
- [8] "EN 50126 – Railway applications. The specification and demonstration of reliability, maintainability and safety (RAMS)", 1999.
- [9] "IEC 15408 – Information technology – Security technique – Evaluation criteria for IT security", 1999.
- [10] W. Royce, "Managing the Development in Large Software Systems", *Proceedings of IEEE WESCOM*, 1970.
- [11] G. Müller-Ettrich, *Objektorientierte Prozessmodelle: UML einsehen mit OOTC, V-Modell, Objectory*, Addison-Wesley, 1999.
- [12] N.G. Leveson, *Safeware: System Safety and Computers*, Addison-Wesley, 1995.
- [13] "EN 50159-1: Railway Applications – Safety-Related Communication in Closed Transmission Systems", 2001
- [14] D. Reinert, M. Schaefer (Publisher), *Sichere Bussysteme in der Automation*, Hüthig Verlag, Heidelberg, ch. 4, 2001.
- [15] G. Stoneburner, "Toward a Unified Security-Safety Model", *IEEE Computer*, Vol. 39, pp. 96-97, 2006.
- [16] T. Novak, T. Tamandl, "Architecture of a Safe Node for a Fieldbus System", *Proceedings of the 5<sup>th</sup> IEEE International Conference on Industrial Informatics*, Vol. 1, pp. 101-106, 2007 .
- [17] A. Treytl, T. Novak, "Practical Issues on Key Distribution in Power Line Networks", *Proceedings of the 10<sup>th</sup> IEEE International Conference on Emerging Technologies and Factory Automation Proceedings*, Vol. 2, pp. 83-90, 2005.
- [18] W. Stallings, *Cryptography and Network Security*, Prentice Hall, 2003.
- [19] W. Granzer, W. Kastner, G. Neugschwandtner, F. Praus. "Security in Networked Building Automation Systems", *Proceedings of IEEE International Workshop on Factory Communication Systems*, pp. 283-292, 2006.
- [20] K. Sørby, "Relationship between security and safety in a security-safety critical system: Safety consequences of security threats", *M.S. thesis*, Norwegian University of Science and Technology (NTNU), Department of Computer and Information Science, Norway, Trondheim, ch. 9, 2003.