

Welcome Messages

Keynotes

Author Index

Committees

Program at a Glance

Thanks to our Sponsors

Local Information

Technical Program

Copyright

© 2008 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.

[www.etfa2008.org](http://www.etfa2008.org)



Tuesday

9/16/2008

**Opening Ceremony**

Room: 5

9:00 AM - 9:30 AM

OC      **Opening Ceremony**

*Session Chair(s): Alexander Fay*

Paper starts at page

**Welcome by the President of the Helmut-Schmidt-University**

*Hans Christoph Zeidler*

**Official opening of ETFA 2008 by the IEEE IES President**

*Kouhei Ohnishi*

**Keynote**

Room: 5

9:30 AM - 10:30 AM

K 1      **Keynote Speech**

*Session Chair(s): Paul Drews*

Paper starts at page



**Intelligent Mechatronics and Robotics**

*Fumio Harashima, Satoshi Suzuki*

**Keynote**

Room: 5

11:00 AM - 12:00 PM

K 2      **Keynote Speech**

*Session Chair(s): James Hung*

Paper starts at page



**Networks, Multicore, and Systems Evolution - Facing the timing beast**

*Rolf Ernst*

WiP Room: 1 1:00 PM - 3:00 PM  
 S 1 Automation Systems

Session Chair(s): Thilo Sauter, Athanasios Kalogeras

Paper starts at page

	<b>Orchestration of Time-Constrained BPEL4WS Workflows</b> <i>Markus Mathes, Roland Schwarzkopf, Tim Dörnemann, Steffen Heinzl, Bernd Freisleben</i>	1
	<b>An evolutionary approach for the industrial introduction of virtual commissioning</b> <i>Rainer Drath, Peter Weber, Nicolas Mauser</i>	5
	<b>A Practical Preprocessing Treatment for Pipeline Leak Locating Improving</b> <i>Marllene Daneti</i>	9
	<b>SARBAU - An IP-fieldbus based Building Automation Network</b> <i>Stefan Knauth, Rolf Kistler, Christian Jost, Alexander Klapproth</i>	13
	<b>Aspects of Development and Engineering of a Migration Solution for Existing Heterogeneous Distributed Automation Systems</b> <i>Christian Hahn, Robert Lehmann, Martin Wollschlaeger</i>	17
	<b>Integrated Real-Time System for Perishable Freight Transport Management</b> <i>Athanasios Kalogeras, Konstantinos Charatsis, Ioannis Mourtos, Fotios Liotopoulos, Georgios Asimakopoulos, Panagiotis Konstantinopoulos</i>	21
	<b>An IEC 61499 based run-to-run controller for chemical mechanical planarization process</b> <i>Kiah Mok Goh, Benny Tjahjono, Abdul Manaf, Anton Aenderoomer</i>	25
	<b>Graphical representation of Factory Automation Markup Languages</b> <i>Fabian Lopez, Edurne Irisarri, Elisabet Estevez, Marga Marcos</i>	29
	<b>e-based inter-enterprise supply chain Kanban for demand and order fulfilment management</b> <i>L.S. Chai</i>	33
	<b>On Full Aspect Conveyed Object Inspection at High Speed</b> <i>Marc Pearson, Tim Clarke</i>	36
	<b>An existing complete House Control System based on the REFLEX Operating System: Implementation and Experiences over a Period of 4 Years</b> <i>Karsten Walther, Reinhardt Kamapke, Joerg Nolte</i>	40
	<b>Modules, version and variability management in automation engineering of machine and plant manufacturing</b> <i>Tze Ying Sim, Fang Li, Birgit Vogel-Heuser</i>	46
	<b>Automation Objects for Product Service System Enabler Device</b> <i>Kiah Mok Goh, Benny Tjahjono, James Joseph, Li Qun Zhuang</i>	50
	<b>Dynamic Operations and Manpower Scheduling for High-Mix, Low-Volume Manufacturing</b> <i>Tay Jin Chua, Tian Xiang Cai, Mei Wan Joyce Low</i>	54
	<b>Determination of Launching Parameters for Throwing Objects in Logistic Processes with direct Hits</b> <i>Heinz Frank</i>	58
	<b>An Approach to use Model Driven Design in Industrial Automation</b> <i>Elisabet Estévez, Marga Marcos</i>	62
	<b>Improving program flexibility and application engineering for decentralized control in factory automation</b> <i>Hartmut Ruedele, Florian Kantz</i>	66
	<b>Aquaculture Production Quality Certification Model Utilizing Web Semantics and Wireless Technologies</b> <i>Konstantinos Charatsis, Athanasios Kalogeras, Christos Alexakos, Panagiotis Konstantinopoulos, Joanna Iliopoulou Georgoudaki</i>	70

Tuesday

9/16/2008

Track 4






Room: 2

1:00 PM - 3:00 PM

S 1 Factory and process automation

Session Chair(s): Orlando Arrieta, Andrei Lobov

Paper starts at page

 <b>Evaluation of Sequential Function Charts Execution Techniques. The Active Steps Algorithm.</b>	74
<i>Ramón Piedrafita Moreno, José Luis Villarroel Salcedo</i>	
 <b>Rapid prototyping of logic control in industrial automation exploiting the generalized actuator approach</b>	82
<i>Andrea Paoli, Matteo Sartini, Andrea Tilli</i>	
 <b>Selecting orchestrator paths in manufacturing lines: alternatives to scheduling</b>	90
<i>Corina Popescu, Jose L. Martinez Lastra</i>	
 <b>Structured Reactive Controllers and Transformational Planning for Manufacturing</b>	97
<i>Thomas Ruehr, Dejan Pangercic, Michael Beetz</i>	
 <b>An algorithm to compensate for large data dropouts in Networked Control Systems</b>	105
<i>Pablo Millán, Isabel Jurado, Carlos Vivas, Francisco Rodríguez</i>	

Track 4






Room: 3

1:00 PM - 3:00 PM

S 2 Modeling and identification

Session Chair(s): Pedro Balaguer, Ubirajara Moreno

Paper starts at page

 <b>Constraints Graph Based Approach for The Control of Time Critical Systems</b>	113
<i>Patrice Bonhomme</i>	
 <b>Identification of Incompatible states in Mode Switching</b>	121
<i>Gregory Faraut, Laurent Piétrac, Eric Niel</i>	
 <b>Observability analysis of interpreted Petri nets under partial state observations using estimations reachability graph</b>	129
<i>Luis Aguirre-Salas, Alejandra Santoyo-Sanchez</i>	
 <b>Robust control of a manufacturing system: flow-quality approach</b>	137
<i>Achraf Jabeur Telmoudi, Lotfi Nabli, Radhi M'hiri</i>	
 <b>Real Number Laplace Transformation-based Identification for First-order System including Time-delay</b>	143
<i>Satoshi Suzuki, Katsuhisa Furuta</i>	

Tuesday

9/16/2008

Track 6






Room: 108

1:00 PM - 3:00 PM

S 1 Human robot interface and telerobotics

Session Chair(s): *Monica Ballesta*

Paper starts at page

 <b>Speaker Selection Algorithm Using Audio And Video Information In A Cluttered Environment</b>	150
<i>Yonseob Lim, Jongsuk Choi</i>	
 <b>Analysis of machine operation skills using hand discrete movement</b>	156
<i>Satoshi Suzuki, Fumio Harashima</i>	
 <b>Object-transportation control for a human-operated robotic manipulator</b>	164
<i>Naoki Uchiyama, Atsushi Mori, Yuichiro Kajita, Shigenori Sano, Shoji Takagi</i>	
 <b>Teleoperation mechanisms in a Multi-Agent System</b>	170
<i>Vasco Santos, Pedro Santana, Luís Correia, José Barata</i>	
 <b>Shared Control of a Pan-Tilt Camera on an All-terrain Mobile Robot</b>	177
<i>Carlos Cândido, Pedro Santana, Luís Correia, José Barata</i>	

SS 02







Room: 109

1:00 PM - 3:00 PM

SS 02-1 Development of Automation Systems: The impact of IEC standards

Session Chair(s): *Georg Frey, Kleanthis Thramboulidis*

Paper starts at page

 <b>An IEC 61499 Interpretation and Implementation Focused on Usability</b>	184
<i>Florian Wagner, Joachim Bohl, Georg Frey</i>	
 <b>CEC Designer: Domain Specific Modelling for the Industrial Automation Based on the IEC 61499 Standard</b>	192
<i>Marco Colla, Tiziano Leidi, Murat Kunt, Jean-Philippe Thiran</i>	
 <b>Framework for Management of Replicated IEC 61499 Applications</b>	200
<i>Adriano Santos, Mario de Sousa</i>	
 <b>An Engineering Method for Batch Process Automation using a Component Oriented Design based on IEC 61499</b>	207
<i>Wilfried Lepuschitz, Alois Zoitl</i>	
 <b>Implementation Alternatives for the OMAC State Machines Using IEC 61499</b>	215
<i>Nils H. Hagge, Bernardo Wagner</i>	
 <b>A Survey of Distributed Intelligence in Automation in European Industry, Research and Market</b>	221
<i>Ivanka Terzic, Alois Zoitl, Bernard Favre-Bulle, Thomas Strasser</i>	

Tuesday










9/16/2008

WiP Room: 1 4:00 PM - 5:30 PM

S 2 Computational Intelligence

Session Chair(s): Thilo Sauter, Athanasios Kalogeras

Paper starts at page





 <b>Application-based approach for automatic texture defect recognition on synthetic surfaces</b>	229
<i>Marcus Niederhöfer, Volker Lohweg</i>	
 <b>Integrating Agents and Soft Computing in Intelligent Manufacturing System Models</b>	233
<i>Luiz Márcio Spinosa, Leandro Coelho</i>	
 <b>Efficient failure-free Foundry Production</b>	237
<i>Yoseba Penya, Pablo García Bringas, Argoitz Zabala</i>	
 <b>Modular Assembly Machine - Ontology Based Concept</b>	241
<i>Ivanka Terzic, Munir Merdan, Alois Zoitl, Ingo Hegny</i>	
 <b>Gesture Recognition Using Evolution Strategy Neural Network</b>	245
<i>Johan Hägg, Batu Akan, Baran Cürüklü, Lars Asplund</i>	
 <b>A biological inspired multi-agent based shop floor control architecture for manufacturing systems</b>	249
<i>Dania A. El Kebbe, Juan Gomez-Fernandez</i>	
 <b>Green Surveillance Applications</b>	253
<i>Javier Silvestre-Blanes</i>	
 <b>Descending Deviation Optimization Techniques For Scheduling Problems</b>	257
<i>Kevin McCarty, Milos Manic</i>	
 <b>Refining the Window Size of Sliding Window Operations in Running Data Processing Systems</b>	261
<i>Bernhard Wolf, Mario Neugebauer</i>	

Track 4 Room: 2 4:00 PM - 5:30 PM

S 3 Process control I

Session Chair(s): Ramón Piedrafita, Corina Popescu

Paper starts at page

 <b>Considerations on PID Controller Operation: Application to a Continuous Stirred Tank Reactor</b>	265
<i>Orlando Arrieta, Ramon Vilanova, Victor M. Alfaro, Romualdo Moreno</i>	
 <b>Analytical Robust Tuning of PI Controllers for First-Order-Plus-Dead-Time Processes</b>	273
<i>Victor M. Alfaro, Ramon Vilanova, Orlando Arrieta</i>	
 <b>Sucker-Rod Pumping System: Simulator and Dynamic Level Control Using Downhole Pressure</b>	282
<i>Bernardo Ordonez, Andres Codas, Ubirajara Moreno, Alex Teixeira</i>	
 <b>Multivariable PID Control Tuning: A Controller Validation Approach</b>	289
<i>Pedro Balaguer, Norhaliza Abdul Wahab, Reza Katebi, Ramon Vilanova</i>	

Tuesday

9/16/2008

SS 06


Room: 105

4:00 PM - 5:30 PM

SS 06 Building and Home Automation


Session Chair(s): Alexander Klapproth, Stefan Knauth

Paper starts at page

 **An Adaptive Network Architecture for Home- and Building Environments**


295

*Rolf Kistler, Stefan Knauth, Alexander Klapproth*

 **A Data Exchange Format for the Engineering of Building Automation Systems**

303

*Stefan Runde, Alexander Fay*

 **Functional safety and system security in automation systems - a life cycle model**

311

*Thomas Novak, Albert Treytl*

 **Localization by Superposing Beats: First Laboratory Experiments and Theoretical Analyzes**

319

*Matthias Schneider, Ralf Salomon*

Track 6


Room: 108

4:00 PM - 5:30 PM

S 2 Automation and Sensors


Session Chair(s): Juan Jesus Garcia

Paper starts at page

 **Practical Obstacle Avoidance Using Potential Field for a Nonholonomic Mobile Robot with Rectangular Body**


326

*Hiroaki Seki, Satoshi Shibayama, Yoshitsugu Kamiya, Masatoshi Hikizu*

 **Localization in a wide range of industrial environments using relative 3D ceiling features**


333

*Daniel Lecking, Oliver Wulf, Bernardo Wagner*

 **Optimal Test-Point Positions For Calibrating An Ultrasonic Lps System**


338

*F. Daniel Ruiz, Jesús Ureña, José M. Villadangos, Isaac Gude, J. Jesús García, Alvaro Hernández, Ana Jiménez*

 **Two Camera System for Robot Applications; Navigation**

345

*Jörgen Lidholm, Fredrik Ekstrand, Lars Asplund*

 **A fast Visual Line Segment Tracker**

353

*Peer Neubert, Teresa Vidal-Calleja, Simon Lacroix, Peter Protzel*

SS 02


Room: 109

4:00 PM - 5:30 PM

SS 02-2 Development of Automation Systems: The impact of IEC standards

Session Chair(s): Georg Frey, Kleanthis Thramboulidis

Paper starts at page

 **Restricting IEC 61131-3 Programming Languages for use on High Integrity Applications**


361

*Mario de Sousa*

 **Transformation of existing IEC 61131-3 automation projects into control logic according to IEC 61499**


369

*Christoph Sünder, Monika Wenger, Christian Hanni, Ivo Gosetti, Heinrich Steininger, Josef Fritsche*

 **Analyzing the Liveliness of IEC 61499 Function Blocks**

377

*Nils H. Hagge, Bernardo Wagner*

 **A Formal Approach to Check and Schedule Reconfigurable Embedded Control Systems**

383

*Mohamed Khalgui, Olfa Mosbahi, Hans-Michael Hanisch*

## Track 2

Room: 110





4:00 PM - 5:30 PM

S 1

## Real-Time Ethernet Networks

Session Chair(s): *Francoise Simonot-Lion, Julian Proenza*

Paper starts at page

	<b>Segmentation of Standard Ethernet Messages in the Time-triggered Ethernet</b>	392
	<i>Vaclav Mikolasek, Astrit Ademaj, Stanislav Racek</i>	
	<b>An Evaluation of Switched Ethernet and Linux Traffic Control for Real-Time Transmission</b>	400
	<i>Joan Vila-Carbó, Joaquim Tur-Masanet, Enrique Hernández-Orallo</i>	
	<b>A performance analysis of EtherCAT and PROFINET IRT</b>	408
	<i>Gunnar Prytz</i>	
	<b>An Arbitration-based Access Scheme for EtherCAT Networks</b>	416
	<i>Gianluca Cena, Adriano Valenzano, Claudio Zunino</i>	



WiP Room: 1 9:00 AM - 11:00 AM

## S 3 Dependability Aspects

Session Chair(s): Thilo Sauter, Athanasios Kalogeras

Paper starts at page

	<b>A Mechanism for Deadline Missing Prediction in Systems based on Distributed Threads</b>	424
	<i>Patricia Della M�ea Plentz, Carlos Montez, R�omulo Silva de Oliveira</i>	
	<b>Accurate Modeling Of Repair Time In Two-Machine Production Lines</b>	428
	<i>Hassanein Amer, Ramez Daoud</i>	
	<b>Web services on Deeply Embedded Devices with Real-Time Processing</b>	432
	<i>Guido Moritz, Steffen Pr�uter, Frank Golaowski, Dirk Timmermann</i>	
	<b>Proposal of an Industrial Information System Model for Automatic Performance Evaluation</b>	436
	<i>Eduardo Alves Portela Santos, Eduardo de Freitas Rocha Loures, Fernando Deschamps, Marco Antonio Buseti de Paula</i>	
	<b>A Simulation Approach to a Real-Time Ethernet Protocol: EtherCAT</b>	440
	<i>Lucia Seno, Claudio Zunino</i>	
	<b>Verification and Analysis of Dependable Automotive Communication Systems based on HW/SW Co-Simulation</b>	444
	<i>Michael Karner, Eric Armengaud, Christian Steger, Reinhold Wei�, Daniel Watzenig, Gernot Knoll</i>	
	<b>A Model for Security Management of SCADA Systems</b>	448
	<i>Ivamo M. dos Anjos, Agostinho M. Brito Jr., Paulo S. Motta Pires</i>	
	<b>Modeling Flexible Mechatronical Based Assembly Systems through Simulation Support</b>	452
	<i>Martijn Rooker, Thomas Strasser, Gerhard Ebenhofer, Michael Hofmann, Ricardo Velez</i>	
	<b>Development of a Flexible Gateway Platform for Automotive Networks</b>	456
	<i>Andreas Puhm, Peter Roessler, Marcus Wimmer, Rafael Swierczek, Peter Balog</i>	
	<b>Why IEEE 1394 ("FireWire") might not be a perfect choice for factory automation today - a case study from the printing industry</b>	460
	<i>Andreas Rehkopf, Johannes Weber, Hans-Detlef Groeger</i>	
	<b>Using a CORBA Synchronous Scheduling Service in Pick&amp;Place Operations</b>	464
	<i>Isidro Calvo, Itziar Cabanes, Adri�n Noguero, Asier Zubizarreta, Luis Almeida, Marga Marcos</i>	
	<b>Denial-of-Service in Automation Systems</b>	468
	<i>Wolfgang Granzer, Christian Reinisch, Wolfgang Kastner</i>	
	<b>Real-Time Enabled Debugging for Distributed Systems</b>	472
	<i>Georg Gaderer, Patrick Loschmidt, Thilo Sauter</i>	
	<b>Network Diagnostics for Industrial Ethernet</b>	476
	<i>Oliver Kleineberg, Max Felser</i>	
	<b>Security in Virtual Automation Networks</b>	480
	<i>Dirk Reinelt, Mario Wolframm</i>	
	<b>Designing and Verifying Media Management in ReCANcentrate</b>	484
	<i>Manuel Barranco, Juli�n Proenza, Lu�s Almeida</i>	
	<b>Use of Interleaving and Error Correction to Infrared Patterns for the Improvement of Position Estimation Systems</b>	488
	<i>Nikos Petrellis, Fotios Gioulekas, Michael Birbas, John Kikidis, Alexios Birbas</i>	
	<b>A Secure Agent Platform for Active RFID</b>	492
	<i>Albert Treytl, Werner Spenger, Bilal Riaz</i>	
	<b>Clock Synchronization of PTP-based Devices through PROFINET IO Networks</b>	496
	<i>Paolo Ferrari, Alessandra Flammini, Daniele Marioli, Stefano Rinaldi, Emiliano Sisinni, Andrea Taroni, Francesco Venturini</i>	

Wednesday

9/17/2008

Track 4






Room: 2

9:00 AM - 11:00 AM

S 4 Applications

Session Chair(s): J. Jesús García

Paper starts at page

 <b>Event-Based Control and Wireless Sensor Network for Greenhouse Diurnal Temperature Control: A Simulated Case Study</b>	500
<i>Andrzej Pawlowski, José Luis Guzmán, Francisco Rodríguez, Manuel Berenguel, José Sánchez, Sebastián Dormido</i>	
 <b>Petri Nets based Coordination of Flexible Autonomous Guided Vehicles in Flexible Manufacturing Systems</b>	508
<i>David Herrero-Pérez, Humberto Martínez-Barberá</i>	
 <b>Resource Management and Usage in highly flexible and adaptable Manufacturing Systems</b>	516
<i>Michael Heinze, Joern Peschke, Arndt Lueder</i>	
 <b>Improvement of output voltage using six-phase matrix converter</b>	524
<i>Manuel Ortega, Francisco Jurado</i>	
 <b>An Application of BPEL for Service Orchestration in an Industrial Environment</b>	530
<i>Juha Puttonen, Andrei Lobov, Jose Luis Martinez Lastra</i>	

Track 4






Room: 3

9:00 AM - 11:00 AM

S 5 Fault detection, diagnostics and prognostics

Session Chair(s): Thomas Wagner

Paper starts at page

 <b>Fault Diagnosis of Electrical Systems using Interpreted Petri Nets</b>	538
<i>Alejandra Santoyo Sanchez, Elvia Ruiz Beltran, Luis Aguirre Salas, Victor Ortiz Muro</i>	
 <b>Extension of model-reference based estimator for fault isolation in a bioprocess</b>	547
<i>Nabil Kabbaj, Andrei Doncescu</i>	
 <b>Network Calculus Based Fault Diagnosis Decision-Making for Networked Control Systems</b>	552
<i>Christophe Aubrun, Jean-Philippe Georges, Dominique Sauter, Eric Rondeau</i>	
 <b>Diagnosis of Intermittent Fault Dynamics</b>	559
<i>Antonio Correcher, Emilio García, Francisco Morant, Ramón Blasco-Giménez, Eduardo Quiles</i>	
 <b>A Neural Network MultiAgent Architecture Applied to Fieldbus Intelligent Control</b>	567
<i>Vinicius Machado, Adriaio Doria Neto, Jorge Dantas de Melo, Leonardo Ramalho, Juliana Medeiros</i>	

Track 3





Room: 105

9:00 AM - 11:00 AM

S 1 Scheduling

Session Chair(s):

Paper starts at page

 <b>Scheduling of Semi-Independent Real-Time Components: Overrun Methods and Resource Holding Times</b>	575
<i>Moris Behnam, Insik Shin, Thomas Nolte, Mikael Nolin</i>	
 <b>Adaptive real-time scheduling for legacy applications</b>	583
<i>Luca Abeni, Luigi Palopoli</i>	
 <b>Scheduling Analysis of Distributed Real-Time Systems Under Functional Constraints</b>	591
<i>Alexander Metzner</i>	
 <b>Exact Scheduling Analysis of Accumulatively Monotonic Multiframe Tasks Subjected to Release Jitter and Arbitrary Deadlines</b>	600
<i>Areej Zuhily, Alan Burns</i>	

Wednesday

9/17/2008

Track 1






Room: 109

9:00 AM - 11:00 AM

S 1 Information Technology in Automation I

Session Chair(s): Kai Hansen, Wolfgang Kastner

Paper starts at page

-  **Generic Service Information System Architecture - A Reference Model Based Approach for Evaluating Information Systems in Industrial Service** 608  
*Michael Amberg, Timo Holm, Kristian Dencovski, Mathias Maurmaier*
-  **AutomationML – the glue for seamless Automation Engineering** 616  
*Rainer Drath, Arndt Lüder, Jörn Peschke, Lorenz Hundt*
-  **Challenges in the Development of Mechatronic Systems: The Mechatronic Component** 624  
*Kleanthis Thramboulidis*
-  **XML-based Middleware Approach for industrial wireless Communication Systems** 632  
*Volker Schuermann, Aurel Buda, Joerg F. Wollert*
-  **OPC UA supporting the automated engineering of production monitoring and control systems** 640  
*Miriam Schleipen*

Track 2






Room: 110

9:00 AM - 11:00 AM

S 2 Industrial Wireless Communications I

Session Chair(s): Christos Koulamas, Nicolas Navet

Paper starts at page

-  **Exploiting Publish/Subscribe Communication in Wireless Mesh Networks for Industrial Scenarios** 648  
*Andre Herms, Michael Schulze, Joerg Kaiser, Edgar Nett*
-  **Synchronized Wireless Sensor Networks for Coexistence** 656  
*Paolo Ferrari, Alessandra Flammini, Daniele Marioli, Emiliano Sisinni, Andrea Taroni*
-  **Some Factors Affecting Performance of a Wireless Sensor Network – Entropy-Based Analysis** 664  
*Marko Paavola, Mika Ruusunen*
-  **Performance Evaluation of a Compression Algorithm for Wireless Sensor Networks in Monitoring Applications** 672  
*Ivanovitch Medeiros Dantas Silva, Luiz Affonso Guedes, Francisco Vasques*
-  **On the Timeliness of Multi-Hop Non-Beaconed ZigBee Broadcast Communications** 679  
*Paulo Bartolomeu, José Fonseca, Francisco Vasques*

Keynote


Room: 5

11:30 AM - 12:30 PM

K 3 Keynote Speech

Session Chair(s): J. David Irwin

Paper starts at page

-  **Wireless Control in Theory, Practice and Production**  
*Jan-Erik Frey*

WiP

Room: 1

1:30 PM - 3:30 PM

S 4

Modelling and Tools

Session Chair(s): Thilo Sauter, Athanasios Kalogeras

Paper starts at page

 <b>Customer-oriented Innovation of Engineering Tools – a Holistic Methodology to Close the Gap to Customer Productivity</b>	687
<i>Kristian Dencovski, Thomas Wagner</i>	
 <b>Concept for Proactive Ramp-up Validation of Body-in-White Lines</b>	693
<i>Sven Mandel, Thomas Bär, Alexander Fay</i>	
 <b>Virtual Prototyping through Co-simulation of a Cartesian Plotter</b>	697
<i>Marcel A. Groothuis, Arjen S. Damstra, Jan F. Broenink</i>	
 <b>Communication Performance Simulation for Object Access of BACnet Web Service Building Facility Monitoring Systems</b>	701
<i>Chuzo Ninagawa, Tomotaka Sato, Yahiko Kawakita</i>	
 <b>Sharing IO Devices using Hardware Virtualization Method for Component-Based Industrial Controllers</b>	705
<i>Tatsuya Maruyama, Tsutomu Yamada</i>	
 <b>On Working with the Concept of Integration Ontologies</b>	709
<i>Andreas Gössling, Martin Wollschlaeger</i>	
 <b>XML-based Modeling of an Alarm Management</b>	713
<i>Annerose Braune, Stefan Hennig</i>	
 <b>Towards Migrating Legacy Real-Time Systems to Multi-Core Platforms</b>	717
<i>Farhang Nemat, Johan Kraft, Thoman Nolte</i>	
 <b>Message-Oriented and Workflow-Based Inter-Process Communication for Distributed Manufacturing</b>	721
<i>Patrick Otto, Erik Hennig, Martin Wollschlaeger</i>	
 <b>Rapid Migration and Commissioning of Industrial Equipment</b>	725
<i>Volodymyr Vasyutynskyy, Jens Naake, Andre Roeder, Klaus Kabitzsch</i>	
 <b>Feasibility Analysis for Networked Control Systems by Simulation in Modelica</b>	729
<i>Liu Liu, Georg Frey</i>	
 <b>Leveraging Model-driven Development for Automation Systems Development</b>	733
<i>Mathias Maurmaier</i>	

## Track 4

Room: 2

1:30 PM - 3:30 PM

## S 6 Automation systems

Session Chair(s): Andrzej Pawlowski, David Herrero-Pérez

Paper starts at page

-  **An asymptotic discrete second order sliding mode control law for highly non stationary systems** 738  
*Mohamed Mihoub, Ahmed Said Nouri, Ridha Ben Abdennour*
-  **Efficient management of an advanced data acquisition system with real time streaming** 745  
*Enrique García, Juan García, Jesús Ureña, Álvaro Hernández, Ana Jiménez, M<sup>a</sup> Jesus Diaz*
-  **Application Of The Supervisory Control Theory In The Project Of A Robot-Centered, Variable Routed System Controller** 751  
*Eduardo Portela, Daniel Silva, Agnelo Vieira, Marco Buseti*
-  **Environment Modelling for the Robust Motion Planning and Control of Planar Rigid Robot Manipulators** 759  
*Luca Capisani, Tullio Facchinetti, Antonella Ferrara, Alessandro Martinelli*
-  **Application of Latent Nestling Method using Coloured Petri Nets for the Fault Diagnosis in the Wind Turbine Subsets** 767  
*Leonardo Rodríguez Urrego, Emilio García Moreno, Francisco José Morant Anglada, Antonio Correcher Salvador, Eduardo Quiles Cucarella*

## Track 3






Room: 105

1:30 PM - 3:30 PM

## S 2 Real-Time Systems

Session Chair(s):

Paper starts at page

-  **Pinpointing Interrupts in Embedded Real-Time Systems using Context Checksums** 774  
*Daniel Sundmark, Henrik Thane*
-  **Framework for Real-Time Analysis in Rubus-ICE** 782  
*Kaj Hänninen, Jukka Mäki-Turja, Staffan Sandberg, John Lundbäck, Mats Lindberg, Mikael Nolin, Kurt-Lennart Lundbäck*
-  **Automatic Refinement-based Specification of Feasible Control Tasks in Benchmark Production Systems** 789  
*Mohamed Khalgui, Hans-Michael Hanisch*
-  **A Quantitative Study on Automatic Validation of the Diagnostic Services of Electronic Control Units** 799  
*Philipp Peti, Armin Timmerberg, Thomas Pfeffer, Simon Müller, Christoph Rätz*
-  **Functional and Structural Properties in the Model-Driven Engineering Approach** 809  
*Daniela Cancila, Roberto Passerone*

## Track 6





Room: 108

1:30 PM - 3:30 PM

## S 3 Simultaneous Localization and Mapping (SLAM)

Session Chair(s): Eduardo Montijano

Paper starts at page

-  **Delayed Inverse-Depth Feature Initialization for Sound-Based SLAM** 817  
*Rodrigo Munguia, Antoni Grau*
-  **Analysis of Map Alignment Techniques in visual SLAM systems** 825  
*Monica Ballesta, Oscar Reinoso, Arturo Gil, Miguel Julia, Luis Paya*
-  **Line-Based Incremental Map Building Using Infrared Sensor Ring** 833  
*Danilo Navarro García, Gines Benet Gilabert, Francisco Blanes*
-  **3D-Based Monocular SLAM for Mobile Agents Navigating in Indoor Environments** 839  
*Dejan Pangercic, Radu Bogdan Rusu, Michael Beetz*

## Track 1





Room: 109

1:30 PM - 3:30 PM

## S 2 Information Technology in Automation II

Session Chair(s): Georg Frey, Jürgen Jasperneite

Paper starts at page

-  **Towards a Time-Constrained Web Service Infrastructure for Industrial Automation** 846  
Markus Mathes, Steffen Heinzl, Bernd Freisleben
-  **Extending the Watchdog Pattern for Multi-threaded Windows based Traffic Management and Control Applications** 854  
Christoph Stoegerer, Wolfgang Kastner
-  **A Novel Method for Auto Configuration of Realtime Ethernet Networks** 861  
Jahanzaib Imtiaz, Karl Weber, Juergen Jasperneite, Gunnar Lessmann, Franz-Josef Goetz
-  **A Lookup Service in an Interconnected World of Uniquely Identified Objects** 869  
Elias Polytachos, Nektarios Leontiadis, Stylianos Eliakis, Katerina Pramatarí

## Track 2





Room: 110

1:30 PM - 3:30 PM

## S 3 Industrial Wireless Communications II

Session Chair(s): Max Felser, Christos Koulamas

Paper starts at page

-  **Meeting Reliability and Real-Time Demands in Wireless Industrial Communication** 877  
Magnus Jonsson, Kristina Kunert
-  **Is CSMA/CA really efficient against interference in a Wireless Control System? An experimental answer** 885  
Matteo Bertocco, Giovanni Gamba, Alessandro Sona
-  **Evaluating Severe Noise Interference in IEEE 802.15.4 based Location Systems** 893  
José Oliveira, Paulo Bartolomeu, José Fonseca, Luís Costa
-  **When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard** 899  
Anna N. Kim, Fredrik Hekland, Stig Petersen, Paula Doyle

## Track 4





Room: 2

4:00 PM - 5:30 PM

## S 7 Computer and control systems

Session Chair(s): Christophe Aubrun, Leonardo Rodríguez Urrego

Paper starts at page

-  **Optimal On-line (m,k)-firm Constraint Assignment for Real-time Control Tasks Based on Plant State Information** 908  
Flavia Felicioni, Jia Ning, Françoise Simonot-Lion, Song YeQiong
-  **Triangular Decoupling with Simultaneous Disturbance Rejection for General Linear Time Delay Systems via Measurement Output Feedback** 916  
Fotis N. Koumboulis, George E. Panagiotakis
-  **Step State-feedback Supervisory Control of Discrete Event Systems using Interpreted Petri Nets** 926  
Alejandra Santoyo Sanchez, Antonio Ramirez Trevino, Carlos De Jesus Velasquez, Luis Aguirre Salas
-  **Structuring of Large Scale Distributed Control Programs with IEC 61499 Subapplications and a Hierarchical Plant Structure Model** 934  
Thomas Strasser, Martijn Rooker, Gerhard Ebenhofer, Alois Zoitl, Christoph Sünder, Antonio Valentini, Allan Martel

## Track 3

Room: 105





4:00 PM - 5:30 PM

S 3

## Sensor Networks

Session Chair(s):

Paper starts at page

 <b>A Topology Management Protocol with Bounded Delay for Wireless Sensor Networks</b>	942
<i>Emanuele Toscano, Lucia Lo Bello</i>	
 <b>Web-service enabled Wireless Sensors in SOA environments</b>	952
<i>Domnic Savio, Stamatis Karnouskos</i>	
 <b>FZepel: RF-level Power Consumption Measurement (RF-PM) for Zigbee Wireless Sensor Network-Towards Cross Layer Optimization</b>	959
<i>Md. Rezaul Hoque Khan, Roberto Passerone, David Macii</i>	
 <b>CoReDac: Collision-Free Command-Response Data Collection</b>	967
<i>Thiemo Voigt, Fredrik Österlind</i>	

## Track 6

Room: 108



4:00 PM - 5:30 PM

S 4

## Modelling and simulation

Session Chair(s): Antoni Grau

Paper starts at page

 <b>Modeling of MR Fluid Actuator Enabling Safe Human-Robot Interaction</b>	974
<i>Muhammad Rehan Ahmed, Ivan G Kalaykov, Anani V Ananiev</i>	
 <b>Sensor and actuator modeling of a realistic wheeled mobile robot simulator</b>	980
<i>José Gonçalves, José Lima, Hélder Oliveira, Paulo Costa</i>	
 <b>Humanoid Robot Simulation with a Joint Trajectory Optimized Controller</b>	986
<i>José Luis Lima, José Alexandre Gonçalves, Paulo Gomes Costa, António Paulo Moreira</i>	
 <b>Position-Based Navigation Using Multiple Homographies</b>	994
<i>Eduardo Montijano, Carlos Sagues</i>	

## Track 1

Room: 109




4:00 PM - 5:30 PM

S 3

## Information Technology in Automation III

Session Chair(s): Georg Frey, Jürgen Jasperneite

Paper starts at page

 <b>Optimized FPGA Implementations of Demanding PLC Programs Based on Hardware High-Level Synthesis</b>	1002
<i>Christoforos Economakos, George Economakos</i>	
 <b>BOUNCE, a Concept to Measure Picosecond Time Intervals with Standard Hardware</b>	1010
<i>Ralf Joost, Ralf Salomon</i>	
 <b>Performance Investigation and Optimization of IEEE802.15.4 for Industrial Wireless Sensor Networks</b>	1016
<i>Mohsin Hameed, Henning Trsek, Olaf Graeser, Juergen Jasperneite</i>	

## Track 2

Room: 110

4:00 PM - 5:30 PM

S 4


## Applications and Innovations

Session Chair(s): *Jose Alberto Fonseca, Marga Marcos*

Paper starts at page

 **Synchronization in a Force Measurement System Using EtherCAT**


1023

*Mattias Rehnman, Tobias Gentzell* **Reactivity Analysis of different Networked Automation System Architectures**

1031

*Jürgen Greifeneder, Georg Frey* **Using Wireless Sensor Networks to Enable Increased Oil Recovery**

1039

*Simon Carlsen, Stig Petersen, Amund Skavhaug, Paula Doyle* **Simulative Investigation of Intermediate Checksum Schemes in the Presence of Deadlines**

1049

*Andreas Willig*



WiP Room: 1 9:00 AM - 10:30 AM

S 5 Control Systems

Session Chair(s): Thilo Sauter

Paper starts at page

	<b>Next Generation of Embedded Controllers: Developing FPGA-based reconfigurable controllers using Matlab/Simulink</b>	1055
	<i>T. Barlas, M. Moallem</i>	
	<b>Smith predictor based intelligent control of multiple-input-multiple-output systems with unknown delays</b>	1059
	<i>Jorge Herrera, Asier Ibeas, Salvador Alcantara, Ramon Vilanova, Pedro Balaguer</i>	
	<b>Using Neuroevolution for Optimal Impedance Control</b>	1063
	<i>Jose de Gea, Frank Kirchner</i>	
	<b>Multi-Domain Model-Driven Design of Industrial Automation and Control Systems</b>	1067
	<i>Thomas Strasser, Martijn Rooker, Gerhard Ebenhofer, Ingo Hegny, Monika Wenger, Christoph Sünder, Allan Martel, Antonio Valentini</i>	
	<b>Online Management and Control System for growing of monocrystal semiconductor materials in multi-zone furnaces</b>	1072
	<i>Dirk Bräuer, Andreas Rehkopf</i>	
	<b>A java based tool for distributed control systems</b>	1076
	<i>Mikel Eguiraun, Josu Jugo</i>	
	<b>A Closed Loop Welding Controller for a Rapid Manufacturing Process</b>	1080
	<i>Giovanni Muscato, Giacomo Spampinato, Luciano Cantelli</i>	
	<b>Extended Kalman filtering using wireless sensor networks</b>	1084
	<i>Pietro Muraca, Paolo Pugliese, Giuseppe Rocca</i>	
	<b>A neuro-fuzzy delay compensator for distributed control systems</b>	1088
	<i>Ana Antunes, Fernando Dias, José Vieira, Alexandre Mota</i>	
	<b>Stabilization of a 5-link Bipedal Robot by means of Dorsal Movement Compensation</b>	1092
	<i>Luiz R. Douat, Eugênio B. Castelan, Ubirajara F. Moreno</i>	
	<b>Analysis of evaluation metrics for networked control systems</b>	1096
	<i>Carlos H. Costa, Carlos B. Montez, Ubirajara F. Moreno</i>	
	<b>Component based Colored Petri Net model for Ethernet based Networked Control Systems</b>	1100
	<i>Abouelabbas Ghanaim, Georg Frey</i>	
	<b>Adaptation of Powered Wheelchairs for Quadriplegic Patients with Reduced Strength</b>	1104
	<i>Margarida Urbano, José Fonseca, Urbano Nunes, Luís Figueiredo, Arminda Lopes</i>	
	<b>Supervisory System for Hybrid Productive Systems based on Bayesian Networks and OO-DPT Nets</b>	1108
	<i>Roy Andres Gomez, Jose Isidro Garcia Melo, Paulo Eigi Miyagi</i>	

## Track 4





Room: 2

9:00 AM - 10:30 AM

## S 8 Distributed control

Session Chair(s): David Gómez-Gutiérrez

Paper starts at page

 <b>Function blocks for decentralised analysis of product flow paths</b>	1112
<i>Gustavo Quirós, Martin Mertens, Ulrich Epple</i>	
 <b>UML-Based Modeling and Model-Driven Development of Distributed Control Systems</b>	1120
<i>Francesco Basile, Pasquale Chiacchio, Domenico Del Grosso</i>	
 <b>Evaluation of Effectiveness and Impact of Decentralized Automation</b>	1128
<i>Thomas Wagner, Andreas Schertl, Jürgen Elger, Jan Vollmar</i>	
 <b>Measuring the Effort of a Reconfiguration Processes</b>	1137
<i>Amro Farid, Wuttiaphat Covanich</i>	

## WiP

Room: 3

9:00 AM - 10:30 AM

## S 6 Wireless Communications

Session Chair(s): Athanasios Kalogeras

Paper starts at page

 <b>Porting application between wireless sensor network software platforms: TinyOS, MANTIS and ZigBee</b>	1145
<i>Mohammad Mostafizur Rahman Mozumdar, Francesco Gregoretti, Luciano Lavagno, Laura Vanzago</i>	
 <b>Management Of A Real Factory Simulation Connected With A Physical Platform Using Rfid-Imsii Methodology</b>	1149
<i>Julio C. Encinas, Javier de las Morenas, Andrés García Higuera, José Manuel Pastor García, Rafael Otaí Simal</i> <b>"Paper withdrawn"</b>	
 <b>Investigating wireless networks coexistence issues through an interference aware simulator</b>	1153
<i>Matteo Bertocco, Giovanni Gamba, Alessandro Sona, Federico Tramarin</i>	
 <b>An Experimental Evaluation on Using TDMA over 802.11 MAC for Wireless Networked Control Systems</b>	1157
<i>Gennaro Boggia, Pietro Camarda, Alfredo Grieco, Giammarco Zacheo</i>	
 <b>DSTiPE Algorithm for Fuzzy Spatio-Temporal Risk Calculation in Wireless Environments</b>	1161
<i>Kurt Derr, Milos Manic</i>	
 <b>Distributed Asset Tracking using Wireless Sensor Network</b>	1165
<i>Li Qun Zhuang, Dan Hong Zhang, Jing Bing Zhang, Ian Kamajaya</i>	
 <b>Preamble Detection for Wireless Clock Synchronization in Frequency Selective Fading Channels</b>	1169
<i>Aneeq Mahmood, Georg Gaderer</i>	
 <b>Modular Wireless Fieldbus Gateway For Fast and Reliable Sensor/Actuator Communication</b>	1173
<i>Ralf Heynicke, Housam Wattar, Dirk Krüger, Gerd Scholl</i>	
 <b>Genetic Machine Learning Approach for Data Fusion Applications in Dense Wireless Sensor Networks</b>	1177
<i>Alex Pinto, Benedito Bitencort, Mário Dantas, Carlos Montez, Francisco Vasques</i>	
 <b>Wireless Technologies for Safe Automation – Insights in Protocol Development</b>	1181
<i>Axel Sikora, Dirk Lill</i>	
 <b>Evaluating WiMAX for Vehicular Communication Applications</b>	1185
<i>André Costa, Hugo Proenca, Paulo Pedreiras, José Fonseca, Alvaro Gomes, Joao Nuno Matos, Jorge Sales Gomes</i>	
 <b>On the adequacy of 802.11p MAC protocols to support safety services in ITS</b>	1189
<i>Nuno Ferreira, José Fonseca, J. Sales Gomes</i>	
 <b>CWFC: A Contention Window Fuzzy Controller for QoS support on IEEE 802.11e EDCA</b>	1193
<i>Salvatore Vittorio, Emanuele Toscano, Lucia Lo Bello</i>	

Thursday

9/18/2008

Track 3





Room: 105

9:00 AM - 10:30 AM

S 4 Real Time Communication

Session Chair(s):

Paper starts at page

-  **Self-configuration of an Adaptive TDMA wireless communication protocol for teams of mobile robots** 1197  
*Frederico Santos, Luis Almeida, Luis Seabra Lopes*
-  **Properties of BuST and Timed Token Protocols in Managing Hard Real-Time Traffic** 1205  
*Gianluca Franchino, Giorgio Buttazzo, Tullio Facchinetti*
-  **Less Pessimistic Worst Case Delay Analysis for Packet-Switched Networks** 1213  
*Mattias Wecksten, Magnus Jonsson*
-  **Probabilistic upper bounds for heterogeneous flows using a Static Priority Queueing on an AFDX network** 1220  
*Frédéric Ridouard, Jean-Luc Scharbarg, Christian Fraboul*

SS 05





Room: 109

9:00 AM - 10:30 AM

SS 05 Industrial Agents

Session Chair(s): *Paulo Leitao, Francisco Maturana*

Paper starts at page

-  **Decision Support System in a Service-oriented Control Architecture for Industrial Automation** 1228  
*Paulo Leitao, Marco Mendes, Armando Colombo*
-  **Distributed Multi Sensor Agent for Composite Curing Control** 1236  
*Francisco Maturana, Dan L. Carnahan, Donald D. Theroux, Ken H. Hall*
-  **Determination of the Itinerary of Imprecise Mobile Agents using an Adaptive Approach** 1244  
*Luciana Rech, Carlos Montez, Rômulo de Oliveira, Fábio Reis Cecin, Cláudio Geyer*
-  **Control the chaos in agent based manufacturing systems** 1252  
*Kamel Benaïssa, Daniel Diep, Alexandre Dolgui*

Track 5




Room: 110

9:00 AM - 10:30 AM

S 1

Session Chair(s):

Paper starts at page

-  **Application of a Group Search Optimization based Artificial Neural Network to Machine Condition Monitoring** 1260  
*Shan He, Xiaoli Li*
-  **Neural Network Modeling of Magnetic Hysteresis** 1267  
*Vahab Akbarzadeh, Maryam Davoudpour, Alireza Sadeghian*
-  **A neural network delay compensator for networked control systems** 1271  
*Ana Antunes, Fernando Dias, Alexandre Mota*

Thursday

9/18/2008

Track 4


Room: 2

11:15 AM - 12:30 PM

S 9 Design tools

Session Chair(s): Domenico Del Grosso

Paper starts at page

 **Automatic generation of PLC code beyond the nominal sequence**  
*Knut Guettel, Peter Weber, Alexander Fay*

1277

 **Design-Time Management of Run-Time Data in Industrial Embedded Real-Time Systems Development**  
*Andreas Hjertström, Dag Nyström, Mikael Nolin, Rikard Land*

1285

 **Automatic Generation of Bond Graph Models of Process Plants**  
*Sebastian Beez, Alexander Fay, Nina Thornhill*

1294

Track 4


Room: 3

11:15 AM - 12:30 PM


S10 Process control II

Session Chair(s): Amro Farid


Paper starts at page

 **Network based controller applied to a highly dynamic system**  
*Michael Morawski, Antoni Zajaczkowski*

1302

 **From monotone inequalities to Model Predictive Control**  
*Guezzi Abdelhak, Philippe Declerck, Jean-Louis Boimond*

1310

 **Centralized PID Control by Decoupling for TITO Processes**  
*Fernando Morilla, Francisco Vazquez, Juan Garrido*

1318

SS 04

Room: 108

11:15 AM - 12:30 PM


SS 04 Auto-ID Applications in the supply chain

Session Chair(s): Athanasios Kalogeras, Ioannis Mourtos


Paper starts at page

 **Simulation and Design for 3D RFID Application**  
*Liu Wei, Wong Ming Mao, Tan Chak*

1326

 **Traceability applications based on Discovery Services**  
*Jose Juan Cantero, Miguel Angel Guijarro, Guillermo Arrebola, Ernesto Garcia, Janie Baños, Mark Harrison, Thomas Kelepouris*

1332

 **A Low-Cost Perspective in Identifier-Based Services of Supply Chains**  
*Zsolt Kemeny, Elisabeth Ilie-Zudor, Marcell Szathmari, Laszlo Monostori, Erik A. F. Langius*

1338

SS 08


Room: 109

11:15 AM - 12:30 PM


SS 08 Interactive media with personalized networked devices

Session Chair(s): Raffaele Bolla, Mingyu Lim

Paper starts at page

 **A general collaborative platform for mobile multi-user applications**  
*Mingyu Lim, Niels Nijdam, Nadia Magnenat-Thalmann*

1346

 **A Context-Aware Architecture for QoS and Transcoding Management of Multimedia Streams in Smart Homes**  
*Raffaele Bolla, Matteo Repetto, Stefano Chessa, Francesco Furfari, Mark Asbach, Mathias Wien, Bernhard Reiterer, Hermann Hellwagner, Rik Van de Walle, Saar De Zutter*

1354

 **Design and Implementation of a wearable, context-aware MR framework for the Chloe@University application**  
*Xavier Righetti, Achille Peternier, Mathieu Hopmann, Daniel Thalmann*

1362

Thursday

9/18/2008

Track 5

Room: 110

11:15 AM - 12:30 PM

S 2

Session Chair(s):

Paper starts at page



**Hippocampal-like Categorization of Object Views: A Self-Organizing Learning Approach to Vision Modeling using Stochastic Grammar Inference and Associative Memory**

1370

*Peter Michael Goebel, Markus Vincze, Bernard Favre-Bulle*



**Cultural Differential Evolution Approach to Optimize the Economic Dispatch of Electrical Energy Using Thermal Generators**

1378

*Leandro dos Santos, Adriano Del Vigna de Almeida, Viviana Cocco*



**Meta-Heuristic Approaches for a Soft Drink Industry Problem**

1384

*Claudio Toledo, José Filho, Paulo França*

Keynote

Room: 5

1:30 PM - 2:30 PM

K 4

Keynote Speech

Session Chair(s):

Paper starts at page



Track 4

Room: 2

2:30 PM - 4:00 PM

S11

Hybrid systems

Session Chair(s): *Fernando Morilla*

Paper starts at page



**Parallel Timestep Simulation Scheduling (PTSS) with Variable Time Increments for Factory Simulation Applications**

1392

*Jürgen Roßmann, Gerrit Alves*



**Towards Step-Wise Safe Switching Climate Control for a Greenhouse**

1400

*Fotis N. Koumboulis, Maria P. Tzamtzi*



**Joint state-mode observer design for switched linear systems**

1408

*David Gómez-Gutiérrez, Guillermo Ramírez-Prado, Antonio Ramírez-Treviño, José Javier Ruiz-León*



**Control of a Constant Turning Force System via Step-Wise Safe Switching Iterative Feedback Tuning**

1416

*Fotis N. Koumboulis, Maria P. Tzamtzi, Christoforos E. Economakos*

Thursday

9/18/2008

Track 3

Room: 105


2:30 PM - 4:00 PM

S 5


Platforms

Session Chair(s):


Paper starts at page

 **Hardware Acceleration for Verifiable, Adaptive Real-Time Communication**  
*Sebastian Fischmeister, Insup Lee, Robert Trausmuth*


1425

 **A supervisor implementation approach in Discrete Controller Synthesis**  
*Emil Dumitrescu, Mingming Ren, Laurent Piétrac, Eric Niel*

1433

 **Using Neural Networks for Quality Management**  
*Mohamad Jaber, Jacques Combaz, Loïc Strus, Jean-Claude Fernandez*

1441

 **Comparison of FPGA-based Implementation Alternatives for Complex Algorithms in Networked Embedded Systems – the Encryption Example**  
*Enrico Heinrich, Sebastian Staamann, Ralf Joost, Ralf Salomon*

1449

SS 03


Room: 109

2:30 PM - 4:00 PM


SS 03 Embedded Systems Security & Dependability

Session Chair(s): *Dimitrios Serpanos*


Paper starts at page

 **Creating An Elliptic Curve Arithmetic Unit For Use In Elliptic Curve Cryptography**  
*Apostolos Fournaris, Odysseas Koufopavlou*

1457

 **Modelling and Designing Reliable On-Chip-Communication Devices in MpSoCs with Real-Time Requirements**  
*Maurice Sebastian, Rolf Ernst*

1465

 **Secure and Customizable Software Applications in Embedded Networks**  
*Fritz Praus, Thomas Flanitzer, Wolfgang Kastner*

1473

Track 5

Room: 110

2:30 PM - 4:00 PM


S 3

Session Chair(s):


Paper starts at page

 **Decentralized Routing Control for Guided Transportation Systems**  
*Alexander Fay, Stefan Jerenz, Frank Schumacher*


1481

 **Integrated Automated Design Approach for Building Automation Systems**  
*Stefan Runde, Henrik Dibowski, Alexander Fay, Klaus Kabitzsch*

1488

 **Production order life cycle in agent-based distributed manufacturing**  
*Aleksey Bratukhin*

1496

 **Planned lead times for one-level assembly system with service level constraint**  
*Alexandre Dolgui, Mohamed Aly Ould Louly, Faicel Hnaïen*

1504

Closing Ceremony

Room: 5

4:00 PM - 4:15 PM

CC Closing ceremony

Session Chair(s): *Alexander Fay*

Paper starts at page

Invitation to ETFA 2009

*Antoni Grau*

# Functional Safety and System Security in Automation Systems – A Life Cycle Model

Thomas Novak  
Vienna University of Technology,  
Institute of Computer Technology  
Gusshausstrasse 27-29  
1040 Vienna, Austria  
novakt@ict.tuwien.ac.at

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

## Abstract

*Industrial and building automation systems are more and more important in industry and buildings. New services and novel fields of application call for dependable systems. Two very important properties of such a system are functional safety and system security. In the opposite of today's development where safety and security are treated separately, investigating security together with safety leads to a reduction of effort in the different phases of system life. That is because they have some similar objectives, but realized by different measures. The intention of the paper is to present a way of developing a safe and secure system as well as to show the associated benefit with special focus on building automation.*

## 1. Introduction

Historically, safety and security issues have been treated separately. Especially, safety systems are setup and operated totally disjointed from other systems. That is, each domain has its own physically separated system and gateways are required to connect them. For safety systems additionally absence of reaction is required and has to be proven usually resulting in a limited read-only access to the safety system.

Upcoming trends such as remote access via the Internet, advanced control operations or cost reduction by using shared networks, not limited but obvious in the area of building automation, advise to rethink this separation and setup concepts for systems that allow common usage by safety, security, HVAC (heating, ventilation and air conditioning), and lighting and shading. Using redundancies in building automation control systems by integrating safety critical, security relevant and standard operation into a single communication system would allow for big savings.

But these trends break up the isolated structure of existing networks and therefore introduce new risks and

threats concerning safety and security and set new challenges to the safety and security measures in existing systems. Concerning security today's automation systems and networks are in general lacking efficient security features. If available security is an extensions that is seldom used and often has non-negligible drawbacks (e.g. [1],[2]). In the same way automation systems lack native support for safety and have been enhanced with safety features on application level (e.g. [3]). What is in common is that dependencies between different operation modes, and safety and security in particular are not considered. Safety and security are examined independently not considering potential hazardous side effects on each other.

In a first approach embedding security measures are to guarantee the correct execution of all safety relevant operations in a mixed operation environment.

This goal requires that the systems offer a flexible security framework that on the one hand handles the correct usage of resources needed by safety, e.g. QoS parameters like keep alive intervals, communication times, the implicit access control demanded by the safety application, and on the other hand also offers the same and other services like access rights or authentication to other applications.

This paper introduces a possible common approach investigating security together with safety throughout the whole system life that on the one hand leads to a reduction of effort in the different phases of development and on the other hand aims at the design of systems which have security and safety in their core. The intention of the paper is to present a life cycle approach based on ideas mentioned in [12] – using existing international standards, IEC 61508 [7] and IEC 15408 also known as Common Criteria (CC) [11], and their methodologies – that allows for a combined approach towards security and safety. The particular focus is set on safety and security in building automation.

The remainder of the paper is structured as follows: Section 2 describes security and safety goals with their commonalities. Section 3 introduced the safety-security life cycle model. Finally, section 4 presents rules for



conflict resolution and a measure assessment. The practical examples given to illustrate the concepts are taken from SafetyLon-Project [3] that strives for making LonWorks safe, from the authors activities related to secure industrial and building automation systems and the standardization of safe and secure systems in CEN.

## 2. Common Procedure: Integrity, Authentication and Authorization

Looking at the goals of safety and security similarities can be identified that show potential for a combined synergetic approach. In particular the common procedure of integrity check, authentication and authorization is a main building block for applications in both areas.

### 2.1. Definitions

“*Functional safety* is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs” [7].

*Security* is concerned with the protection of assets from threats, where *threats* are categorized as the potential for abuse of protected assets” [11] In the domain of security there are two main subdomains: network security or internet security, and system security or computer security [15].

### 2.2. Safety and Security Goals

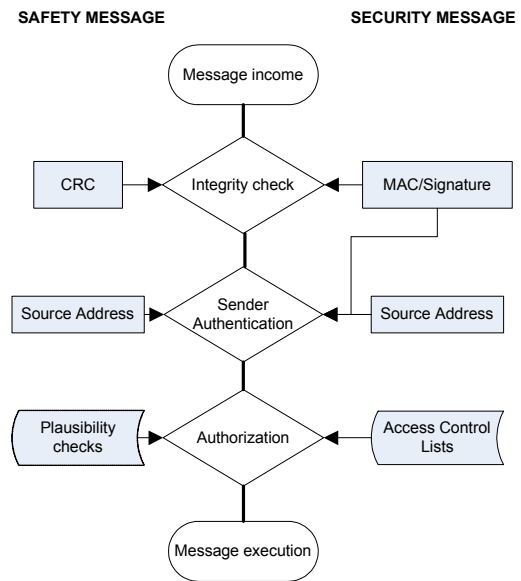
In order to understand the potential of synergies given between safety and security the goals of the two areas should be analyzed:

Safety goals are

1. Integrity, which demands the correct operation of the system under all defined circumstances with in a fixed period of time. It is usually divided into stochastic (hardware) integrity and systematic integrity.
2. Authentication, which demands that a message is coming from the correct source. A common approach is source based addressing.
3. Availability is not necessarily a direct safety goal since a non-available system can find a simple fail-safe state by going to no-operation, yet for practical reasons this trivial solution is not desired.
4. Authorization is usually implemented implicitly by allowing authenticated operation. Additionally, a check for maximum plausibility is sometimes applied, for example to check timing values.

Security goals are

1. Confidentiality, meaning that only authorized entities must be able to read confidential data,
2. Integrity, stating that no unauthorized entity must be able to change data without being detected,
3. Availability, mandating that data is on-hand when it is needed



**Figure 1 Common procedure: integrity, authentication and authorization**

4. Authentication, allowing to determine the sender/creator of a message
5. Authorization, defining access rights.
6. Non-Repudiation, giving evidence that the sender/creator of a message issued the message.

Looking at the security goals relevant for automation systems confidentiality and non-repudiation<sup>1</sup> can be neglected for the systems of interest in automation ([1],[2],[4]). Hence, comparing the remaining important security goals with the safety procedure a common pattern between safety and security can be identified.

A chain starting with integrity verification, authentication followed by an authorization is given (see Figure 1). Measures in this chain are differently implemented in safety and security since they aim at different sources of failures, but pursue the same goals; Security aims at protection and defense of threats from intentional attacks, safety measures are a protection against malfunction of the system itself including fault tolerance, safety integrity and fault resistance [5].

E.g., safety authorization is based on maximum plausibility, i.e. is the value within a fixed range, or even simpler allows everything that passes the authorization stage. In contrast, security demands fixed access control lists (white or black lists). Similar for the integrity, CRC (cyclic redundancy check) codes computable by everyone are sufficient against stochastic failures, whilst security necessitates cryptography that requires the knowledge of a secret key to properly verify the integrity of a message. Looking at this example replacing the

<sup>1</sup> Non-repudiation is of big importance and rarely used in actual operation. It is only used as posterior measure for tracking, e. g. billing or making lists of accesses of maintenance personal.



individual measures for integrity protection (cryptographic message authentication code (MAC) and CRC) with a jointly used MAC fulfills the requirements for both domains.

Yet, finding these commonalities is not that straight forward since measures can need different efforts or even find no common equivalent. Optimization goes much beyond simple replacements; they need a holistic analysis that requires considerations of safety and security in the complete life cycle from development, to operation and disposal.

### 3. Life Cycle Model

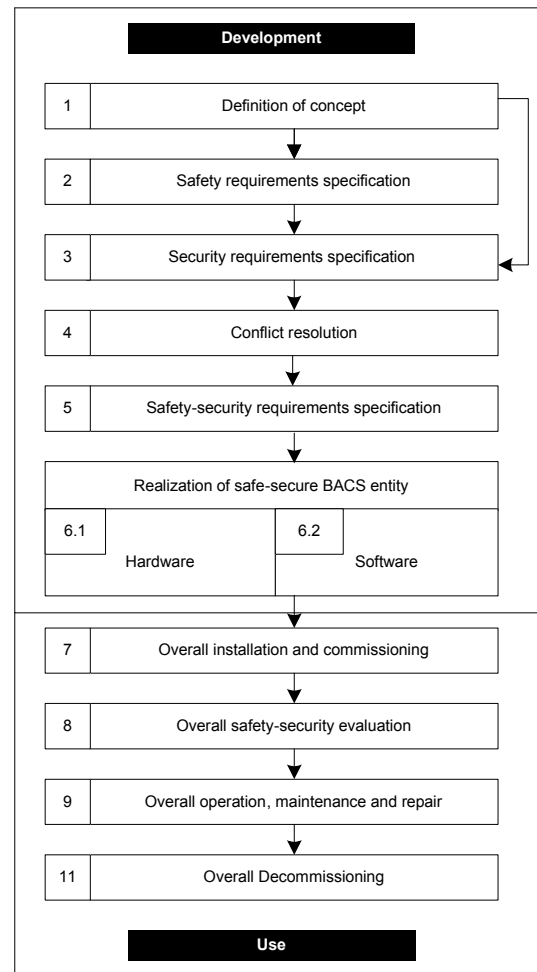
A life cycle model is a structured and systematic model covering the *development* and *use* phase of a system. Within the paper a life cycle model is used as generic term for every procedure starting with a product's conception and ending with its disposal. Or, in other words a life cycle model specifies a logical activity flow of a project.

#### 3.1. Life Cycle Approaches

A life cycle approach has become 'best practice' in the safety domain. Examples of safety life cycles can be found in [6] or in the international standard for functional safety IEC 61508 [7]. There has been a common understanding that activities such as fault avoidance and fault control must be applied at different stages of the life cycle. Often safety assessment work has been confined to assessing whether the proposed architecture meets the target failure probabilities [8]. Less attention was paid to the installation, maintenance and disposal phase [9]. Therefore, a lot of serious safety problems occurred during that phases.

Similar approaches, albeit less detailed and accepted, have been development in the security domain. In [10] it is outlined that building any type of software securely is only possible if security issues are considered during all phases of the life cycle. Hence, seven so-called touchpoints (a set of best practices) are introduced, each of them applicable to a different life cycle phase. In the international standard IEC 15408 [11], also known as Common Criteria (CC), security related activities for the various life cycle phases are specified. They are organized in classes such as activities for requirement specification or installation. Additionally, CC specifies a way of how to receive security requirements. In general, the trend to ensure security during the various stages of a product life is clearly perceptible. Its importance is growing due to the increasing complexity and connectivity of security critical systems

Whereas in the safety domain life cycle models are specified, the security domain very often determines activities relating to security, but does not define a model, i.e. the flow or order of activities.



**Figure 2 Safety and security life cycle model**

The basic idea of the safety-security lifecycle presented in Figure 2 is to use the safety lifecycle from IEC 61508 and integrate the security approach specified in Common Criteria (CC). Requirements how to proceed are given for every phase of the system life. Moreover, activities are added to consider safety and security dependences resulting from integrating safety and security.

The two international standards IEC 61508 and CC are not application specific. They are providing a set of requirements and procedures to be used in different applications. They are chosen as basis of the proposed life cycle model because they have a good coverage of functional safety and security aspects. And the standards are considered to be well-accepted in their domains. In addition, both make a classification and a comparison of systems possible by specifying different levels: four safety integrity levels for safety related and seven evaluation assurance levels for security related systems. The rigor and amount of requirements increases with higher levels.

The safety-security life cycle model is divided into two major parts:

1. The first part includes activities related to the development of an entity in an automation system, e.g. a node. The development phase includes safety dependent and security dependent activities. In addition, an approach to deal with conflicts resulting from contradicting safety and security requirements is integrated into the development phase.
2. The second block is related to the use of the automation system and refers to all activities during the use of the complete system.

Although activities of both phases are shown in a sequential way in Figure 2, the life cycle model only intends to show that activity  $n+1$  requires input of activity  $n$ . For the sake of readability recursions that will occur with the life cycle are not included in this figure and activities may be required to be redone during system life to receive a safe-secure system, e.g., conflict resolution (discussed later in the paper) may reveal a conflict that has an impact on the hardware environment. Hence, safety and security requirements have to be investigated again.

### 3.2. Development Phase

The development phase is the first phase of the safety-security lifecycle model. Stages 1 and 2 are following IEC 61508, stage 3 is following the Common Criteria. Stages 4 to 5 are additional new activities to handle dependencies between safety and security. These stages are of great importance since the steps defined here set the base for the second use phase. In the end, stage 6 deals with the realization of an entity.

#### 3.2.1. Definition of the Concept:

As mentioned in [12], the development phase begins with definition of the concept that is input to the safe dependent and the security dependent part. First of all the purpose and the scope of the automation system in general and its entities in particular must be defined. It is important to know what the BACS is used for, its field of application. Additionally, it is required to specify the scope: Are there 10000 or only 100 nodes in the automation system? Are they connected to an intranet or even to the Internet?

#### 3.2.2. Safety Requirements Specification

The safety dependent part starts with a safety scope definition where the boundaries of the entity in an automation network are determined. Next a hazard and risk analysis is performed within the aforementioned boundaries. The hazards can result from failures on the network such as delay of messages or result from failures on the entity like memory failures. The hazards are identified and the risk coming from the hazards is assessed. If the risk is not acceptable, i.e. higher than the target safety level, safety functions must be specified to reduce the risk, e.g., a CRC implemented to detect stochastic failures. Requirements on such functions are

the output of the safety dependent part comprised in the safety requirements specification.

#### 3.2.3. Security Requirement Specification

Results from the safety investigation and definition of the concept are input to the security dependent part of the safety-security life cycle model. First, the security environment is examined: the physical environment and assets, i.e. information and resources that require protection. Typical examples of assets in automation systems are sensor or actuator data. Next, the assets are valued and threats to them are specified. A typical threat to sensor data is deliberate manipulation. Moreover, the risk resulting from a threat is estimated. The measures to reduce the risk or in other words requirements on the security functions required to protect the assets are specified according to the value of the asset and the risk of threat to the asset. E.g., to detect manipulation of sensor data a message authentication code (MAC) needs to be integrated.

#### 3.2.4. Conflict Resolution:

Safety requirements and security requirements are investigated in the conflict resolution activity. Interaction between the different kinds of requirements is examined. Conflicts between safety and security requirements need to be resolved. Section 4 introduces a conflict resolution policy for this.

#### 3.2.5. Realization of a Safe-Secure Entity

This activity is separated into hardware and software realization as it is common practice and suggested in IEC 61508. Very often realization means to enhance a standard automation system with safety-security functionality ([2],[3]). Hardware realization deals with the design of a hardware architecture including standard components such as a standard network access unit on a node, and the development of programmable and non-programmable hardware. For example, a node in an automation system uses a two channel architecture ([3],[13]). Safe-secure software to be integrated into the software of an existing automation system is located above layer 7 (application layer) of the ISO/OSI reference model [13]. Examples are PROFIsafe and SafetyLon, or an approach presented in [1] to secure LonWorks. Such approaches have the advantage that they do not require to change the layers of the standard protocol stack and allows for interoperability aspects.

In general, hard- and software realization applies standard mechanism in development. However, the requirements on the quality are higher compared to standard development. E.g., software artifacts have to be tested with a great amount of test cases to reach a high testing coverage.

### 3.3. Use Phase

The use phase is concerned with the installation, commissioning, operation, maintenance and disposal of the automation system. In opposite to the development phase which is unique for every entity of the system such as the node or gateway, in the use phase activities are relating to the whole automation system and must consider the overall interaction among all entities installed in a particular installation.

#### 3.3.1. Overall Installation and Commissioning

In this activity the different entities are integrated into the automation system. Therefore, the safe-secure entities must be identified clearly in order to transfer the communication parameters to the designated nodes. The parameters like timing values are used to handle the safe-secure communication. Cryptographic keys applied to perform cryptographic operations like calculating a MAC must be distributed to the various entities.

#### 3.3.2. Overall Safety-Security Validation

In the field of safety (IEC 61508) the summary of safety requirements is considered to be the specification of intended use and system requirements. Hence, safety validation is the process of comparing system behavior with the safety requirements specification(s). In the context of security (IEC 15408), security objectives are a statement of intent. Seen from a more general point of view, safety-security validation is concerned with investigating if risks have been mitigated properly and the risk mitigation strategy is working. E.g., validation means checking if integrity of the node is ensured constantly.

#### 3.3.3. Overall Operation, Maintenance and Repair

Operation covers all activities required to operate the BACS in a safe-secure way. As a consequence, the issues like the ones mentioned next should be addressed: how to test that the data transferred during commissioning was successfully stored on the designated entity; how to switch from commissioning to operation of the system; how to update cryptographic keys; and finally how to recover from network failures due to stochastic or systematic failures, or intentional attacks.

Maintenance and repair comprises activities such as how to gather diagnostic information in order to react to failures. Another topic is the replacement of a safe-secure entity, or modification of communication parameters. Maintenance regarding reconfiguration of an automation system in general is a very challenging task. Just think of an airport with ten thousands of nodes. It is not acceptable to shut down the complete system when a node shall be replaced or configuration parameters shall be changed, just because safety and security ought not to be endangered. Sophisticated management of maintenance is a necessity.

#### 3.3.4. Decommissioning

It is the last stage of the safety-security lifecycle. There are three ways of understanding decommissioning: The whole system, an entity or a logical communication path between two entities can be decommissioned. Similar to maintenance a ordered decommissioning needs to be performed to maintain the safety-security of the system.

An important fact of the presented parts of the use phase is that it can only facilitate measures that are planned and implemented in the development phase. If new (safety-security) requirements arise, an appropriate return to the development phase is required in order to solve the conflict.

## 4. Conflict Resolution Approach

Integrating safety and security causes more or less interaction in every stage of the life cycle – both coincident goals and conflicts. Identity (coincident) means that safety and security strive for the same with equal or different effort. In opposite to identity, conflict indicates that safety and security pursue contradicting things. Of course, there are also areas where they do not interact. These requirements are then considered to be independent.

Conflicts or identities between safety and security are always result of conflicting or identical requirements or conflicting measures due to identical requirements. Consequently, to figure out and resolve conflicts between safety and security requirements, it is necessary to examine interdependencies. That is why an activity for conflict resolution is integrated into the development phase (Figure 2).

After activity 3 of the development phase 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 the safety and security requirements complementary? Do security requirements contradict safety requirements and vice versa? Therefore the conflict resolution approach at the requirement level is applied. The result is a conflict-free set of requirements.

Next, the measures implemented to satisfy the conflict-free requirements are checked. Only these measures are cross-checked that are different although they result from the same requirement, stated once during safety and a second time during security requirement specification (Figure 3). After measures assessment has been performed, a threat-hazard and risk analysis is carried out to verify the correctness of the decisions made during conflict resolution and measure assessment. Especially, the conflict resolution policy is checked if it delivers the appropriate result with regard to the field of application of the automation system.

#### 4.1. Requirement Level

Even though safety and security have the same major goals as mentioned in section 2, they reduce risk to the goals because of different reasons. Put succinctly, safety is concerned with reducing risk to the system itself, whilst security strives for minimizing risk to information and resources referred to as assets resulting from malicious attacks. Accordingly, it is very likely that requirements how to minimize risk differ. Even worse, it is almost inevitable that these requirements contradict each other. Hence, a methodology has to be specified that presents a clear and concise, and easy to handle way of conflict resolution. It requires a specification of a conflict resolution first, a separation of requirements into two groups next to perform the conflict resolution itself afterwards.

##### 4.1.1. Conflict Resolution Policy

A conflict resolution policy must be specified. It is a set of rules that enables the developer to allow for the particular point of view. The rules specify which requirement has to be preferred in a particular situation. A conflict resolution can be unique for the complete automation system, a subsystem like a node, or even for a part of an entity in the system (e.g. the firmware). Within the paper the policy consists of two rules applicable to a (sub)system:

1. Prefer safety requirements to security requirements if security has a negative impact on safety (see also section 4.1.3).
2. Otherwise, use security

Yet very simple, this policy reflects today's best practice and (legal) requirements for general (building) control applications.

##### 4.1.2. Categorization of Requirements

The requirements are categorized into three groups: a list of detective, and a list of preventive as well as corrective requirements. Detective requirements aim at only detecting faults and attacks, e.g. 'Integrity of system data is detected'. Preventive requirements have the goal to prevent faults or attacks. In the safety domain such requirements are specified to avoid faults (fault avoidance). Finally, corrective requirements additionally specify the corresponding response to a fault or an attack. Preventive and especially corrective requirements may influence processes or systems and are therefore subject to investigation in the conflict resolution approach. Detective requirements must not influence the system and therefore require no conflict resolution.

The particular consequences of a requirement determine its characterization as can be seen from the following industrial control example. A security as well as safety requirement is to check the message regarding data integrity. If the system only provides reporting the violation to a monitoring station and do not influence the process the requirement is detective. In case the taken

measures will prevent the occurrence of the failure, e.g. corrupted messages are filtered, the requirement must be categorized preventive. Finally if the system reacts on the violation by, e.g., going to a safe state or actively correct the value the requirement is of the category correcting.

In practical applications detective requirements are a 'last resort' to detect faults or attacks that have not been or could not have been prevented by measures derived from preventive and corrective requirements.

##### 4.1.3. Perform Conflict Resolution

Third, the conflict resolution itself is performed. Each requirement is evaluated regarding its action item. That is, the action and the reaction to a failure or attack is evaluated. The action item is checked against the other action items of corrective or preventive requirements. If there is no conflict, the requirement is considered to be a final safety-security requirement. Otherwise, the conflict resolution policy is applied and one of the requirements is discarded. In the end, a conflict-free set of requirements is setup.

**Table 1 Corrective safety and security requirements**

Failure/incident	Safety requirement	Security requirement
Hardware failure	Fail-safe state of node	Fail-secure state of single microcontroller
Integrity failure	Discard message	Discard message; after 5 successive incidents send message to network management device to signal attack.
Message lost	Fail-safe state of consumer	none
Disclosure of key	none	Stop communication until new key available

The following example is given to get an idea of the conflict resolution process. Table 1 shows four corrective safety and security requirements, respectively. The first failure is a 'Hardware failure'. For instance, the online volatile memory test revealed a fault in a sector of the RAM resulting in a failure of the first safety chip. From the safety point of view it is required that the safety chip switches to fail-safe state immediately. Since both chips absolutely must agree on every task that should be executed (two channel architecture), fail-safe state of one results in fail-safe state of the complete node. Security requirement says that the first chip has to go to fail-secure state and the second one takes over. The conflict is solved according to the given policy (section 4.1.1) by taking the safety and discarding the security requirement, since security has a negative impact on safety.

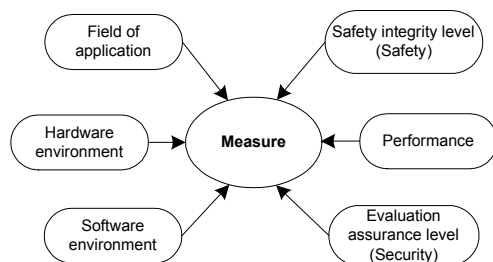
The second failure ‘Integrity failure’ results in similar safety and security requirements. Such a failure is detected due to CRC or MAC mismatches. Here, the safety requirement is included in the security requirement, since the MAC cryptographically protects the integrity (stronger measure) . As security does not influence safety in a negative way, the security requirement is chosen – rule two of the conflict resolution approach applies. Failure 3 and incident 4 have no cross impact on security and safety, respectively. Consequently, the safety requirement as a reaction to ‘Message lost’ and the security requirement to ‘Disclosure of key’ is determined to be a final safety-security requirement.

#### 4.2. Function Level

Conflict resolution at the function level or also called measure assessment is the second part of the conflict resolution approach. Measures are derived from the conflict-free set of safety-security requirements resulting from the first part of the conflict resolution. One of the many motivations to design a common approach is to benefit from synergies on applying measures. Consequently, safety and security measures and synergies gained are classified in three groups: (1) such that directly match (i.e. safety and security measure are equal), (2) such that are unique for safety and security, (3) and such that require different efforts [12].

Measure assessment has to be only performed when safety and security measures are classified to be of group 3: different measures with different effort are derived from the same requirement. Just that group of measures exhibit conflicts regarding e.g., computational power, throughput, computation time, memory resources or application constraints. Measures of the other groups are either identical or unique and thus cannot cause conflicts per definition. The conflict resolution on function level uses six factors as shown in Figure 4 to assess the safety and security measure. In the following an example of a measure assessment is given.

In a safe system the requirement ‘Ensure integrity of data on a node or data in a message’ is granted by means of a CRC. In a secure system similar measures are used. Instead of the CRC a cryptographic message authentication code (MAC) is used that cannot be



**Figure 3 Measure assessment**

recalculated without the knowledge of the appropriate key. According to the node address and only in case of a verified message CRC or MAC, data can be read or written.

To gain a synergy, a proper solution is to replace the CRC by the MAC since the security measure also withstands safety attacks to the integrity of data. If such a replacement can take place, it is evaluated by the measure assessment. First, safety integrity must not be jeopardized, i.e. the same safety integrity level (SIL) must be reached as it was before the replacement of the safety measure. In other words, a MAC must be selected that grants the same level of integrity than the non-secure CRC does. Second, according to the evaluation assurance level (EAL) a minimum strength of function is specified in order that the MAC chosen cannot be defeated. Third, software and hardware environment has to be considered. Using a cryptographic algorithm being implemented in hardware, results in less computational time than calculating the same algorithm in software. Furthermore, memory resources of embedded devices are low compared to PCs and have also to be considered. Finally, performance of measures and the impact on field of application are examined: Generating and verifying a 8 byte MAC on a smartcard takes about 50 ms of time whereas the process of calculating a CRC lasts about 300-500  $\mu$ s. In some applications such as fire alarm systems the difference in execution time is acceptable, but for applications like emergency push buttons with an required overall reaction time, i.e. time from pressing the button on Node A and stopping a machine connected to Node B, of less than 150 ms [13] 100ms (50ms for message protection and 50ms for message verification) is a none acceptable delay. According to the conflict resolution policy a final decision about the usage of the measure is taken.

### 5. Application Synergies

A main application focus at the moment is the combination of fire alarm systems and general building control. In particular application synergies could be achieved by a combination of fire system ventilation and HVAC. On the one hand fire dampers and ventilation flaps could be integrated and on the other hand the air condition can be used to exhaust smoke. A main requirement is that the HVAC must be turned off as soon as smoke is detected to prevent spreading of smoke and that the safety system gains full control of the HVAC system. Security is an enabler for the combined approach since it allows to distinguish between nodes of the safe and the secure system. Proper message authentication and integrity protection is required. For the combination fire system and HVAC the conflict resolution is rather simple since on the requirement level the safety functionality is always dominant compared to the comfort functionality of HVAC and on the measure

assessment also timing constraints in both applications are also very relaxed.

But synergies can go further: in restricted areas the access control service can be integrated into the system also setting security demands. E.g., the fire system must be able to open doors only in escape direction and the security measures must be increased in strength to avoid attacks. Also dual use of systems that detect the presence of persons are thinkable, but it is questionable if they fulfill the requirements for human safety not to lock a person in case of fire.

## 6. Conclusion

The possibilities to gain synergies by taking a common approach towards safety and security in building automation systems is given in many areas: at the non-functional measure level like verification and validation tools, risk analysis techniques, or testing techniques. However, it is not well-known that synergies can be gained at the requirement level or at the functional measure level (e.g. CRC vs. MAC) as presented in the paper. Gaining synergies is possible since safety and security strive for some identical goals. This fact is often honored, yet little effort to combine the fields is given because applications are thought to be either safety or security critical.

As a consequence, the paper presents a life cycle model trying to integrate safety and security in an automation system. In particular, a strategy is given how to resolve conflicts between safety and security. To address conflicts due to requirements and different implementations of measures a two step conflict resolution framework is presented, resolving conflicts at the requirement and at the function level. Such a life cycle model and its included conflict resolution are the basis of combining formerly separated networks for safety, e.g., fire alarm system, and for security, e.g., access control, and operation, e.g. heating, ventilation and air condition, or lighting and shading.

Some ideas presented in the paper have already been submitted to standardization as a working draft. Since 2007 the topic is treated as a working item in European Standardization CEN, Technical Committee (TC) 247, Working Group (WG) 4, called "Building Automation, Controls and Building Management". The goal is to create an European and later on international standard for functional safety and system security in building automation and control systems. The standard ought to be application independent and a generic standard for safety and security in building automation systems.

## References

[1] C. Schwaiger, A. Treytl. Smart Card Based Security for Fieldbus Systems. In *Proceedings of 9th IEEE Conference*

*on Emerging Technologies and Factory Automation*, Volume 1, pp. 398-406, 2003.

[2] A. Treytl, T. Sauter, C. Schwaiger. Security Measures in Automation Systems - a Practice-Oriented Approach. In *Proceedings of 10th IEEE International Conference on Emerging Technologies and Factory Automation*, Volume 2, pp. 847-855, 2005

[3] T. Novak, T. Tamandl. Architecture of a Safe Node for a Fieldbus system. In *Proceedings of the 5th IEEE International Conference on Industrial Informatics*, Vol. 1, pp. 101-106, 2007.

[4] M. Naedele. Standardizing industrial IT security - a first look at the IEC approach. In *Proceedings of Emerging Technologies and Factory Automation ETFA 2005*, Volume 2, pp. 19-22, 2005.

[5] U. Baumgarten, C. Eckert. Mobil und trotzdem sicher?. *it+ti 5/2001*, pp. 254-263, Oldenbourg Verlag, 2001.

[6] W.F. Bates. Safety-related system design in power system control and management. In *Proceedings of the 4th International Conference on Power System Control and Management*, pp. 15-20, 1996.

[7] International Electrotechnical Commission. *IEC 61508 – Functional safety of electric/electronic/programmable electronic safety-related systems*. IEC, 1998.

[8] D. J. Smith, K. G. L. Simpson. *Functional Safety – A straightforward guide to applying IEC 61508 and related standards*, Elsevier Butterworth-Heinemann, Oxford, 2<sup>nd</sup> edition, 2004.

[9] P. Wratil, M. Kieviet. *Sicherheitstechnik für Komponenten und Systeme*. Hüthig Verlag, Heidelberg, 2007.

[10] G. McCraw. *Software Security – Building Security In*. Addison-Wesley, Boston, 2006.

[11] International Electrotechnical Commission. *IEC 15408 – Information technology – Security technique – Evaluation criteria for IT security*. IEC, 2<sup>nd</sup> edition, 2005.

[12] T. Novak, A. Treytl, P. Palensky. Common Approach to Functional Safety and System Security in Building Automation and Control Systems. In *Proceedings of the 12th IEEE International Conference on Emerging Technologies and Factory Automation*, pp. 1141-1148, 2007.

[13] D. Reinert, M. Schaefer (Publisher). *Sichere Bussysteme in der Automation*. Hüthig Verlag, Heidelberg, 2001.

[14] A. Burns, J. McDermid, J. Dobson. On the meaning of Safety and Security. *The Computer Journal*, Vol. 35, No. 1, pp. 3-15, 1992.

[15] W. Stallings. *Cryptography and Network Security*. Prentice Hall, 2003.

[16] B. Schneier. *Secrets and Lies – Digital Security in a Networked World*. John Wiley & Sons, Inc., New York, 2000.