1. Record Nr. UNISA996490364703316

Titolo	Model-based safety and assessment : 8th international symposium, IMBSA 2022, Munich, Germany, September 5-7, 2022 : proceedings / / Christel Seguin, Marc Zeller and Tatiana Prosvirnova, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer Nature Switzerland AG, , [2022] ©2022
ISBN	3-031-15842-3
Descrizione fisica	1 online resource (270 pages)
Collana	Lecture notes in computer science ; ; 13525
Disciplina	518.1
Soggetti	Computer logic Computer science Algorithms
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Safety Analysis Automation -- An AEBS Use Case for Model-Based System Design Integrating Safety Analyses and Simulation -- 1 Challenges and State of the Art -- 2 An Integrated MBSE/MBSA Methodology for ADAS -- 3 Function Concept -- 3.1 Regulatory Requirements (UNECE) -- 3.2 Test Protocol (Euro NCAP) -- 3.3 Stakeholder Constraints, Goals, and Assumptions -- 3.4 Extracting Top-Level Function Requirements -- 3.5 Hazard and Risk Assessment (HARA) -- 4 Designing the AEBS Functional Architecture -- 4.1 Functional Architecture Modeling and Refinement -- 4.2 Functional Behavior Modeling -- 4.3 Iterations of the Functional Architecture Driven by Analyses and Simulation -- 5 Moving from the Functional to the Physical Architecture -- 5.1 Allocation of Functional Architecture to Physical Architecture -- 5.2 Trade Studies to Identify Optimal Implementation Solutions -- 5.3 Iterations of the Physical Architecture Driven by Analyses and Simulation -- 6 Conclusion -- References -- COMPASTA: Extending TASTE with Formal Design and Verification Functionality -- 1 Introduction -- 2 The COMPASTA Approach -- 3 An Illustrative Example -- 4 Conclusions -- References -- MBSA Practices -- MBSA in Aeronautics: A Way to Support Safety Activities -- 1 Introduction --

2 Related Works -- 3 Case Study Description -- 3.1 System Description -- 3.2 Safety Requirements -- 4 Safety Assessment with MBSA -- 4.1 General Process -- 4.2 Iteration "n" -- 4.3 Iteration "n + 1" -- 5 Conclusion -- References -- Modeling the Variability of System Safety Analysis Using State-Machine Diagrams -- 1 Introduction -- 2 Related Work -- 3 Background -- 3.1 Software Product Lines and Base Variability Resolution -- 3.2 The ISO 26262 Safety Lifecycle -- 3.3 CHESS Framework and CHESS State-Based Analysis -- 4 A State-Based Dependable Software Product Line.
4.1 Domain Engineering Phase -- 4.2 Application Engineering Phase -- 5 Evaluation -- 5.1 Hybrid Braking System -- 5.2 HBS: Domain Engineering Phase -- 5.3 HBS: Application Engineering Phase -- 6 Conclusions -- References -- Model-Based Safety Analysis: A Practical Experience -- 1 MBSA at Safran Aircraft Engines -- 1.1 Needs -- 1.2 2018-2021: Exploration and Maturity Increase -- 1.3 State of the Art -- 2 Exploration of Approaches -- 2.1 Modelling a Physical Phenomenon with Effects Upstream -- 2.2 Re-use of Existing Models -- 2.3 Reliability of Dynamic Systems -- 3 New Challenges -- References -- Practical Application of Model-Based Safety Analysis to the Design of Global Operating System of New Rolling Stock on Automatic Metro Lines -- 1 Introduction of MBSA in Railway Context -- 2 Related Works -- 3 Automatic Metro Lines System Case Study -- 4 Methodology of MBSA Deployment -- 5 Proposed and Used Tools and Methods -- 5.1 Architecture and Behavioral Specification -- 5.2 GOS Component Library Development -- 5.3 System Modeling from the Library -- 5.4 Launch RAMS Analysis -- 6 Case Study Analysis -- 7 Discussion -- 8 Conclusion and Future Works -- References -- Plug-and-Produce... Safely! -- 1 Introduction -- 2 Background and Related Work -- 3 Use Case -- 4 I4.0-enabled Safety Engineering -- 5 A Worked Example -- 6 Conclusion -- References -- Causal Models and Failure Modeling Strategies -- Strategies for Modelling Failure Propagation in Dynamic Systems with AltaRica -- 1 Introduction -- 2 Case Study Description -- 3 Related Works -- 3.1 Static and Dynamic Failure Propagation Models -- 3.2 AltaRica Modelling Language -- 4 Case Study Modelling and Analysis Using AltaRica DataFlow -- 4.1 Issues Raised by Failure Propagation Modelling of Systems with Control Feedback Loops -- 4.2 ``Cut the Loop'' Solution -- 4.3 The ``Dirac'' Solution.
4.4 The ``Double Flow'' Solution -- 4.5 Summary -- 5 Conclusion and Perspectives -- References -- Towards Causal Model-Based Engineering in Automotive System Safety -- 1 Introduction -- 2 Related Work -- 2.1 Terminology of Scenarios -- 2.2 Sources of Knowledge -- 3 Causal Models -- 3.1 Terminology of Causal Models -- 3.2 Inference in Causal Models -- 4 Causal Models and Scenario-Based Testing -- 4.1 Models in Automotive Safety Engineering -- 4.2 Development of Causal Models -- 4.3 Towards Discovering Edge and Corner Cases -- 5 Conclusion -- References -- Performance Assessment of an Offshore Windmill Farm with AltaRica 3.0 -- 1 Introduction -- 2 Case Study: An Offshore Windmill Farm -- 3 AltaRica 3.0 Modelling Language and Assessment Tools -- 4 Case Study Modelling and Assessment -- 4.1 Modelling the Technical System -- 4.2 Modelling the Environment -- 5 Experiments -- 6 Conclusion and Perspectives -- References -- Component Fault and Deficiency Tree (CFDT): Combining Functional Safety and SOTIF Analysis -- 1 Introduction -- 2 Background: Component Fault Tree (CFT) -- 3 Component Fault and Deficiency Tree (CFDT) -- 4 Analysis Using Component Fault and Deficiency Trees -- 5 Conclusions and Future Work -- References -- Designing Mitigations of Faults and Attacks -- A Capella-Based Tool for the Early Assessment

of Nano/Micro Satellites Availability -- 1 Introduction -- 2 ELMASAT Tool -- 2.1 System Architecture in Capella -- 2.2 Building an Availability Assessment Viewpoint -- 2.3 Availability Computation -- 3 Case Study -- 4 Related Work -- 5 Conclusion -- References -- Analysing the Impact of Security Attacks on Safety Using SysML and Event-B -- 1 Introduction -- 2 Generic Architecture of Networked Control System -- 3 SysML Representation of NCSs -- 4 Modelling and Refinement in Event-B -- 5 From SysML to Event-B: Translation Methodology.
6 Analysing the Impact of Cyber Attacks on Safety -- 7 Related Work -- 8 Conclusion -- References -- Data Based Safety Analysis -- A Deep Learning Framework for Wind Turbine Repair Action Prediction Using Alarm Sequences and Long Short Term Memory Algorithms -- 1 Introduction -- 2 Research Questions -- 3 Methodology -- 3.1 Data Preparation and Pre-processing -- 3.2 Building the LSTM Network -- 3.3 Training of the LSTM Network -- 3.4 Testing and Prediction -- 4 Results and Discussion -- 4.1 Results -- 4.2 Benefits for Industry -- 4.3 Integration into Industry -- 4.4 Current Limitations -- 5 Conclusions and Future Work -- References -- Tool Paper: Time Series Anomaly Detection Platform for MATLAB Simulink -- 1 Motivation and General Concept -- 2 Related Work -- 3 Dataset -- 3.1 Dataset from Simulation of Unmanned Aerial Vehicle (UAV) -- 3.2 Dataset from Simulation of Autonomous Vehicle System (AVS) -- 3.3 Real World Dataset: Secure Water Treatment (SWaT) -- 4 Data Preprocessing -- 4.1 Normalization and Standardization -- 4.2 Data Preparation for Deep Learning Models -- 5 Deep Learning Models -- 5.1 Deep Learning Approaches for Anomaly Detection -- 5.2 Hyperparameters -- 5.3 Predictive Models -- 5.4 Reconstructive Models -- 6 Anomaly Detection -- 6.1 Problem Statement -- 6.2 Supervised Thresholding -- 6.3 Unsupervised Dynamic Thresholding -- 6.4 Online Detection Block -- 7 Conclusion -- 7.1 Results -- 7.2 Limitation and Future Work -- References -- Keep Your Distance: Determining Sampling and Distance Thresholds in Machine Learning Monitoring -- 1 Introduction -- 1.1 SafeML -- 1.2 Motivation -- 1.3 Paper Contribution and Outline -- 2 Background and Related Work -- 3 Methodology -- 3.1 Process Workflow -- 3.2 Experiment Setup -- 4 Results -- 4.1 Preliminary Findings -- 4.2 Experiment Results -- 5 Conclusion and Future Work -- References.
Dynamic Risk Assessment -- Engineering Dynamic Risk and Capability Models to Improve Cooperation Efficiency Between Human Workers and Autonomous Mobile Robots in Shared Spaces -- 1 Introduction -- 2 Safe Human-Robot Cooperation -- 2.1 Safe Human-Robot Cooperation in Smart Logistics -- 2.2 Related Work -- 3 Situation-Aware Behavior Safety Analysis -- 3.1 Method Overview -- 3.2 Behavior Causality Model Engineering -- 3.3 Dynamic Safety Monitoring Architecture Integration -- 4 Expected Efficiency Benefit Evaluation -- 4.1 Passing Scenario -- 4.2 Overtake Scenario -- 5 Conclusion -- References -- SafeDrones: Real-Time Reliability Evaluation of UAVs Using Executable Digital Dependable Identities -- 1 Introduction -- 2 Background -- 2.1 Fault Tree Analysis -- 2.2 Reliability Modelling Using Semi-Markov Processes (SMP) -- 2.3 Reliability Modeling Using Arrhenius Equation -- 2.4 The Executable Digital Dependable Identity (EDDI) -- 3 Methodology -- 4 Experimental Implementation -- 5 Experimental Results -- 5.1 Reliability Analysis of the Fault-Free Scenario -- 5.2 Reliability Analysis of the Faulty Scenario -- 6 Conclusion and Future Work -- A Appendix -- A.1 Proposed Fault Tree of a Generic UAV -- References -- Author Index.