Vol.2011-SE-172 No.9
Vol.2011-EMB-21 No.9
2011/5/18

ソフトウェア高安全性分析技術の現状と課題

山本修一郎[†]　芳川　大佑[††]

本稿では，ソフトウェア要求やアーキテクチャ設計などを対象とした高安全性分析技術の動向について，研究課題を対象分野，範囲，生産物，プロセス，特性の観点で分類することにより報告する．

Research Issues On Software Safety Analysis and Validation

Shuichiro Yamamoto[†]　Daisuke Yoshikawa[††]

In this paper, research issues on software safety analysis and validation are investigated. Classification of research issues is proposed based on target domains, scopes, processes, products, and properties of system safety technologies.

1. はじめに

社会的に影響のある事故の原因になることから，ソフトウェアの安全性が注目されている．ソフトウェアの安全性を分析確認する技術が従来から組込みシステム分野で研究されている．しかし，ソフトウェア安全性技術の研究範囲は広範に拡大してきているので，全体像を把握する取り組みが必要になる．

ソフトウェアはその運用環境から要求された機能を実行するための契機に反応して運用環境に対して応答結果をもたらす．このとき，ソフトウェアが運用環境に対して危険な結果をもたらすことがなければ，ソフトウェアは安全であるといえる．そこでソフトウェアが安全であること，すなわち環境に対して危険でないことを分析して確認する技術が必要になる．このとき環境に対してどの程度の危険性があるか，逆に言えばどの程度安全性を持つかを分析することも重要になる．本稿ではこのような技術をソフトウェア高安全性分析技術と呼ぶ．

[†] 名古屋大学情報連携統括本部情報戦略室 Strategy Office, Information a, Nagoya University
[††] 名古屋大学工学部電気電子・情報工学科 Department of Information Engineering, School of Engineering, Nagoya University

以下では，ソフトウェア高安全性分析技術の研究動向を，対象分野，範囲，生産物，プロセス，特性の観点から分類することを提案する．これにより，ソフトウェア高安全性分析技術に詳しくない読者に対してこれまでの研究動向を紹介するとともに，これから求められる研究の方向を提示できる．またソフトウェア高安全性分析技術研究ならびに，その知識体系の構築，さらに安全なソフトウェアの開発を推進することなどが期待される．

2. 課題

参考文献に挙げたソフトウェア高安全性技術の研究を，①対象とするソフトウェア分野，②扱う範囲がソフトウェアの内部，外部，相互作用のどれなのか，③ソフトウェア生産物として何を選択するのか，④どのようなプロセスで分析するのか，⑤どのような特性を分析できるのかという 5 つの観点から分類すると以下のようになった．

2.1 対象分野

高安全性基幹システム（safety critical systems），自動車システム，分散システム，自律ロボット，医療ロボット，人間と共生するロボット，組込みソフトウェア，家電，家電ネットワーク，複雑なシステム，SoS (System of Systems)，ISO26262 を必要とするシステムなどの分野に対してソフトウェア高安全性分析技術が研究されている．またこれらの特定分野に限定されない技術も研究されている．

2.2 範囲

システム全体，コンポーネント，運用環境，人間との相互作用，動的相互作用，組織的技術的要因，機能間相互作用に着目したソフトウェア高安全性分析技術が研究されている．

2.3 生産物

アーキテクチャ設計，システム設計，表現モデル（安全性，故障，危険性など），安全性ケース（Safety Case），フィーチャ（Feature）に着目したソフトウェア高安全性分析技術が研究されている．前世紀にはソフトウェア生産物としてコードに対する安全性分析が研究されてきた．21 世紀になると設計や要求に対する安全性技術が盛んに研究されるようになっている．最近はアーキテクチャ記述言語として AADL や SysML を対象にした研究が活発化している．

2.4 プロセス

ソフトウェア高安全性分析プロセスとして，①ハザード分析，リスク分析，故障モード識別などの改善，②多様な高安全性分析手法の統合，共通性分析，③要求分析，アーキテクチャ指向設計，タスク分析，人間エラー分析などとの統合，④開発・保守・運用プロセスとの統合，⑤重大性や，安全性などの検証，⑥グローバルソフトウェア開発，プロダクトライン開発，アジャイル開発などにおける高安全性分析などが研究

Vol.2011-SE-172 No.9
Vol.2011-EMB-21 No.9
2011/5/18

されている．

2.5 特性

安全性要求，機能安全性，ディペンダビリティ，セキュリティなどの特性についてソフトウェア高安全性分析技術が研究されている．またソフトウェアの高安全性を分析する上での分析効率，時間効率，作業品質，作業の複雑性，一貫性，追跡性などの特性についてソフトウェア高安全性分析技術が研究されている．

3. 高安全性分析技術

ソフトウェア高安全性分析確認技術には，ハードウェアに対する高安全化技術が適用されている[Leve95]．主なソフトウェア高安全性分析確認技術を方法，入力，出力，使用される知識の観点から比較すると下表のようになる．

表１　主なソフトウェア高安全性分析技術

技法	方法	入力	出力	知識
FTA	ハザード原因をブール論理で分析 ①システム定義 ②故障木をトップダウン作成 ③定性分析 ④定量分析	トップ故障 コード 設計	故障木 分析結果 原因事象	トップ故障
FMEA	①コンポーネント定義 ②コンポーネント故障 ③コンポーネント，システム影響分析 ④故障モード結果確率，深刻度分析	詳細設計	FMEA 分析表 (コンポーネント，故障率，故障モード，モード別故障割合，影響)	故障モード 故障率
ETA	故障対策を成功失敗で確率的に分析 ①防御システム定義 ②イベント木をトップダウン作成 ③分岐を追跡して事故をモデル化	潜在故障 設計 分岐確率	イベント木 事故モデル	潜在故障
CCA	①重大事象を定義 ②重大事象の原因結果図を作成 ③重大事象の潜在的影響を伝搬分析	重大事象	原因結果図	重大事象
HAZOP	①設計が期待する運用意図 ②意図からの潜在的逸脱 ③逸脱の原因 ④逸脱の結果	設計	HAZOP 分析表 (ガイドワード，逸脱，原因，結果)	ガイドワード

また，安全性ケースでは GSN(Goal Structuring Notation)についての研究が進んでいる．GSN はソフトウェアが外部に対して安全性を保障する技術である．表 1 の HAZOP はソフトウェアが外部環境に与えるハザードに着目した分析技術である．これに対して FTA，FMEA などはソフトウェア内部の故障に着目した分析技術である．この観点から下図に示すようなソフトウェアの高安全性分析技術を分類できることが分かる．ここで，追跡性(Tracability)や設計理由(Design Rational)の研究はソフトウェア内部に着目した保証技術である．この最後の種類の研究はソフトウェア高安全性技術としてはまだほとんど研究されていないようである．

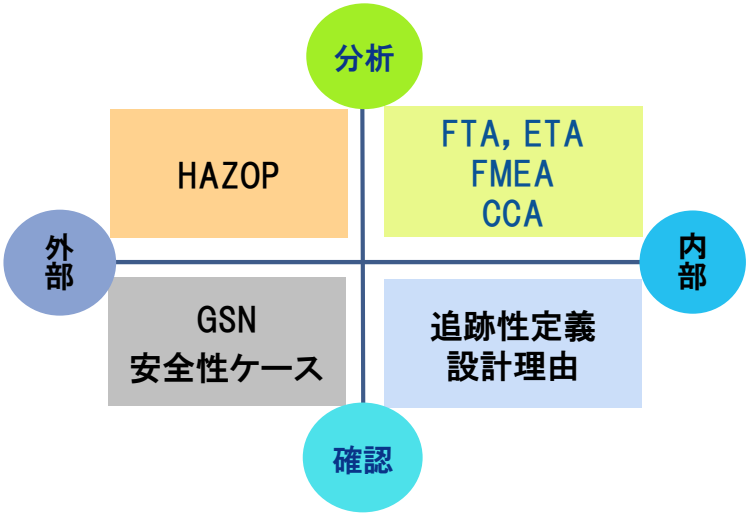

図１　ソフトウェア高安全性分析保証技術の関係

4. 高安全性メタモデル

表 1 に示したように高安全性分析技術には共通要素があることから，安全性に関する概念を体系化することでメタモデルを定義できる可能性がある．OMG ではシステムアシュアランス（Systems Assurance, http://sysa.omg.org/）についてソフトウェアアシュアランス(Software Assurance Metamodel, SAEM)や安全性論証(Argument Metamodel, ARM)についてのメタモデルを標準化しようとしている．今後は FMEA や FTA, HAZOP

Vol.2011-SE-172 No.9
Vol.2011-EMB-21 No.9
2011/5/18

などのソフトウェア高安全性分析技術の共通概念と SAEM や ARM などのメタモデルを統合していく必要がある．

5. 高安全性開発メタプロセス

高安全性分析技術の手順には表 1 から分かるように，リスク（ハザード）識別とその分析，影響の定義，安全性確認というような共通点がある．これをまとめると図 2 のような高安全性開発のメタプロセスにまとめることができる．

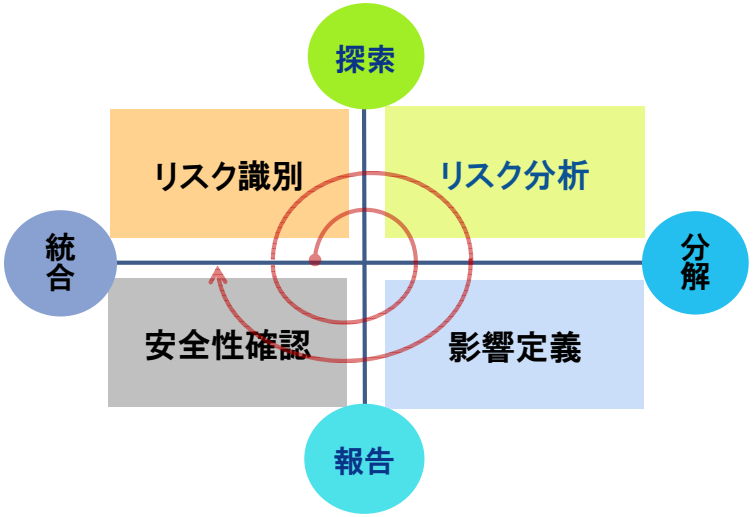

図 2　ソフトウェア高安全性開発プロセス

6. ソフトウェア高安全性知識の構成

ソフトウェア高安全性開発プロセスで提示したように，ソフトウェア高安全性分析技術に関する知識を体系的に整理することができればソフトウェアを高安全化に資することができる．以下では安全性知識体系の試案として①運用環境分析②システム分析③リスク識別④リスク分析⑤安全性評価確認⑥知識管理の 6 個の知識領域から構成できることを示す．

6.1 運用環境分析

システムの運用活動を分析するために，①運用環境分析②ステークホルダ分析③タスク分析などを実施する．

6.2 システム分析

システムの内部構造を分析するために，①システムアーキテクチャ②コンポーネント構成③コネクタ関係④相互作用分析などを実施する．

6.3 リスク識別

ハザード，故障モードを抽出し，その妥当性，完全性を確認するために，①抽出準備②抽出活動指揮③抽出結果の文書化④抽出結果確認などを実施する．

6.4 リスク分析

リスクに対して，システムと環境への影響，重大性を分析するために，①対象要素定義②判断根拠の分析③影響分析④重大性分析⑤原因分析⑥対策定義などを実施する．

6.5 安全性評価確認

リスク対策と安全性要求との適合性を評価，安全性リスクを摘出するために，①リスク対策評価②リスク緩和策割付③組織準備判断④安全性要求判断⑤安全性評価確認などを実施する．

6.6 知識管理

システム，環境に対する故障，危険，安全管理知識を管理するために，①故障モード知識②危険要因知識③安全管理知識④安全性知識の追跡性管理などを実施する．

7. おわりに

本稿では，ソフトウェア高安全性分析技術について調査することにより，研究課題を対象分野，範囲，生産物，プロセス，特性の観点から分類する方法を提案した．また，高安全性生産物と開発プロセスについてのメタモデルが必要になることを指摘した．さらに，ソフトウェア高安全性知識体系について，運用環境分析，システム分析，リスク識別，リスク分析，安全性評価確認，知識管理からなる構成案を提案した．

今後，本調査手法に基づいてより詳細にソフトウェア高安全性分析技術の調査を進め，高安全性生産物のメタモデルを具体化する予定である．また高安全性開発プロセスについて具体的な評価が必要である．さらに安全性は非機能要求であるからセキュリティやディパンダビリティなども考慮した高安全性要求工学やアーキテクチャ設計との統合方式についても研究していく予定である．

参考文献

[Bate03] Iain Bate, Richard Hawkins, John McDermid, A contract-based approach to designing safe systems, SCS '03: Proceedings of the 8th Australian workshop on Safety critical systems and software , Volume 33 ,2003, pp.25-36

[Bere07] Berenbach, B.; Wolf, T., , Global Software Engineering, ICGSE 2007. Second IEEE International Conference on A unified requirements model; integrating features, use cases, requirements, requirements analysis and hazard analysis, 2007 , Page(s): 197 - 203

Vol.2011-SE-172 No.9
Vol.2011-EMB-21 No.9
2011/5/18

[Bern08] Simona Bernardi, José Merseguer and Dorina C. Petriu, Adding Dependability Analysis Capabilities to the MARTE Profile, Model Driven Engineering Languages and Systems, Lecture Notes in Computer Science, 2008, Volume 5301/2008, 736-750

[Bohm10] P. Böhm and T. Gruber , A Novel HAZOP Study Approach in the RAMS Analysis, E. Schoitsch (Ed.): SAFECOMP 2010, LNCS 6351, pp. 15–27, 2010

[Davi09] David, P.; Idasiak, V.; Kratz, F., Improving reliability studies with SysML, Reliability and Maintainability Symposium, Annual , pp.527 - 532,2009

[Desp06] G. Despotou , T. Kelly, Extending Safety Deviation Analysis Techniques to Elicit Flexible Dependability Requirements, proceedings of the 1st IEE International Conference on System Safety, 2006

[Desp07a] G. Despotou, T. Kelly. An Argument Based Approach for Assessing Design Alternatives and Facilitating Trade-offs in Critical Systems. Journal of System Safety Vol.43 No.2 March-April 2007, System Safety Society.

[Desp07b] Georgios Despotou, Tim Kelly, Design and Development of Dependability Case Architecture during System Development, System Safety Conference. System Safety Society, 2007

[Ditt10] T. Dittel and H.-J. Aryus, How to “Survive” a Safety Case According to ISO 26262, E. Schoitsch (Ed.): SAFECOMP 2010, LNCS 6351, pp. 97–111, 2010.

[Gies06] Holger Giese and Matthias Tichy, Component-Based Hazard Analysis: Optimal Designs, Product Lines, and Online-Reconfiguration, Computer Safety, Reliability, and Security, 2006 – Springer, Lecture Notes in Computer Science, 2006, Volume 4166, Pages 156-169

[Gies04] Holger Giese, Matthias Tichy, and Daniela Schilling, Compositional Hazard Analysis of UML Component and Deployment Models, Computer Safety, Reliability, and Security, Lecture Notes in Computer Science, Volume 3219/2004, 166-179, 2004

[Godd93] Goddard, P.L. , Validating the safety of embedded real-time control systems using FMEA, Proceedings on Reliability and Maintainability Symposium, pp. 227 – 230, 1993.

[Godd00] Goddard, P.L., Software FMEA techniques, Reliability and Maintainability Symposium, 2000. Proceedi gs. Annual 2000 , Page(s): 118 - 123

[Grun08] Lars Grunske and Jun Han, A Comparative Study into Architecture-Based Safety Evaluation Methodologies using AADL’s Error Annex and Failure Propagation Models, 11th IEEE High Assurance Systems Engineering Symposium, pp.283-292, 2008

[Guil10a] D. Martin-Guillerez, J. Guiochet, D. Powell, and C. Zanon, “A UMLbased method for risk analysis of human-robot interactions,” in 2nd International Workshop on Software Engineering for Resilient Systems., ACM, Apr. 2010

[Guil10b] Damien Martin-Guillerez_y, J´er´emie Guiochet_y, David Powell, Experience with a Model-based Safety Analysis Process for an Autonomous Service Robot, The Seventh IARP Workshop on Technical Challenges for Dependable Robots in Human Environments, 2010, http://spiderman-2.laas.fr/DRHE2010/final_papers/1-1-02-martin.pdf

[Guio10] Jérémie Guiochet, Damien Martin-Guillerez, David Powell, "Experience with Model-Based User-Centered Risk Assessment for Service Robots," hase, pp.104-113, 2010 IEEE 12th International Symposium on High-Assurance Systems Engineering, 2010

[Guio04] J. Guiochet, G. Motet, C. Baron, and G. Boy, “Toward a humancentered uml for risk analysis - application to a medical robot,” in Proc. of the 18th IFIP World Computer Congress (WCC), Human Error, Safety and Systems Development (HESSD04), C. Johnson and P. Palanque, Eds. Kluwer Academic Publisher, 2004, pp. 177–191.

[Gumz09] Gumzej M., M. Colnaric, W. Halang, Safety shell for specification-PEARL oriented UML real-time projects, Computer Languages, Systems and Structures, Vol. 35, No.3, pp. 277-292, 2009

[Habl04] Habli I., Kelly T. P., “Process and Product Certification Arguments: Getting the Balance Right”, Workshop on Innovative Techniques for Certification of Embedded Systems, in Conjunction the 12th IEEE Real-Time and Embedded Technology and Applications Symposium, San Jose, California, USA, April 2006

[Habl09] Ibrahim Mustafa Habli, Model-Based Assurance of Safety-Critical Product Lines, PhD Thesis, 2009, http://www-users.cs.york.ac.uk/~ihabli/Papers/PhDThesis(Habli).pdf

[Habl10] Ibrahim Habli, Richard Hawkins and Tim Kelly, Software safety: relating software assurance and, software integrity, Int. J. Critical Computer-Based Systems, Vol. 1, No. 4, 2010, pp.364-383

[Habl10a] Ibrahim Habli and Tim Kelly, A Safety Case Approach to Assuring Configurable Architectures of Safety-Critical Product Lines, ISARCS 2010, Holger Giese (Ed.): Architecting Critical Systems, First International Symposium, ISARCS 2010, Proceedings. Lecture Notes in Computer Science 6150 Springer 142-160, 2010

[Habl10b] Ibrahim Habli, Ireri Ibarra, Roger Rivett, Tim Kelly , Model-Based Assurance for Justifying Automotive Functional Safety, 10AE-0181, SAE International, 2010

[Hans04] Klaus Marius Hansen, Lisa Wells and Thomas Maier, HAZOP Analysis of UML-Based Software Architecture Descriptions of Safety-Critical Systems, Proceedings of NWUML 2004, pp.1-23, 2004.

[Hate10] D. Hatebur and M. Heisel, A UML Profile for Requirements Analysis of Dependable Software, E. Schoitsch (Ed.): SAFECOMP 2010, LNCS 6351, pp. 317–331, 2010.

[Hawk03] R. Hawkins, I. Toyn and I. Bate: An Approach to designing safety critical systems using the Unified Modeling Language. Proc. Workshop Critical systems development with UML, 2003.

Vol.2011-SE-172 No.9
Vol.2011-EMB-21 No.9
2011/5/18

[Hech04] Hecht, H.; Xuegao An; Hecht, M., Computer aided software FMEA for unified modeling language based software, Reliability and Maintainability, 2004 Annual Symposium - RAMS 2004 , Page(s): 243 - 248

[Heim07] Mats P.E. Heimdahl, Safety and Software Intensive Systems: Challenges Old and New, Future of Software Engineering (FOSE'07), 2007

[Hell02] G. Helmer, J. Wong, M. Slagell, V. Honavar , L. Miller and R. Lutz, A Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System, Requirements Engineering *Jl*. Vol. 7 No. 4, 2002, 177-220.

[Holl08] C.M. Holloway, SAFETY CASE NOTATIONS: ALTERNATIVES FOR THE NON-GRAPHICALLY INCLINED?, In Proc. of the IET 3nd International Conference on System Safety, 2008

[Hong02] Hong Zhu , Yanlong Zhang , Qingning Huo , Sue Greenwood, Application of Hazard Analysis to Software Quality Modelling, pp. 139-145, 26th Annual International Computer Software and Applications Conference , 2002

[Hyeo10] HyeonJeong Kim; Wong, W.E.; Debroy, V.; DooHwan Bae, Bridging the Gap between Fault Trees and UML State Machine Diagrams for Safety Analysis, Software Engineering Conference (APSEC), 2010 17th Asia Pacific , 2010 , Page(s): 196 - 205

[Ibar05] Erendira Ibarra-alvarado, Software Hazard Analysis for X-By-Wire Applications, Satellite Events at the MoDELS 2005 Conference, Lecture Notes in Computer Science, 2006, Volume 3844/2006, 341-342, 2005

[Iwu03] F. Iwu. A Framework for Achieving Safety in Model-Based Designs. In *Proceedings of the 5th Cabernet Plenary Workshop*, Madeira Portugal, 2003.

[Iwu06] Frantz Iwu_, Andy Galloway, John McDermid, Ian Toyn, Integrating safety and formal analyses using UML and PFS

[Joha01] Johannessen, P.; Grante, C.; Alminger, A.; Eklund, U.; Torin, J.; Hazard analysis in object oriented design of dependable systems, Dependable Systems and Networks, 2001. DSN 2001. International Conference on , 2001 , Page(s): 507 - 512

[John10] C.W. Johnson and S. Raue, On the Safety Implications of E-Governance, E. Schoitsch (Ed.): SAFECOMP 2010, LNCS 6351, pp. 402–417, 2010

[Kais10] Bernhard Kaiser, Vanessa Klaas, Stefan Schulz, Christian Herbst and Peter Lascych, Integrating System Modelling with Safety Activities, Lecture Notes in Computer Science, 2010, Volume 6351, Computer Safety, Reliability, and Security, Pages 452-465

[Kell04] T. P. Kelly and R. A.Weaver. The goal structuring notation– a safety argument notation. In Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, 2004.

[Kell07] Tim Kelly , Using software architecture techniques to support the modular certification of safety-critical systems, SCS '06: Proceedings of the eleventh Australian workshop on Safety critical systems and software, 2007

[Korn10] Andrew J. Kornecki, Janusz Zalewski, Safety and security in industrial control, CSIIRW '10: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research,2010

[Lawr96] Lawrence, J.D., Software Safety Hazard Analysis, NUREG/CR-6430, UCRL-ID-122514, Lawrence Livermore Natinal Laboratory, 1996.

[Leve95] N. Leveson. *Safeware: System Safety and Computers*. Addison-Wesley,1995.

[Lutz93] Lutz, R.R., Targetting safety-related errors during software requirements analysis, in Proceedings SIGSOFT ’93, Foundations of Software Engineering, 1993

[Lutz96] Lutz, R.R.; Woodhouse, R.M., Contributions of SFMEA to requirements analysis , Requirements Engineering, 1996., Proceedings of the Second International Conference on , Page(s): 44 – 51, 1996

[McDe02] John McDermid, Software Hazard and Safety Analysis, Formal Techniques in Real-Time and Fault-Tolerant Systems, Lecture Notes in Computer Science, Volume 2469/2002, 23-34,2002

[Medi09] Ben Swarup Medikonda and Seetha Ramaiah Panchumarthy, A Framework for Software Safety in Safety-Critical Systems, SIGSOFT Software Engineering Notes Page 1 March 2009 Volume 34 Number 2, pp.1-9

[Medi10] Ben Swarup Medikonda and P. Seetha Ramaiah, Integrated safety analysis of software-controlled critical systems, SIGSOFT Software Engineering Notes Page 1-7, Volume 35 Issue 1, January 2010

[NASA00] Failure Modes and Effects Analysis (FMEA) A Bibliography, NASA/SP—2000–6110, 2000

[Pali10] R. Palin and I. Habli, Assurance of Automotive Safety – A Safety Case Approach, E. Schoitsch (Ed.): SAFECOMP 2010, LNCS 6351, pp. 82–96, 2010

[Papa99] Yiannis Papadopoulos , John A. Mcdermid, Hierarchically Performed Hazard Origin and Propagation Studies, Proceedings of SAFECOMP'99, the 18 th International Conference on Computer Safety, Reliability and Security , pp.139-152, 1999

[Papa04] Papadopoulos, Y. Parker, D. Grante, C., Automating the failure modes and effects analysis of safety critical systems , High Assurance Systems Engineering, 2004. Proceedings. Eighth IEEE International Symposium on, 310 – 311, 2004

[Patr08] Patrick H. S. Brito, Rogério de Lemos and Cecília M. F. Rubira, Development of Fault-Tolerant Software Systems Based on Architectural Abstractions, Lecture Notes in Computer Science, 2008, Volume 5292, Software Architecture, Pages 131-147

[Pent02] Haapanen Pentti, Helminen Atte, FAILURE MODE ANDEFFECTS ANALYSISOF

SOFTWARE-BASEDAUTOMATION SYSTEMS, STUK-YTO-TR 190 / AUGUST 2002
[Pola06] Fiona Polack, Thitima Srivatanakul∗, Tim Kelly, and John Clark, Deviational analyses for validating regulations on real systems, International Workshop on Regulations Modelling and their Validation & Verification REMO2V'06, pp.813-817, 2006
[Pola08] Fiona Polack, Argumentation and the Design of Emergent Systems, 2008
[Pops03] Goseva-Popstojanova, K., et al.: Architectural-level risk analysis using UML. IEEE Transactions on Software Engineering 29(10), 946–960, 2003
[Pric08] Chris Price and Neal Snooke, An Automated Software FMEA, Proceedings of the International System Safety Regional Conference, Singapore, April 2008
[Rees97] Reese, J.D.; Leveson, N.G , Software Deviation Analysis , Proceedings of the 1997 (19th) International Conference on Software Engineering, Page(s): 250 – 260, 1997
[Sand10] A. Sandberg et al., Model-Based Safety Engineering of Interdependent Functions in Automotive Vehicles, E. Schoitsch (Ed.): SAFECOMP 2010, LNCS 6351, pp. 332–346, 2010
[Schr07]Schreiber, S.; Schmidberger, T.; Fay, A.; May, J.; Drewes, J.; Schnieder, E., UML-based safety analysis of distributed automation systems, Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on, 2007 , Page(s): 1069 - 1075
[Shou05] SHOURONG LU and WOLFGANG A. HALANG , JANUSZ ZALEWSKI, Component-based HazOp and Fault Tree Analysis in Developing Embedded Real-Time Systems with UML , 4th WSEAS International Conference on ELECTRONICS, CONTROL and SIGNAL PROCESSING, Miami, Florida, USA, 17-19 November, 2005 (pp.150-155)
[Somm03] Sommerville, I. 2003. 'An Integrated Approach to Dependability Requirements Engineering'. Proc. *11th Safety-Critical Systems Symposium*, Bristol. 3-15, Springer
[Soze07] Hasan Sozer, Bedir Tekinerdogan, and Mehmet Aksit, Extending Failure Modes and Effects Analysis Approach for Reliability Analysis at the Software Architecture Design Level, R. de Lemos et al. (Eds.): Architecting Dependable Systems IV, LNCS 4615, pp. 409–433, 2007
[Thra10] Thramboulidis, K.; Scholz, S., Integrating the 3+1 SysML view model with safety engineering, IEEE Conference on , pp.1-8
[Trou08] Troubitsyna, E., Elicitation and Specification of Safety Requirements , Systems, 2008. ICONS 08. Third International Conference on , Page(s): 202 – 207, 2008
[Vyas09] Vyas, P.; Mittal, R.K., Operation Level Safety Analysis for Object Oriented Software Design Using SFMEA , Advance Computing Conference, 2009. IACC 2009. IEEE International , Page(s): 1675 – 1679, 2009
[Wang09] Wang Wentao; Zhang Hong; , FMEA for UML-Based Software, WRI World Congress on Software Engineering, 2009. WCSE '09. , 2009 , Page(s): 456 - 460
[Weav02] Weaver, R.A., McDermid, J.A. (2002): Software Safety Arguments: Towards a Systematic Categorisation of Evidence. *Proc. 20th International System Safety Conference*, Denver USA, System Safety Society
[Weav03] R. A. Weaver, J. Fenn, T. P. Kelly, “A Pragmatic Approach to Reasoning about the Assurance of Safety Arguments” in *Proceedings of 8th Australian Workshop on Safety Critical Systems and Software (SCS'03)*, Canberra, Australia 2003. Published in *Conferences in Research and Practice in Information Technology Series*, P. Lindsay and T. Cant (Eds.), vol.33, Australian Computer Society, 2003.
[Wolf10] Wolforth, Ian, Walker, Martin, Grunske, Lars, and Papadopoulos, Y., Generalizable safety annotations for specification of failure patterns, Software Practice and Experience, 2010, vol.40, pp.453-483, 2010
[Wu07] Weihang Wu and Tim Kelly, Towards Evidence-Based Architectural Design for Safety-Critical Software Applications, Lecture Notes in Computer Science, 2007, Volume 4615, Architecting Dependable Systems IV, Pages 383-408
[Xiao10] Xiaocheng Ge, Richard F. Paige and John A. McDermid, Analysing System Failure Behaviours With PRISM, 2010 Fourth IEEE International Conference on Secure Software Integration and Reliability Improvement Companion
[Xiao10] Xiaocheng Ge, Richard F. Paige and John A. McDermid, An Iterative Approach for Development of Safety-Critical Software and Safety Arguments, 2010 Agile Conference, 2010
[Yaco02] Sherif M. Yacoub and Hany H. Ammar, A methodology for architecture-level reliability risk analysis, IEEE Trans. on Software Engineering, 2002, vol. 28, No.6, pp.529-547, 2002
[Yan08] Ben Yan; Nakamura, M.; Matsumoto, K.-i., Deriving Safety Properties for Home Network System Based on Goal-Oriented Hazard Analysis Model, Future Generation Communication and Networking, 2008. FGCN '08. Second International Conference on 2008 , Page(s): 428 - 436
[Yan09] Ben Yan, Masahide Nakamura, Lydie du Bousquet, and Ken-ichi Matsumoto, Improving Reusability of Hazard Analysis Model with Hazard Template for Deriving Safety Properties of Home Network System, International Journal of Smart Home Vol.3, No.2, April,pp.71-87, 2009
[Zafa05] Zafar, S. and R.G. Dromey. Integrating Safety and Security Requirements intoDesign of an Embedded System. in Asia-Pacific Software Engineering Conference.2005. Taipei, Taiwan: IEEE Computer Society.