Maritta Heisel
Peter Liggesmeyer
Stefan Wittmann (Eds.)

Computer Safety, Reliability, and Security

LNCS 3219

23nd International Conference, SAFECOMP 2004
Potsdam, Germany, September 2004
Proceedings

Springer

Maritta Heisel Peter Liggesmeyer
Stefan Wittmann (Eds.)

Computer Safety, Reliability, and Security

23rd International Conference, SAFECOMP 2004
Potsdam, Germany, September 21-24, 2004
Proceedings

Springer

Volume Editors

Maritta Heisel
Westfälische Wilhelms-Universität Münster
Institut für Informatik
Einsteinstr. 62, 48149 Münster, Germany
E-mail: heisel@uni-muenster.de

Peter Liggesmeyer
Fraunhofer Institut Experimentelles Software Engineering
Sauerwiesen 6, 67661 Kaiserslautern, Germany
E-mail: Peter.Liggesmeyer@t-online.de

Stefan Wittmann
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn, Germany
E-mail: stefan.wittmann@bsi.bund.de

Library of Congress Control Number: 2004112221

CR Subject Classification (1998): D.1-4, E.4, C.3, F.3, K.6.5

ISSN 0302-9743
ISBN 3-540-23176-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11317234 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3219

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

The importance of safety and security is growing steadily. Safety is a quality characteristic that traditionally has been considered to be important in embedded systems, and security is usually an essential property in business applications. There is certainly a tendency to use software-based solutions in safety-critical applications domains, which increases the importance of safety engineering techniques. These include modelling and analysis techniques as well as appropriate processes and tools. And it is surely correct that the amount of confidential data that require protection from unauthorized access is growing. Therefore, security is very important. On the one hand, the traditional motivations for addressing safety and security still exist, and their relevance has improved. On the other hand, safety and security requirements occur increasingly in the same system. At present, many software-based systems interact with technical equipment and they communicate, e.g., with users and other systems. Future systems will more and more interact with many other entities (technical systems, people, the environment). In this situation, security problems may cause safety-related failures. It is thus necessary to address safety *and* security. It is furthermore required to take into account the interactions between these two properties.

Since their start in 1979 the SAFECOMP conferences have provided a platform for discussing topics related to dependable applications of computer systems. This requires us to deal with system aspects including hardware and software. Additionally, it is necessary to address a variety of properties, e.g., safety, security, reliability, and availability. The SAFECOMP conferences discuss research results, technical innovations, tools, processes, and organizational aspects. And they provide a forum for exchanging ideas between researchers and industry.

This year's program underlined system aspects. The majority of the contributions presented approaches that address complete systems including hardware, software, and the environment. The technical content covered a wide range from formal to informal methods. It seems that each approach is characterized by specific preconditions and has its own application domain.

We are convinced that the reader of this book will get valuable information on how to improve the safety and security of computer-based systems.

Authors from 17 countries all over the world responded to the call for papers. Out of 63 submitted papers, 24 were selected for the conference. We wish to thank the members of the International Programme Committee and the external reviewers for their excellent review work and fruitful discussions in setting up the programme of SAFECOMP 2004. They also helped a lot to disseminate all announcements.

We would like to express our special thanks to Massimo Felici. He maintained the tool CyberChair for us, and, being the organizer of the last two

SAFECOMPs, he was our oracle and early warning system of what could possibly go wrong.

Sincere thanks go to the invited speakers, Andreas Pfitzmann, Didier Essamé and Ralf G. Herrtwich, and the session chairpersons for their support.

Setting up the technical programme of the conference was one thing, to actually make SAFECOMP 2004 happen was another. Our organizing team Katrin Augustin, Hans-Peter Wagner, Carsten von Schwichow and Holger Schmidt did their best to make this event a success, and they did an outstanding job. Thank you.

Last but not least our special thanks go to the Hasso-Plattner-Institute in Potsdam for providing the premises, the conference infrastructure and the answers to all our questions.

Our best wishes go to the organizers of SAFECOMP 2005 in Norway, and we hope that SAFECOMP 2004 motivated many attendees to support next year's conference.

Potsdam, Germany
July 2004

Peter Liggesmeyer
Maritta Heisel
Stefan Wittmann

Organization

General Chair

Peter Liggesmeyer, Germany

Programme Co-chairs

Maritta Heisel, Germany
Stefan Wittmann, Germany

EWICS TC7 Chair

Udo Voges, Germany

Organizing Committee

Katrin Augustin, Germany
Hans-Peter Wagner, Germany

International Programme Committee

S. Anderson, UK
H. Bezecny, Germany
R. Bharadwaj, USA
R. Bloomfield, UK
S. Bologna, Italy
A. Bondavalli, Italy
B. Buth, Germany
P. Daniel, UK
M. Felici, UK
R. Genser, Austria
C. Goring, UK
J. Gorski, Poland
B.A. Gran, Norway
W. Grieskamp, Germany
E. Großpietsch, Germany
W. Halang, Germany
M. Heiner, Germany
M. Heisel, Germany
C. Heitmeyer, USA
C. Johnson, UK
M. Kaâniche, France
K. Kanoun, France
F. Koob, Germany
F. Koornneef, The Netherlands
B. Krämer, Germany
D. Kügler, Germany
P. Ladkin, Germany
P. Liggesmeyer, Germany
O. Mäckel, Germany
M. v.d. Meulen, UK
O. Nordland, Norway
A. Pasquini, Italy
G. Rabe, Germany
F. Redmill, UK
M. Rothfelder, Germany
J. Rushby, USA
F. Saglietti, Germany
T. Santen, Germany
E. Schoitsch, Austria
J. Souquières, France
W. Stephan, Germany
L. Strigini, UK
M. Sujan, UK
P. Traverso, Italy
J. Trienikens, The Netherlands
M. Ullmann, Germany
U. Voges, Germany
A. Weinert, Germany
M. Wilikens, Italy
R. Winther, Norway
S. Wittmann, Germany
E. Wong, USA
Z. Zurakowski, Poland

External Reviewers

C.P. van Beers
R. Carvajal-Schiaffino
I. Eusgeld
J. Jacky
H. Kelter
C. Kollmitzer
J. Krinke
J. Lei
R. Leszczyna
J. Li
P. Lollini
A. Nonnengart
S. Pozzi
G. Rock
M. Roveri
L. Save
H. Schwigon
D. Sona
N. Tillmann
A. Villafiorita

Lecture Notes in Computer Science

For information about Vols. 1–3137

please contact your bookseller or Springer

Vol. 3263: M. Weske, P. Liggesmeyer (Eds.), Object-Oriented and Internet-Based Technologies. XII, 239 pages. 2004.

Vol. 3260: I. Niemegeers, S.H. de Groot (Eds.), Personal Wireless Communications. XIV, 478 pages. 2004.

Vol. 3258: M. Wallace (Ed.), Principles and Practice of Constraint Programming – CP 2004. XVII, 822 pages. 2004.

Vol. 3256: H. Ehrig, G. Engels, F. Parisi-Presicce (Eds.), Graph Transformations. XII, 451 pages. 2004.

Vol. 3255: A. Benczúr, J. Demetrovics, G. Gottlob (Eds.), Advances in Databases and Information Systems. XI, 423 pages. 2004.

Vol. 3254: E. Macii, V. Paliouras, O. Koufopavlou (Eds.), Integrated Circuit and System Design. XVI, 910 pages. 2004.

Vol. 3253: Y. Lakhnech, S. Yovine (Eds.), Formal Techniques in Timed, Real-Time, and Fault-Tolerant Systems. X, 397 pages. 2004.

Vol. 3250: L.-J. (LJ) Zhang, M. Jeckle (Eds.), Web Services. X, 300 pages. 2004.

Vol. 3249: B. Buchberger, J.A. Campbell (Eds.), Artificial Intelligence and Symbolic Computation. X, 285 pages. 2004. (Subseries LNAI).

Vol. 3246: A. Apostolico, M. Melucci (Eds.), String Processing and Information Retrieval. XIV, 316 pages. 2004.

Vol. 3242: X. Yao, E. Burke, J.A. Lozano, J. Smith, J.J. Merelo-Guervós, J.A. Bullinaria, J. Rowe, P. Tiňo, A. Kabán, H.-P. Schwefel (Eds.), Parallel Problem Solving from Nature - PPSN VIII. XX, 1185 pages. 2004.

Vol. 3241: D. Kranzlmüller, P. Kacsuk, J.J. Dongarra (Eds.), Recent Advances in Parallel Virtual Machine and Message Passing Interface. XIII, 452 pages. 2004.

Vol. 3240: I. Jonassen, J. Kim (Eds.), Algorithms in Bioinformatics. IX, 476 pages. 2004. (Subseries LNBI).

Vol. 3239: G. Nicosia, V. Cutello, P.J. Bentley, J. Timmis (Eds.), Artificial Immune Systems. XII, 444 pages. 2004.

Vol. 3238: S. Biundo, T. Frühwirth, G. Palm (Eds.), KI 2004: Advances in Artificial Intelligence. XI, 467 pages. 2004. (Subseries LNAI).

Vol. 3232: R. Heery, L. Lyon (Eds.), Research and Advanced Technology for Digital Libraries. XV, 528 pages. 2004.

Vol. 3229: J.J. Alferes, J. Leite (Eds.), Logics in Artificial Intelligence. XIV, 744 pages. 2004. (Subseries LNAI).

Vol. 3225: K. Zhang, Y. Zheng (Eds.), Information Security. XII, 442 pages. 2004.

Vol. 3224: E. Jonsson, A. Valdes, M. Almgren (Eds.), Recent Advances in Intrusion Detection. XII, 315 pages. 2004.

Vol. 3223: K. Slind, A. Bunker, G. Gopalakrishnan (Eds.), Theorem Proving in Higher Order Logics. VIII, 337 pages. 2004.

Vol. 3221: S. Albers, T. Radzik (Eds.), Algorithms – ESA 2004. XVIII, 836 pages. 2004.

Vol. 3220: J.C. Lester, R.M. Vicari, F. Paraguaçu (Eds.), Intelligent Tutoring Systems. XXI, 920 pages. 2004.

Vol. 3219: M. Heisel, P. Liggesmeyer, S. Wittmann (Eds.), Computer Safety, Reliability, and Security. XI, 339 pages. 2004.

Vol. 3217: C. Barillot, D.R. Haynor, P. Hellier (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2004. XXXVIII, 1114 pages. 2004.

Vol. 3216: C. Barillot, D.R. Haynor, P. Hellier (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2004. XXXVIII, 930 pages. 2004.

Vol. 3212: A. Campilho, M. Kamel (Eds.), Image Analysis and Recognition. XXIX, 862 pages. 2004.

Vol. 3211: A. Campilho, M. Kamel (Eds.), Image Analysis and Recognition. XXIX, 880 pages. 2004.

Vol. 3210: J. Marcinkowski, A. Tarlecki (Eds.), Computer Science Logic. XI, 520 pages. 2004.

Vol. 3208: H.J. Ohlbach, S. Schaffert (Eds.), Principles and Practice of Semantic Web Reasoning. VII, 165 pages. 2004.

Vol. 3207: L.T. Yang, M. Guo, G.R. Gao, N.K. Jha (Eds.), Embedded and Ubiquitous Computing. XX, 1116 pages. 2004.

Vol. 3206: P. Sojka, I. Kopecek, K. Pala (Eds.), Text, Speech and Dialogue. XIII, 667 pages. 2004. (Subseries LNAI).

Vol. 3205: N. Davies, E. Mynatt, I. Siio (Eds.), UbiComp 2004: Ubiquitous Computing. XVI, 452 pages. 2004.

Vol. 3203: J. Becker, M. Platzner, S. Vernalde (Eds.), Field Programmable Logic and Application. XXX, 1198 pages. 2004.

Vol. 3202: J.-F. Boulicaut, F. Esposito, F. Giannotti, D. Pedreschi (Eds.), Knowledge Discovery in Databases: PKDD 2004. XIX, 560 pages. 2004. (Subseries LNAI).

Vol. 3201: J.-F. Boulicaut, F. Esposito, F. Giannotti, D. Pedreschi (Eds.), Machine Learning: ECML 2004. XVIII, 580 pages. 2004. (Subseries LNAI).

Vol. 3199: H. Schepers (Ed.), Software and Compilers for Embedded Systems. X, 259 pages. 2004.

Vol. 3198: G.-J. de Vreede, L.A. Guerrero, G. Marín Raventós (Eds.), Groupware: Design, Implementation and Use. XI, 378 pages. 2004.

Vol. 3194: R. Camacho, R. King, A. Srinivasan (Eds.), Inductive Logic Programming. XI, 361 pages. 2004. (Subseries LNAI).

Vol. 3193: P. Samarati, P. Ryan, D. Gollmann, R. Molva (Eds.), Computer Security – ESORICS 2004. X, 457 pages. 2004.

Vol. 3192: C. Bussler, D. Fensel (Eds.), Artificial Intelligence: Methodology, Systems, and Applications. XIII, 522 pages. 2004. (Subseries LNAI).

Vol. 3191: M. Klusch, S. Ossowski, V. Kashyap, R. Unland (Eds.), Cooperative Information Agents VIII. XI, 303 pages. 2004. (Subseries LNAI).

Vol. 3190: Y. Luo (Ed.), Cooperative Design, Visualization, and Engineering. IX, 248 pages. 2004.

Vol. 3189: P.-C. Yew, J. Xue (Eds.), Advances in Computer Systems Architecture. XVII, 598 pages. 2004.

Vol. 3187: G. Lindemann, J. Denzinger, I.J. Timm, R. Unland (Eds.), Multiagent System Technologies. XIII, 341 pages. 2004. (Subseries LNAI).

Vol. 3186: Z. Bellahsène, T. Milo, M. Rys, D. Suciu, R. Unland (Eds.), Database and XML Technologies. X, 235 pages. 2004.

Vol. 3185: M. Bernardo, F. Corradini (Eds.), Formal Methods for the Design of Real-Time Systems. VII, 295 pages. 2004.

Vol. 3184: S. Katsikas, J. Lopez, G. Pernul (Eds.), Trust and Privacy in Digital Business. XI, 299 pages. 2004.

Vol. 3183: R. Traunmüller (Ed.), Electronic Government. XIX, 583 pages. 2004.

Vol. 3182: K. Bauknecht, M. Bichler, B. Pröll (Eds.), E-Commerce and Web Technologies. XI, 370 pages. 2004.

Vol. 3181: Y. Kambayashi, M. Mohania, W. Wöß (Eds.), Data Warehousing and Knowledge Discovery. XIV, 412 pages. 2004.

Vol. 3180: F. Galindo, M. Takizawa, R. Traunmüller (Eds.), Database and Expert Systems Applications. XXI, 972 pages. 2004.

Vol. 3179: F.J. Perales, B.A. Draper (Eds.), Articulated Motion and Deformable Objects. XI, 270 pages. 2004.

Vol. 3178: W. Jonker, M. Petkovic (Eds.), Secure Data Management. VIII, 219 pages. 2004.

Vol. 3177: Z.R. Yang, H. Yin, R. Everson (Eds.), Intelligent Data Engineering and Automated Learning – IDEAL 2004. XVIII, 852 pages. 2004.

Vol. 3176: O. Bousquet, U. von Luxburg, G. Rätsch (Eds.), Advanced Lectures on Machine Learning. IX, 241 pages. 2004. (Subseries LNAI).

Vol. 3175: C.E. Rasmussen, H.H. Bülthoff, B. Schölkopf, M.A. Giese (Eds.), Pattern Recognition. XVIII, 581 pages. 2004.

Vol. 3174: F. Yin, J. Wang, C. Guo (Eds.), Advances in Neural Networks - ISNN 2004. XXXV, 1021 pages. 2004.

Vol. 3173: F. Yin, J. Wang, C. Guo (Eds.), Advances in Neural Networks – ISNN 2004. XXXV, 1041 pages. 2004.

Vol. 3172: M. Dorigo, M. Birattari, C. Blum, L. M. Gambardella, F. Mondada, T. Stützle (Eds.), Ant Colony, Optimization and Swarm Intelligence. XII, 434 pages. 2004.

Vol. 3170: P. Gardner, N. Yoshida (Eds.), CONCUR 2004 - Concurrency Theory. XIII, 529 pages. 2004.

Vol. 3166: M. Rauterberg (Ed.), Entertainment Computing – ICEC 2004. XXIII, 617 pages. 2004.

Vol. 3163: S. Marinai, A. Dengel (Eds.), Document Analysis Systems VI. XI, 564 pages. 2004.

Vol. 3162: R. Downey, M. Fellows, F. Dehne (Eds.), Parameterized and Exact Computation. X, 293 pages. 2004.

Vol. 3160: S. Brewster, M. Dunlop (Eds.), Mobile Human-Computer Interaction – MobileHCI 2004. XVII, 541 pages. 2004.

Vol. 3159: U. Visser, Intelligent Information Integration for the Semantic Web. XIV, 150 pages. 2004. (Subseries LNAI).

Vol. 3158: I. Nikolaidis, M. Barbeau, E. Kranakis (Eds.), Ad-Hoc, Mobile, and Wireless Networks. IX, 344 pages. 2004.

Vol. 3157: C. Zhang, H. W. Guesgen, W.K. Yeap (Eds.), PRICAI 2004: Trends in Artificial Intelligence. XX, 1023 pages. 2004. (Subseries LNAI).

Vol. 3156: M. Joye, J.-J. Quisquater (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2004. XIII, 455 pages. 2004.

Vol. 3155: P. Funk, P.A. González Calero (Eds.), Advances in Case-Based Reasoning. XIII, 822 pages. 2004. (Subseries LNAI).

Vol. 3154: R.L. Nord (Ed.), Software Product Lines. XIV, 334 pages. 2004.

Vol. 3153: J. Fiala, V. Koubek, J. Kratochvíl (Eds.), Mathematical Foundations of Computer Science 2004. XIV, 902 pages. 2004.

Vol. 3152: M. Franklin (Ed.), Advances in Cryptology – CRYPTO 2004. XI, 579 pages. 2004.

Vol. 3150: G.-Z. Yang, T. Jiang (Eds.), Medical Imaging and Augmented Reality. XII, 378 pages. 2004.

Vol. 3149: M. Danelutto, M. Vanneschi, D. Laforenza (Eds.), Euro-Par 2004 Parallel Processing. XXXIV, 1081 pages. 2004.

Vol. 3148: R. Giacobazzi (Ed.), Static Analysis. XI, 393 pages. 2004.

Vol. 3147: H. Ehrig, W. Damm, J. Desel, M. Große-Rhode, W. Reif, E. Schnieder, E. Westkämper (Eds.), Integration of Software Specification Techniques for Applications in Engineering. X, 628 pages. 2004.

Vol. 3146: P. Érdi, A. Esposito, M. Marinaro, S. Scarpetta (Eds.), Computational Neuroscience: Cortical Dynamics. XI, 161 pages. 2004.

Vol. 3144: M. Papatriantafilou, P. Hunel (Eds.), Principles of Distributed Systems. XI, 246 pages. 2004.

Vol. 3143: W. Liu, Y. Shi, Q. Li (Eds.), Advances in Web-Based Learning – ICWL 2004. XIV, 459 pages. 2004.

Vol. 3142: J. Diaz, J. Karhumäki, A. Lepistö, D. Sannella (Eds.), Automata, Languages and Programming. XIX, 1253 pages. 2004.

Vol. 3140: N. Koch, P. Fraternali, M. Wirsing (Eds.), Web Engineering. XXI, 623 pages. 2004.

Vol. 3139: F. Iida, R. Pfeifer, L. Steels, Y. Kuniyoshi (Eds.), Embodied Artificial Intelligence. IX, 331 pages. 2004. (Subseries LNAI).

Vol. 3138: A. Fred, T. Caelli, R.P.W. Duin, A. Campilho, D.d. Ridder (Eds.), Structural, Syntactic, and Statistical Pattern Recognition. XXII, 1168 pages. 2004.

Table of Contents

Transportation

Software Development

Fault Tree Analysis

Invited Talk

Formal Methods and Systems

Security and Quality of Service

Hazard and Risk Analysis

Why Safety and Security Should and Will Merge

Andreas Pfitzmann

Fakultät Informatik
TU Dresden
D-01062 Dresden
pfitza@inf.tu-dresden.de

In the past, IT-systems at most were either safety-critical (i.e. no catastrophic consequences for the environment of the IT-system) or security-critical (i.e. even determined attackers cannot gain unauthorized access to information within and/or withhold resources of the IT-system). In future, more and more IT-systems will be both, safety- and security-critical. The reason for this is that IT-systems are embedded in ever more influential parts of our living- and working environment and that these embedded IT-systems are networked – be it to enhance their functionality now (or just as an option for future use), be it to ease maintenance.

Of course the safety community might (and should) issue warnings against this attitude of system design, because it undermines the classical way to engineer and validate safety. Of course the security community should frankly admit that using the present IT-infrastructures incorporating all kinds of unmanaged design complexity, security is mainly unachievable. But my experience of 20+ years in the area of security and privacy suggests that our warnings will not be heard or at least downplayed with arguments like:

- "These tiny embedded systems can't cause serious catastrophes, so safety is not an issue." (But if you network many systems and their failures might therefore occur at the same cause, the consequences might be much more serious.)
- "Is security really an issue? Who should have both a possibility and a motivation to attack?" (But if networking gets ever more pervasive and conflicts in our real world are not going to disappear, the answer will soon be: quite a few. But when this manifests itself on a larger scale – remember the warnings against viruses and worms issued more than 15 years from now – fixing the problem within a reasonable time span will be impossible.)

Therefore, the safety and security communities should combine and integrate efforts to designand build the networked embedded systems as secure and safe as possible given the constraints of legacy systems to be used and functionality deemed necessary for the end-users.

So far so easy to argue and understand. But do we have a chance to successfully combine and integrate? I hope so:

- Fail-safe and confidentiality as an essential security property have many structural similarities as do providing at least a gracefully degraded service and availability as another essential security property.

M. Heisel et al. (Eds.): SAFECOMP 2004, LNCS 3219, pp. 1–2, 2004.

- We have many mechanisms useful both for fault tolerance (security against unintentional "attacks") and security, where discerning between unintentional and intentional is mainly interesting for legal consequences, since stupid errors made in a complex IT-systems tend to behave quite intelligent in other parts of the systems or w.r.t. its output.

This suggests that unifying our approaches is both necessary and promising.

The Deconstruction of Safety Arguments Through Adversarial Counter-Argument

James M. Armstrong[1] and Stephen E. Paynter[2]

[1] Centre for Software Reliability, School of Computing Science,
University of Newcastle Upon Tyne, United Kingdom.
J.M.Armstrong@newcastle.ac.uk
[2] MBDA UK Ltd, Filton, Bristol, United Kingdom.
stephen.paynter@mbda.co.uk

Abstract. The project Deconstructive Evaluation of Risk In Dependability Arguments and Safety Cases (DERIDASC) has recently experimented with techniques borrowed from literary theory as safety case analysis techniques. This paper introduces our high-level method for "deconstructing" safety arguments. Our approach is quite general and should be applicable to different types of safety argumentation framework. As one example, we outline how the approach would work in the context of the Goal Structure Notation (GSN).

1 Deconstruction in a Safety Context

French philosopher Jacques Derrida's concept of *deconstruction* rests upon the idea that, ironically enough, the meaning of an argument is a function of observations that it excludes as irrelevant and the perspectives that it opposes either implicitly or explicitly. On the one hand, if we recognise an opposing argument explicitly, we might be tempted to misrepresent it as weaker than we really feel it to be; but if this misrepresentation is detected, or if our own arguments do not convince, we may succeed only in perpetuating the opposing view. On the other hand, if we try to suppress our acknowledgment of credible doubt, we leave the reader mystified as to why we feel the need to argue our conclusion. To 'deconstruct' an argument is to try to detect such failures of "closure". Such failures need not necessarily lead one to an opposed conclusion (Armstrong & Paynter 2003, Armstrong 2003).

A deconstruction of an argument tries to show how the argument undercuts itself with acknowledgements of plausible doubts about its conclusion and betrays a nervous desire for the truth of assumptions and conclusions rather than unshakeable confidence. This perspective recognizes that deductive argument is unequal to the tasks of resolving contradictions and unifying the different explanatory narratives that underlie our debates. The deconstruction of a deductive argument has two stages. The *reversal* stage develops a counter-argument from clues offered within the original argument; the *displacement* stage compares the two arguments. In the safety assessment context we view reversal as an opportunity for the reassessment of the existing safety acceptance criteria.

A safety argument is required to be inferentially valid in some sense and its empirical premises must be *justified* in such a way that they seem plausible. Empirical

M. Heisel et al. (Eds.): SAFECOMP 2004, LNCS 3219, pp. 3–16, 2004.

claims can attain the status of knowledge only by means of supporting evidence of varying reliability. This is recognized in logics of justified belief that allow premises to be "warranted" to differing degrees; for example, Toulmin (1958). Starting with the *reversal* stage of safety argument deconstruction we ignore the warrantedness of the premises: instead, we try to produce a counter-argument that seems warrantable. Hence we provisionally assume that we could find sufficient evidence for justified belief in our counter-argument. In the *displacement* stage we deal with the relative strength of the warrants and backing evidence for both argument and counter-argument. Hopefully, after reversal we will be able to see that one argument (or both) is (are) unsatisfactory and act accordingly (either accept the system or require more risk reduction). However, there is a possibility that we get two opposing arguments that are "sufficiently" warranted. A deconstruction must explicitly recognize and analyze this particular failure of "closure". To question the "closure" of an argument is to try and find a possibility that has been excluded but which when re-introduced undermines faith in the argument by suggesting a plausible counter-argument. Thus the process of deconstruction is in the final analysis *adversarial.*

Section 2 of this paper presents a brief example of safety argument deconstruction using the Goal Structuring Notation (GSN). As yet we have no pragmatic justification (e.g. cost-benefit) for the use of safety argument deconstruction in safety processes. Therefore, in Section 3 we confine ourselves to a philosophical justification in terms of the lack of deductive closure in any non-absolute argument: we show that when safety decision makers act upon "sufficiently justified" beliefs – as they do when they accept or reject safety-critical systems – they are necessarily committing themselves to a variant of the 'lottery paradox'. We explain this using a *Warranted Deduction Schema* we have developed for the comparison of arguments and counter-arguments. Sections 4 examines political aspects of deconstruction in terms of the *Warranted Deduction Schema.* Section 5 outlines future issues in the pragmatic justification of safety argument deconstruction.

2 An Example: The Goal Structuring Notation

The example deconstruction in this section is done in the context of the Goal Structuring Notation (GSN) and is adapted from Kelly (1998). The example argues a sufficiency of protection against a risk of catastrophic failure. In the source text, the example is only part of a larger GSN argument and thus some of the questions we put are answered there or are not relevant. We have taken the example out of its original context to illustrate the process of deconstruction. GSN is intended to make the structure of arguments clearer than in free text. Thus it provides a neutral and convenient format for the (de)construction of safety counter-arguments. GSN specifies:

- Goals (best expressed as predicates)
- Goal Decomposition (top down)
- Strategies (for explaining goal decompositions)
- Solutions (direct information sources)
- Justifications (for explaining rationale)
- Assumptions