ADELARD

FROM DEPENDABILITY TO SECURITY-INFORMED SAFETY

A PERSONAL PERSPECTIVE

Dr Robert Stroud, CEng (MIET)
Principal Consultant
Adelard LLP

rjs@adelard.com

1st July 2018

PT/XXX/YYY/ZZ

Adelard LLP, 24 Waterside, 44-48 Wharf Road, London N1 7UX
T +44 20 7832 5850 E office@adelard.com W www.adelard.com

“Changing the way engineers think”

INTRODUCTION

MOTIVATION

- Initial thoughts on a unified conceptual model for safety and security
- Intended to provoke discussion
- Would like to invite comment and feedback from WG 10.4 community

- DISCLAIMER
  - Ideas are still evolving, no consensus – waiting for the block chain to commit
  - My personal thoughts and opinions
  - Not necessarily the thoughts and opinions of my colleagues at Adelard

ACKNOWLEDGMENT

- It is a privilege and an honour to be able to present these preliminary thoughts to an audience including Al, Brian and Carl, but sadly not Jean-Claude

Basic Concepts and Taxonomy of Dependable and Secure Computing

Algirdas Avižienis, *Fellow, IEEE*, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, *Senior Member, IEEE*

Abstract—This paper gives the main definitions relating to dependability, a generic concept including as special case such attributes as reliability, availability, safety, integrity, maintainability, etc. Security brings in concerns for confidentiality, in addition to availability and integrity. Basic definitions are given first. They are then commented upon, and supplemented by additional definitions, which address the threats to dependability and security (faults, errors, failures), their attributes, and the means for their achievement (fault prevention, fault tolerance, fault removal, fault forecasting). The aim is to explicate a set of general concepts, of relevance across a wide range of situations and, therefore, helping communication and cooperation among a number of scientific and technical communities, including ones that are concentrating on particular types of system, of system failures, or of causes of system failures.

Index Terms—Dependability, security, trust, faults, errors, failures, vulnerabilities, attacks, fault tolerance, fault removal, fault forecasting.

1 Introduction

This paper aims to give precise definitions characterizing the various concepts that come into play when addressing the dependability and security of computing and communication systems. Clarifying these concepts is surprisingly difficult when we discuss systems in which there are uncertainties about system boundaries. Furthermore, the very complexity of systems (and their specification) is often a major problem, the determination of possible causes or consequences of failure can be a very subtle process, and there are (fallible) provisions for preventing faults from causing failures.

Dependability is first introduced as a global concept that subsumes the usual attributes of reliability, availability, safety, integrity, maintainability, etc. The consideration of security brings in concerns for confidentiality, in addition to availability and integrity. The basic definitions are then commented upon and supplemented by additional definitions. **Boldface** characters are used when a term is defined, while *italic* characters are an invitation to focus the reader's attention.

This paper can be seen as an attempt to document a minimum consensus on concepts within various specialties in order to facilitate fruitful technical interactions; in addition, we hope that it will be suitable 1) for use by other bodies (including standardization organizations) and 2) for educational purposes. Our concern is with the concepts: words are only of interest because they unequivocally label concepts and enable ideas and viewpoints to be shared. An important issue, for which we believe a consensus has not yet emerged, concerns the measures of dependability and security; this issue will necessitate further elaboration before being documented consistently with the other aspects of the taxonomy that is presented here.

The paper has no pretension of documenting the state-of-the-art. Thus, together with the focus on concepts, we do not address implementation issues such as can be found in standards, for example, in [30] for safety or [32] for security.

The dependability and security communities have followed distinct, but convergent paths: 1) dependability has realized that restriction to nonmalicious faults was addressing only a part of the problem, 2) security has realized that the main focus that was put in the past on confidentiality needed to be augmented with concerns for integrity and for availability (they have been always present in the definitions, but did not receive as much attention as confidentiality). The paper aims to bring together the common strands of dependability and security although, for reasons of space limitation, confidentiality is not given the attention it deserves.

Preceding Work and Goals for the Future. The origin of this effort dates back to 1980, when a joint committee on "Fundamental Concepts and Terminology" was formed by the TC on Fault-Tolerant Computing of the IEEE CS and the IFIP WG 10.4 "Dependable Computing and Fault Tolerance." Seven position papers were presented in 1982 at a special session of FTCS-12 [21], and a synthesis was presented at FTCS-15 in 1985 [40] which is a direct predecessor of this paper, but provides a much less detailed classification, in particular of dependability threats and attributes.

- *A. Avižienis is with Vytautas Magnus University, K. Donelaicio 58 LT-3000 Kaunas, Lithuania and the University of California at Los Angeles, 4731 Boelter Hall, Los Angeles, CA 90024-1596. E-mail: aviz@adm.vdu.lt, aviz@cs.ucla.edu.*
- *J.-C. Laprie is with LAAS-CNRS, 7 Avenue du Colonel Roche, 31077 Toulouse, France. E-mail: laprie@laas.fr.*
- *B. Randell is with the School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Rd., UK NE1 7RU. E-mail: Brian.Randell@newcastle.ac.uk.*
- *C. Landwehr is with the Institute for Systems Research, 2151 A.V. Williams Building, University of Maryland, College Park MD 20742. E-mail: clandwehr@nsf.gov.*

Manuscript received 25 June 2004; accepted 25 Aug. 2004.
For information on obtaining reprints of this article, please send e-mail to: tdsc@computer.org, and reference IEEECS Log Number TDSC-0097-0604.

1545-5971/04/$20.00 © 2004 IEEE Published by the IEEE Computer Society

AGENDA

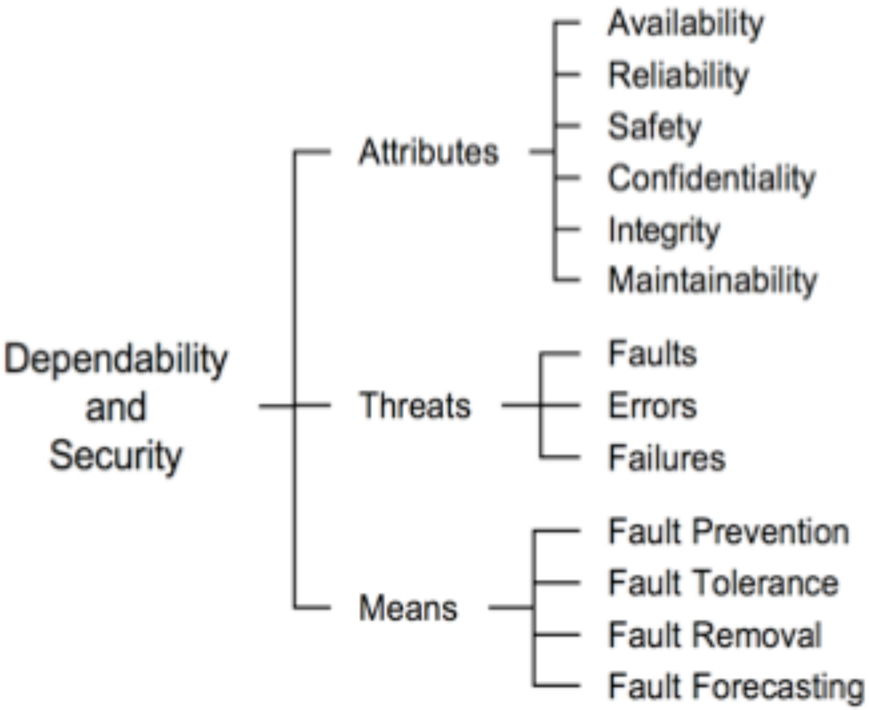
- Introduction
- Dependability 101
- Safety 101
- Security 101
- Security-informed safety
- Discussion and conclusions

“There are several excuses for using one’s own unconventional terminology, none of them respectable…”

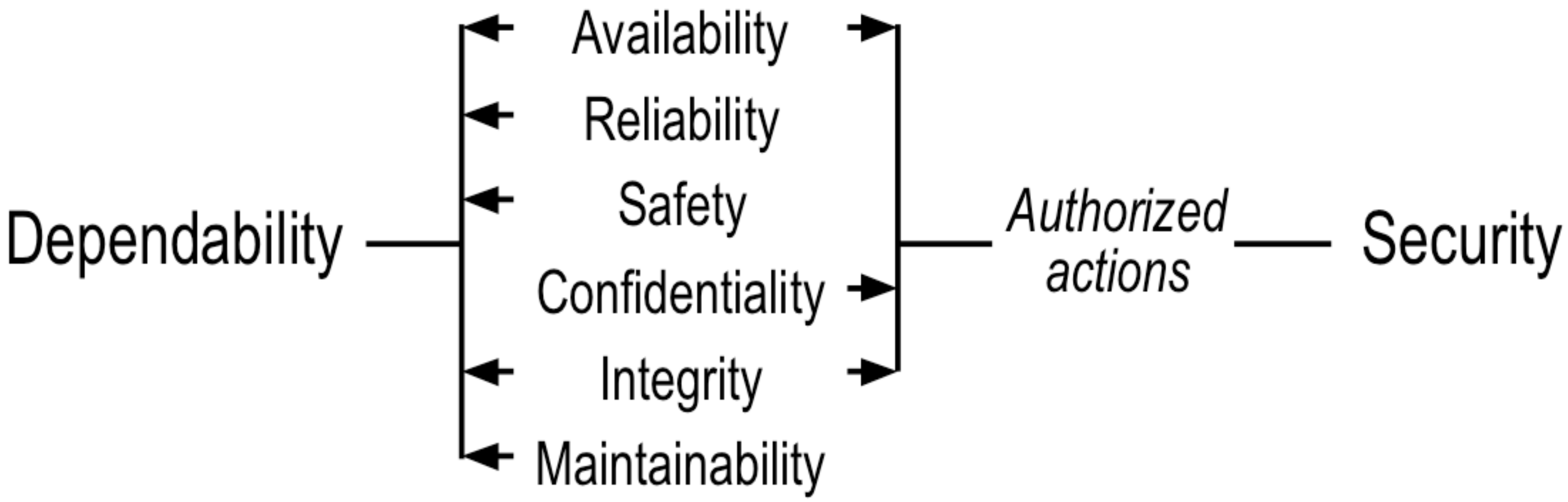
Brian Randell

DEPENDABILITY 101

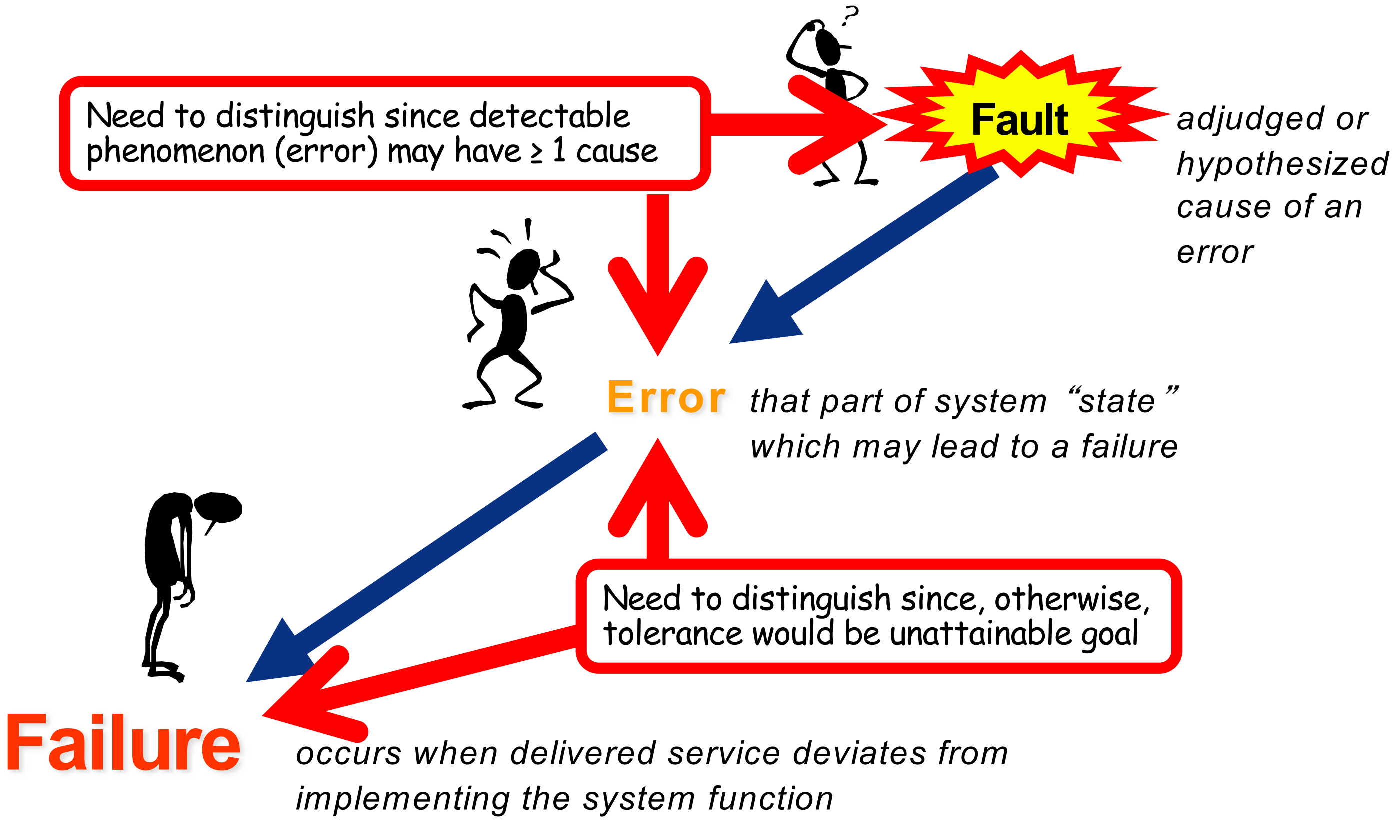
THE DEPENDABILITY AND SECURITY "TREE"



DEPENDABILITY “VERSUS” SECURITY



FAULT, ERROR, FAILURE



« Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi »

Auguste Kerckhoffs, 'La cryptographie militaire', *Journal des sciences militaires*, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Feb. 1883

SECURITY 101

WHAT IS SECURITY?

- Security can be defined as "**the state of being free from danger or threat**"
- Thus, achieving security requires guarding against potential dangers and threats
- *"Security can be sub-divided into*
  - *Physical security*
  - *Personnel security*
  - ~~*Information security*~~ ***Cyber Security***
- *The best way to provide effective security is to use a combination of security measures from all three disciplines*
- *This creates a 'multi-layered' security regime, with each layer reinforcing against the weaknesses of the next"*

Centre for the Protection of National Infrastructure (CPNI)
https://www.cpni.gov.uk

WHAT IS CYBER SECURITY?

- After much debate…
  - "Cyber security is the security of cyber space"

    High Integrity Systems Group (HISG), Railway Safety and Standards Board (RSSB)

- Securing cyber space requires a combination of
  - Physical security
  - Personnel security
  - Cyber security

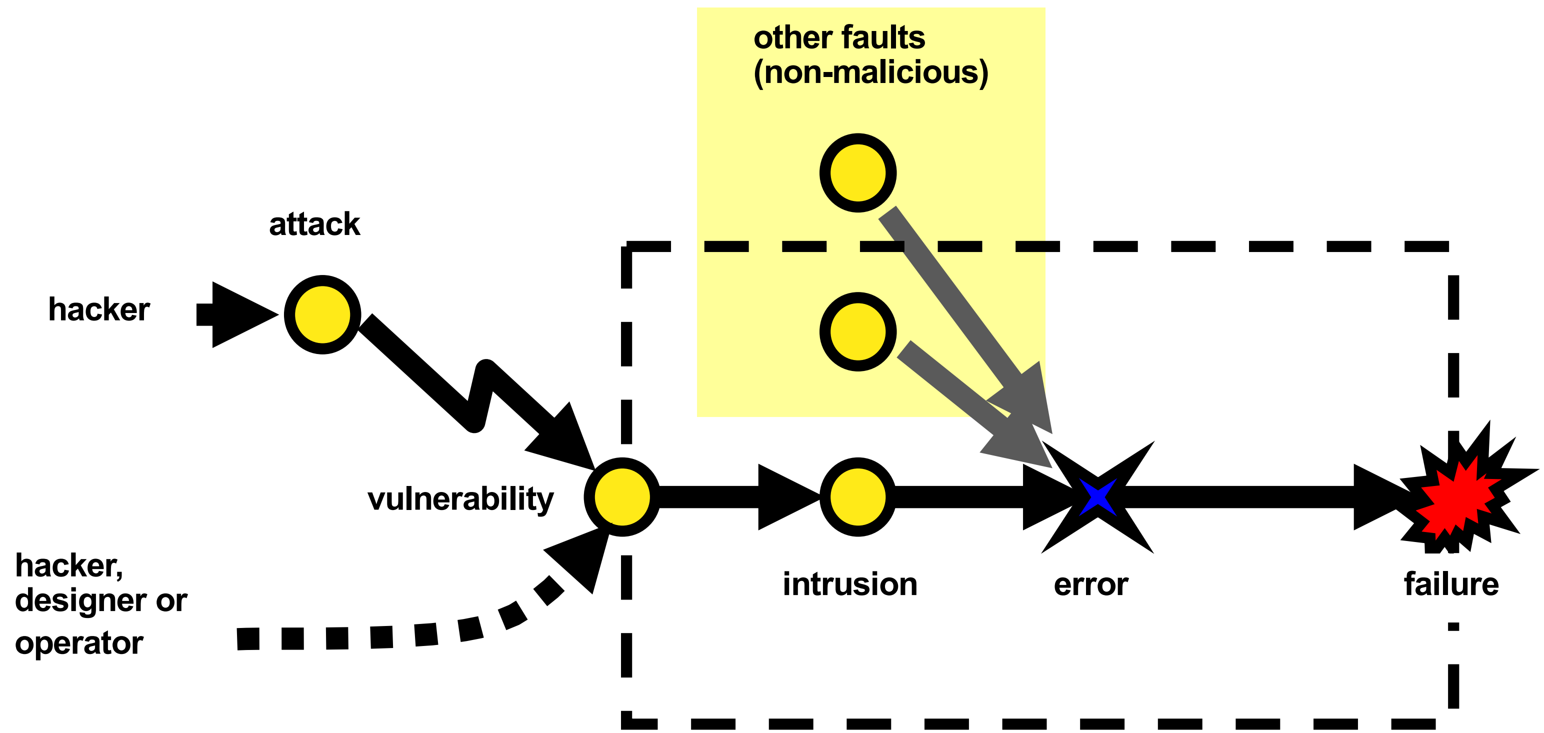
- Hmm– something not quite right there…

SOME (COMPUTER) SECURITY TERMINOLOGY

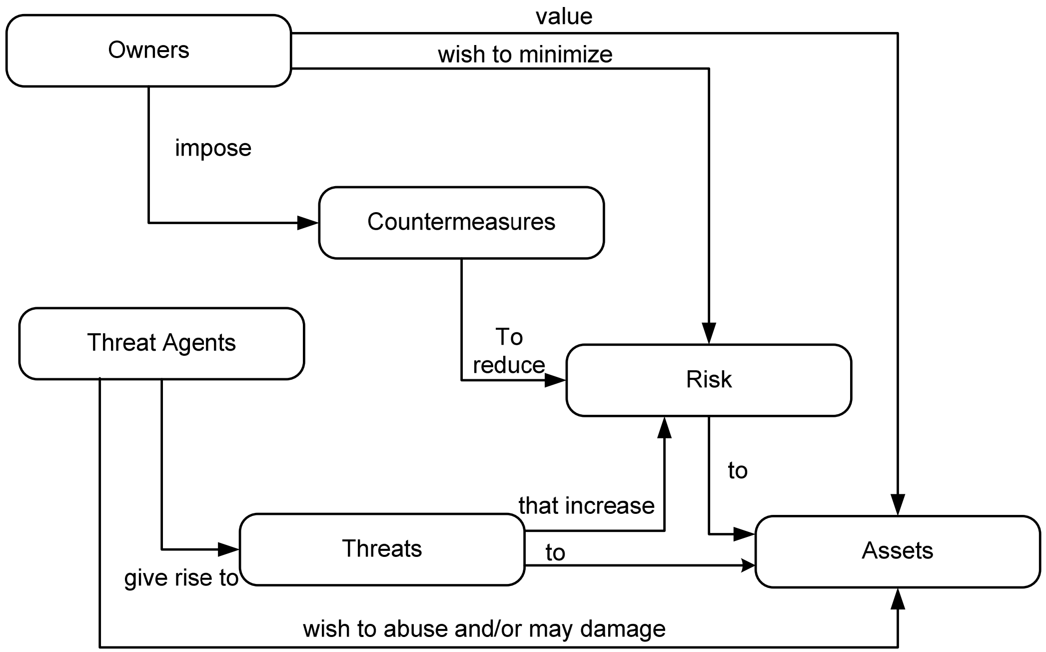
- A ***vulnerability*** is a weak point in a computer system. It may be a flaw in a piece of software that runs in a privileged mode, a poorly chosen password, or a misconfigured rule enforced by a firewall. It could even be a dependence on a service or piece of information external to the system. [...]
- A ***threat*** is an intent to inflict damage on a system. Different individuals and groups have different abilities to carry out a threat (through *attacks*), and the determination of the nature of threat against which a system must be defended should drive the decisions about its *security architecture* – its structure from the security perspective. [...]
- The ***risk*** assumed by the owner or administrator of a system is the likelihood that the system will not be able to enforce its security policy (including the continuation of critical operations) in the face of an attack. Thus risk is a function of both the exposure of the system's vulnerabilities in the context of its security architecture and the level of threat manifested against the system at a given time. [...]

Carl Landwehr, "Computer Security" (2001), available from **http://www.landwehr.org/**

ATTACK, VULNERABILITY, INTRUSION



SECURITY CONCEPTS AND RELATIONSHIPS



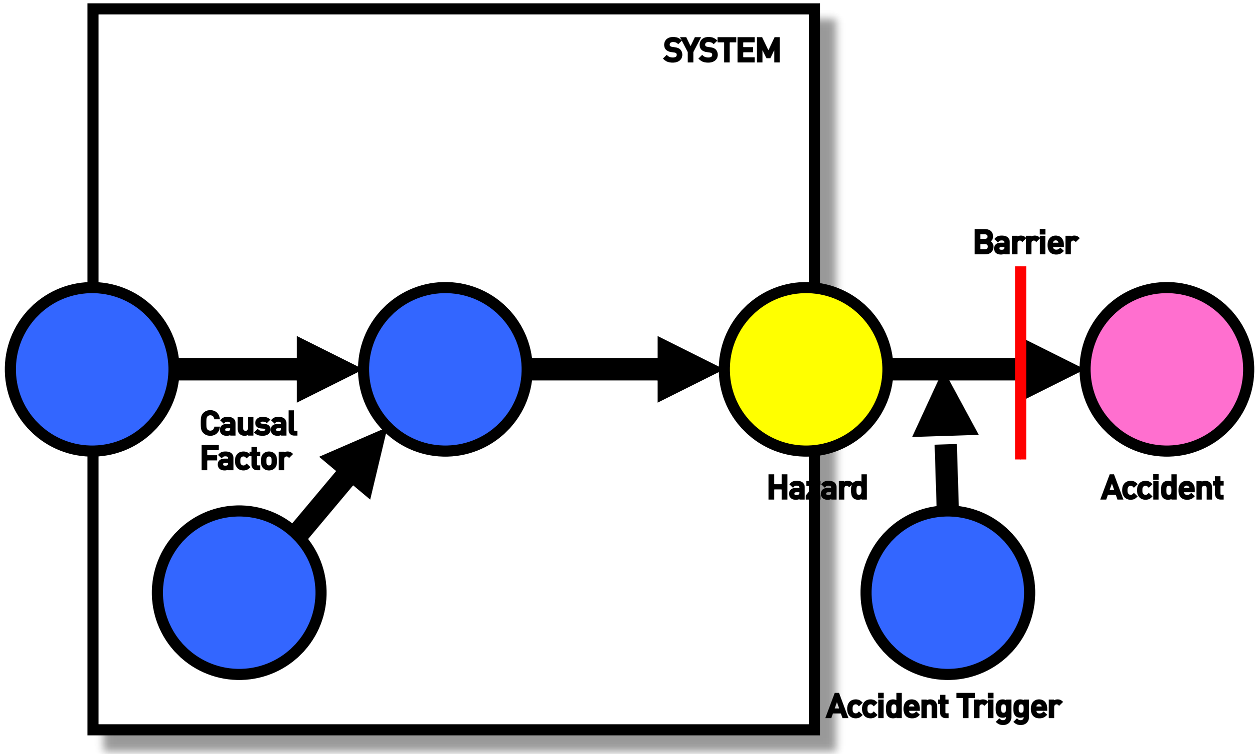
ISO/IEC 15408-1 (Common Criteria) Information Technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

"As low as reasonably practicable (ALARP)"

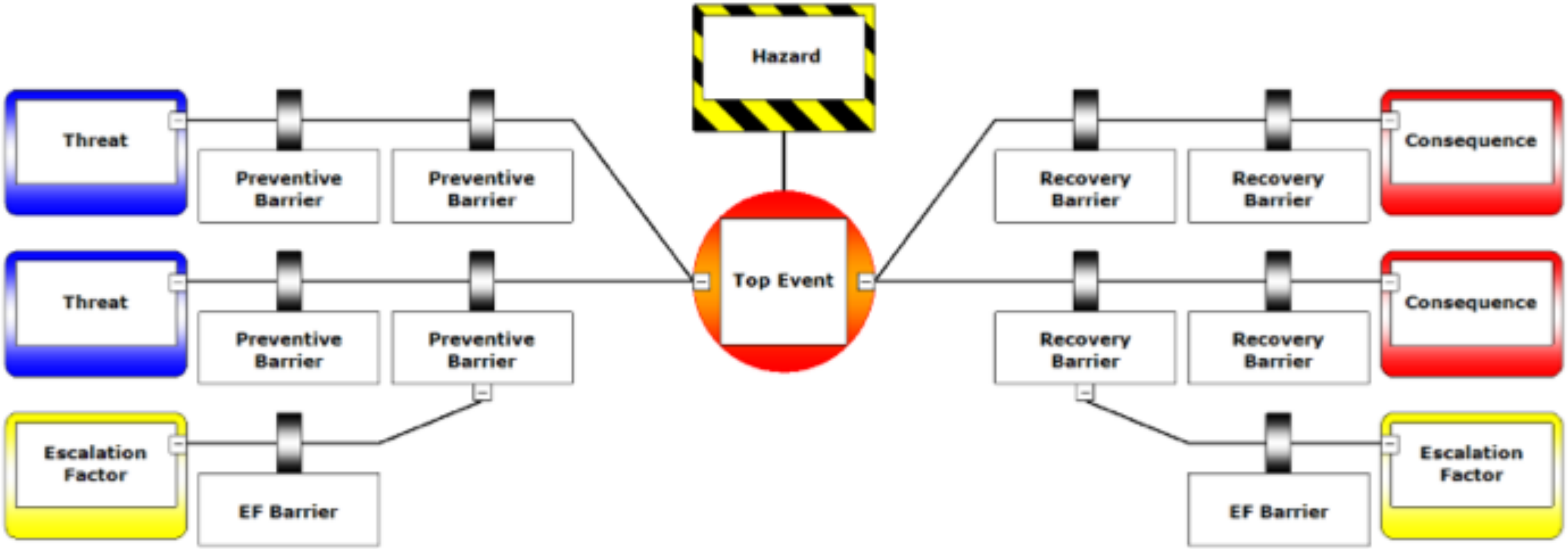
SAFETY 101

UK PERSPECTIVE

SYSTEM BOUNDARY IN SAFETY ANALYSIS (YELLOW BOOK)

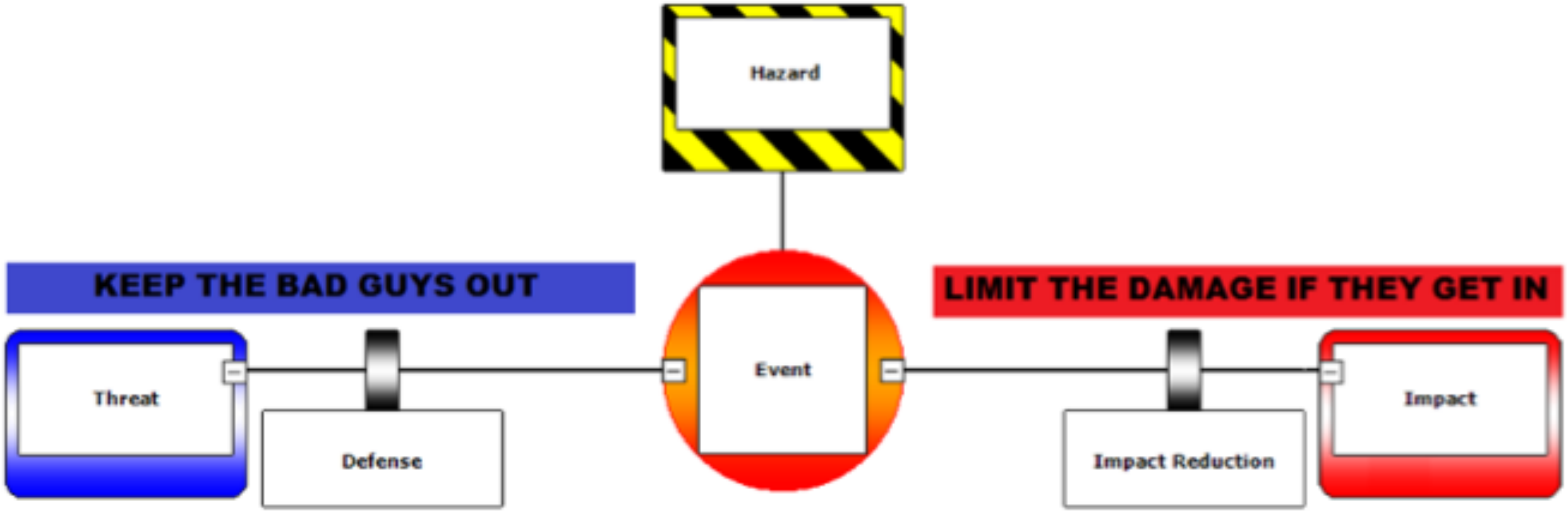


BOW TIE DIAGRAM



https://www.cgerisk.com/knowledgebase/The_bowtie_method

EXAMPLE – CYBER BOW TIE



https://pisquare.osisoft.com/groups/security/blog/2016/08/02/bow-tie-for-cyber-security-0x01-how-to-tie-a-cyber-bow-tie

KEY SAFETY CONCEPTS AND DEFINITIONS

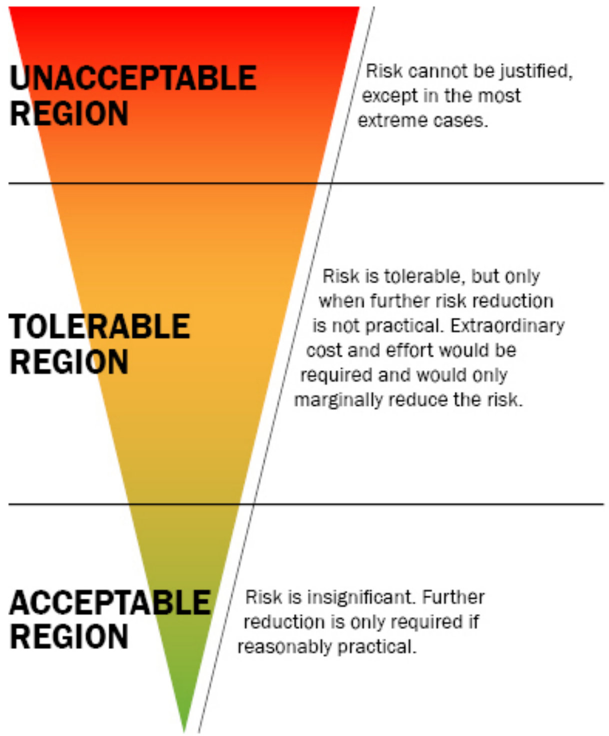
- **Safety** – freedom from unacceptable risk
- **Risk** - combination of the probability of occurrence of harm and the severity of that harm
- **Harm** – physical injury or damage to the health of people or damage to property or the environment
- **Hazard** – potential source of harm
- Causal factor??
- Severity??
- Unacceptable??

BS EN 61508-4:2010, Functional safety of electrical/ electronic/programmable electronic safety related systems, Part 4: Definitions and abbreviations

THE CARROT DIAGRAM

"'Reasonably practicable' is a narrower term than 'physically possible' ... a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them."

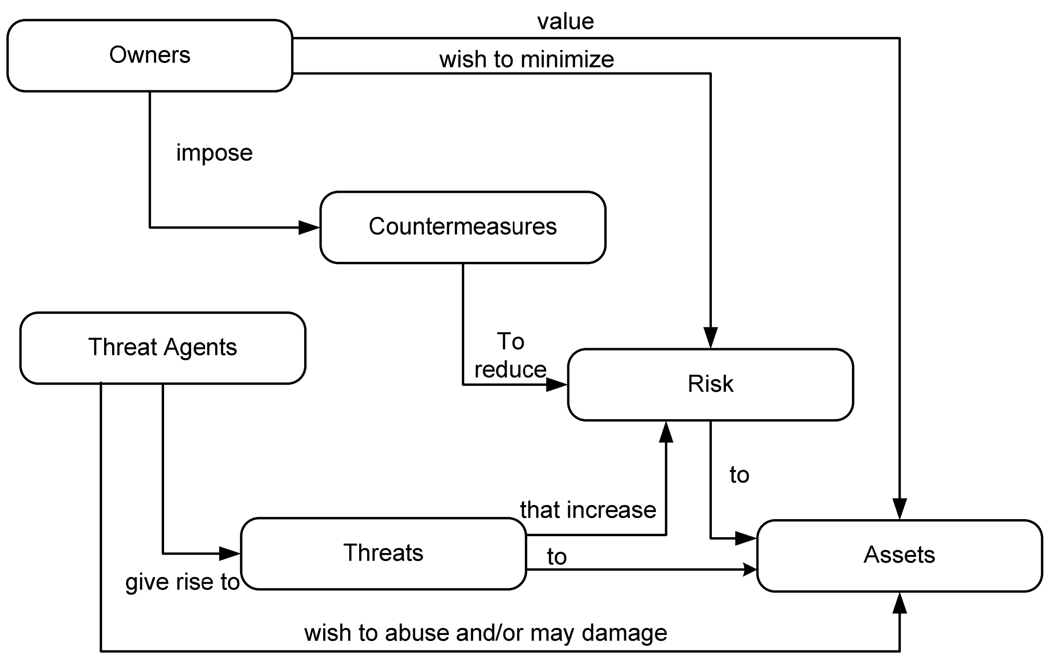
UK Court of Appeal, Edwards v. National Coal Board, 1949.



“If it’s not secure, it’s not safe”

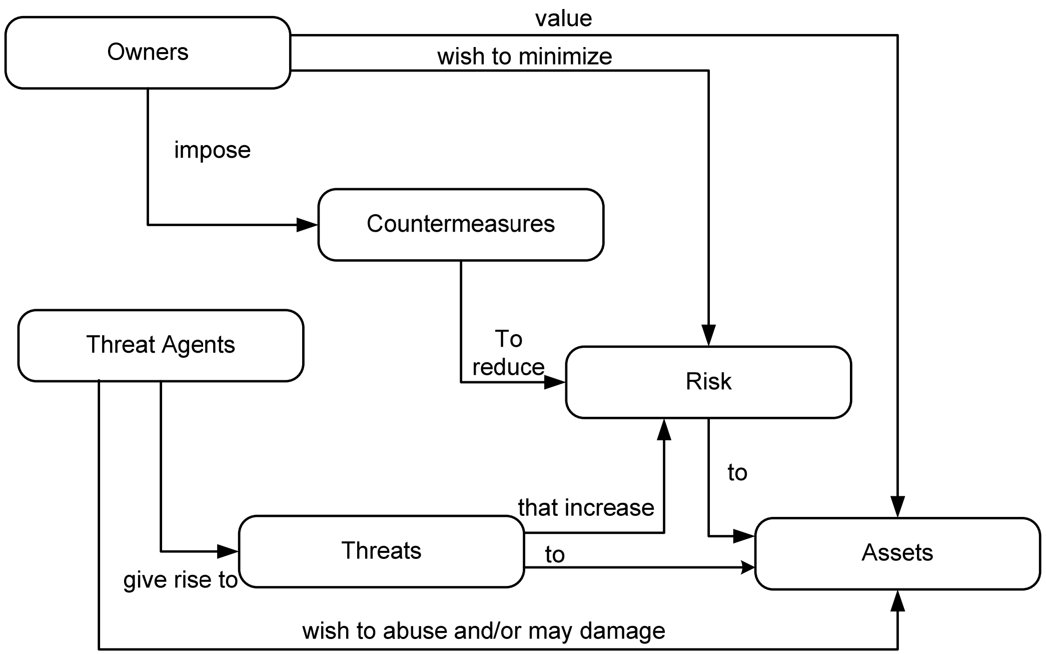
TOWARDS A COMBINED APPROACH

SECURITY CONCEPTS AND RELATIONSHIPS



ISO/IEC 15408-1 (Common Criteria) Information Technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

SECURITY / SAFETY CONCEPTS AND RELATIONSHIPS

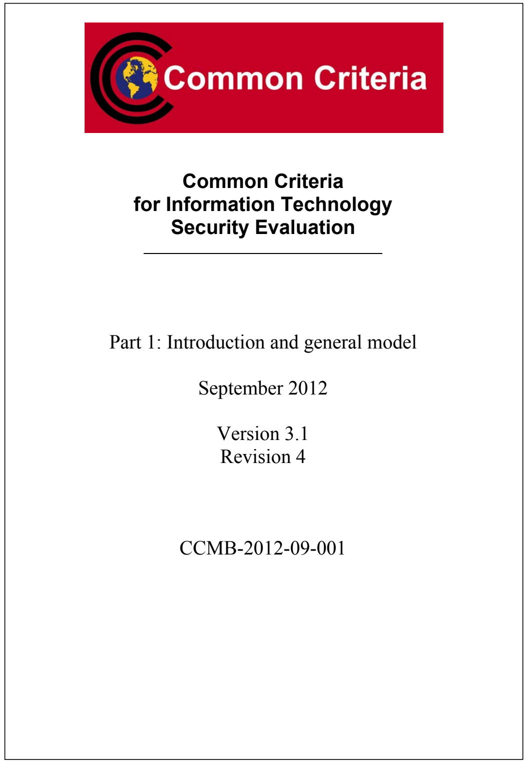


ISO/IEC 15408-1 (Common Criteria) Information Technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

WHAT IS A THREAT AGENT?

- *"Examples of threat agents include hackers, malicious users, non-malicious users (who sometimes make errors), computer processes and accidents."*
- **Common Criteria for Information Technology Security Evaluation**
- Part 1: Introduction and general model September 2012
- Version 3.1, Revision 4 Page 39, Paragraph 213

(The block chain has committed and it's in the ledger, so it must be true…)


Common Criteria

Common Criteria for Information Technology Security Evaluation

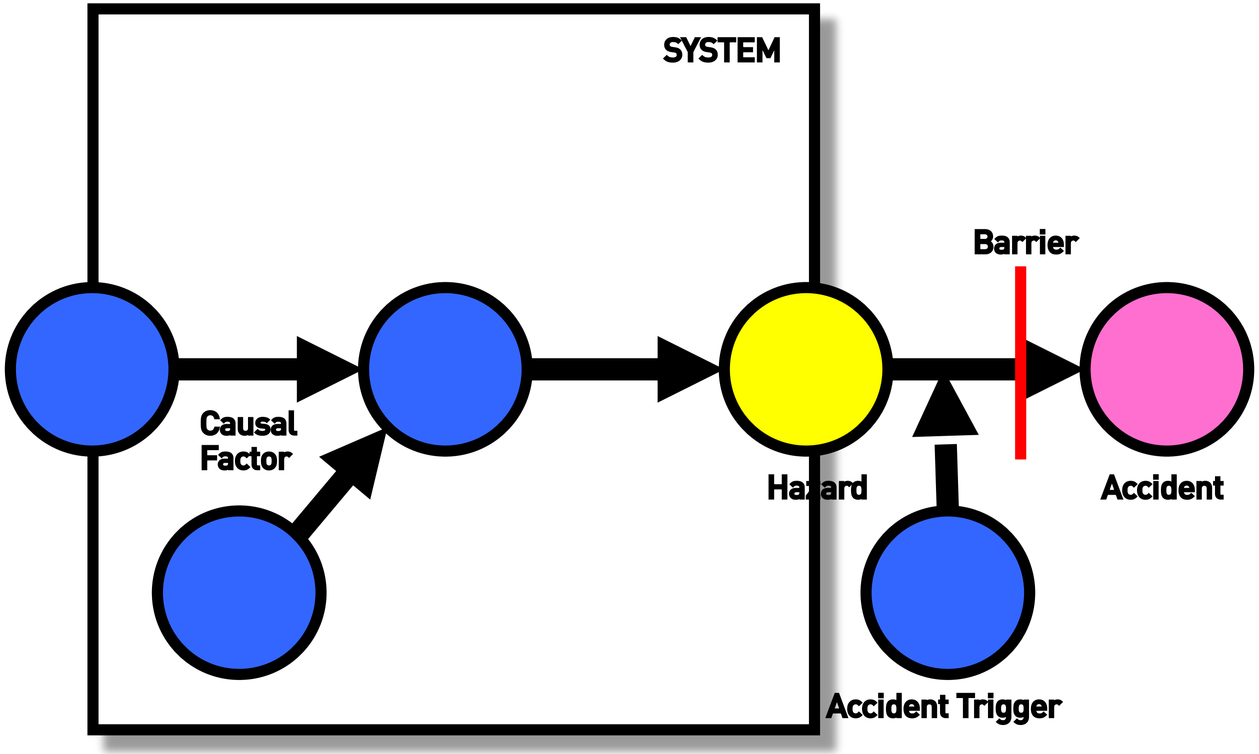
Part 1: Introduction and general model

September 2012

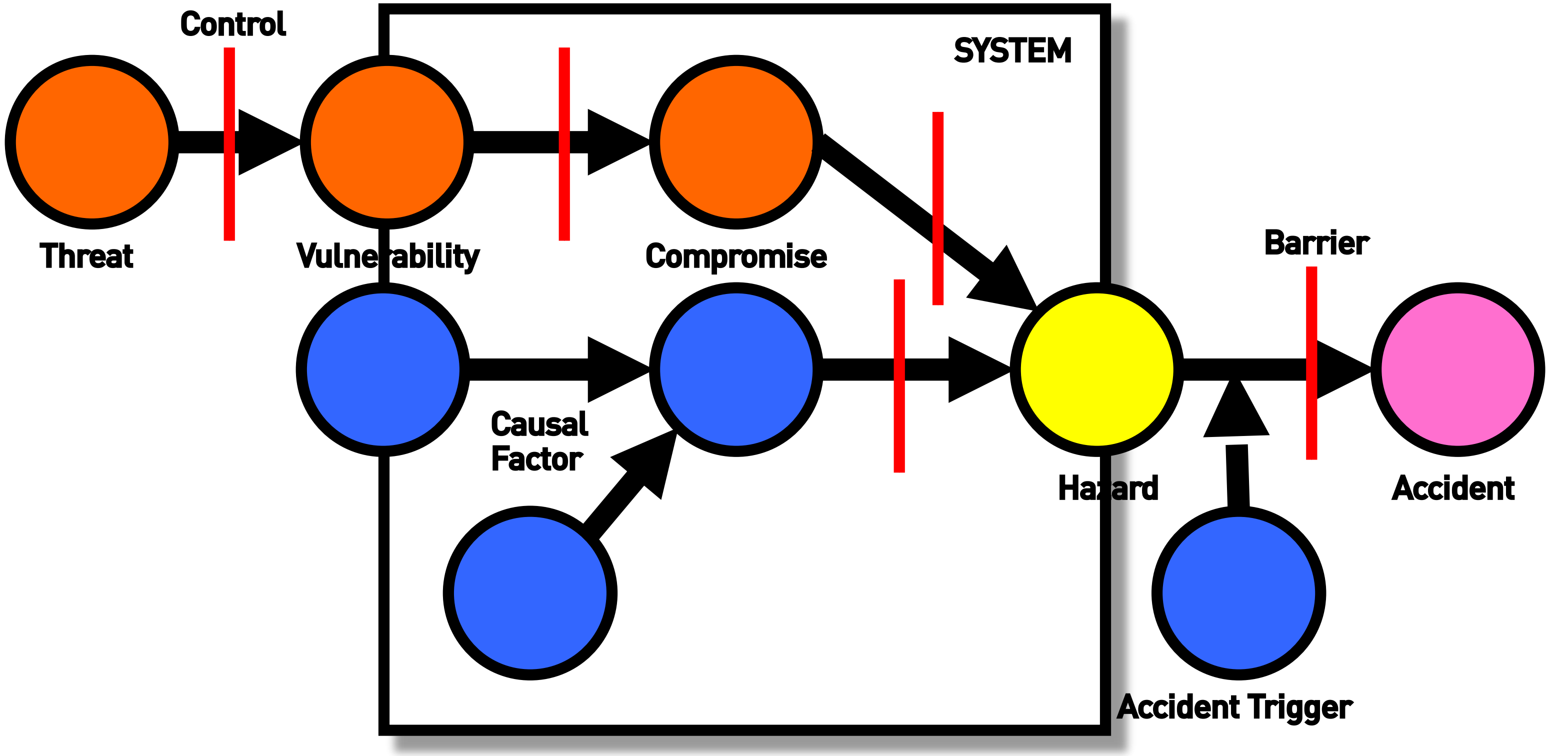
Version 3.1
Revision 4

CCMB-2012-09-001

SYSTEM BOUNDARY IN SAFETY ANALYSIS (YELLOW BOOK)



SYSTEM BOUNDARY FOR SAFETY AND SECURITY ANALYSIS



OBSERVATIONS

- There are no security hazards, there are only system hazards
- There are threats to the safety of the system
- Some of the threats are malicious, some of them are deliberate, some of them are accidental
- Regardless of the source of the threat, the consequence is the same

- **A safety analysis that did not consider security threats would be deficient**
- **Consideration of security threats might change the likelihood of a hazard, but not the consequence of the hazard**
- **Hence, security has an impact on safety risk but not safety hazards**

KEY MESSAGE

“If it’s not secure, it’s not safe”

"In my opinion, security is roughly where safety was 10 years ago. We know how to do safety but we don't know how to do security. How can I be confident that all the possible security threats have been identified?"

Professional Head of Safety, July 2017 (personal communication)

DISCUSSION

LAST WORD

- *"After the present extensive iteration, what future opportunities and challenges can we foresee that will prompt the evolution of the taxonomy? Certainly, we recognize the desirability of further:*
    - *expanding the discussion of ~~security~~* ***safety*** *[…]*
    - *analyzing issues of trust and the allied topic of* ***risk management****, and*
    - *searching for unified* ***measures*** *of dependability and security.*

IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004 11

Basic Concepts and Taxonomy of Dependable and Secure Computing

Algirdas Avižienis, *Fellow*, *IEEE*, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, *Senior Member*, *IEEE*

Abstract—This paper gives the main definitions relating to dependability, a generic concept including as special case such attributes as reliability, availability, safety, integrity, maintainability, etc. Security brings in concerns for confidentiality, in addition to availability and integrity. Basic definitions are given first. They are then commented upon, and supplemented by additional definitions, which address the threats to dependability and security (faults, errors, failures), their attributes, and the means for their achievement (fault prevention, fault tolerance, fault removal, fault forecasting). The aim is to explicate a set of general concepts, of relevance across a wide range of situations and, therefore, helping communication and cooperation among a number of scientific and technical communities, including ones that are concentrating on particular types of system, of system failures, or of causes of system failures.

Index Terms—Dependability, security, trust, faults, errors, failures, vulnerabilities, attacks, fault tolerance, fault removal, fault forecasting.

1 Introduction

This paper aims to give precise definitions characterizing the various concepts that come into play when addressing the dependability and security of computing and communication systems. Clarifying these concepts is surprisingly difficult when we discuss systems in which there are uncertainties about system boundaries. Furthermore, the very complexity of systems (and their specification) is often a major problem, the determination of possible causes or consequences of failure can be a very subtle process, and there are (fallible) provisions for preventing faults from causing failures.

Dependability is first introduced as a global concept that subsumes the usual attributes of reliability, availability, safety, integrity, maintainability, etc. The consideration of security brings in concerns for confidentiality, in addition to availability and integrity. The basic definitions are then commented upon and supplemented by additional definitions. **Boldface** characters are used when a term is defined, while *italic* characters are an invitation to focus the reader's attention.

This paper can be seen as an attempt to document a minimum consensus on concepts within various specialties in order to facilitate fruitful technical interactions; in addition, we hope that it will be suitable 1) for use by other bodies (including standardization organizations) and 2) for educational purposes. Our concern is with the concepts: words are only of interest because they unequivocally label concepts and enable ideas and viewpoints to be shared. An important issue, for which we believe a consensus has not yet emerged, concerns the measures of dependability and security; this issue will necessitate further elaboration before being documented consistently with the other aspects of the taxonomy that is presented here.

The paper has no pretension of documenting the state-of-the-art. Thus, together with the focus on concepts, we do not address implementation issues such as can be found in standards, for example, in [30] for safety or [32] for security.

The dependability and security communities have followed distinct, but convergent paths: 1) dependability has realized that restriction to nonmalicious faults was addressing only a part of the problem, 2) security has realized that the main focus that was put in the past on confidentiality needed to be augmented with concerns for integrity and for availability (they have been always present in the definitions, but did not receive as much attention as confidentiality). The paper aims to bring together the common strands of dependability and security although, for reasons of space limitation, confidentiality is not given the attention it deserves.

Preceding Work and Goals for the Future. The origin of this effort dates back to 1980, when a joint committee on "Fundamental Concepts and Terminology" was formed by the TC on Fault-Tolerant Computing of the IEEE CS and the IFIP WG 10.4 "Dependable Computing and Fault Tolerance." Seven position papers were presented in 1982 at a special session of FTCS-12 [21], and a synthesis was presented at FTCS-15 in 1985 [40] which is a direct predecessor of this paper, but provides a much less detailed classification, in particular of dependability threats and attributes.

- *A. Avižienis is with Vytautas Magnus University, K. Donelaicio 58 LT-3000 Kaunas, Lithuania and the University of California at Los Angeles, 4731 Boelter Hall, Los Angeles, CA 90024-1596. E-mail: aviz@adm.vdu.lt, aviz@cs.ucla.edu.*
- *J.-C. Laprie is with LAAS-CNRS, 7 Avenue du Colonel Roche, 31077 Toulouse, France. E-mail: laprie@laas.fr.*
- *B. Randell is with the School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Rd., UK NE1 7RU. E-mail: Brian.Randell@newcastle.ac.uk.*
- *C. Landwehr is with the Institute for Systems Research, 2151 A.V. Williams Building, University of Maryland, College Park MD 20742. E-mail: clandwehr@nsf.gov.*

Manuscript received 25 June 2004; accepted 25 Aug. 2004.
For information on obtaining reprints of this article, please send e-mail to: tdsc@computer.org, and reference IEEECS Log Number TDSC-0097-0604.

1545-5971/04/$20.00 © 2004 IEEE Published by the IEEE Computer Society

ADELARD

“[...] groundbreaking new security guideline that addresses the longstanding problem of how to engineer trustworthy, secure systems—systems that can provide continuity of capabilities, functions, services, and operations during a wide range of disruptions, threats, and other hazards”

Ron Ross, Rethinking cybersecurity from the inside out
http://nist-takingmeasure.blogs.govdelivery.com/rethinking-cybersecurity/

SYSTEMS SECURITY ENGINEERING

NIST SP 800-160

- In November 2016, NIST published a new standard on Systems Security Engineering – according to the principal author:
  - *"[…] the most important publication that I have been associated with in my two decades of service at NIST" (Ron Ross)*
- The full title of the standard is
  - **NIST SP 800-160** - Systems Security Engineering - *Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
- The idea is to add security engineering considerations to an existing standard on systems engineering
  - **ISO/IEC/IEEE 15288** – Systems and software engineering — System life cycle processes
- The standard runs to nearly 250 pages and is ***very*** comprehensive…

System Life Cycle Processes

Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

Agreement Processes	Organization Project-Enabling Processes	Technical Management Processes	Technical Processes
• Acquisition • Supply	• Life Cycle Model Management • Infrastructure Management • Portfolio Management • Human Resource Management • Quality Management • Knowledge Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement • Quality Assurance	• Business or Mission Analysis • Stakeholder Needs and Requirements Definition • System Requirements Definition • Architecture Definition • Design Definition • System Analysis • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal

Source: *ISO/IEC/IEEE 15288: 2015*

"This standard requires […] malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety lifecycle phases."

IEC 61508-1:2010, Clause 1.2 (j)

SECURITY IN SAFETY STANDARDS