Terminology Proposal: Redundancy for Fault Tolerance

Author:
Johannes Specht, University of Duisburg-Essen

Contributors:
Markus Jochim, General Motors Company
Wilfried Steiner, TTTech Computertechnik AG

Introduction

San Antonio 2012 (cmp. Gen2 Assumptions):

- *<various Syntax> vs. Static Redundancy* vs. *Protection Switching* vs. *MSTP* vs. *Seamless Redundancy* vs. 2oo3 …

- A common terminology seemed useful …

- … there is an existing terminology since the 80s commonly used in the field of Fault Tolerant Systems (or beyond fault tolerance, *Dependable* Systems)

Goals of this Presentation

- Give a brief overview of literature, basic concepts and terminology.

- Propose selected terminology for current work in 802.1:
  - Set the redundancy related terminology found in the Gen2 Assumptions slides into a structured context w.r.t. fault tolerance
  - Allow classification of upcoming and existing related concepts in 802.1
  - Simplify future communication in 802.1

- Focus on technical aspects during system operation, w.r.t. fault tolerance and redundancy

No Goals of this Presentation

This presentation will not:

- Define new names for specific mechanisms of 802.x

- Provide a complete overview of everything related to fault tolerant systems and beyond, e.g. :
  - Detailed fault classification
  - Consideration of fault forecasting related topics, etc.
  - Scopes beyond system operation like specification, repair, …

- Consider redundancy beyond the scope of fault tolerance, e.g. to improve bandwidth or computation speed

A BRIEF OVERVIEW

Dependability

- Dependability
  - Global concept to subsume reliability, availability, safety, integrity, maintainability, etc.
  - Community active in research, development and science
  - Provides general and specific concepts to avoid system failures

- Application Areas
  - High Availability Computing, Telephone Switching Systems
  - Automotive, e.g. Steer-by-Wire, Damping Control Systems, etc.
  - Aerospace, e.g. High-Lift Systems
  - Railway Signaling Systems
  - …

Literature

Comprehensive/in depth explanations are found in these books:

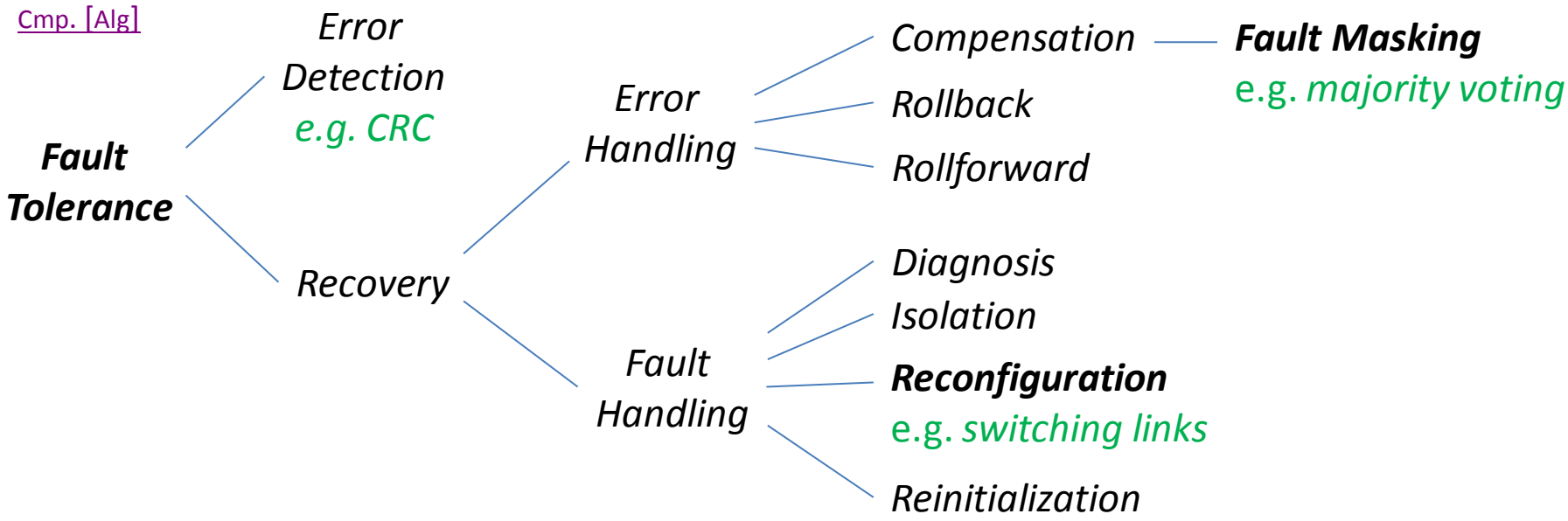
Ref.	Description
[La]	**Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese** Jean-Claude Laprie (ed.) Springer-Verlag, Wien 1992, ISBN 3-211-82296-8
[Ech]	**Fehlertoleranzverfahren** *(German Book following the terminology of [Ran])* Klaus Echtle, University of Duisburg-Essen Springer-Verlag, 1990, ISBN 978-3-540-52680-3 http://dc.informatik.uni-essen.de/Echtle/all/buch_ftv/
[Ran]	**Computing Systems Reliability – An Advanced Course** Tom Anderson, Brian Randell, University of Newcastle upon Tyne Cambridge University Press, 1979, ISBN 0-521-22767-4

More Literature …

… with overviews/details of this slide deck:

Ref.	Description
[Alg]	**Basic Concepts and Taxonomy of Dependable and Secure Computing** Algirdas Avizienis, Fellow, IEEE, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, Senior Member, IEEE IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, January-March 2004 http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1335465
[Nel]	**Fault-Tolerant Computing: Fundamental Concepts** Victor P. Nelson, Auburn University IEEE Computer, Vol. 23, Issue 7, 1990 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=56849&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D56849

Overview of Fault Tolerance Techniques



→There is a widely used terminology, classification and hierarchical structure of techniques

→**Redundancy** is a mandatory prerequisite for various fault tolerance mechanisms

-General Terminology

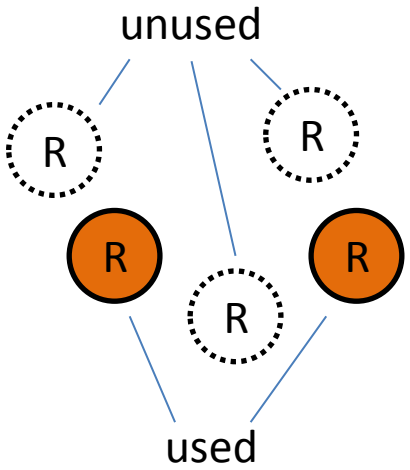
-Classification Criteria for Redundancy

PROPOSED TERMINOLOGY

General Terminology: Reconfiguration

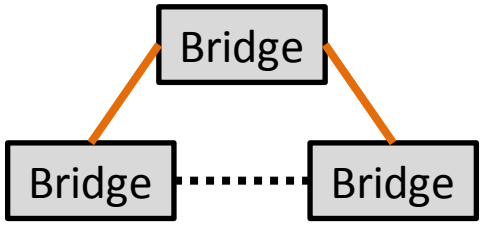
- ***Reconfiguration*:**

  [La][Ech] (w.r.t. fault tolerance) ***Reconfiguration*** of a system is commonly used for consecutive fault passivation, e.g. by replacing faulty resources by previously unused *resources*.

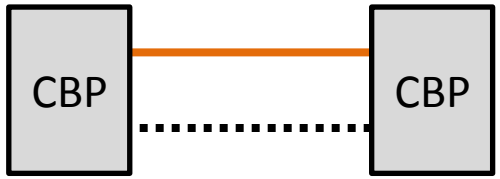


Examples

RSTP



Protection Switching



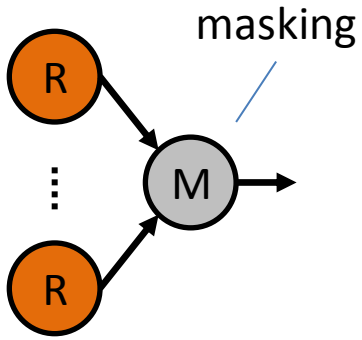
802.1 AS

Switching to another clock source/grand-master

General Terminology: Fault Masking

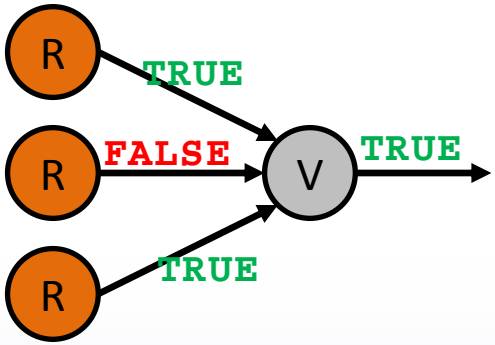
- ***Fault Masking:***

  [La][Ech] Fault masking is the systematic application of error compensation (even in absence of errors).

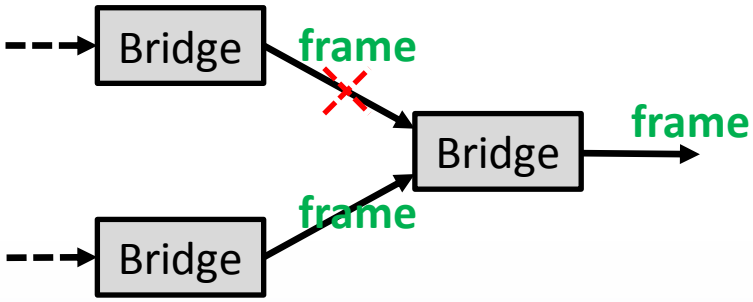


Examples

Majority Voting



802.1 „Seamless Redundancy“



Fault Tolerant Clock Sync.

http://www.ieee802.org/1/files/public/docs2012/new-avb-wsteiner-fault-tolerant-clock-synchronization-0112-v01.pdf

Redundancy: Classification Criteria

Restricting on a small and (hopefully) useful set, the following classification criteria for redundancy are proposed:

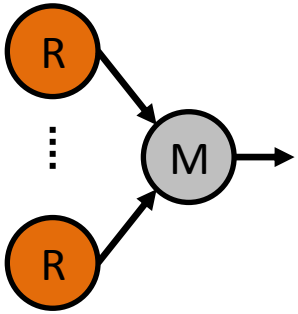
1. *Activation* of Redundancy (cmp. [Nel][Ech])

2. *Types* of Redundancy (cmp. [La][Ech])

Activation of Redundancy

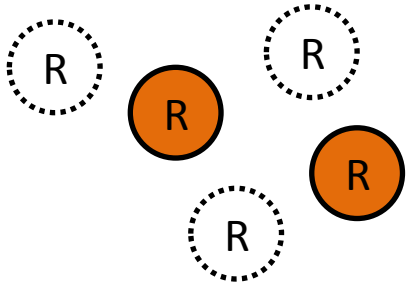
- ***Static** Redundancy*:

  Redundancy (redundant streams, links, topologies, …) is continuously used by the service of interest, regardless whether faults are present or not. Faults are tolerated by e.g. *fault masking*.



- ***Dynamic** Redundancy*:

  Redundancy is activated on demand by a service of interest in presence of faults typically after *reconfiguration*.



Static vs. Dynamic Redundancy

	Static Redundancy	Dynamic Redundancy
Resource utilization	Resource intensive: Resources are always use, regardless whether faults are present or not. Faults are tolerated by *fault masking*	Resource friendly: Resources are used on demand in presence of faults by *reconfiguration*
Timing behavior	Requires no failover time, i.e. the time consumption is low	Additional failover time required
Reliability	Provides highest short term reliability	Provides high long-term reliability

- *Hybrid Redundancy*:

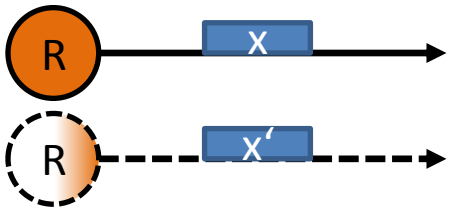
  Comprises various mixed forms of *static* and *dynamic* redundancy to overcome drawbacks of *static* and *dynamic* redundancy.

  Example:

  Fault masking until a certain threshold, followed by *reconfiguration*.

Types of Redundancy

- ***Structural** Redundancy*:
  Multiple resources are used to provide redundancy, e.g. sending a frame twice via disjoint links, ports, paths, …



- ***Time** Redundancy*:
  One resource is used longer to provide redundancy, e.g. sending a frame twice via one link, port, path, …

- Both types can appear in a restricted form (cmp. [La], shown here for time redundancy).

- For specific mechanisms, time- and structural redundancy are not mutual exclusive, e.g. majority voting over three frames, two sent via on link and the third via another link.

Summary of this proposal

The following terminology is proposed to 802.1:

Fault tolerance in General:

- ***Fault Masking***
- ***Reconfiguration***

Redundancy Activation:

- ***Static Redundancy***
- ***Dynamic Redundancy***

Redundancy Types:

- ***Structural Redundancy***
- ***Time Redundancy***

Thank you for your Attention!

Impressions, Questions, Ideas?

Johannes Specht

Dipl.-Inform. (FH)

Dependability of Computing Systems
Institue for Computer Science and
Business Information Systems (ICB)
Faculty of Economics and
Business Administration
University of Duisburg-Essen

Schützenbahn 70
Room SH 502
45127 Essen
GERMANY
T +49 (0)201 183-3914
F +49 (0)201 183-4573

specht@dc.uni-due.de
http://dc.uni-due.de