RiskConsult GmbH
www.riskcon.at

Probabilistic Safety Value Analysis - Basics

RIAAT R.A.M.S
www.riaatsoftware.com

What is RAMS ?

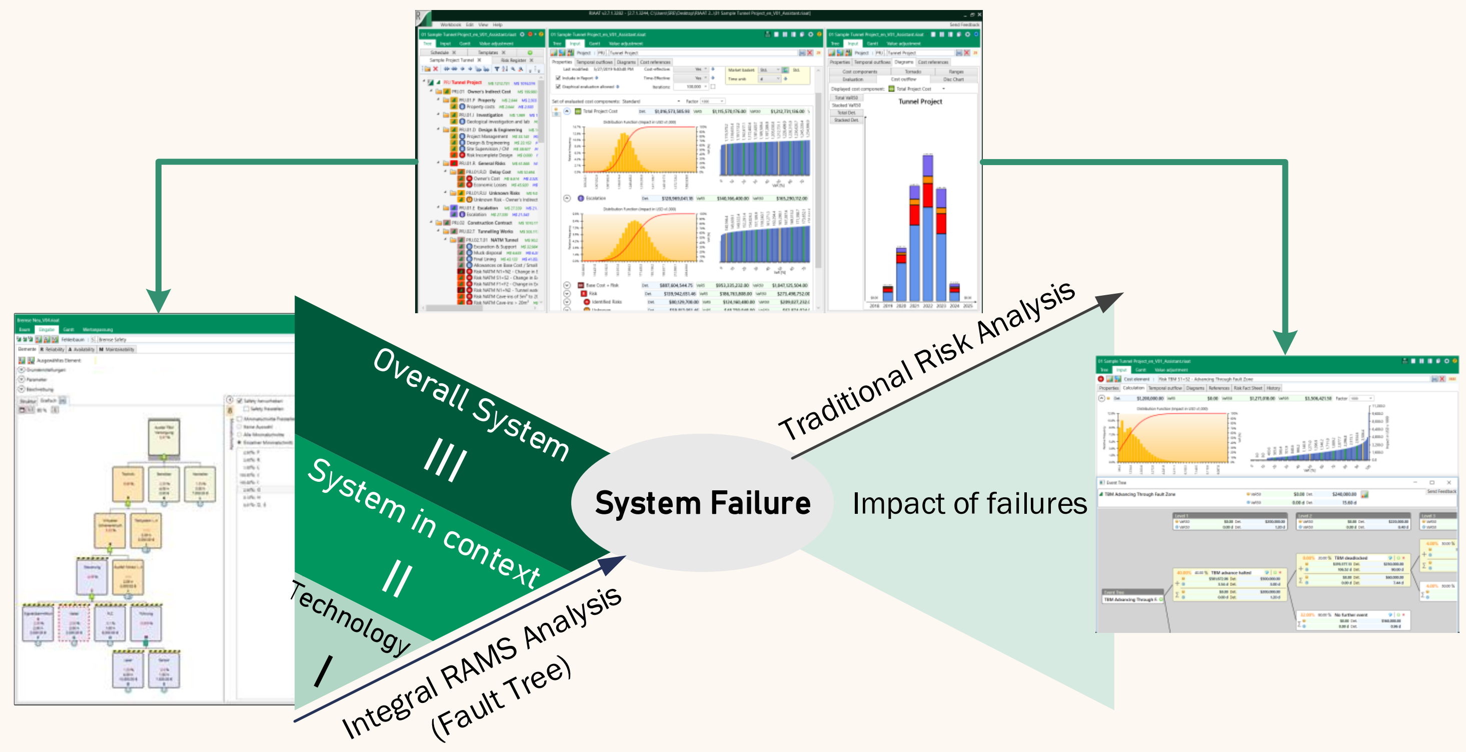
RAMS (**R**eliability, **A**vailability, **M**aintainability, **S**afety) is a process to avoid failures already in the planning stage of projects. RAMS Management ensures that systems are defined, risk analyses are performed, hazards are identified and detailed reviews and safety cases are executed and reported. One specific goal is to provide hard evidence to achieve authorization for operations.

The Fault Tree Analysis (FTA) is the core of RAMS. The FTA depicts the functional system and quantifies all relevant factors to evaluate reliability, availability, maintainability and safety of the complete system. All components of a system will be evaluated systematically and analyzed according to their roles and functions within the system.

RIAAT provides a comprehensive system analysis:

- Evaluation of the soundness of a system: **R**eliability, **A**vailability and **M**aintainability (**RAM**)
- Check if all **S**afety requirements are fulfilled (RAM**S**)
- Modeling of complex scenarios fosters a better understanding of context, causes and effects
- Strong visualization of transparent system models
- Evaluation of critical failure combinations (Minimal Cut Sets)
- Description of potential for optimization by comprehensive assessment and reporting capabilities
- Support of probabilistic methods to model uncertainty
- Intuitive handling of the software
- In compliance with relevant standards and guidelines

RAMS Process



Phase I: Technology (I)

Assessment of Reliability, Availability, Maintainability and Safety of a system in a closed mode (Clean Room). Including Common Cause Factors originating within the analyzed system.

Phase II: System in Context (II)

Assessment of Reliability, Availability, Maintainability and Safety of a system in the foreseeable context. Including external influence and Common Cause Factors originating outside the analyzed system.

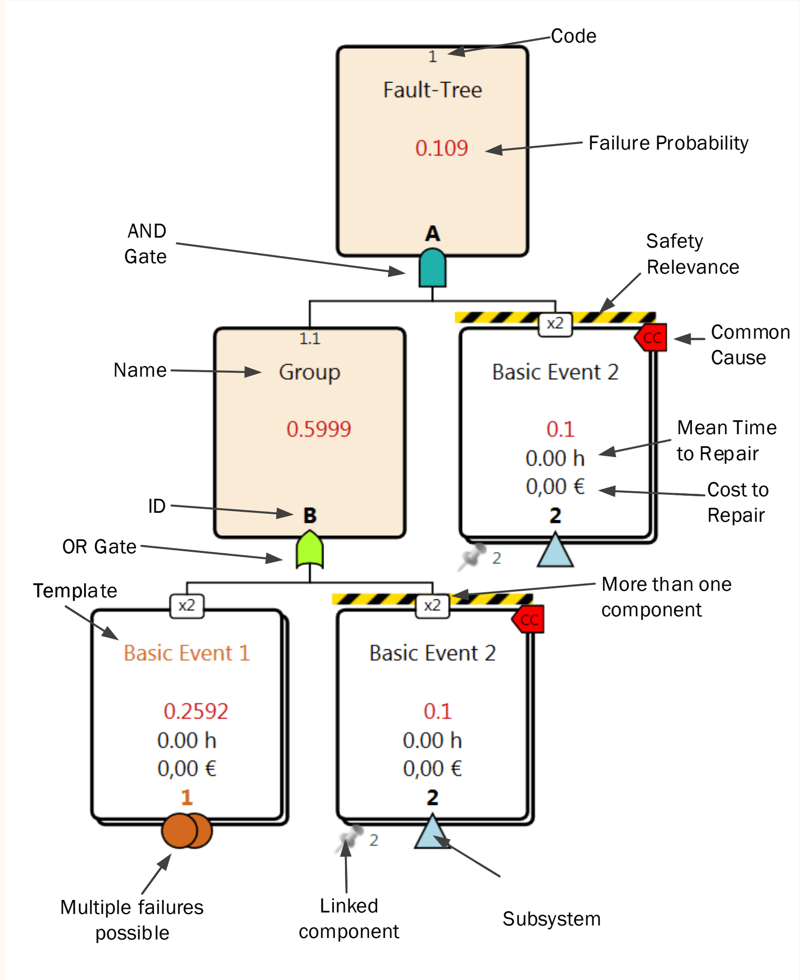
Phase III: Overall System (III)

Assessment of Reliability, Availability, Maintainability and Safety of a system in interaction with higher-level and other parallel systems.

Terms

AP – Analysis Period		
DT – Down Time		UT – Up Time
PMT – Preventive Maintenance Time	ICMT – Immediate Corrective Maintenance Time	DCMT – Deferred Corrective Maintenance Time
	CMT – Corrective Maintenance Time	
MT – Maintenance Time		

Starting at the Top Event (System Failure) all functions and the assigned failure status of the system's components are evaluated. This results in a Boolean Model (Fault Tree) which is quantified by the characteristic reliability values. The logical linking of events is based on the following graphical elements:



OR Gate: The succeeding event happens if at least one of the preceding events have happened.

AND Gate: The succeeding event happens if all of the preceding events have happened.

K Gate: The succeeding event happens if at least k of the preceding events have happened.

Single failure of a component: Model of one failure at maximum within the selected Life Cycle Analysis Period (LCA).

Multiple failure of a component: Model of multiple potential failures within the selected Life Cycle Analysis Period (LCA).

Safety Relevance: Components with this marking will be transferred to a separate safety tree as well.

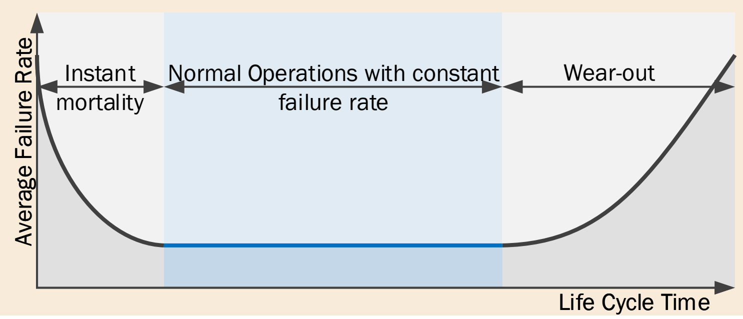
Template: Multiple use of same components.

Subsystem: Placeholder for another system not (yet) analyzed in detail.

Linked Element: The same element has been used multiple times in the fault tree.

Number of components: Compressed depiction for more than one component.

Common Cause: Failure due to the same cause.

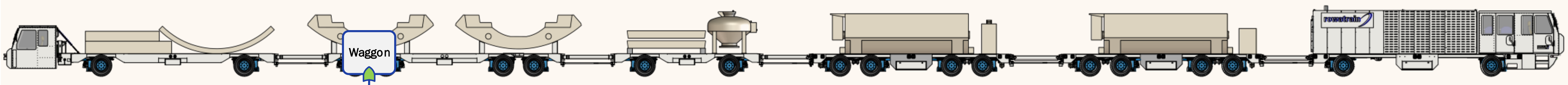


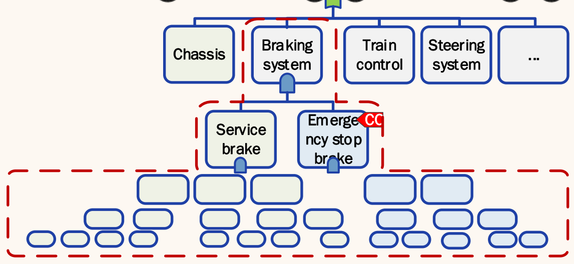
MTBF (Mean Time Between Failure)

MTBF describes the reliability of a component, and is the reciprocal of the failure rate. Assuming that components will be used only in that part of their life cycle where the rate of failures is constant. All failures due to material deficiencies, wear-out and fatigue have to be controlled by quality assurance/quality control and can therefore be excluded.

Probabilistic Safety Value Analysis

Example: Fault tree analysis - braking system as part of a TBM supply train

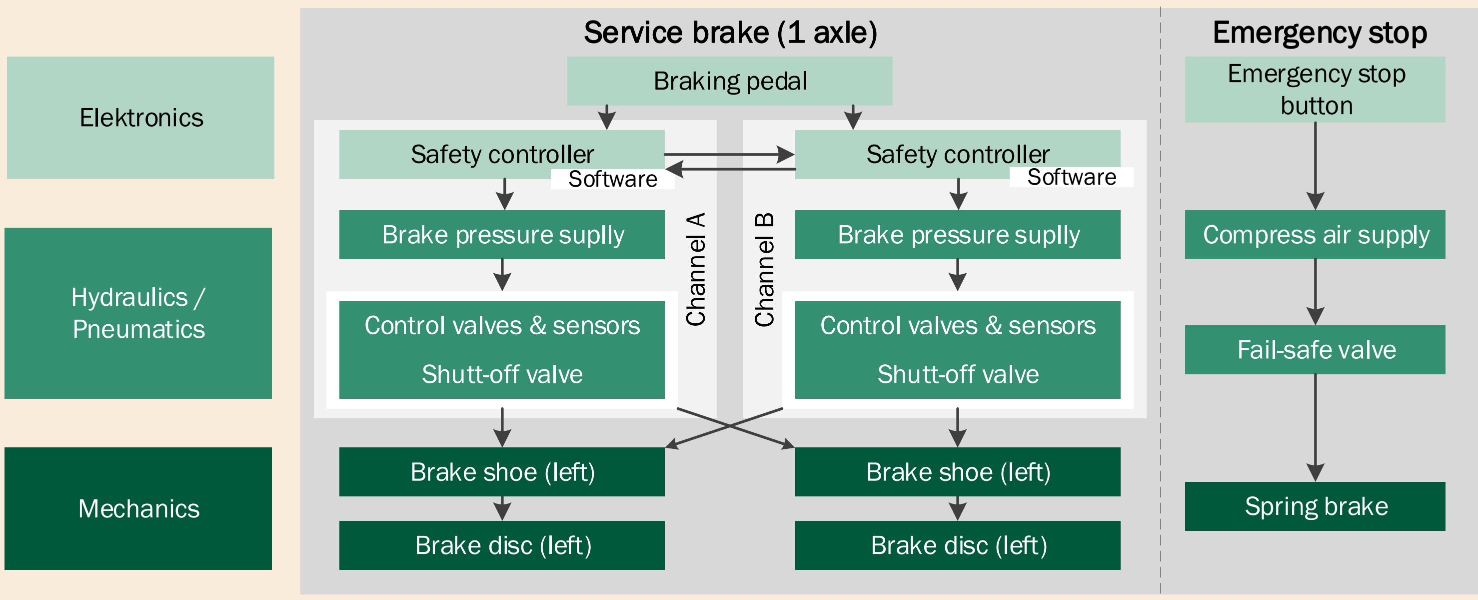




- Depth of analysis (granularity) can be selected individually depending on the system
- Two parallel subsystems: Service brake and emergency brake, can be activated completely independently of each other
- Redundant safety control controlled by the same software → Error = Common Cause
- Brake control via two redundant channels
- Compressed air supply not safety-relevant, as protected by fail-safety valve

System Structure
Identify components, structure the system and determine the critical failure combinations
(Minimal Cut Sets = MS)

- System structure
- Components
- Context/Combinations



Evaluation of components

- MTBF
- Meant time to repair
- Cost to repair

Components	MTBF [a]	Mean time to repair [h] min.	exp.	max.	Cost to repair [$] min.	erw.	max.
Shutt-off valve	150	1	2	4	1000	2000	4000
Brake pressure supply	150	10	16	24	10000	16000	24000
Brake pedal	150	1	2	3	1000	2000	3000
Brake shoe	150	0,5	1	2	500	1000	2000
Brake disc	150	0,5	1	2	500	1000	2000

Common Cause	MTBF [a]
Software failure	10

- List of components in a hazard log
- Probabilistic evaluation of the components (failure frequency, mean time to repair and cost to repair) using three-point estimation
- Determination of maintenance intervals and scope of maintenance
- Definition of a meaningful analysis period in order to obtain meaningful results
- Transfer of values to RIAAT
- Simulation

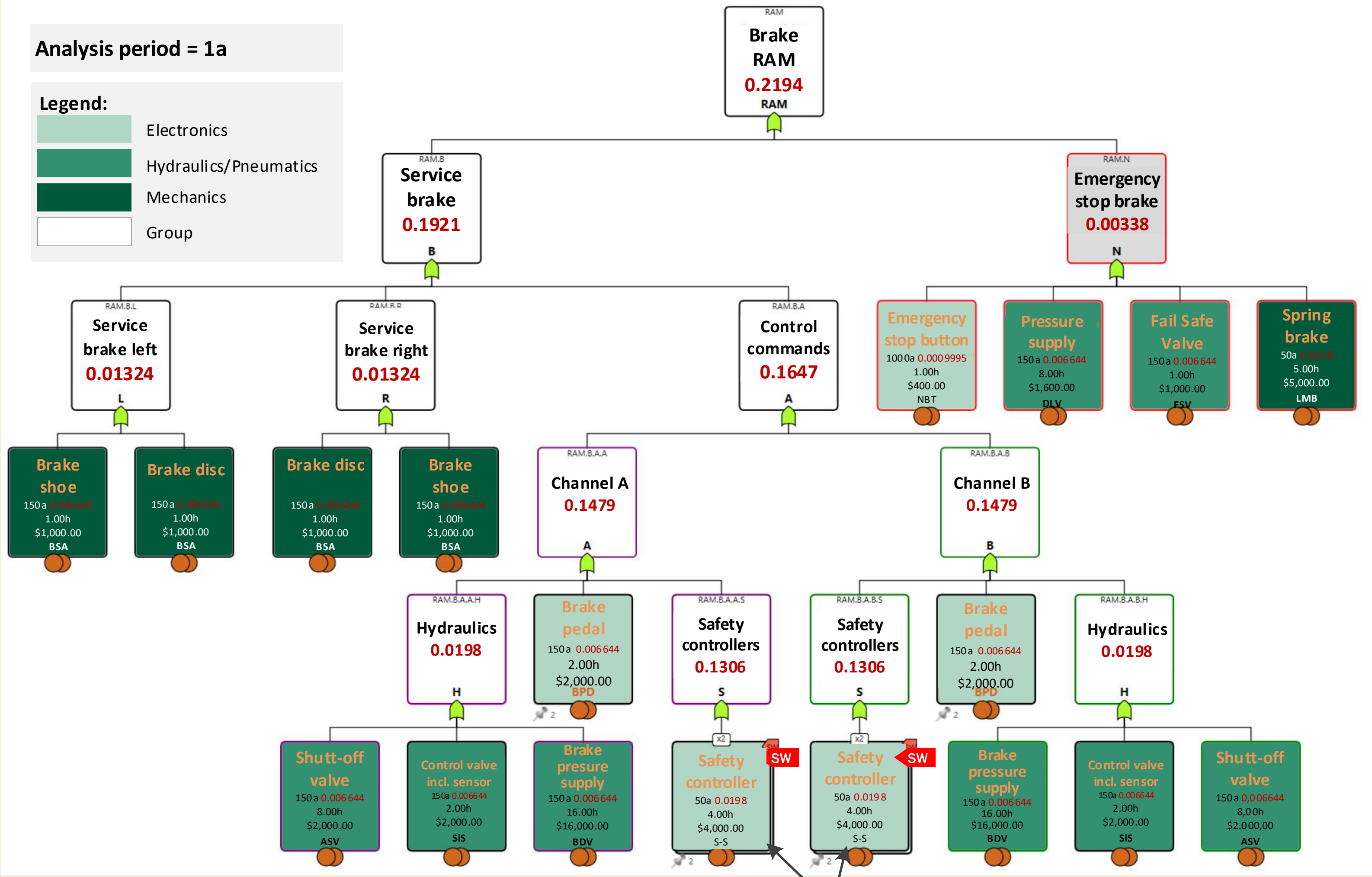
RAM

System Analysis
Identification of Common Cause Factors originating within the system and integration into the Fault Tree

- Numbers from Hazard Log → RIAAT
- Common Cause technology
- Minimal cut sets/Weaknesses
- System optimization

Analysis period = 1a

Legend:
- Electronics
- Hydraulics/Pneumatics
- Mechanics
- Group



Both Safety Controllers can control both channnels

- The RAM system has only OR Gates: If a component fails, it must be replaced immediately. Therefore, every component failure leads to a failure of the overall system.
- Both channels A & B control both braking shoes on the left as well as on the right-hand side.

RiskConsult GmbH
www.riskcon.at

Probabilistic Safety Value Analysis

RIAAT R.A.M.S
www.riaatsoftware.com

Example: Fault tree analysis - braking system as part of a TBM supply train

Results

Evaluation & Assessment

System Optimization

Analysis period

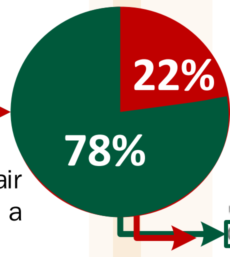
Maintenance intervall

Scope of maintenance

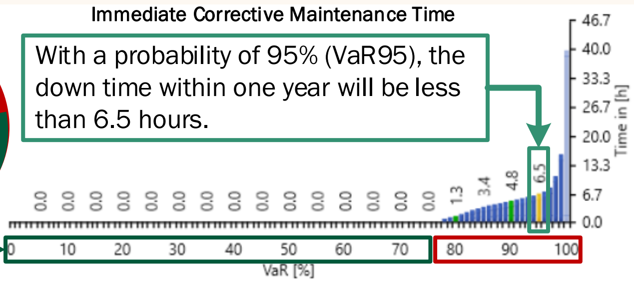
R Reliability

Analysis Period (AP)	1	a
Failure Probability	0.2194	
Reliability	0.7806	

Braking system for one axle will cause repair time and repair costs at least once during the analysis period (1a) with a probability of 22% due to an error.

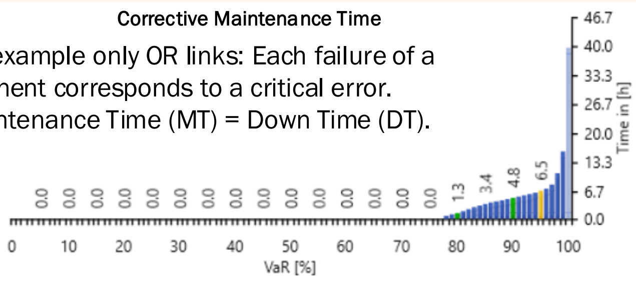


A Availability

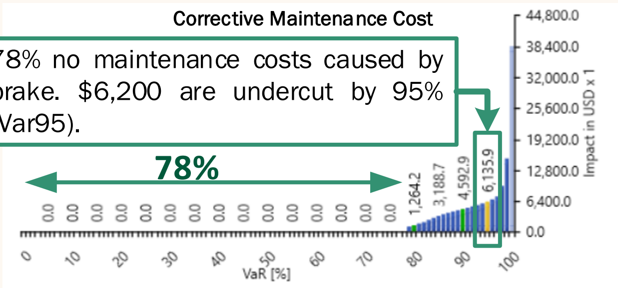


M Maintainability

In the example only OR links: Each failure of a component corresponds to a critical error.
→ Maintenance Time (MT) = Down Time (DT).



78% no maintenance costs caused by brake. $6,200 are undercut by 95% (Var95).



Safety

System Analysis
Identification of Common Cause Factors originating within the system and integration into the Fault Tree

Numbers from Hazard Log → RIAAT

Common Cause technology

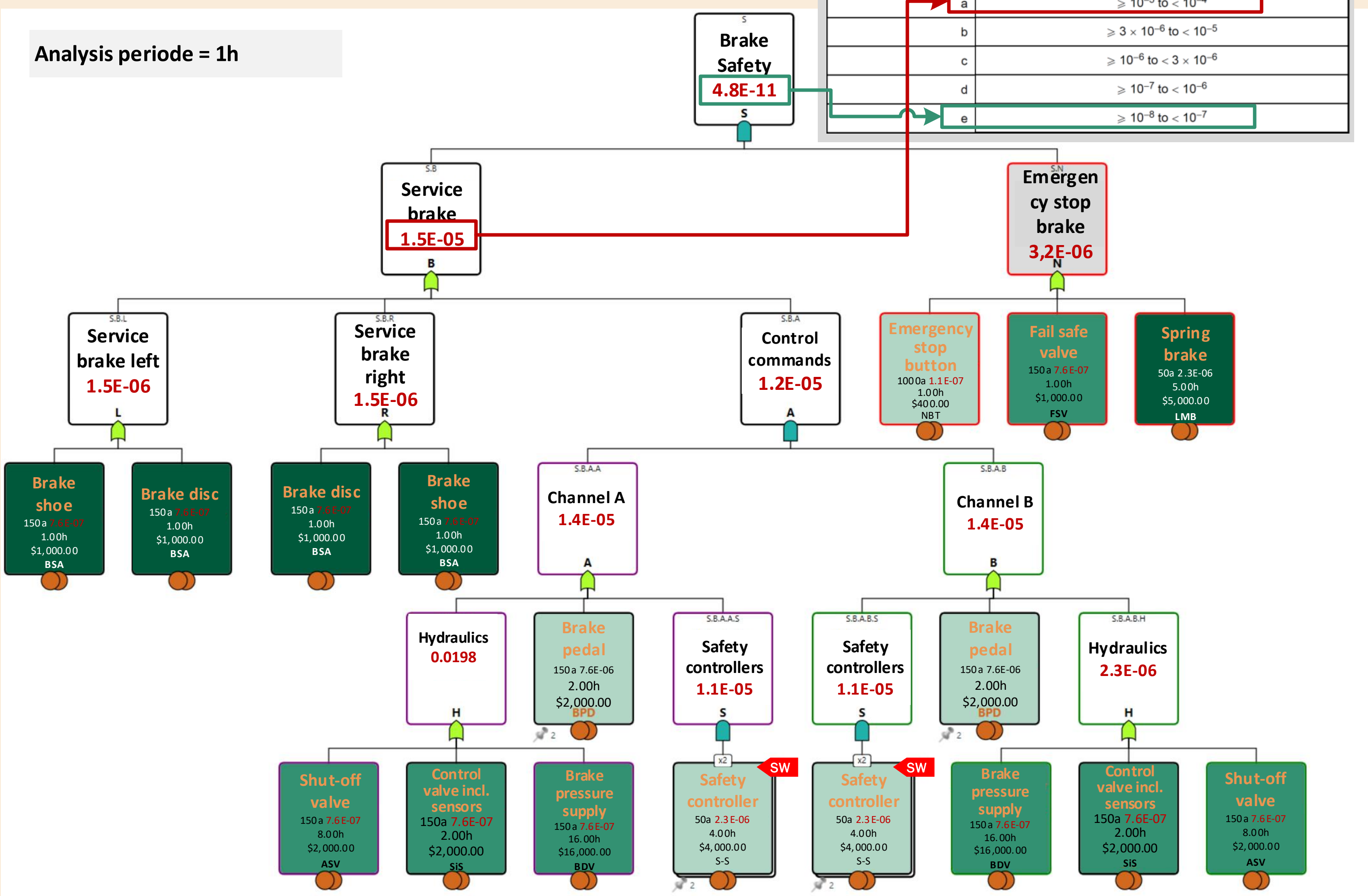
Minimal cut sets/Weaknesses

System optimization

Performance Level (DIN EN ISO 13849)

PL	Average probability of dangerous failure per hour 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

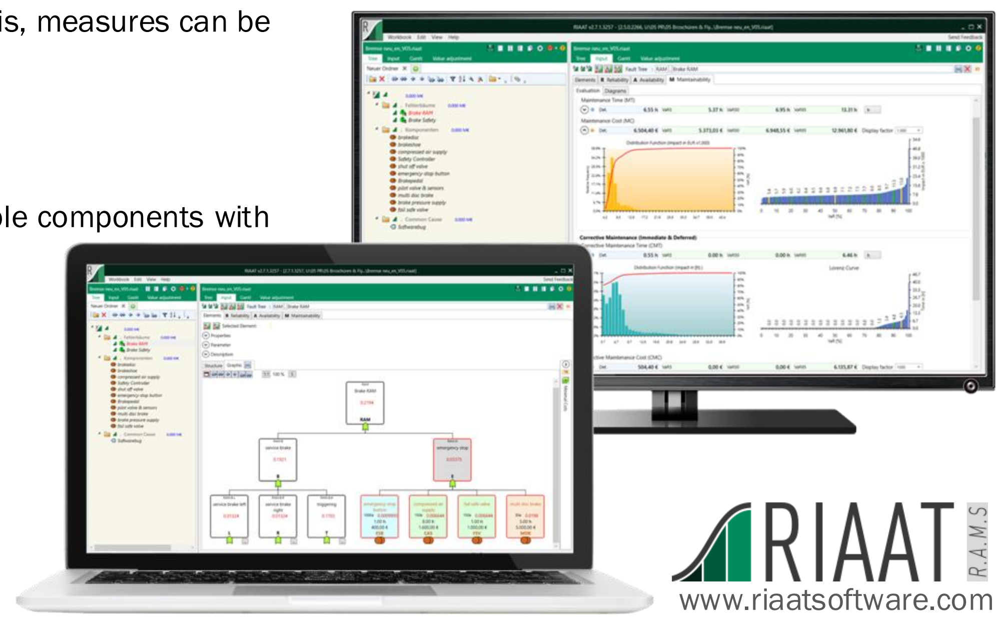
Analysis periode = 1h



Setting measures for optimization

Based on the results of the RAMS analysis, measures can be taken to optimize the system:

- Optimization of the system structure.
- Creation of additional redundancies.
- Replacement of particularly susceptible components with more robust components.
- Installation of monitoring systems
  → Detect faults at an early stage
- Adjustment of maintenance intervals and scope
- Avoidance of Common Cause failures



RIAAT R.A.M.S
www.riaatsoftware.com