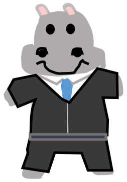
Relationship between safety and management approaches

—Two types of failure and countermeasures—

Mori Takashi

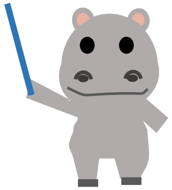
National Traffic, Safety and Environment Laboratory,
National Agency for Automobile and Land Transport Technology, Japan

Actors

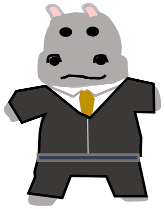


CEO of Hippo Corp.
Motto: Technology and inspiration

Manager of
Electric Dept., Hippo Railway
Motto: Bring inexpensive and better one!



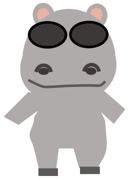
anonymous Hippo
Unknown Consultant
Motto: Knowledge is power!



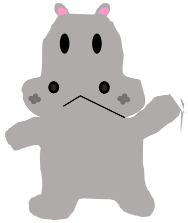
Prof. Ohkaba
Motto: Software must be in good order.

Kabao
Sales, Hippo Corp.
Comment: Absorbing someone's anger makes my wage.

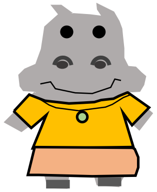
Otakaba
Engineer, Hippo Corp.
Motto: No fun, No engineering!



hacking Hippo
Software developer, Hippo Corp.
Motto: I make the way which no one else can realize.



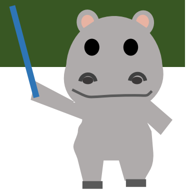
Employee of an affiliate company of Hippo Corp.
Comment: Affiliates always must say "YES, Sir!"



Kabami
Executive Engineer, Hippo Corp.
Motto: Let's work together.

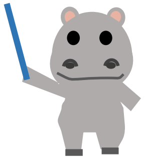
What I want to explain

As this is the last seminar, I will explain the often misunderstood relationship between safety and management approaches.



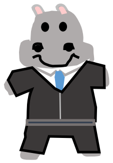
IEC 62278 4.7.1

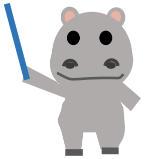
5-1 Safety measures



What measures do you consider to prevent the system from transitioning to an unsafe state?

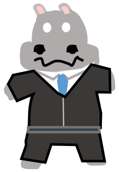
OK. The answer is: the 'fail-safe concept'. If our safety-related system detects a fault, we stop it immediately to maintain the safe side.





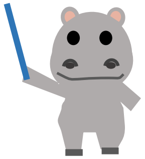
Great! Are there any other measures?

If you detect a fault and stop immediately, I'll consider it a guarantee of safety. That's the idea behind our SIL 4 system.

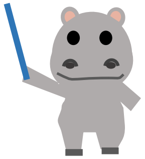


IEC 62278 4.7.1

5-1 Safety measures

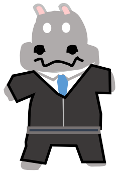


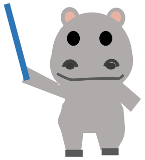
There are two misuses of language. First, the fail-safe approach of Hippo Corp. cannot solve all events; second, the term SIL is used in a different way.



If your product has many bugs, does it work properly? If it were a safety-related feature, would it be safe?

Our technical team is very good. We don't have that problem.

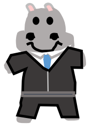




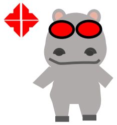
Competence of the technical team! That is not a measure.

5-1 A conversation that railway operators often have

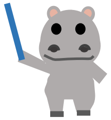
Anyway, it's SIL 4. We're in charge of people's lives. Make the interlocking system with SIL 4.



That's what I'm talking about. We'll cherish that idea in our company, too!

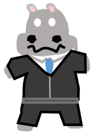


Come on, boss! How much do you think it would cost to build everything with SIL 4 management and technology? Do you want to build even the automatic pathway system with SIL 4? It has nothing to do with safety!



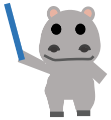
The standard requires that risks are analysed and resources are allocated to the necessary safety in a proportionate manner.

The tolerance is 10^{-9}/h. We have people's lives in our hands. I want proof of everything!



How many software bugs occur? I'm in trouble...

Then you don't have to quantify the software, do the hardware.

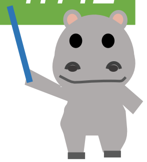


But software also needs some kind of standard, doesn't it?

IEC 62278 4.7.1

5-2 Two types of failure

> *Safety integrity can be viewed as a combination of quantifiable elements (generally associated with hardware, i.e. random failures) and non-quantifiable elements (generally associated with systematic failures in software, specification, documents, processes, etc.).*
>
> *- IEC 62278 4.7.1*



Random failures

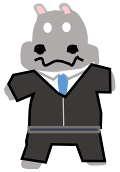
- Operating modes
- Environment
- Stress degradation
- Wear out
- Over stress
- Etc.

Systematic failures in software, specification, documents, processes, etc.

- Errors in requirements
- Design and realisation inadequacies
- Manufacturing deficiencies
- Inherent weaknesses
- Software errors
- Operating instruction deficiencies
- Instruction inadequacies
- Human errors
- Etc.

Extract from Figure 5 – Factors Influencing Railway RAMS of IEC 62278

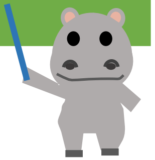
I have something that comes to mind about that.



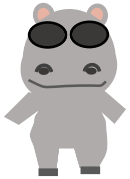
IEC 62278 4.7.1

5-2 Two types of failure

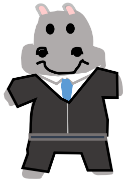
Please answer whether the following examples are random failures, systematic failures or both.



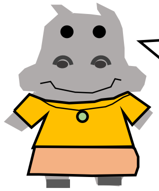
The logic board broke due to unexpectedly high temperatures.



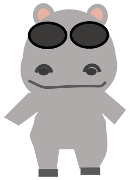
The logic board broke at a normal temperature.



Kabao didn't understand the system conditions so it didn't meet the right specification for Hippo Railway.



The test case did not fulfil all the functions and the product was passed on to the customer.

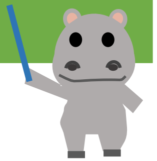


The error rate for systems A and B got so high that the system failed.

IEC 62278 4.7.1

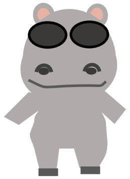
5-2 Two types of failure

Please answer whether the following examples are random failures, systematic failures or both.



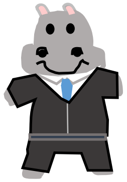
The logic board broke due to unexpectedly high temperatures.

Because they don't have a firm grasp of Hippo Railway's situation, or don't use it at such temperatures. A fault that was bound to happen. It is not the fault of the component. This seems to be a systematic failure.



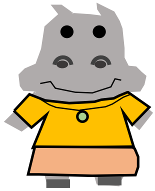
I had the temperature designed properly, but the logic board broke at a normal temperature.

This is likely to be a random failure, as the failure comes from the fact that components have a certain probability of breaking.



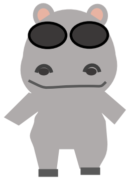
Kabao didn't understand the system conditions so it didn't meet the right specification for Hippo Railway.

It may be that this is because they do not have a firm grasp of Hippo Railway's situation, but the problem seems to lie with the CEO, who entrusted everything to a sales person who could not make a technical decision in the first place. This seems to be a systematic failure.



The test case did not fulfil all the functions and the product was passed on to the customer.

'Omission of test content', meaning that component failure is irrelevant. This seems to be a systematic failure.

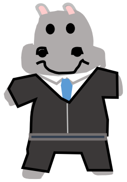


The error rate for systems A and B got so high that the system failed.

It is hard to say. It could be a design error, or it could be a broken component that caused the error. A little more additional investigation into the cause is needed.

IEC 62278 4.7.1

5-2 Two types of failure



We've decided that the frequency of derailments due to signal misrepresentation shall be no more than 10^{-9}/h.

Assignments from CEO orders

Function A: TFFR 10^{-9}/h

Systematic failures

Frequency of design failures to deliver functionality: unknown

Error frequency of software realising function A: unknown

Error frequency of inspections of function A: unknown

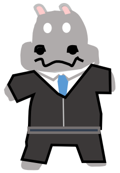
etc.

Random failures

Failure frequency of boards realising function A: 10^{-9}/h

Random failures can set numerical targets.

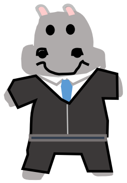
If you've decided on a document error rate, it must be meaningless.



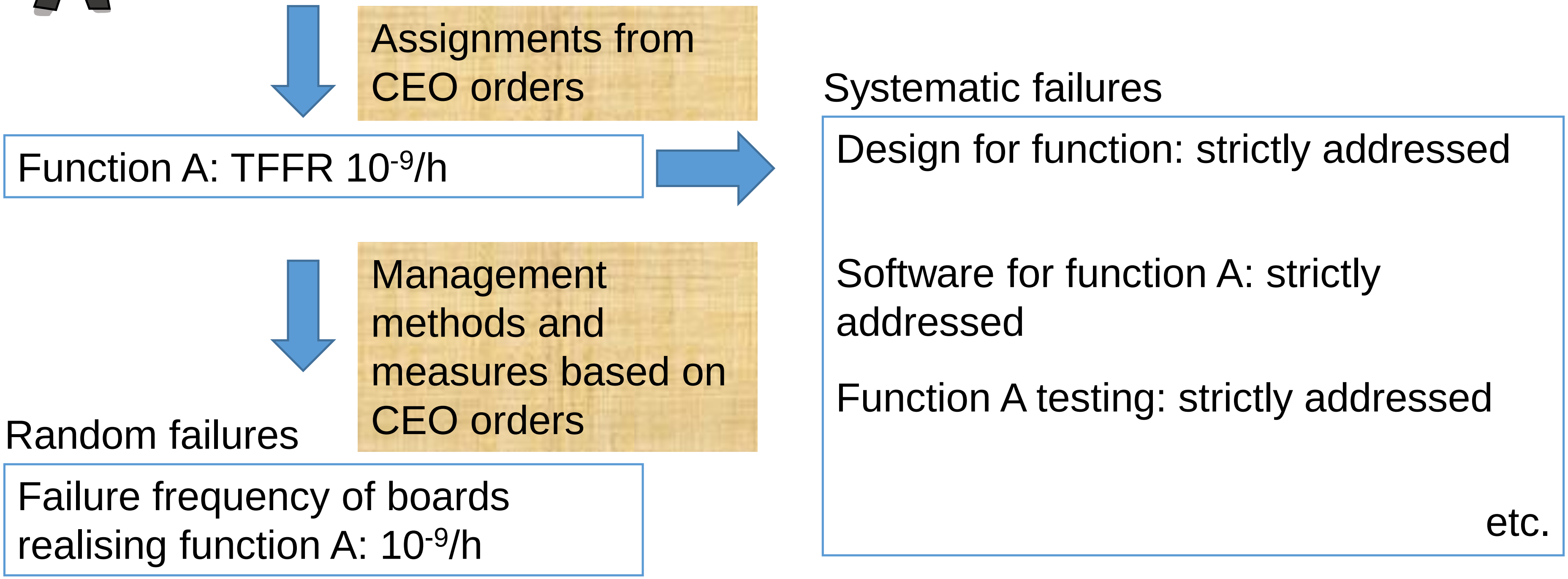
TFFR: Tolerable Functional Failure Rate

IEC 62278 4.7.1

5-2 Two types of failure



We've decided that the frequency of derailments due to signal misrepresentation shall be no more than 10^{-9}/h.



Assignments from CEO orders

Function A: TFFR 10^{-9}/h

Management methods and measures based on CEO orders

Random failures

Failure frequency of boards realising function A: 10^{-9}/h

Systematic failures

Design for function: strictly addressed

Software for function A: strictly addressed

Function A testing: strictly addressed

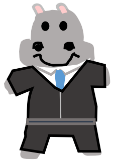
etc.

TFFR: Tolerable Functional Failure Rate

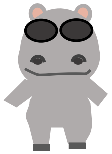
EN 50126-2 10.2.12

5-3 Incorrect use of SILs

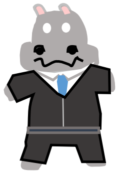
Hippo Railway asked us if we could prepare a SIL 4-compliant processing system. All you can do is say "Yes, we can!".

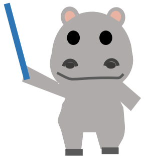


You said that? Are you saying that?
Are you going to run in the US presidential election?



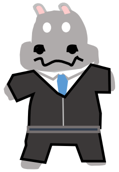
Our super awesome processing system, Hippo-X, is the best in the world! No one will ever catch up to us! Hey, hacking Hippo! You don't trust our product?



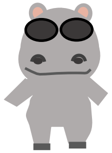


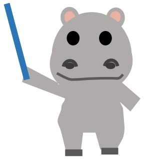
Think about it. If someone puts an application program on the Hippo-X that exceeds its expected processing capacity, will it work properly?

Anyone who puts in that stupid software will be asked to leave.
Our Hippo-X only accepts well-designed software.



Hey boss, if you give me more money, the quality of the software will go sky-high.



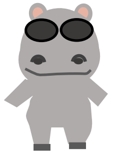


It is said that SILs should not be used as an attribute of the system.

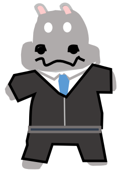
EN 50126-2 10.2.12

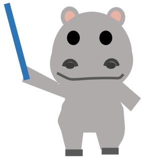
5-3 SILs assigned to functions

SILs are supposed to be assigned to functions.
It's not assigned to systems or subsystems.

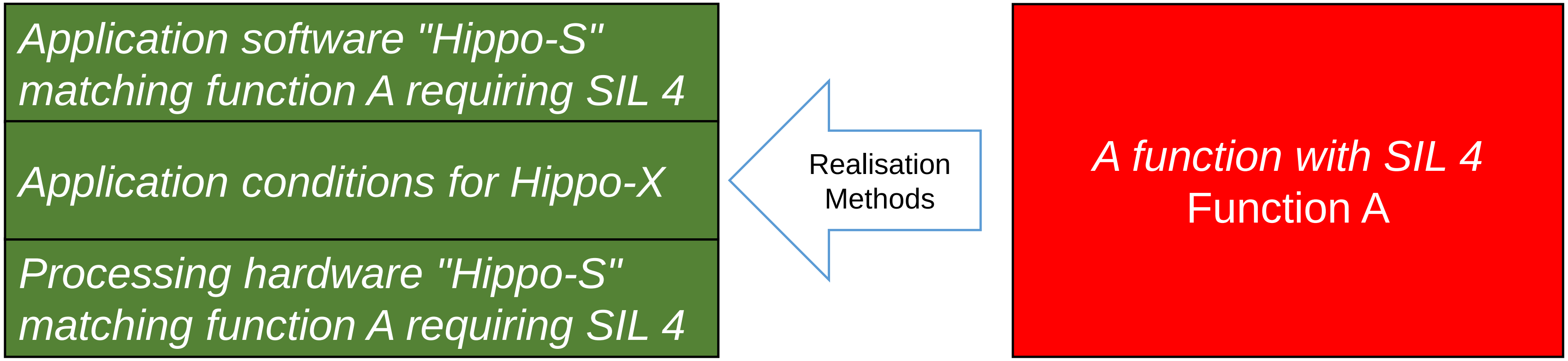


That's not good. Our ad says: **"Our SIL 4-compliant system protects your safe operation! Hippos are always by your side."**





Isn't it a bit scary that these hippos stay with humans all the time?



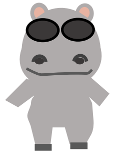
Application software "Hippo-S" matching function A requiring SIL 4

Application conditions for Hippo-X

Processing hardware "Hippo-S" matching function A requiring SIL 4

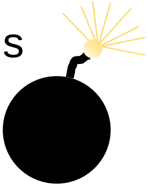
Realisation Methods

A function with SIL 4
Function A

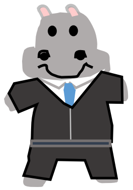


We offer these line-ups to protect "Function A" which requires SIL 4.

If this function fails, serious consequences occur.

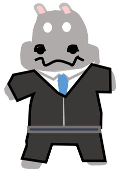


5-3 Safety functions and SIL assignments

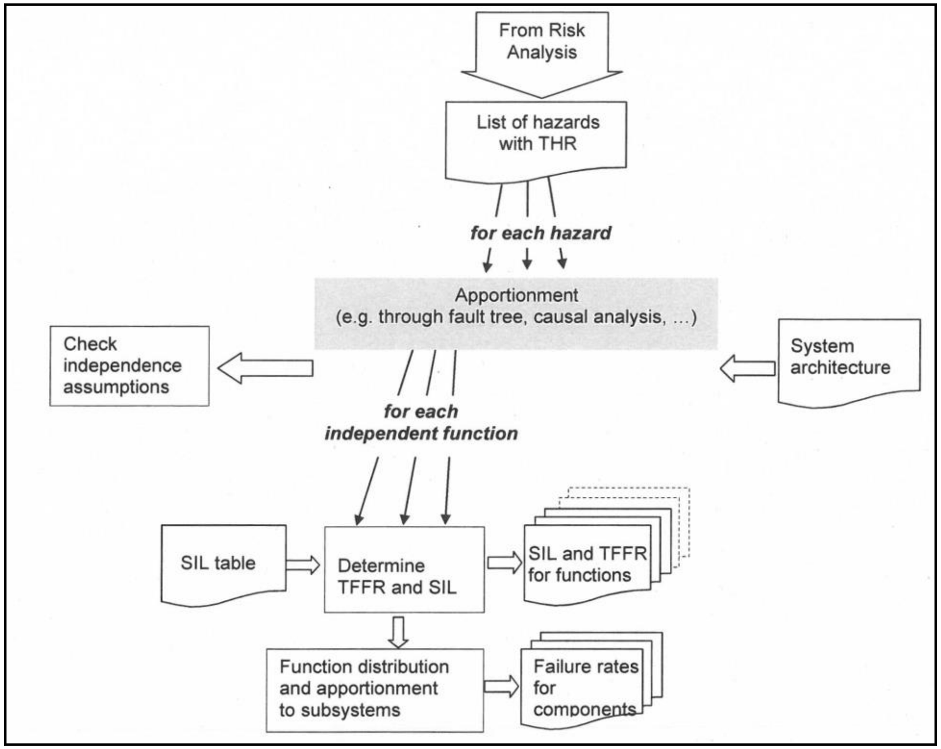


We always say, "This function requires SIL 4", but how is it determined?

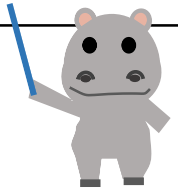
Maybe, but it's customer feedback or sales strategy.



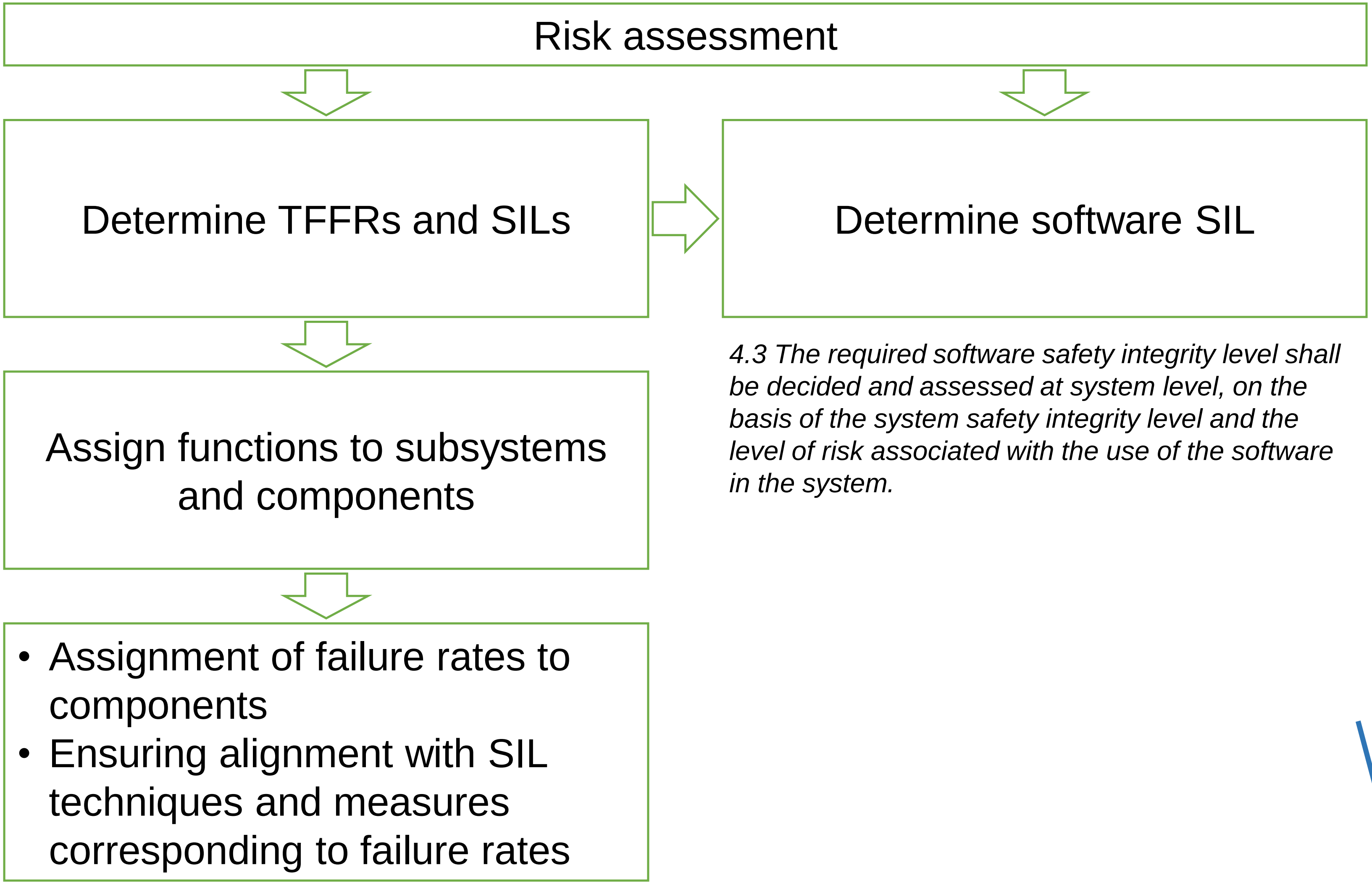
That's not the essence of it.


From Risk Analysis
List of hazards with THR
for each hazard
Apportionment (e.g. through fault tree, causal analysis, ...)
Check independence assumptions
System architecture
for each independent function
SIL table
Determine TFFR and SIL
SIL and TFFR for functions
Function distribution and apportionment to subsystems
Failure rates for components

EN 50126-2 10.2.2. Apportioning safety requirements provides instructions on how to do this.



5-3 SIL functions and responses in components <1>



Risk assessment

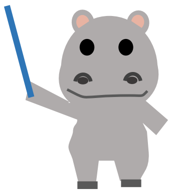
Determine TFFRs and SILs

Determine software SIL

Assign functions to subsystems and components

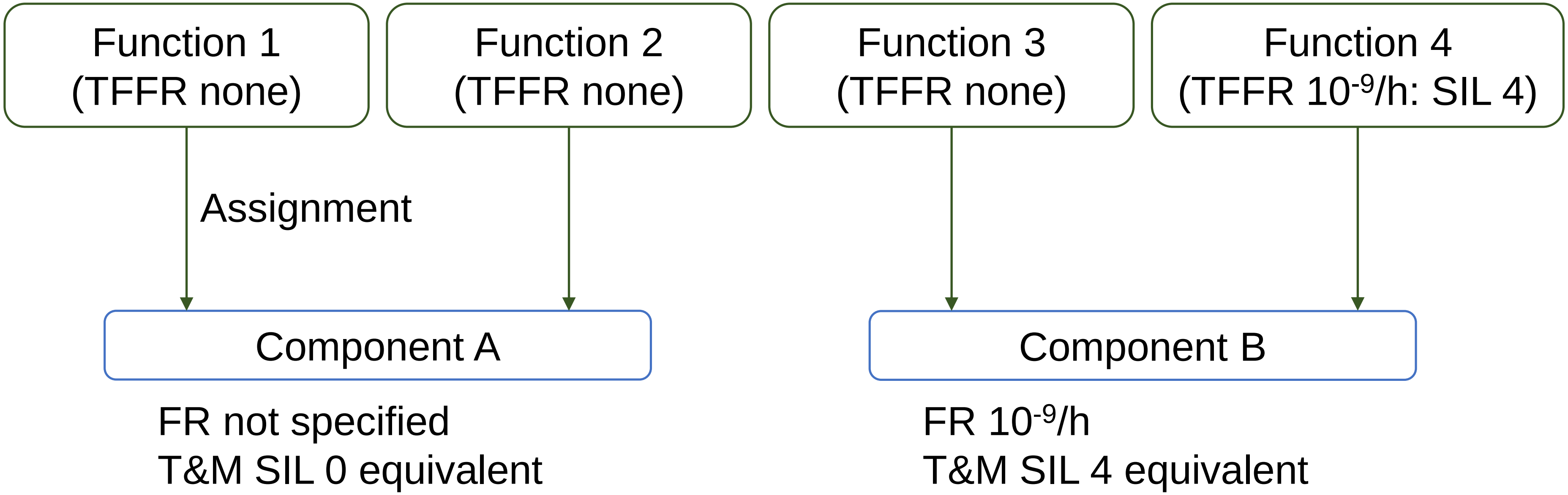
- Assignment of failure rates to components
- Ensuring alignment with SIL techniques and measures corresponding to failure rates

4.3 The required software safety integrity level shall be decided and assessed at system level, on the basis of the system safety integrity level and the level of risk associated with the use of the software in the system.



5-3 SIL functions and responses in components <2>

Assign functions to subsystems and components



Function 1 (TFFR none)

Function 2 (TFFR none)

Function 3 (TFFR none)

Function 4 (TFFR 10^{-9}/h: SIL 4)

Assignment

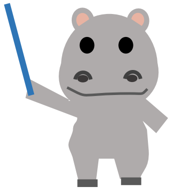
Component A

FR not specified
T&M SIL 0 equivalent

Component B

FR 10^{-9}/h
T&M SIL 4 equivalent

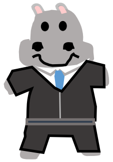
7.3.4.9 Where the software consists of components of different software safety integrity levels then all of the software components shall be treated as belonging to the highest of these levels unless there is evidence of independence between the higher software safety integrity level components and the lower software safety integrity level components.



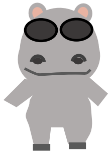
5-3 Summary: It's not that difficult

Safety first! Customer fatalities must be eliminated wherever conceivable.
This is the philosophy of everyone at Hippo Railway.

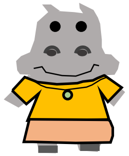
That's right. We value that philosophy too!



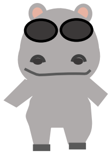
A system that kills passengers if a function goes wrong must be designed so that it can't happen more than once every 100,000 to one million years, which means about 10^{-8} to 10^{-9}/h.



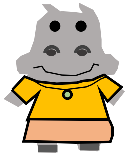
Identify and report on the functions of the system that would be seriously compromised by its loss of functionality, both in terms of safety and availability!



Analysis shows that the locking logic, the signal-present logic and the interface functions of each system could be derailed if a mistake is made. Availability is affected by almost everything except the recording system.

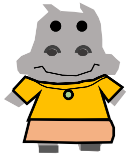


Analyse how tolerant each function is so that the system as a whole has a hazardous case of less than 5×10^{-9}/h.

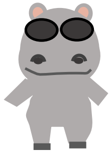


5-3 Summary: It's not that difficult

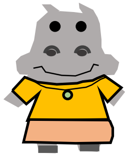
Analyse how tolerant each function is so that the system as a whole has a hazardous case of less than 5×10^{-9}/h.



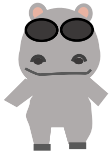
Kabami, you're a real hustler! For safety-related functions, the number of hazardous events per hour should be 1×10^{-9}/hour. We'll have to design the hardware to match this.



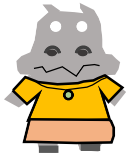
Next I'd ask you to choose your management approaches and techniques and measures so that there are no careless mistakes, no bugs, no errors in the specifications. That would suit a system with very few hazard occurrences.



Kabao should not be left unchecked. We have to check him properly.
But the most dangerous is the boss who casually promises everything to his customers. What do you do, Kabami?



Um...



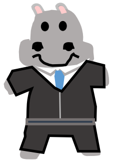
5-3 Summary: It's not that difficult

Concept

Safety first! Customer fatalities must be eliminated wherever conceivable. This is the philosophy of everyone at Hippo Railway.

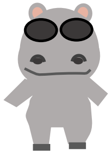
Sales talk (risky but necessary?)

That's right. We value that philosophy too!



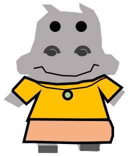
A system that kills passengers if a function goes wrong must be designed so that it can't happen more than once every 100,000 to one million years, which means about 10^{-8} to 10^{-9}/h.

System risk tolerance level (THR)

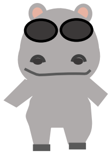


Identify and report on the functions of the system that would be seriously compromised by its loss of functionality, both in terms of safety and availability!

Risk analysis

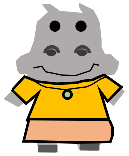


Analysis shows that the locking logic, the signal-present logic and the interface functions of each system could be derailed if a mistake is made. Availability is affected by almost everything except the recording system.



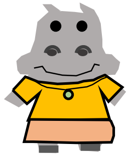
Analyse how tolerant each function is so that the system as a whole has a hazardous case of less than 5 × 10^{-9}/h.

Assigning risk to functions



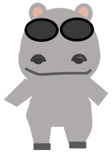
5-3 Summary: It's not that difficult

Analyse how tolerant each function is so that the system as a whole has a hazardous case of less than 5 × 10^{-9}/h.



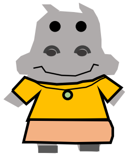
Kabami, you're a real hustler! For safety-related functions, the number of hazardous events per hour should be 1 × 10^{-9}/hour. We'll have to design the hardware to match this.

Tolerable degree of risk to function (TFFR)



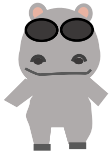
Next I'd ask you to choose your management approaches and techniques and measures so that there are no careless mistakes, no bugs, no errors in the specifications. That would suit a system with very few hazard occurrences.

Safety and management and technology assignment (SIL)

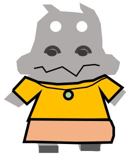


Kabao should not be left unchecked. We have to check him properly.
But the most dangerous is the boss who casually promises everything to his customers. What do you do, Kabami?

Assignment of competencies and roles



Um...



At the end

Thank you for your support over the past year.
See you again somewhere else!