

Searching for and identifying hazards

—Risk analysis and assessment— (RAMS Phase 3)

Mori Takashi

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

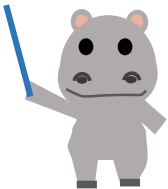
Actors



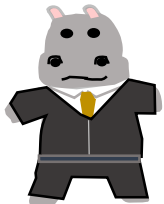
President of Hippo Corp.
Motto: Technology and
inspiration



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.

Previous summary

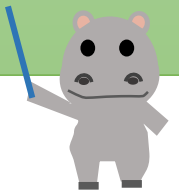
The phase 2 of RAMS is to:

- set numerical targets for the system and conduct preliminary hazard analysis of the system's requirements to provide prospects for the realization of the system;
- make plans for safety and RAM, and make them clear.

The next phase 3

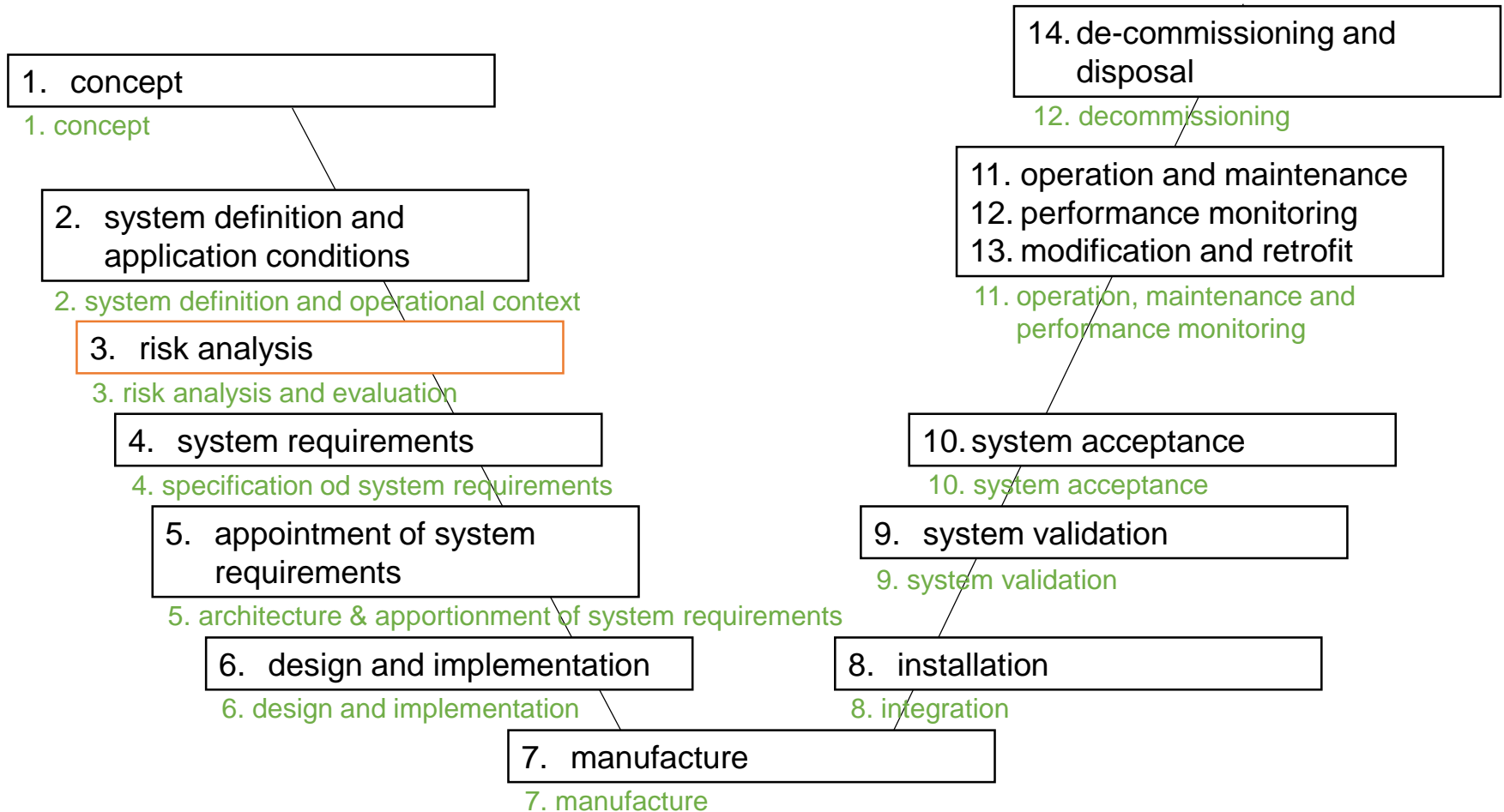
Phase 3: Risk analysis
(IEC 62278)

Phase 3: Risk analysis and evaluation
(EN 50126-1)



System life cycle

IEC 62278 5.2
EN 50126-1 6.2



What is required at this phase

- 3-1 Identify hazards, or factors that have a negative impact on RAM (hereinafter referred to as unwanted factors)
- 3-2 Understand the degree or likelihood of unwanted factors
- 3-3 Determine what to do with unwanted factors
- 3-4 Record unwanted factors



3-1 Identify unwanted factors

3-1 Identify hazards, or factors that have a negative impact on RAM (hereinafter referred to as unwanted factors)

3-2 Understand the degree or likelihood of unwanted factors

3-3 Determine what to do with unwanted factors

3-4 Record unwanted factors



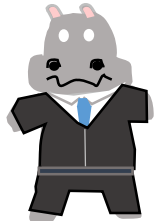
3-1 Identify unwanted factors



You guys, are there any unwanted factors in Hippo Corp.?

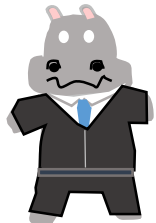


Our corporation may go bankrupt. I may not be paid. I may not be paid for overtime. Our colleagues may quit. I may not be able to take a day off. Our corporation may not buy the books and information we need. The development tools are old. Our systems may be hacked.... There are many unwanted factors.

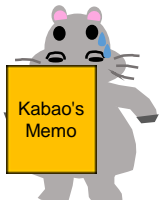


I thought we were like a family....

Our corporation doesn't give me a Hippo brand ice lolly as a treat. I also want a cake.



Well, I'm going to become a transparent hippo because of the difficulties ahead. Our corporation would also disappear. However, I wonder if we can wash it all out with this. Right now, I'm only listening to Otakaba's opinion. What Kabao says has nothing to do with work. If nothing is done, we will be a corporation with terrible working conditions, which is no longer acceptable in our time.



3-1 Identify unwanted factors

IEC 62278 6.3.3.1

EN 50126-1 7.4.2.1-1

IEC 62425 A.4.1.1

EN 50129 A.4.2.3

Empirical approach, and creative or deductive approach



Kabao has written down all the hazards so far, so what we do is to review the materials so far and identify the related ones.

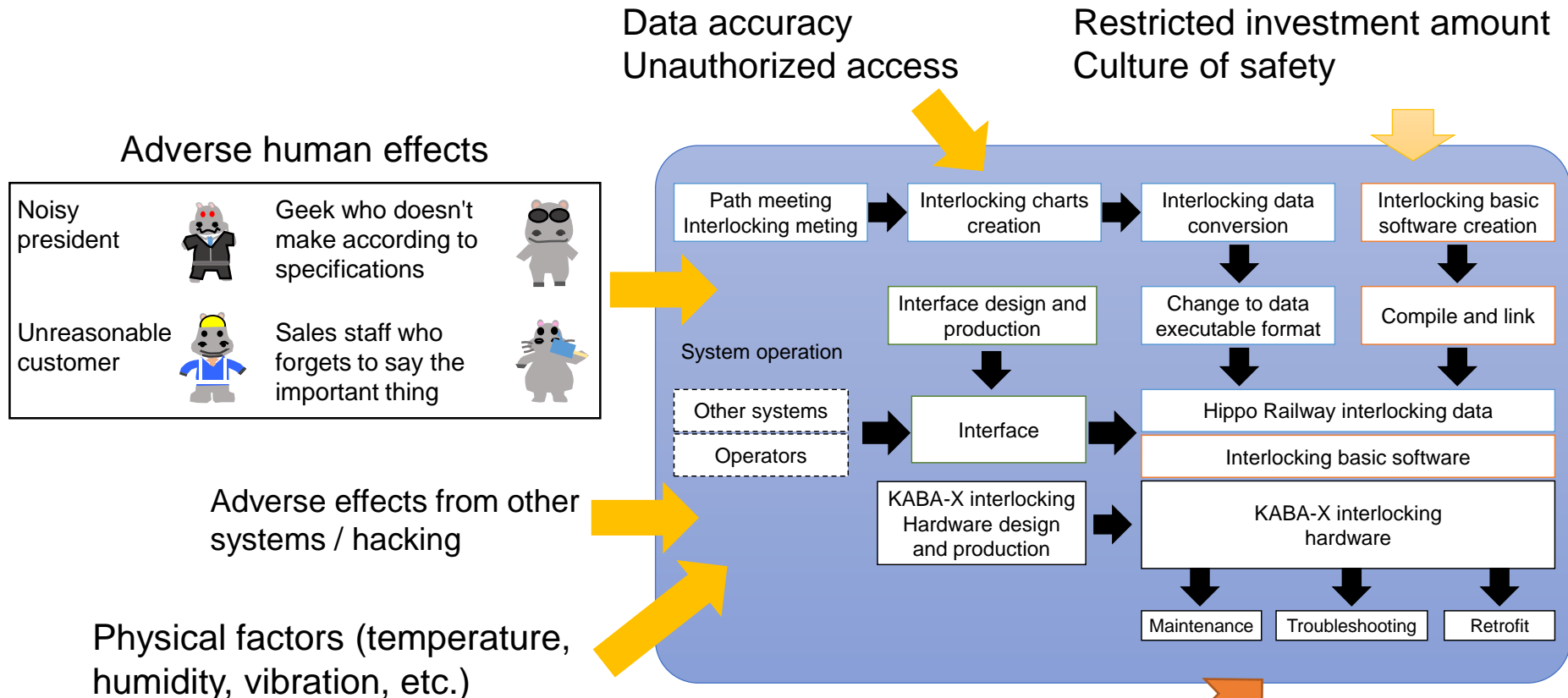
Please leave that area to me. I have written down everything.

It's pretty well managed, but it doesn't include anything that isn't a hazard so far. For that, we need to identify new hazards. Brain-storming, structured what-if studies, Hazard and Operability Studies (HAZOP), Failure Mode and Effects Analysis (FMEA) are examples. These are called creative or deductive approach.

I didn't know that brainstorming, which connects ideas together, is effective.



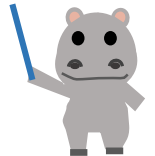
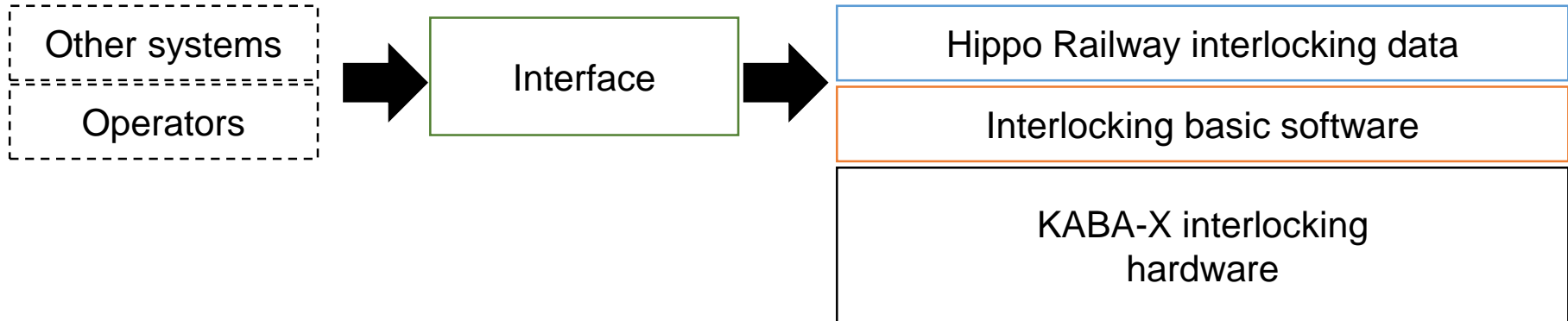
3-1 Difference from the phase 2



In the phase 2, the analysis was based on the premise that the contents are not very clear, but the external factors are known. From now on, we will continue to work on the internal factors.

3-1 Focus on failures to identify undesired events

IEC 62278 6.3.3.1
EN 50126-1 7.4.2.1-1
IEC 62425 A.4.1.1
EN 50129 A.4.2.3



FMEA, which can be said to be a classic hazard analysis, is a technique using the question "What happens if ... ?".

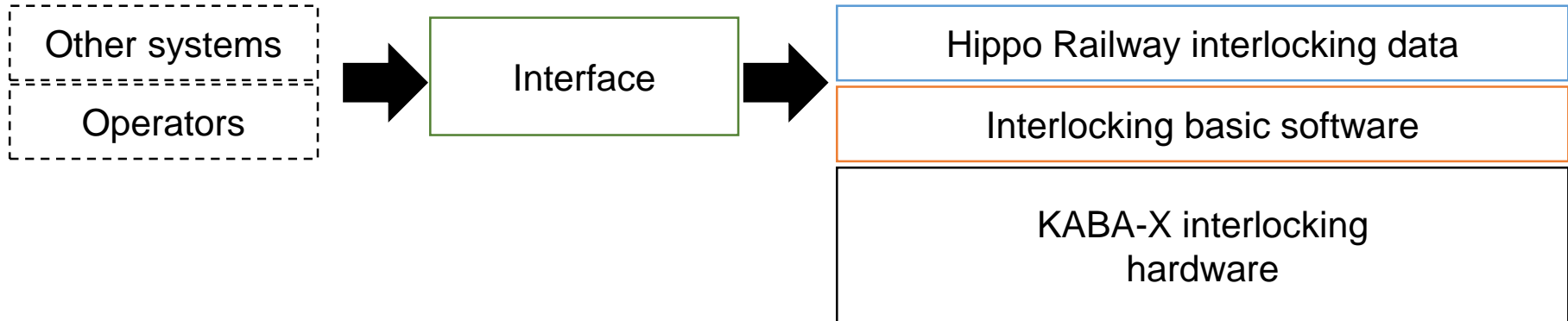
It's impossible for our systems to go wrong. Our employees are designing and manufacturing with all their soul! Our systems are immortal.



I'm glad to hear that, our president! But things with shapes will collapse, and if they don't collapse, no one will update them. Even if it collapses, it is useless if customers are killed.

3-1 Focus on failures to identify undesired events

IEC 62278 6.3.3.1
EN 50126-1 7.4.2.1-1
IEC 62425 A.4.1.1
EN 50129 A.4.2.3



Well, we haven't finished designing the contents yet. You can't tell what kind of failure will happen.

Isn't it the engineer who manages without knowing? I have a secret plan, though.

Our president's eyes are cloudy. That's the eyes when he is not thinking about anything at all.



How about thinking about what kind of event will occur if it is realized at the lowest cost, and taking countermeasures? For example, we Hippo Corp. work together to manually handle all the switchers and signals.



3-1 Extraction of factors focusing on failures

IEC 62278 6.3.3.1 a)
 EN 50126-1 7.4.2.1-1
 IEC 62425 A.4.1.1
 EN 50129 A.4.2.3

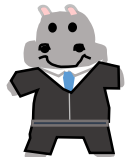
Part	Subsystem-level events	Detailing	Undesired events / severity at higher levels	Frequency	Measures
Interlocking hardware	Stop processing system	System shutdown with signals indicating progress.	Collision / Catastrophic	Conceivable	When the system is stopped, signals are set to stop.
		System shutdown with signals set to stop.	Loss of service / Critical	Conceivable	Maintain a predetermined operating rate.
		System shutdown with no train detection.	Collision / Catastrophic	Conceivable	When the system is stopped, signals are set to stop.
		System shutdown with train detected.	Loss of service / Critical	Conceivable	Maintain a predetermined operating rate.
		The system stops in the middle of switching the switchers, and signals appear in progress.	Derailment / Catastrophic	Conceivable	When the system is stopped, signals are set to stop.
		The system stops when the switchers are locked in the reverse direction, and signals appear in progress.	Collision / Catastrophic	Conceivable	When the system is stopped, signals are set to stop.
		Switchers cannot be unlocked.	Loss of service / Critical	Conceivable	Maintain a predetermined operating rate.

These are the most ridiculous things that could happen.

You can't be too careful.

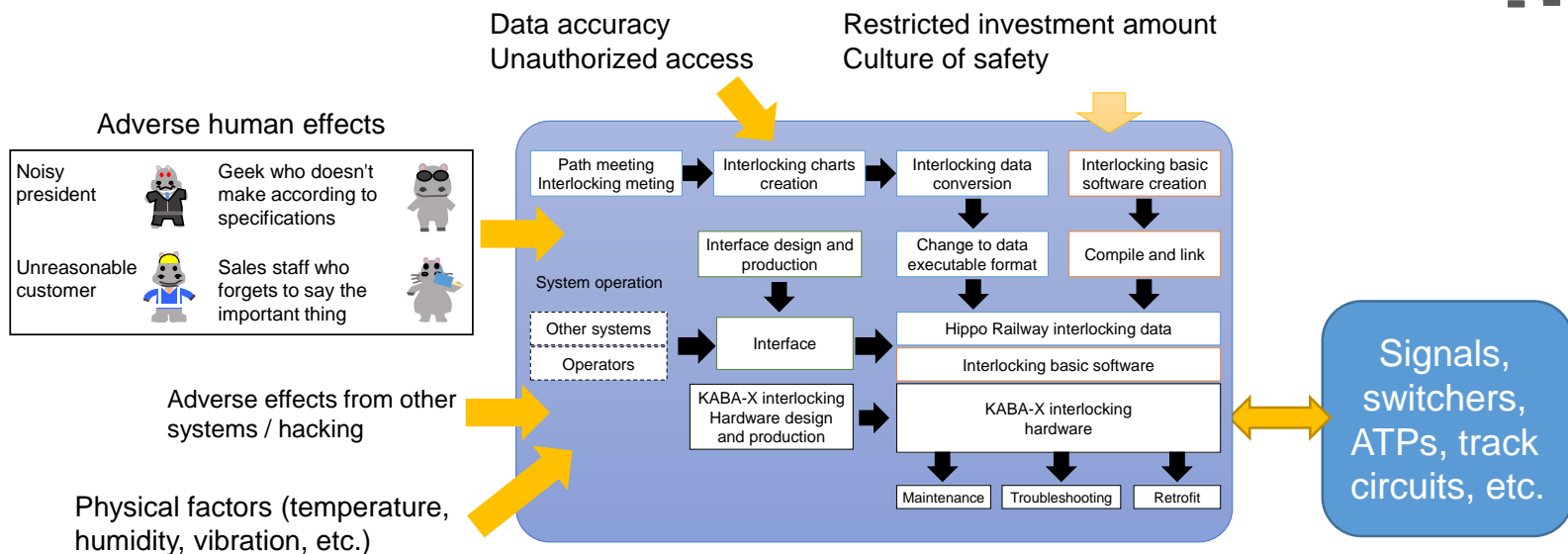
3-1 Identify unwanted factors

IEC 62278 6.3.3.1 b)
EN 50126-1 7.4.2.1-1
IEC 62425 A.4.1.1
EN 50129 A.4.2.3



Isn't there an easier way? FMEA seems to be difficult.

Why don't you try using the HAZOP approach?



The information is flowing, but what if this information does not come, or is wrong, or the order is reversed, or it is too late, or too early? Wouldn't you be able to see something other than collisions, derailments and loss of service?

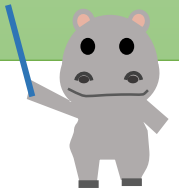


3-1 Summary so far

The identification of undesirable events includes:

- empirical approach, and
- creative or deductive approach.

These are complementary, and it is preferable to employ both approaches.



3-2 Understand the degree or likelihood of unwanted factors

3-1 Identify hazards, or factors that have a negative impact on RAM (hereinafter referred to as unwanted factors)

3-2 Understand the degree or likelihood of unwanted factors

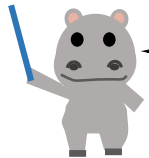
3-3 Determine what to do with unwanted factors

3-4 Record unwanted factors

The degree of a hazard is based upon the frequency of occurrence and severity of consequences. I will explain the frequency of occurrence first.



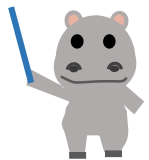
3-2 What is hazardous events?



How are you doing with your evaluation of Kabao?



We have a three-out rule, just like baseball, and when there are three outs, we change.



Didn't you reflect on that the other day? You said you would take good care of your employees. But we can't afford to **repeat the same mistakes**, can we?



It is necessary to take measures to avoid repeating mistakes.



What about trivial mistakes? For example, spilling ice cream on his desk, or making a few typos in his notes?



I don't even pay attention to such things. And **that has very little to do with the management of the company, even if the frequency is high.**

3-2 What is hazardous events?



What if, Kabao embezzled the corporation's money?



You've got to be kidding me! That's not true, not when it comes to Kabao.

I'll follow you for the rest of my life. Please give me an ice lolly!



But if he embezzle, I'll have to fire him. I'll hire him again when he's purified, because Hippo Corp. is family.

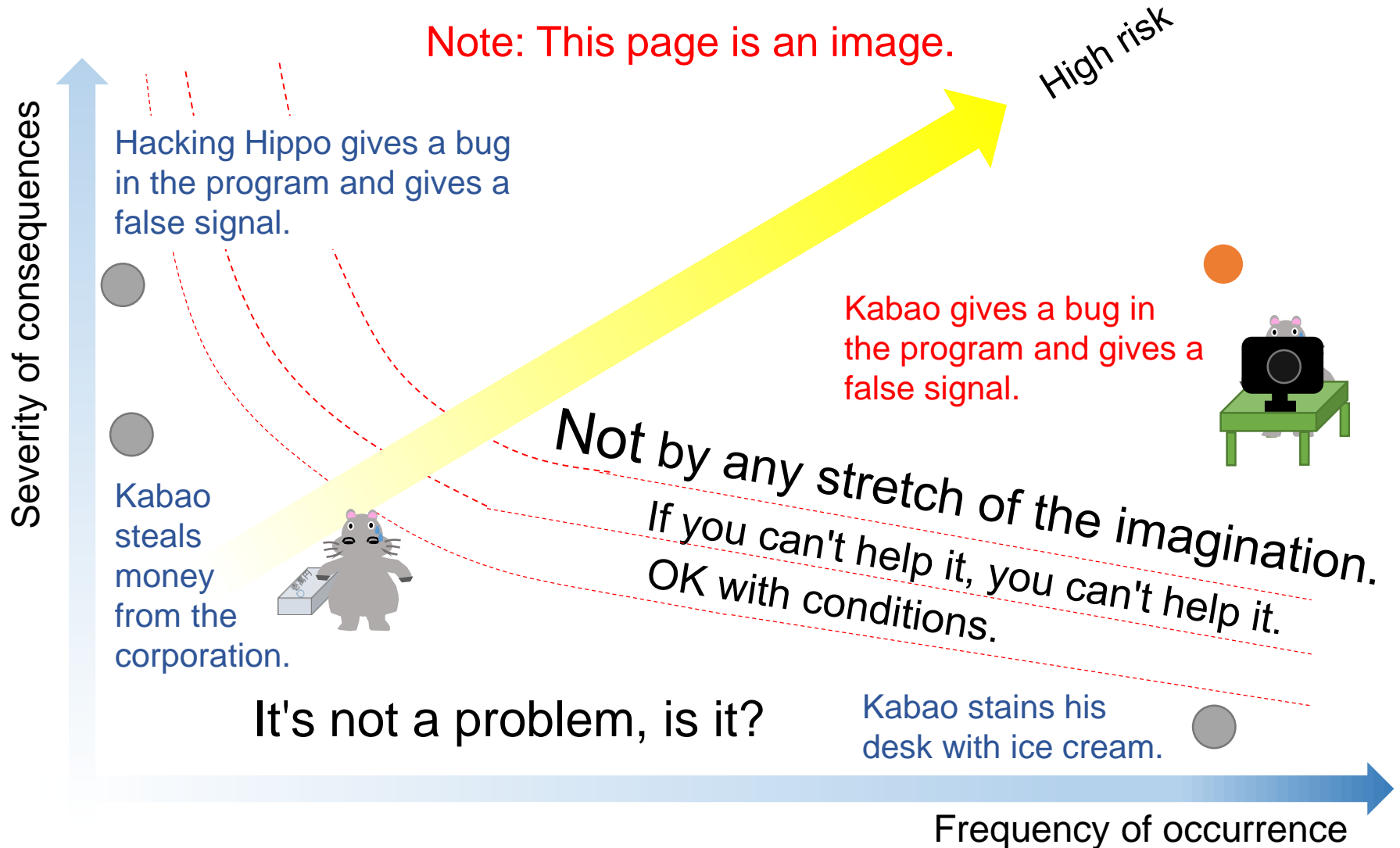


It's still true, isn't it? **Sometimes it's out of the question once, sometimes it's safe to do it again and again.** I guess that's because the impact on the company management is different.

3-2 Degree of hazardous events

IEC 62278 6.3.3.1 c)
EN 50126-1 7.4.2.1-4

Note: This page is an image.



3-2 Frequency of occurrence of hazardous events

IEC 62278 6.3.3.1 c)
IEC 62278 4.6.2.2

Category	Description
Frequent	Likely to occur frequently. The hazard will be continually experienced
Probable	Will occur several times. The hazard can be expected to occur often
Occasional	Likely to occur several times. The hazard can be expected to occur several times
Remote	Likely to occur sometime in the system life cycle. The hazard can reasonably be expected to occur
Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur



It's difficult to quantify exactly from the above category.

3-2 Frequency of occurrence of hazardous events

EN 50126-1 7.4.2.1-4
EN 50126-1 C.2



Quantification is sometimes useful.

Frequency level	Description	Example of a frequency range based on a single item operating 24 h/day	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5,000 h/year
Frequent	Likely to occur frequently. The event will be frequently experienced.	more than once within a period of approximately 6 weeks	more than about 150 times
Probable	Will occur several times. The event can be expected to occur often.	approximately once per 6 weeks to once per year	about 15 to 150 times
Occasional	Likely to occur several times. The event can be expected to occur several times.	approximately once per 1 year to once per 10 years	about 2 to 15 times
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.	approximately once per 10 years to once per 1,000 years	perhaps once at most
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.	approximately once per 1,000 years to once per 100,000 years	not expected to happen within the lifetime
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.	once in a period of approximately 100,000 years or more	extremely unlikely to happen within the lifetime

3-2 Severity of hazardous events

IEC 62278 6.3.3.1 d)
IEC 62278 4.6.2.3
EN 50126-1 7.4.2.1-4
EN 50126-1 C.3



What are the levels of severity?

Severity category	Consequences to persons or environment	Consequences on service/property (related to RAM*)
Catastrophic	<ul style="list-style-type: none">Affecting a large number of people and resulting in multiple fatalities, and/orextreme damage to the environment	Any of the below consequences in presence of consequences to persons or environment
Critical	<ul style="list-style-type: none">Affecting a very small number of people and resulting in at least one fatality, and/orlarge damage to the environment	Loss of a major system
Marginal	<ul style="list-style-type: none">No possibility of fatality, severe or minor injuries only, and/orminor damage to the environment	Severe system(s) damage
Insignificant	<ul style="list-style-type: none">Possible minor injury	Minor system damage

* Not only safety but also unfavorable matters for RAM are subject to risk in EN 50126.

3-2 How do you determine the frequency of security?



But hazardous events are also a security issue these days. There's a guy in my corporation who looks like he's in trouble.



I don't know if this guy will do it or not, but at least he has the skills.



This guy is a safe pie. Just give him some ice lollies and he'll be fine.

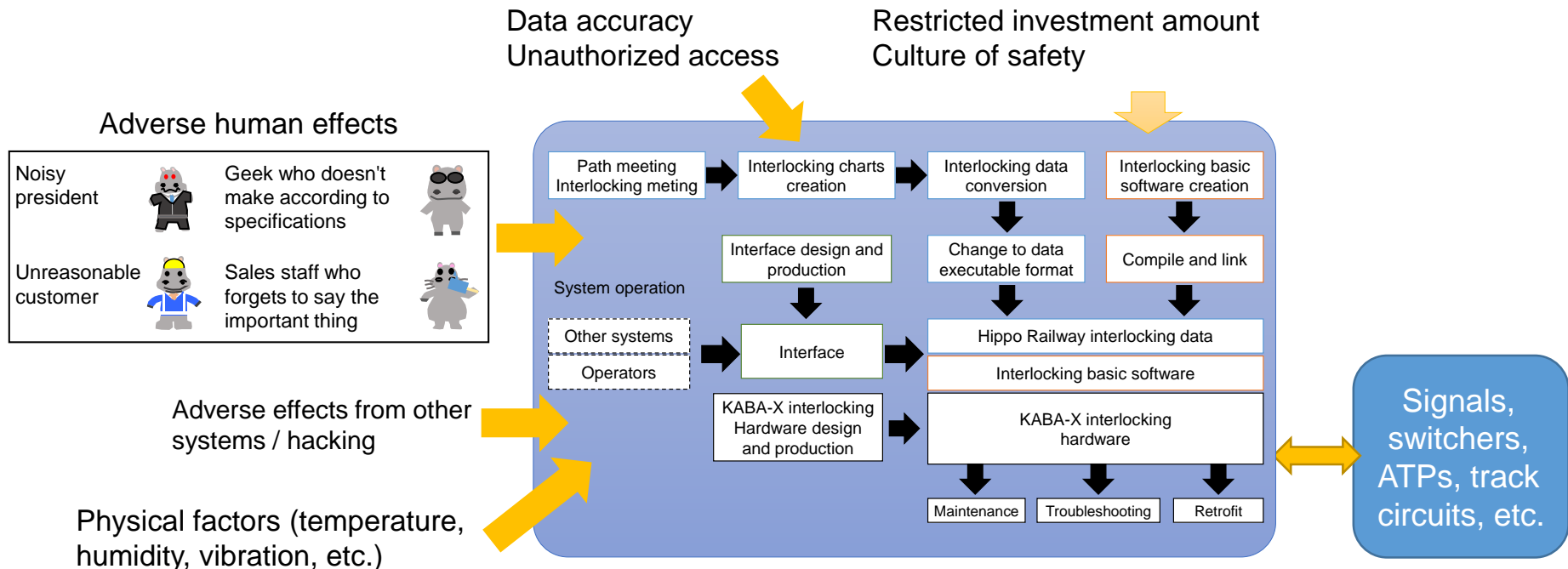


The frequency or probability of security doesn't really come into play. How about judging whether it is easy or difficult to attack?

3-2 Target of attack



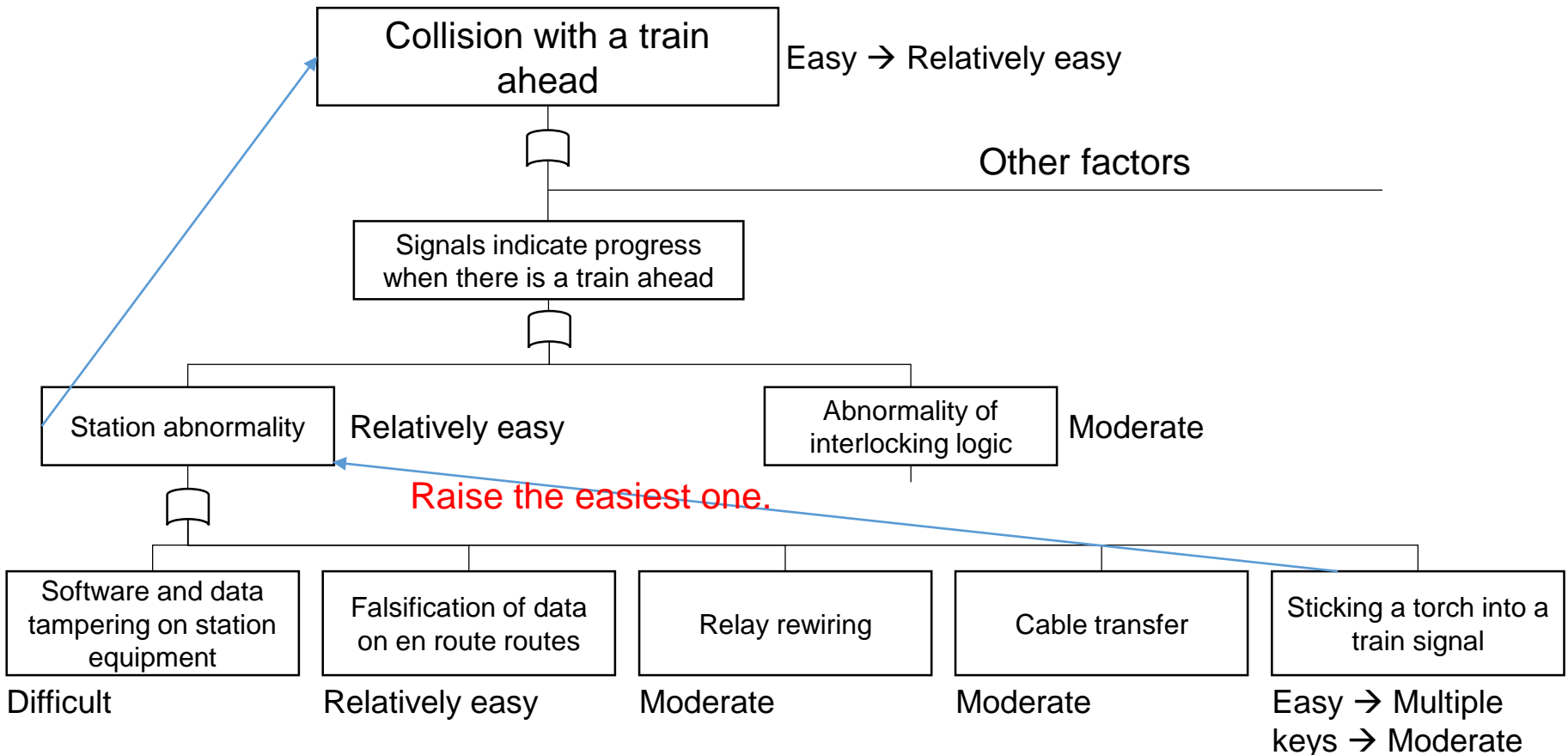
So where should you attack in order to derail and crash your train? Naturally, it's the easiest place to do it.



3-2 Level rating



Sticking a torch into a train signal doesn't require any skill, unless the signal is locked.



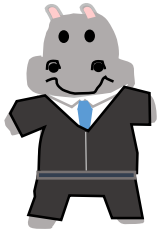
3-3 Dealing with unwanted factors

- 3-1 Identify hazards, or factors that have a negative impact on RAM (hereinafter referred to as unwanted factors)
- 3-2 Understand the degree or likelihood of unwanted factors
- 3-3 Determine what to do with unwanted factors
 - 3-3-1 Three analysis methods (CoP, similar reference systems, individual analysis)
 - 3-3-2 Example of individual analysis
 - 3-3-3 Example of operating rate analysis
- 3-4 Record unwanted factors



3-3 "I'll do anything." – is it the same as doing nothing? Our product is SIL4. (really?)

IEC 62278 6.3.3.1 c)
EN 50126-1 7.4.2.1-4



The interlocking system we produce at Hippo Corp. use SIL4 fail-safe computers and is designed with safety in mind to meet your expectations. **We do everything we can! That's what Hippo Corp. is all about!**

Oh, that's very encouraging! So if we use Hippo Corp. products, we will have a safe and comfortable railway security system.



Of course. We use machines that are SIL4 certified. We don't just use the catchphrase "Hippo Corp. of Trust"! Please trust us, and please use our products for the next system renewal.

Our president is talking too good to be true. How can he say "SIL4" when each function has its own SIL value?



3-3 How to deal with unwanted factors? EN 50126-1 7.4.2.1



But I think you have to decide whether you want to deal with it or not based on some criteria.



I'm the boss and I decide! That's a bit much.



One is the Code of Practice (CoP). This is not specified in the IEC standard (but is specified in EN 50126), but is often used implicitly.



It's a code of implementation. So, I could say that I, the president, made the rules?



That's no good.

3-3-1 Code of Practice

IEC 62278 6.3.3.2
EN 50126-1 7.4.2.1
EN 50126-2 8.3.1



So, how does Hippo Corp. deal with data corruption?

Well, we have a very good engineer, hacking Hippo, who has created an internal standard called KABA-EDP-1 to deal with this.



What's that? Does it have any track record? Is everyone convinced about its content? I don't know if I can trust it.

Hippo Corp. puts the customer first, and I, Kabao, will not sell you something we are not confident in. Hippo Corp. is all about technology! You can be sure of that!



So that's not an explanation at all. Even if you say it's OK, I can't explain it to other people.

Please trust me...



Even if I believed in it, I don't think others would. It's not a religion. Religion can be unfounded, but is that the kind of safety that technology protects?



3-3-1 What we often do in CoP

IEC 62278 6.3.3.2
EN 50126-1 7.4.2.1
EN 50126-2 8.3.1



You have come back. So what is the answer to my previous question?

Well, our hacking Hippo has created an internal standard called "KABA-EDP-1", which is based on the international standard IEC 62280.



Oh, yeah! That's good. But what evidence do you have that it's safe to reflect the thinking behind the standard?

Hippo Corp. puts the customer first, and I, Kabao, will not sell you something we are not confident in. Hippo Corp. is all about technology! You can be sure of that!



There it is again. You don't have to come alone anymore, can an engineer come too?



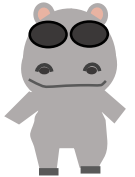
The application of a CoP does not mean that subsequent risk assessments are no longer required.



3-3-1 Code of Practice

IEC 62278 6.3.3.2
EN 50126-1 7.4.2.1
EN 50126-2 8.3.1

The "KABA-EDP-1" corresponds to the threats defined in the proven international standard IEC 62280, and specifies the network and code length to be used with sufficient error detection capability without compromising the safety integrity. This is exactly what is stated in IEC 62280.



In short, it meets the level of the world. Okay, then. But your sales people are all about enthusiasm.



The CoP must be a well-accepted rule in the railway industry and must be properly applied.

3-3-1 Study of similar products



What about error detection codes in similar systems that have been used in the past?

Well, I think it's the same.



OK, but what is Hippo Corp.'s definition of "similar" when it refers to a similar system?

Um, well, I think it means "similar" in English, i.e., "having a resemblance in appearance, character, or quantity, without being identical."



Wouldn't you then be able to say that everything is the same?



There is a definition of what requirements a "similar product" must meet.



3-3-1 Study of similar products

Terms of reference system

- The reference system has a sufficient track record to provide a safe level of acceptance and is therefore suitable for acceptance;
- The reference system has similar functionality and interfaces to the target system;
- The reference system has been in use for a reasonable period of time to view hazards and incidents under conditions similar to those of the target system;
- The reference system is operated under similar environmental conditions to the target system.

If the left is satisfied,

- The risks of the reference system are considered acceptable to the target system;
- The safety requirements of the hazards encompassed by the reference system shall be derived from the safety analysis or from an assessment of the safety record of the reference system;
- The safety requirements shall be listed in the hazard record as safety requirements for the relevant hazard.

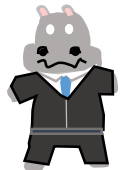


It's hard...



3-3-1 Study of similar products

To put it more simply, if a similar product is used for a similar period of time, environment, usage and interface and there are no particular safety issues, the risk is acceptable. However, the specification of safety requirements for similar products must be risk analysed. It is also not acceptable if there is no record of what hazard the safety requirement is for.



It will be tough to say, "It's the same feature as before, so it's ok". Hey Kabao, I hope you've got the records.

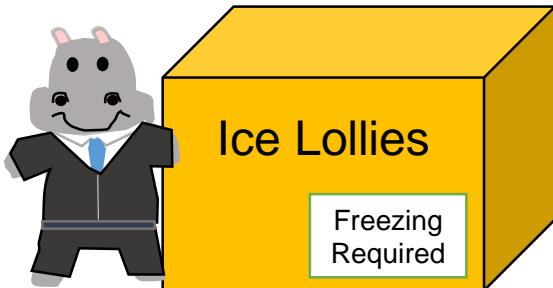
Well, I've got a record of everything we've done so far. You can have them in exchange for ice lollies!



Ice Lollies

Freezing
Required

If it's just an ice lolly, it's cheap!
I've got 100 ice lollies. Eat up, eat up!



3-3-1 Clear risk estimation

IEC 62278 6.3.3.2

EN 50126-2 8.3.3

So there are ways of estimating the risk of products that have never been done before, or that are not in the standard.



Hippo Corp. products should not be at risk. There's no zero risk, though.



This means knowing your current level of risk and reducing it to an acceptable risk.



3-3 Dealing with unwanted factors

- 3-1 Identify hazards, or factors that have a negative impact on RAM (hereinafter referred to as unwanted factors)
- 3-2 Understand the degree or likelihood of unwanted factors
- 3-3 Determine what to do with unwanted factors**
 - 3-3-1 Three analysis methods (CoP, similar reference systems, individual analysis)
 - 3-3-2 Example of individual analysis**
 - 3-3-3 Example of operating rate analysis
- 3-4 Record unwanted factors



3-3-2 Example of clear risk estimation




I wonder how much the Hippo Corp. security system would fail if it were made from a generic CPU board.




Don't underestimate us. We don't offer anything like that.

Well, if that were the case, it would probably happen once a decade or so that the function of output is not fulfilled as defined. That is, about $1.1 \times 10^{-5}/h$.

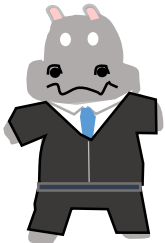


Frequency level	Description	Example of a frequency range based on a single item operating 24 h/day	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5,000 h/year
Frequent	Likely to occur frequently. The event will be frequently experienced.	more than once within a period of approximately 6 weeks	more than about 150 times
Probable	Will occur several times. The event can be expected to occur often.	approximately once per 6 weeks to once per year	about 15 to 150 times
Occasional	Likely to occur several times. The event can be expected to occur several times.	approximately once per 1 year to once per 10 years	about 2 to 15 times
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.	approximately once per 10 years to once per 1,000 years	perhaps once at most
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.	approximately once per 1,000 years to once per 100,000 years	not expected to happen within the lifetime
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.	once in a period of approximately 100,000 years or more	extremely unlikely to happen within the lifetime



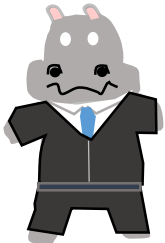
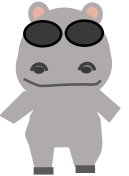
3-3-2 Let's think about the hazard first!

The train carrying hippos derails.



If you're all wiped out, what should I do? Don't die.

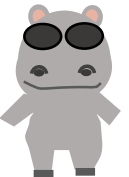
Surprisingly, he is the president who thinks of employees. How often is this acceptable?
Can I use the general-purpose CPU board?



It is an accident that shouldn't happen. No generic products. You have to give maximum protection.

The train carrying hippos derails.

Severity: Death of multiple hippos
Tolerable frequency: priceless
I can't start designing until the value is fixed.

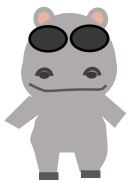


3-3-2 Tolerable frequency/severity

Multiple fatalities

Severity \ Frequency		Insignificant 1	Marginal 2	Critical 3	Catastrophic 4
Frequent	F	Undesirable	Intolerable	Intolerable	Intolerable
Probable	E	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	D	Tolerable	Undesirable	Undesirable	Intolerable
Rare	C	Negligible	Tolerable	Undesirable	Undesirable
Improbable	B	Negligible	Negligible	Tolerable	Tolerable
Highly improbable	A	Negligible	Negligible	Negligible	Negligible

Applying our president's thoughts to the above table, it would be the part surrounded by the green frame. This means that the frequency is "highly improbable".



3-3-2 Tolerable frequency

IEC 62278 6.3.3.2

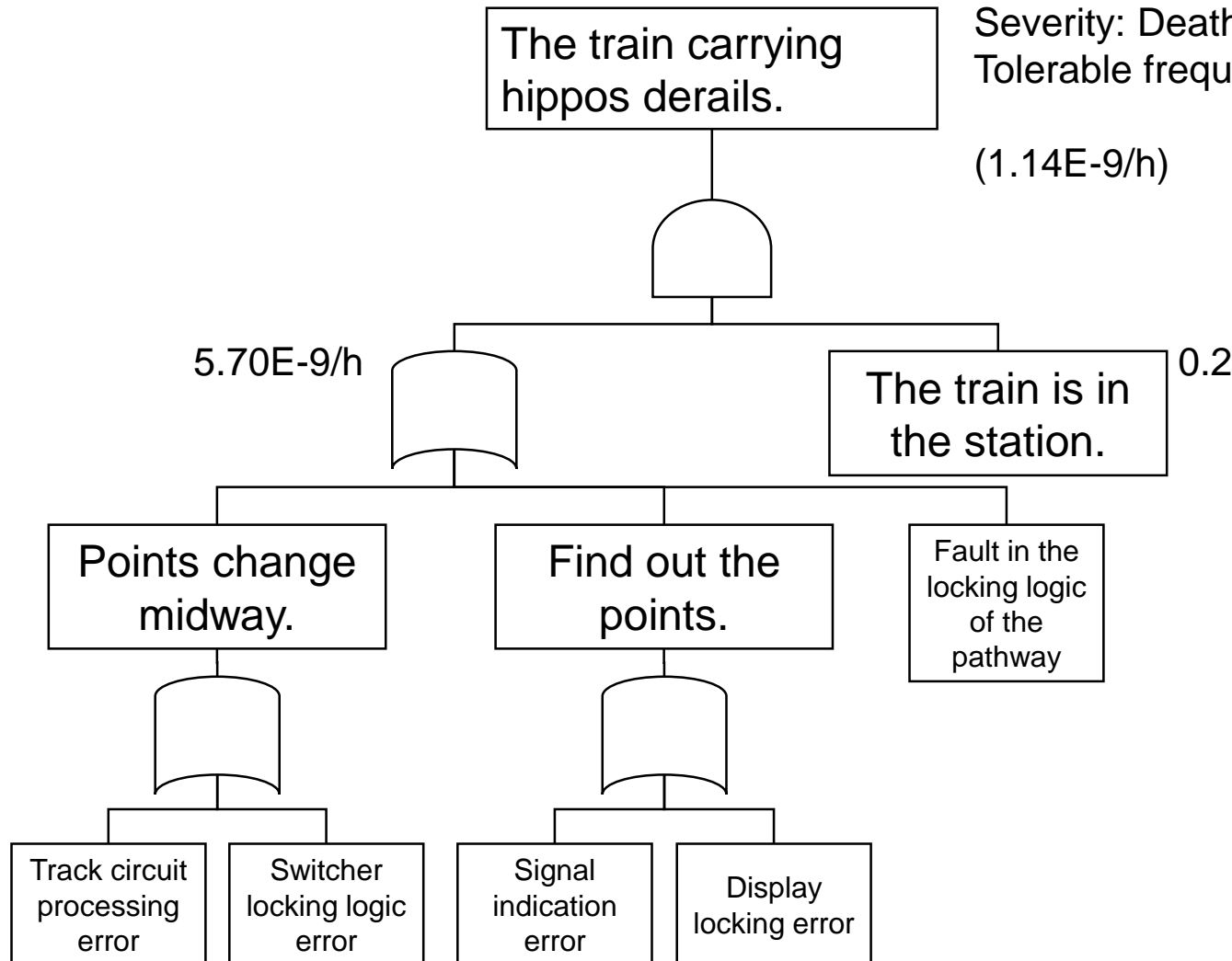
EN 50126-2 8.3.3

Frequency level	Description	Example of a frequency range based on a single item operating 24 h/day	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5,000 h/year
Frequent	Likely to occur frequently. The event will be frequently experienced.	more than once within a period of approximately 6 weeks	more than about 150 times
Probable	Will occur several times. The event can be expected to occur often.	approximately once per 6 weeks to once per year	about 15 to 150 times
Occasional	Likely to occur several times. The event can be expected to occur several times.	approximately once per 1 year to once per 10 years	about 2 to 15 times
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.	approximately once per 10 years to once per 1,000 years	perhaps once at most
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.	approximately once per 1,000 years to once per 100,000 years	not expected to happen within the lifetime
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.	once in a period of approximately 100,000 years or more	extremely unlikely to happen within the lifetime

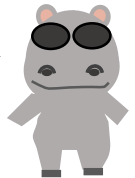
3-3-2 What causes a derailment?

IEC 62278 6.3.3.2

EN 50126-2 8.3.3



It's all set.



3-3-2 Tolerance allocation

IEC 62278 6.3.3.2
EN 50126-2 8.3.3, 10.2.2

The train carrying
hippos derails.

Severity: Death of multiple hippos
Tolerable frequency: Less than once in
100,000 years

(1.14E-9/h)

5.70E-9/h

15-year
failure rate
0.000731252

The train is in
the station.

0.2

Points change
midway.

Find out the
points.

Fault in the
locking logic
of the
pathway

1.00E-9/h
15-year
failure rate
0.000128242

There are likely to
be safety
requirements
regarding the ability
to prevent
accidents in blue.



2.29E-9/h
15-year
failure rate
0.000301505

2.29E-9/h
15-year
failure rate
0.000301505

1.15E-9/h
15-year
failure rate
0.000150753

Track circuit
processing
error

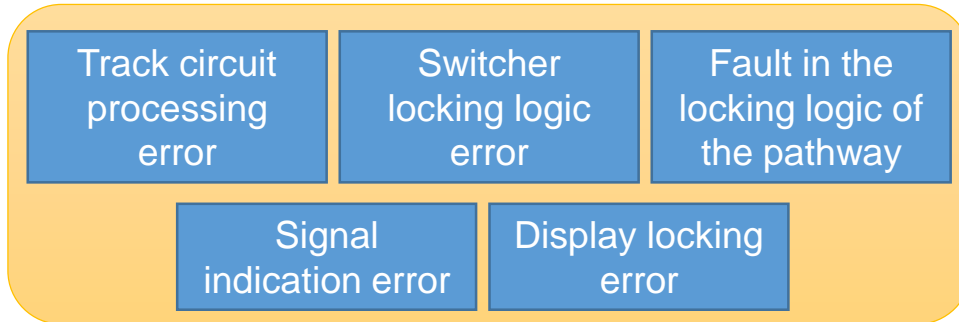
Switcher
locking logic
error

Signal
indication
error

Display
locking error

3-3-2 SIL per function

IEC 62278 6.3.3.2
EN 50126-2 8.3.3, 10.2.3



The function to prevent these hazards is to have an unsafe side transition frequency of $10^{-9}/h$.



Then this function is called SIL4, according to EN 50126-2 Table 2.



Table 2 — SIL quantitative and qualitative measures

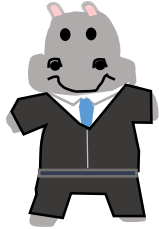
TFFR [h^{-1}]	SIL attribution	SIL qualitative measures
$10^{-9} \leq TFFR < 10^{-8}$	4	Defined in sector-specific standards
$10^{-8} \leq TFFR < 10^{-7}$	3	
$10^{-7} \leq TFFR < 10^{-6}$	2	
$10^{-6} \leq TFFR < 10^{-5}$	1	

Don't forget to recalculate if you have set up a feature to prevent hazards. The same measures across functions can be co-opted, so if that happens, please take that into account in your calculations. Check Common Cause Failure (CCF) for more information.



3-3-2 What do you decide your SIL for?

IEC 62278 6.3.3.2
EN 50126-2 8.3.3, 10.2.6



Well, isn't it enough to make the frequency of unsafe side transition less than $10^{-9}/h$?

Sure, that's fine for hardware and other things where failure rates can be calculated, but why not let Kabao make the software?



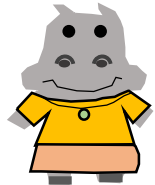
Absolutely not. It's full of bugs. You have to control it well.

When we decide on the level of safety, we can decide on the level of management and the level of technology used as standard.



I see. It's not something that can be done with a single voice from me, is it?

I'm not sure about the software, but you guys are terrible.



3-3-2 What do you decide your SIL for?

IEC 62278 6.3.3.2
EN 50126-2 8.3.3, 10.2.6
IEC 62425 Table E.1

**Table E.1 – Safety planning and quality assurance activities
(referred to in 5.2 and 5.3.4)**

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Checklists	R: checklist of activities and items to be produced		R: checklist of activities and items to be produced	
2 Audit of tasks	R		HR	
3 Inspection of issues of documentation	HR: documents agreed between railway/safety authority and industry		HR: all documents	
4 Review after change in the safety plan	HR			
5 Review of the safety plan after each safety life-cycle phase	HR			

In this way, the level of checks is determined according to safety, so that parts that are not so safety-related can be omitted.

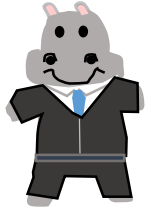
3-3 Risk estimation from models

IEC 62278 6.3.3.2

EN 50126-2 8.3.3

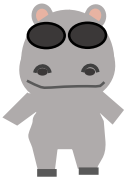
IEC 62425 B.3.1

EN 50129 B.3.1



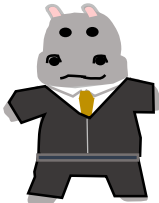
You know the level of safety required for the functioning of the interlocking system individually.

Even in the CoP, this is within the framework of fail safety in IEC 62425, and there is probably quite a lot of precedent for safety system with this kind of mechanism. The degree of safety is also ascertained.

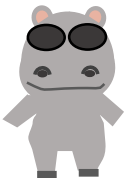


Well, we know that the function of detecting faults and stopping trains is important, but what about the software that makes it work? Do the figures come from software?

For software, depending on the SIL level of the function, a software safety integrity level (SSIL) is determined for the method of realising that function and the rigour of the control method is adjusted.



I see, Prof. Ohkaba. The point is to balance overall cost and safety by focusing management on the important functions and adjusting management accordingly for the less safety-relevant ones.



3-3-3 Is the operating rate of the system increasing?



Does this stop
all the time?

Output

Number of dangerous failures per hour:
 $1 \times 10^{-9}/h$
30-year failure rate: 0.00026

System to realise the function of
detecting dangerous failures and
stopping trains

Number of dangerous failures per hour:
 $1.07 \times 10^{-9}/h$
30-year failure rate: 0.00028

Normal signal

Control unit

Number of failures per hour: $10^{-5}/h$
30-year failure rate: 0.928

3-3-3 How is the operating rate?



Your product may be safe, but it is useless. We only get paid by our customers if our machines work!

We are a safety-first Hippo Corp. I, Kabao, and we cannot sell something we are not confident about to our customers. We are Hippo Corp. of technology! It's absolutely safe!



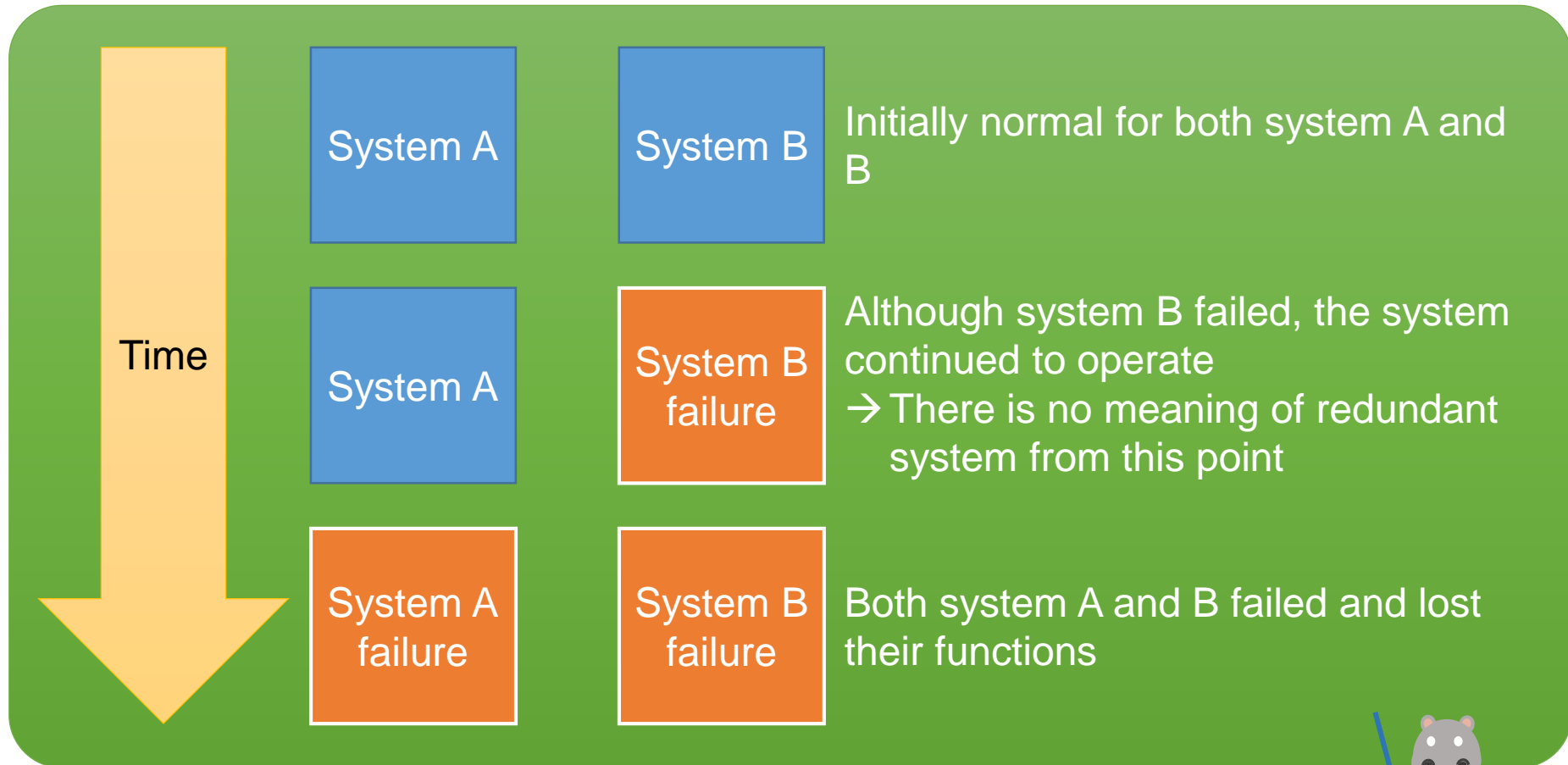
That's safety talk, isn't it? You're not engaging at all. Only 7% of your machines are intact after 30 years, right? Of course that's not good enough.

Um, if you can make it a dual system, I don't see any problem.

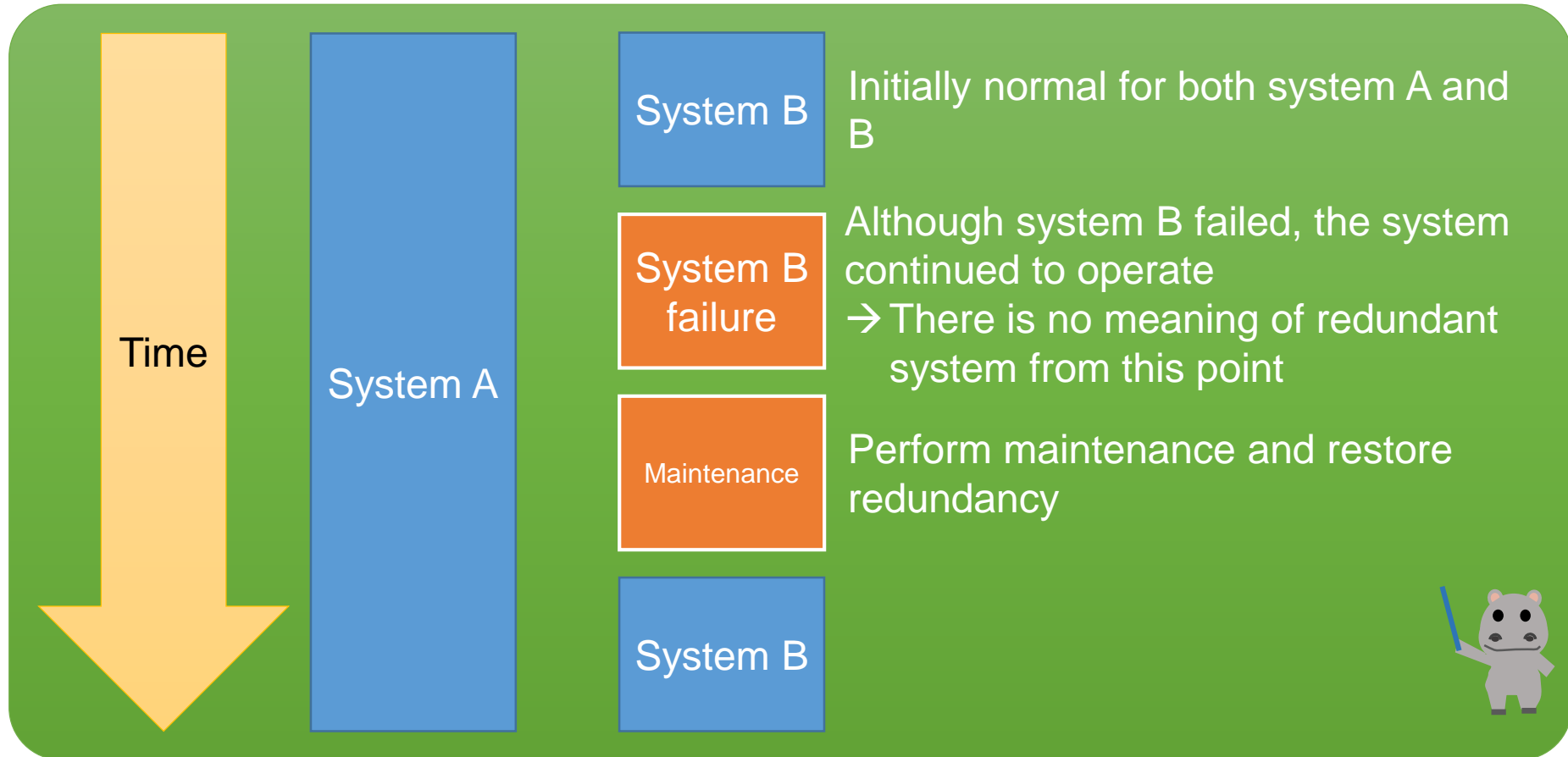


You're full of nonsense. Don't come back, Kabao! Generally speaking, a dual system is useless if it is not maintained and remains broken. Isn't the maintenance interval also relevant?

3-3-3 How is the operating rate?



3-3 How is the operating rate?



As long as one system is out of order or during maintenance and the other is not out of order, the mission can be carried out. Failure detection and quick repair are vital.

3-3-3 Consideration of operating rates

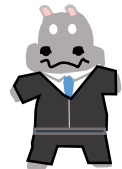


This is why the term "logistics support" is often used in RAMS. The point is that even if a dual system is installed, if it is not replaced in a timely manner after a failure, the operating rate may drop significantly.

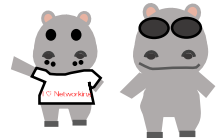
Please make sure you have enough spare parts so that you don't run out. I'm the one who's going to be got angry.



But blindly securing spare parts would increase costs, wouldn't it? It is also key that technicians can rush to Hippo Railway.



Hmmm. This is the difficulty of running a business. Kabao, you should go to Hippo Railway to make sure they know that they have spare parts if they want to ensure availability.
Otakaba! Hacking Hippo! You guys should be able to answer your mobile phones 24 hours a day from tomorrow.



We will leave Hippo Corp. because of poor salary and treatment, and move to Piggy Corp. Thank you for a long time!



3-4 Keep a record

- 3-1 Identify hazards, or factors that have a negative impact on RAM (hereinafter referred to as unwanted factors)
- 3-2 Understand the degree or likelihood of unwanted factors
- 3-3 Determine what to do with unwanted factors
 - 3-3-1 Three analysis methods (CoP, similar reference systems, individual analysis)
 - 3-3-2 Example of individual analysis
 - 3-3-3 Example of operating rate analysis
- 3-4 Record unwanted factors



3-4 Keep a record of any problems



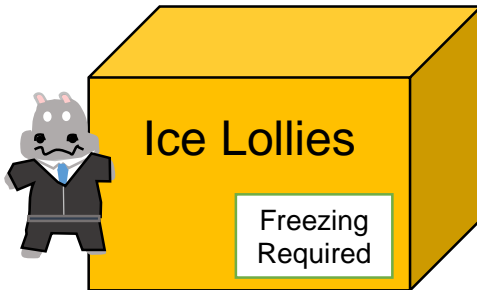
Kabao, you're good at keeping records, aren't you?

I'm keeping a record of all the president's rants and misunderstandings. If only I had this... Mmm-hmm...



Hey, you're threatening me. We're Hippo Corp. family, we're family.

I'm not threatening you. I just said that I have a record. If you think it's a threat, it's because you have something to hide.



Do you want an ice lolly? I have 200. Eat up!

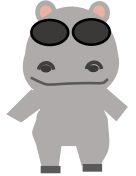
In order for Hippo Corp. to be a good company, we need to record and improve. It's outrageous that you think I'm threatening you. I'll take the ice lollies!



3-4 What is the problem?

IEC 62278 6.3.3.3
EN 50126-1 7.4.2.2

I don't know what Kabao records, but usually I don't want to write about things I don't like, but I know I have to.

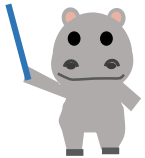


So let's try to organise what we describe a bit.

I've always imagined a "hazard log", where you write down the problem, the severity and frequency, and a coping strategy.

Well, that's a good line, but let's find out what you should write about.

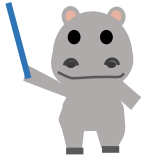
3-4 Purpose of compiling records



What is the purpose of creating a hazard log?



If you can't solve a problem now, you can make a note of it so that you can solve it when the time comes.



Well, it's still on the right track, but I don't think it's much different from "Kabao's Memo".

It should be a document of record that records the decision as to whether a hazard should be dealt with, based on known assumptions about the hazard, the policy for dealing with it, and whether it was carried out in accordance with established procedures, and confirms that there are no problems.

It may also help you to rethink your future designs and your next project.



3-4 It's not enough to write it down.



Make a record of exactly what you have done.



If you don't have a plan to deal with it first, you won't know if you've dealt with it properly.

Purpose of the hazard log

The aim is to record the decision as to whether a hazard should be dealt with, based on known assumptions about the hazard, the policy for dealing with it, and whether it was carried out in accordance with established procedures, to check for any problems and to help ensure safety and quality and future projects.

Conditions for risk analysis

Example 1) As the destination of this system has already been decided, the risk analysis is based on the operating conditions and equipment of the destination as of 2020.

Example 2) Since this system is to be built by Hippo Corp. as a standard system, the analysis will be based on the maximum capacity equipment and operating conditions described in the proposal.

3-4 Example of a hazard log



As IEC 62278 has too many detailed regulations, I have made an example based on EN 50126-1.

Purpose of the hazard log: _____

Corresponding system: _____

Assumptions: _____

No.	Hazards (Concerns)	Likely hazard events	Risk assessment			Measures	Risk assessment after taking measures			Various conditions (depending on other systems and management)
			Severity	Frequency	Risk		Severity	Frequency	Risk	

EN 50126-1 7.4.2.2 Hazard Log

- the purpose of the hazard log;
- each hazard, entities responsible for managing the hazard, and the contributing functions or components;
- likely consequences and frequencies of the sequence of events associated with each hazard, when applicable;
- the risk arising from each hazard (in quantitative or qualitative terms), where appropriate;
- risk acceptance principles selected and in case of explicit risk estimation also the risk acceptance criteria to demonstrate the acceptability of the risk control related to the hazards;
- for each hazard: the measures taken to reduce risks to a tolerable level or to remove the risks;
- exported safety constraints.

Conclusion

3-1 Identify hazards, or factors that have a negative impact on RAM (hereinafter referred to as unwanted factors)

It is advisable to use a combination of empirical and systematic methods of extraction.

3-2 Understand the degree or likelihood of unwanted factors

Frequency and severity are important.

3-3 Determine what to do with unwanted factors

There are methods by CoP, precedent and analysis.

SIL depends on the function, not the system.

3-4 Record unwanted factors

It is not just a record, but a document of record that records the decision as to whether a hazard should be dealt with, based on known assumptions about the hazard, the policy for dealing with it, and whether it was carried out in accordance with established procedures, and confirms that there are no problems.

