Matters to be left to the system / Matters to be done by humans

—To decide the role of the system—

(RAMS Phase 2)

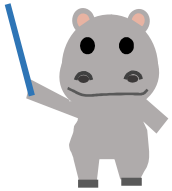
Mori Takashi

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

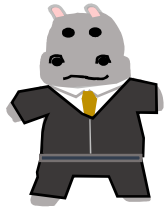
Actors

President of Hippo Corp.
Motto: Technology and inspiration

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



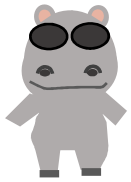
anonymous Hippo
Unknown Consultant
Motto: Knowledge is power!



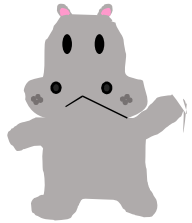
Prof. Ohkaba
Motto: Software must be in good order.

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.

Greetings to everyone

From 1 February 2021, I became a staff member of the National Traffic Safety and Environment Laboratory.

I will continue to devote myself to my work.

Thank you.

Previous summary

The phase 1 of RAMS is to:

share the scope, target, and basic ideas of the system with the people involved.

consider comprehensively what aspect the surrounding situation has.

consider causes (hazard sources: e.g., incorrect wiring) of potentially dangerous events (hazards: e.g., the blue signal light is on instead of the red one) and the management method that seems to be necessary.

A question I received in the last email

I agree with thinking about potential sources of hazards.
But I suppose Hippo Corp.'s management is the biggest source of hazards.

Please leave it to us.

Worker at a manufacturer in Tokyo

Disrespectful! Our finances are sound.

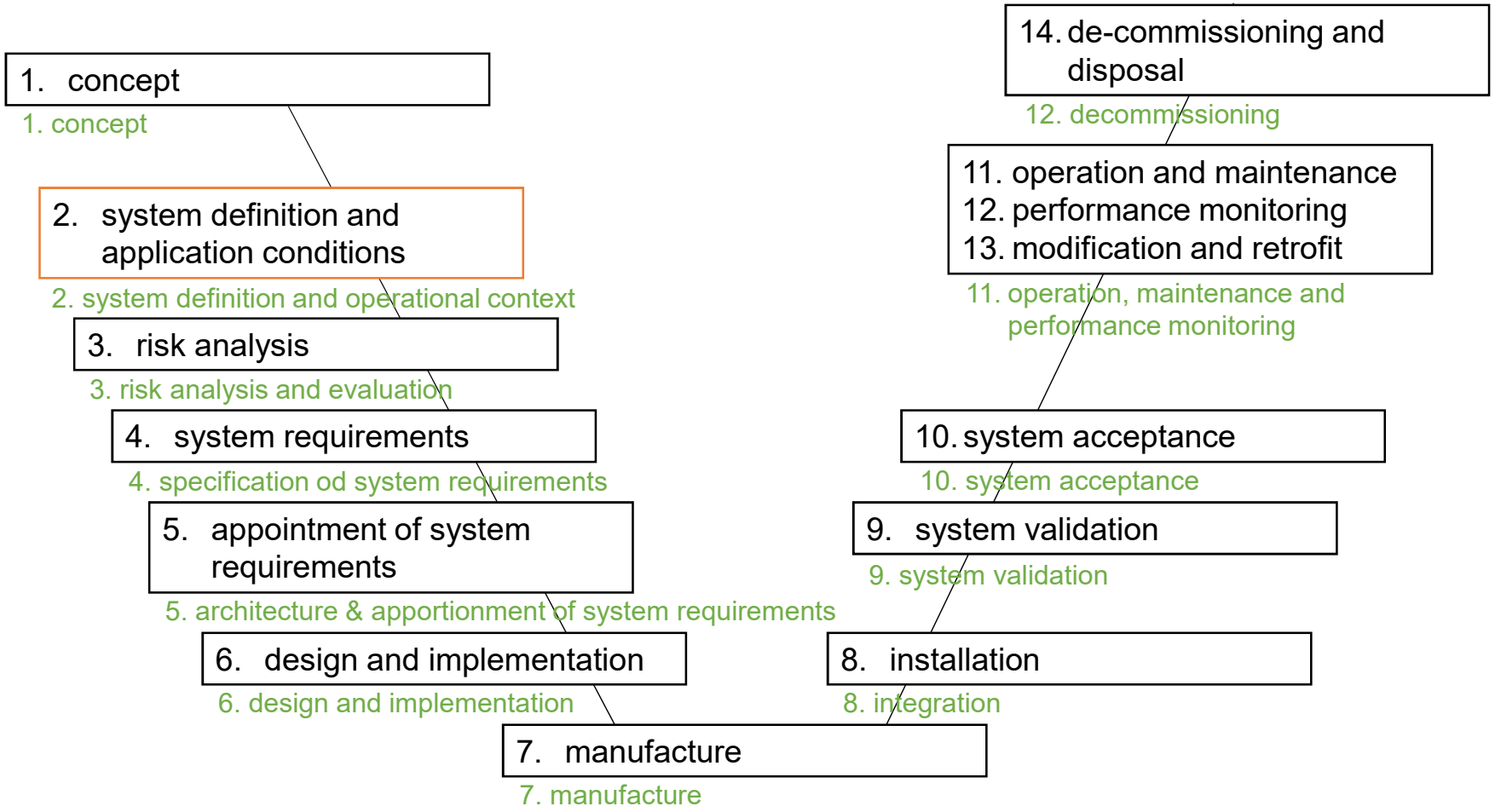
The next phase 2

Phase 2: System definition and application conditions (IEC 62278)

Phase 2: System definition and operational context (EN 50126-1)

System life cycle

IEC 62278 5.2
EN 50126-1 6.2



交通安全環境研究所
National Traffic Safety and Environment Laboratory

*Letters surrounded by squares are defined in IEC 62278, and green letters are defined in EN 50126-1.

What is required at this phase

2-1 Define the system objective

2-2 Define the system mission profile, that is, numerical targets

2-3 In preparation for RAMS analysis

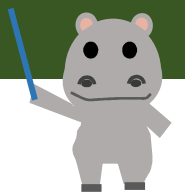
- 2-3-1 Define the system boundary
- 2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system
- 2-3-3 Define the scope of system hazard analysis

2-4 Evaluate the items that may affect RAM and grasp a feeling for them

2-5 Detect hazards and grasp a feeling for them

2-6 Establish the initial RAM Plan for the system

2-7 Establish the initial Safety Plan for the system



2-1 Define the system objective

2-2 Define the system mission profile, that is, numerical targets

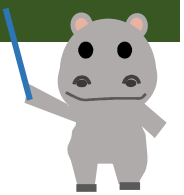
2-3 In preparation for RAMS analysis

- 2-3-1 Define the system boundary
- 2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system
- 2-3-3 Define the scope of system hazard analysis

2-4 Evaluate the items that may affect RAM and grasp a feeling for them

2-5 Detect hazards and grasp a feeling for them

2-6 Establish the initial RAM Plan and Safety Plan for the system



EN 50126-1 7.3.2.1 a)

2-1 The concept should have been developed, but how far the concept can or should be expanded?

I came to a meeting about this centralized interlocking system. How much can Hippo Corp. decide?

Fully automatic! We will leave everything to Hippo Corp.

What does that mean?

For example, we want something like the following:
- even if the system breaks, the equipment can be repaired by itself;
- Hippo Corp. will automatically include the contents decided at the interlocking meeting up to the test with an automatic system;
- if you say a timetable change, the timetable and route will change automatically.

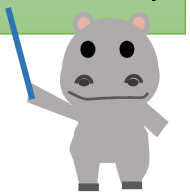
Well, ah, I've never heard of such a thing. I mean...

I haven't said it until now. Because I just thought about it.
We haven't had any minutes so far.

EN 50126-1 7.3.2.1 a)

2-1 Define the system objective

a) the system objective (intended purpose) and its mission profile
– EN 50126-1 7.3.2.1 a)



Defining the system objective leads to the system definition.

I visited Hippo Railway yesterday, but I don't understand what they intended.

You have to clarify it.

Note: In IEC 62278, there is no content to define the objective, probably because it was too obvious to write down. It is written in the successor standard EN 50126-1. Without the intended purpose, it is unlikely that we will be able to proceed to the next phase.

EN 50126-1 7.3.2.1 a)

2-1 Define the system objective

Hippo Railway introduced an electronic interlocking ("EI") system, which requires no complicated wire logic design, to replace an all relay interlocking ("ARI") system for each station.

Because the complexity of the logic is not directly proportional to the size of the EI system, which is different from the ARI system, the EI system only requires small space of the equipment room at a big station.

In order to make better use of these features, instead of installing the EI system at each station, a centralized EI logic unit is set up at a hub station or command center, and only interfaces between equipment are installed at each station. This is called a centralized interlocking system.

⇒ Enables to focus on maintenance works and reduce costs.

As for the assumed availability, the same level as the current level shall be secured, and the same level as the current system shall be guaranteed in the life cycle.

Objective:
By consolidating interlocking system, we aim **to reduce life cycle costs** by streamlining interlocking system, slimming the equipment room itself, and prioritizing maintenance. In addition, **the current level of safety shall be maintained**.

Kabao, You should be slim, too.

Please give me an ice lolly.

2-1 Define the system objective

2-2 Define the system mission profile, that is, numerical targets

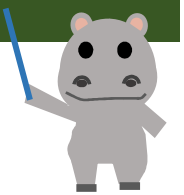
2-3 In preparation for RAMS analysis

- 2-3-1 Define the system boundary
- 2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system
- 2-3-3 Define the scope of system hazard analysis

2-4 Evaluate the items that may affect RAM and grasp a feeling for them

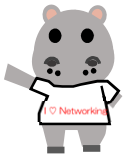
2-5 Detect hazards and grasp a feeling for them

2-6 Establish the initial RAM Plan and Safety Plan for the system

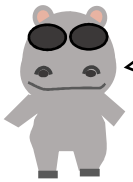


2-2 Define the numerical targets

IEC 62278 6.2.3.1 a)
EN 50126-1 7.3.2.1 a)

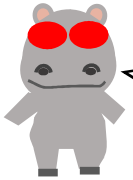


How many stations are there on Hippo Railway?
How long is the processing cycle required?
How many routes are there?
Our president would want to sell the similar product to other operators, but how many routes are acceptable?



How long are you thinking about the replacement cycle? How long is the processing downtime allowed? Think about what happens when it's broke down.

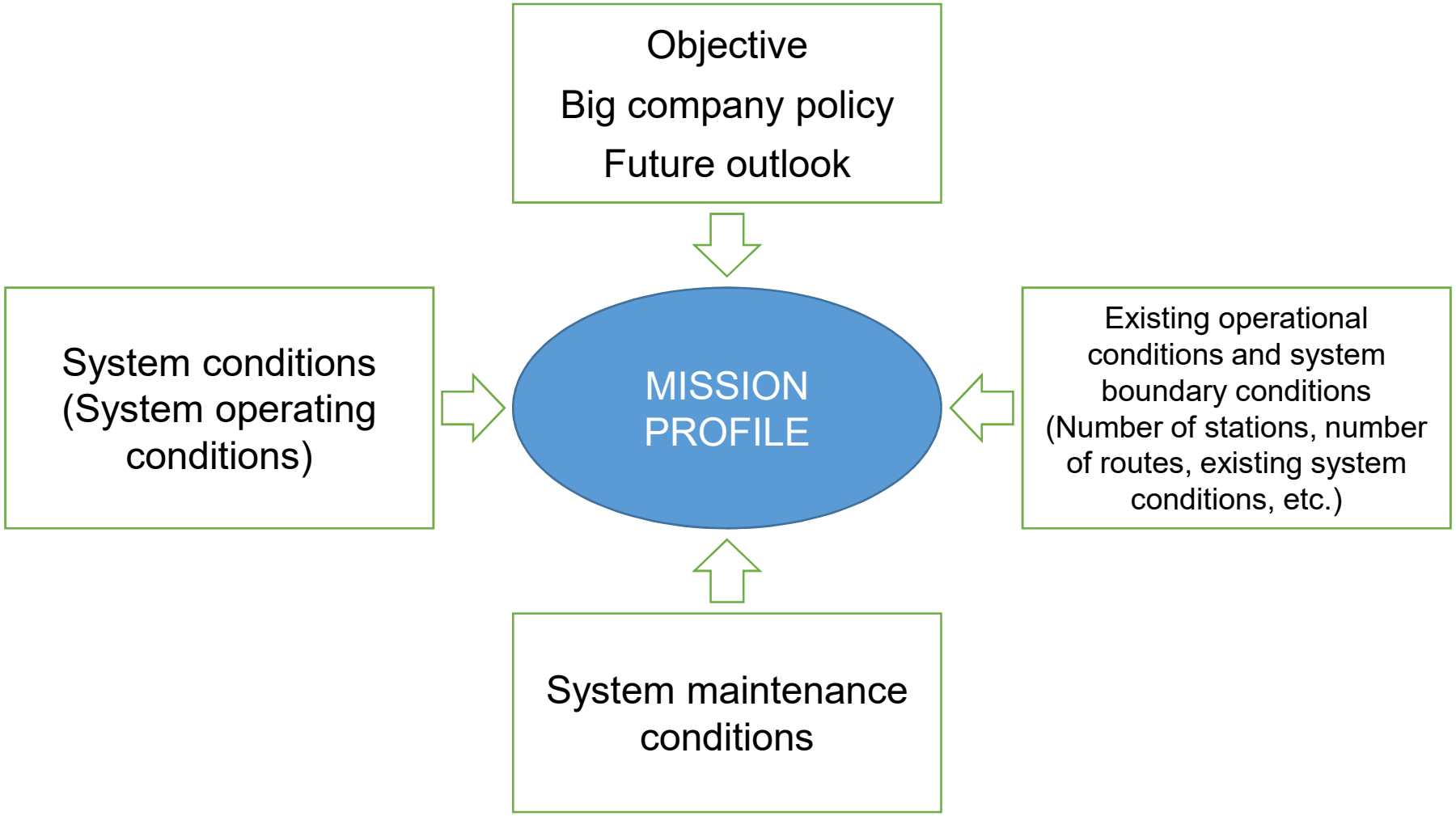
I brought ice lollies. I don't know the answers because I'm a sales staff, so please think about them with everyone except me.



We can't make it! You should check with Hippo Railway and our president. That's a sales role.

2-2 Important matters for setting goals

IEC 62278 6.2.3.1 a), b), c)
EN 50126-1 7.3.2.1 a), b), c)



IEC 62278 6.2.3.1 a), b), c)
EN 50126-1 7.3.2.1 a), b), c)

2-2 Objectives and numerical goals

Hippo Railway is safer than other operators in the same industry. There is an action guideline that the customer's life is prioritized above all else.

- Basically, the ground system should be housed in the equipment room, and air conditioning and uninterruptible power supply can be prepared.
- If the system goes down, all signal operations will be disabled for the entire line section.
- Since no serious system outage has occurred for the past 15 years, it is necessary to have an operating rate equal to or higher than that.

MISSION PROFILE

- The number of stations to be consolidated is 20, and the number of routes is 170.
- The existing interlocking systems and CTC systems at each station will be removed. Leave the route controllers.
- Hippo Corp. wants to support up to about 500 routes at 50 stations in order to sell to other operators.
- Hippo Corp.'s electronic interlockings have a reputation for being a little slow to respond.

- Although the maintenance interval time is set to 3 hours on Hippo Railway, it is not possible to make full use of the interval because other works such as operation of signals and switchers may occur during that interval.
- There is a rule to separate the interlocking system and let the train depart and arrive by hand signal, but it is positioned as a limited operation.

2-2 Objectives and numerical goals

IEC 62278 6.2.3.1 a)
EN 50126-1 7.3.2.1 a)

Kabao, thanks to your interview with Hippo Railway, it seems that the number of routes and the power supply will be decided.

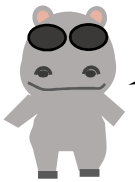
Please give me an ice lolly as a reward.

For safety, can it be quantified?

2-2 Goal setting using safety as an example

IEC 62278 6.2.3.1 a) Annex C
EN 50126-1 Annex B

Hippo Railway is safer than other operators in the same industry. There is an action guideline that the customer's life is prioritized above all else.



The voice of heaven! How should this be quantified?

There is a description of such a parameter example to be decided. Although how to decide is not easy, there are several ways to decide on safety.

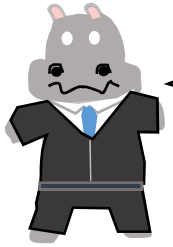
Table C.5 – Examples of safety performance parameters

PARAMETER	SYMBOL	DIMENSION
Mean Time Between Hazardous Failure	MTBF(H)	Time, distance, cycle
Mean Time Between "Safety System Failure"	MTBSF	Time, distance, cycle
Hazard Rate	H(t)	Failures/time, distance, cycle
Safety Related Failure Probability	$F_S(t)$	Dimensionless
Probability of Safe Functionality	$S_S(t)$	Dimensionless
Time to Return to Safety	TTRS	Time

2-2 Hazards and numerical targets

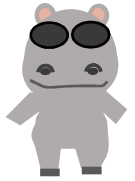
IEC 62278 6.2.3.1 a)
EN 50126-1 Annex C

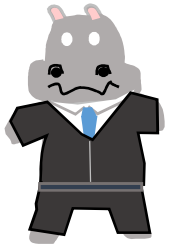
The train carrying hippos derails.



If even one of you died, what should I do? Don't die.

Surprisingly, he is the president who thinks of employees. How often is this acceptable?

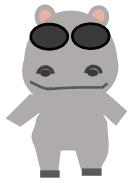




It is an accident that shouldn't happen. You have to give maximum protection.

The train carrying hippos derails.

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



2-2 What can happen?

IEC 62278 6.2.3.1 a)
EN 50126-1 Annex C

If the train derails, the hippos will be wiped out.

Table C.4 — Severity categories (example 1 related to RAMS)

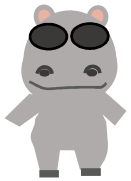
Severity category	Consequences to persons or environment	Consequences on service/property
Catastrophic	• Affecting a large number of people and resulting in multiple fatalities, and/or • extreme damage to the environment	Any of the below consequences in presence of consequences to persons or environment
Critical	• Affecting a very small number of people and resulting in at least one fatality, and/or • large damage to the environment	Loss of a major system
Marginal	• No possibility of fatality, severe or minor injuries only, and/or • minor damage to the environment	Severe system(s) damage
Insignificant	• Possible minor injury	Minor system damage

2-2 What is aimed for?

IEC 62278 6.2.3.1 a)
EN 50126-1 Annex C

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			Death of multiple people

Applying our president's thoughts to the table (EN 50126-1 Table C.9), it would be the part surrounded by the red frame. This means that the frequency is "highly improbable".



2-2 Tolerable frequency

IEC 62278 6.2.3.1 a)
EN 50126-1 Annex C

Table C.1 — Frequency of occurrence of hazardous events with examples for quantification (time based)

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 5000 h/year
		Expected to happen	
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

Once every 100,000 years. We will design a good quality product.

2-2 Summary so far

IEC 62278 6.2.3.1 a)
EN 50126-1 Annex C

System definition, conditions

↓

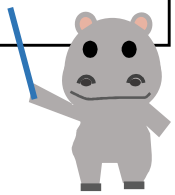
Specific quantification

↓

If it is difficult to quantify,

↓

utilize precedents and risk matrices.



2-1 Define the system objective

2-2 Define the system mission profile, that is, numerical targets

2-3 In preparation for RAMS analysis

2-3-1 Define the system boundary

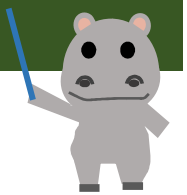
2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system

2-3-3 Define the scope of system hazard analysis

2-4 Evaluate the items that may affect RAM and grasp a feeling for them

2-5 Detect hazards and grasp a feeling for them

2-6 Establish the initial RAM Plan and Safety Plan for the system



2-3 What about the boundary?

IEC 62278 6.2.3.1 b)
EN 50126-1 7.3.2.1 b)

IEC 62278 6.2.3.1 b)

b) the system boundary, including:
- interfaces with physical environment;
- interfaces with other technological systems;
- interfaces with humans;
- interfaces with other Railway Authorities;

Changed to "interfaces and interactions"
Changed from "other Railway Authorities" to "other railway duty holders"

EN 50126-1 7.3.2.1 b)

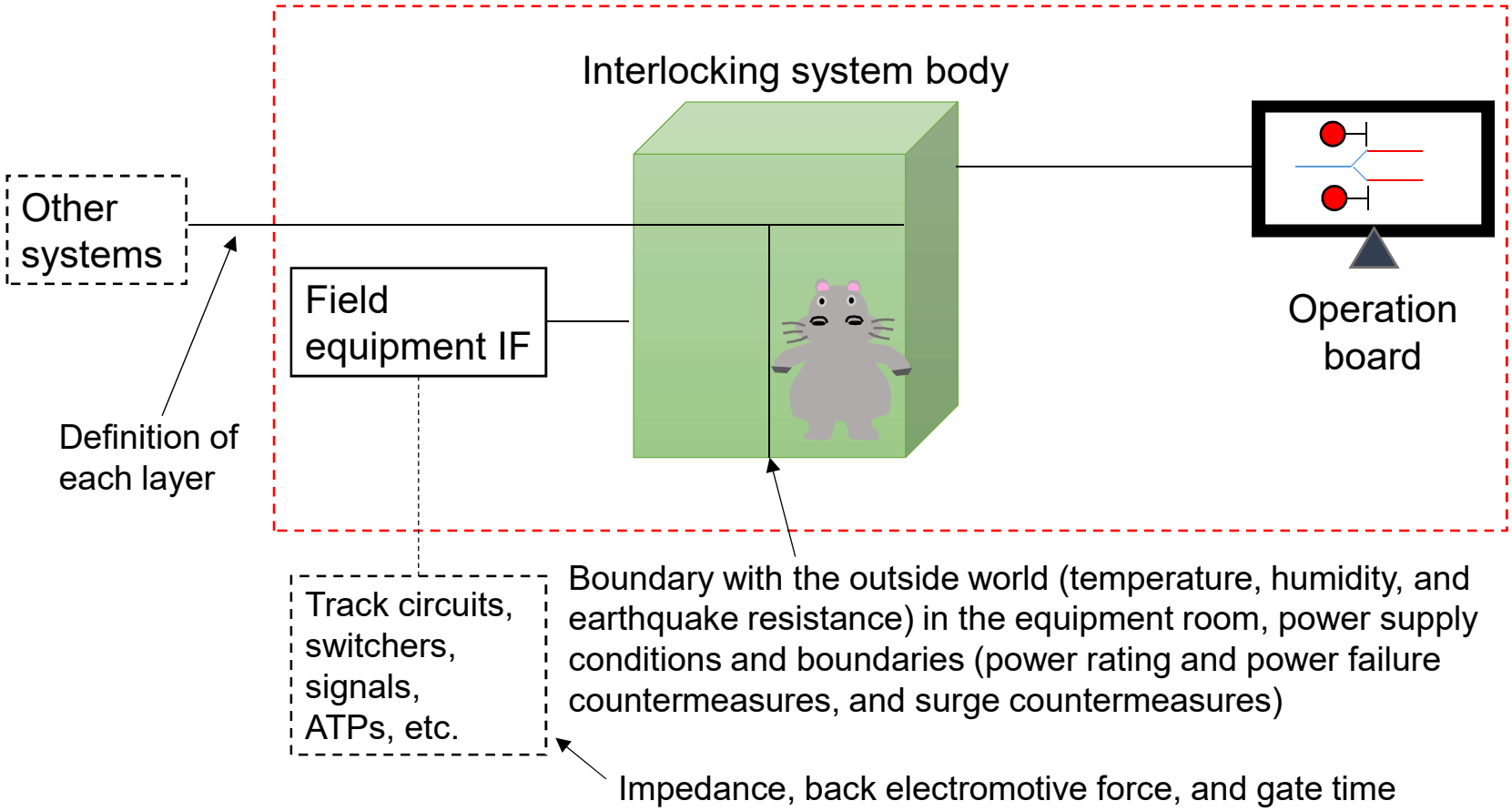
b) the system boundary, including:
- interfaces and interactions with physical environment (e.g. climatic conditions, mechanical conditions, altitude) and with other systems;
- interfaces and interactions with other technological systems;
- interfaces and interactions with humans;
- interfaces and interactions with other railway duty holders;

I'm not sure, but the number of characters is increasing at the bottom. Let Kabao translate it.

2-3 What is the boundary?

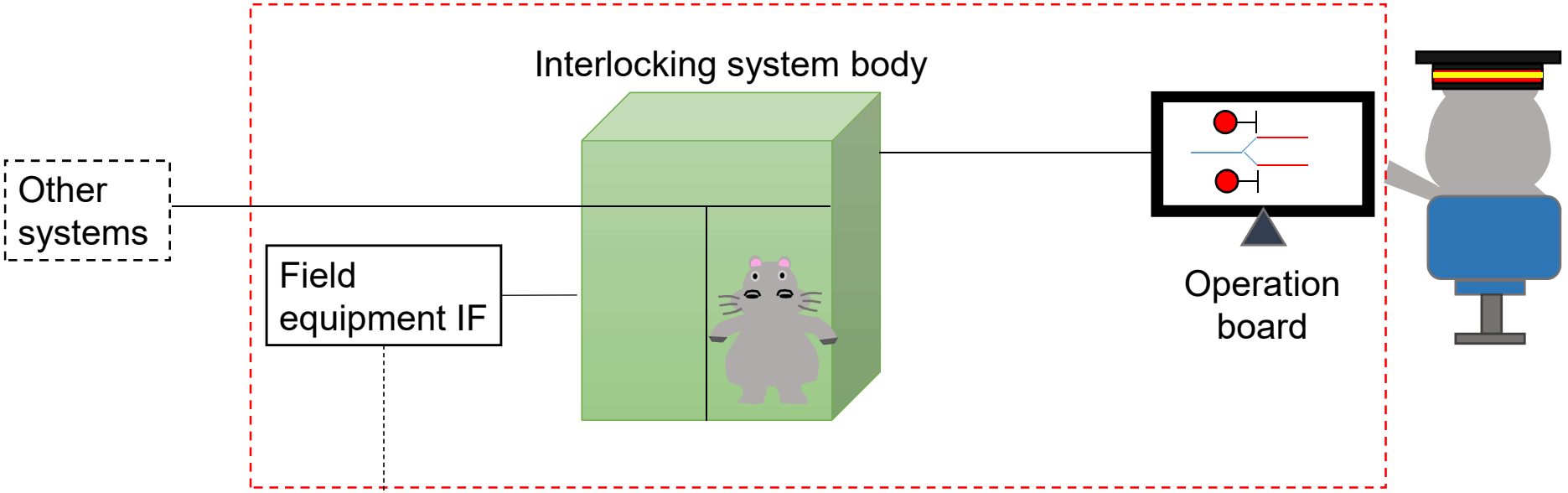
IEC 62278 6.2.3.1 b)
EN 50126-1 7.3.2.1 b)

Aren't these the one that comes to mind as a boundary?



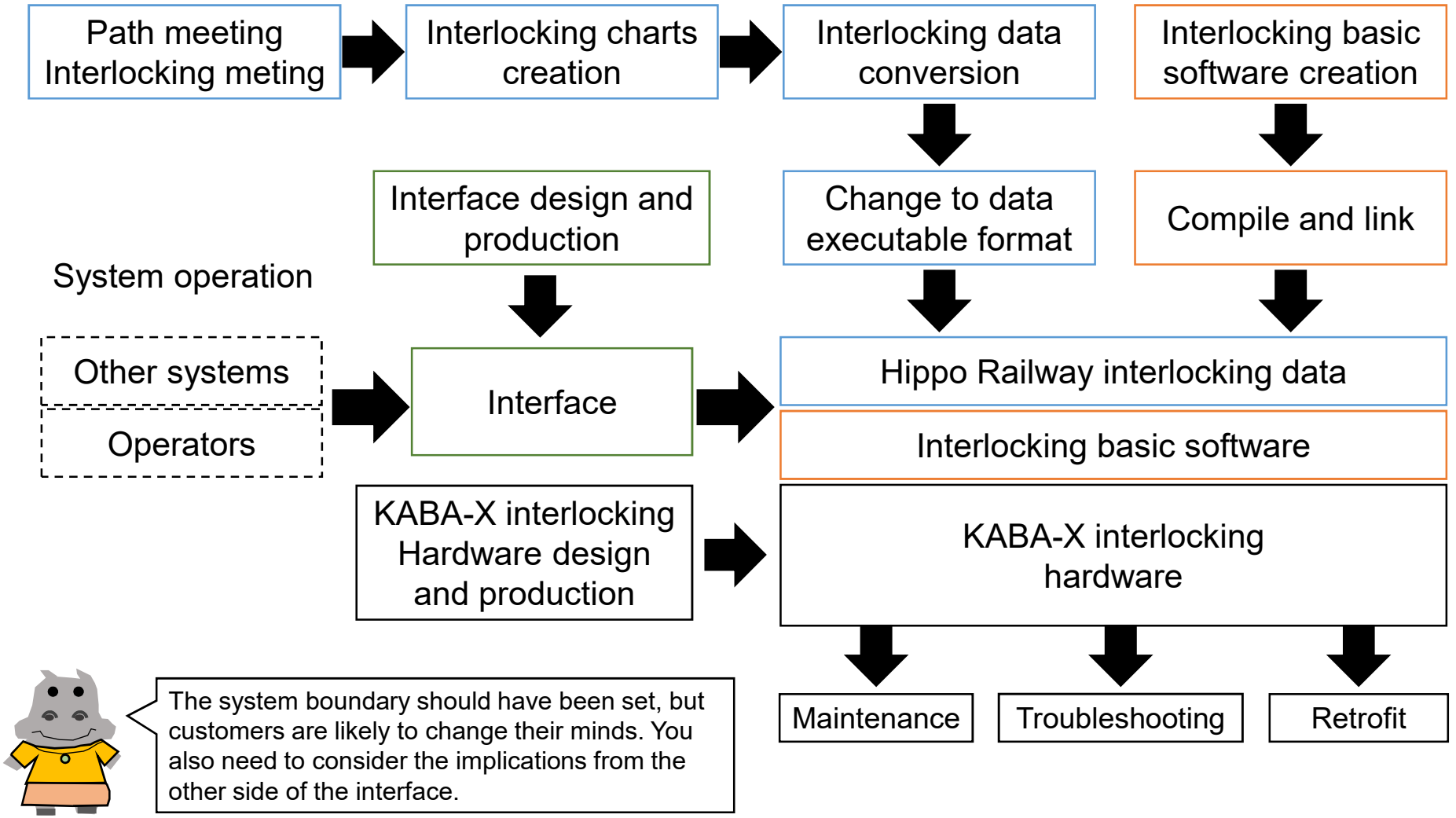
2-3 What about the boundary?

IEC 62278 6.2.3.1 b)
EN 50126-1 7.3.2.1 b)



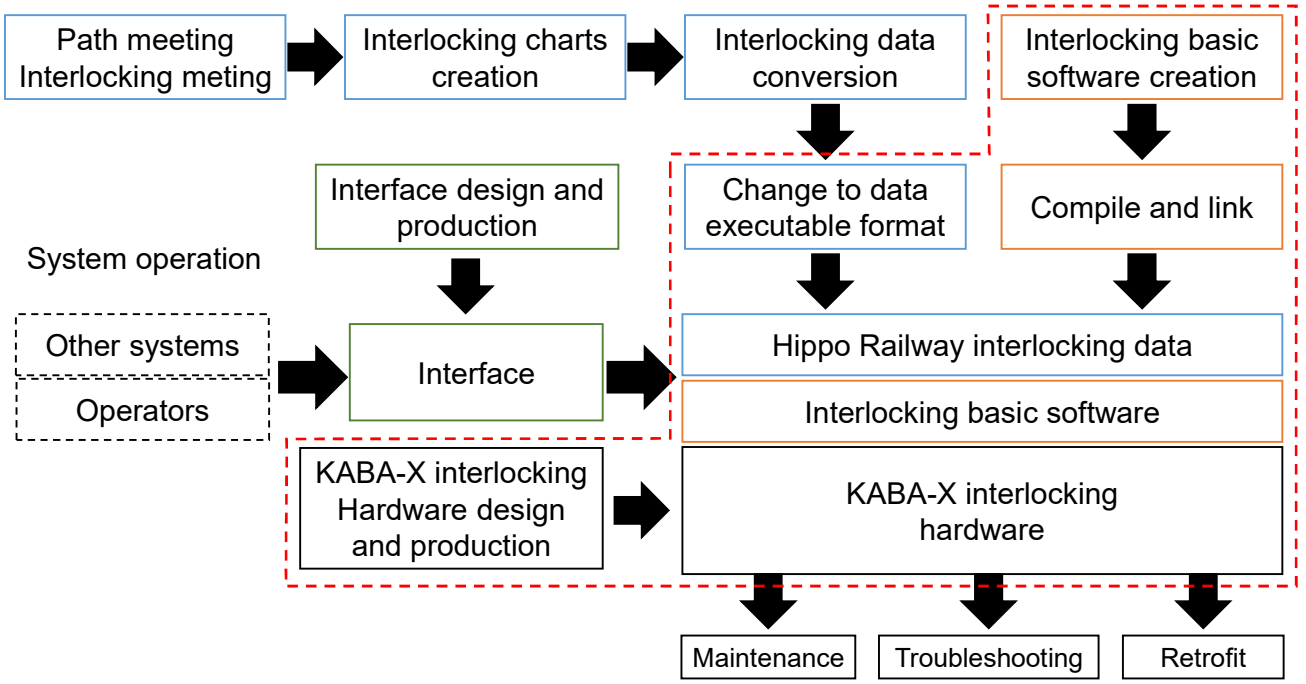
2-3 Various boundaries

IEC 62278 6.2.3.1 b)
EN 50126-1 7.3.2.1 b)



2-3 Determine the division of responsibilities

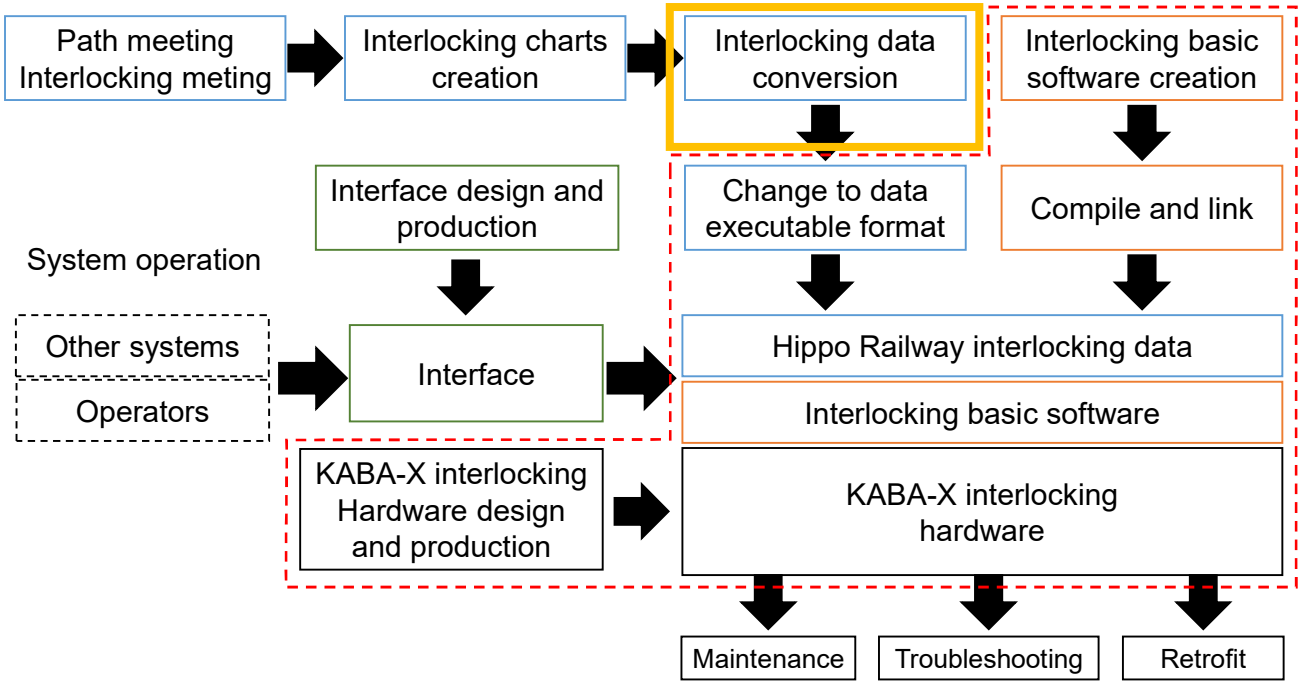
IEC 62278 6.2.3.1 b)
EN 50126-1 7.3.2.1 b)



Obviously, we are in charge of the area inside the red dotted line, but what about the others? We don't think we are in charge of anything other than maintenance, troubleshooting, and retrofit, but there may be nothing clear.
The interface is case by case. They might use the interface by other systems.
The system operation would be handled by Hippo Railway.
Also, the boundaries are not clear between what humans do and what machines do.

2-3 Determine the division of responsibilities

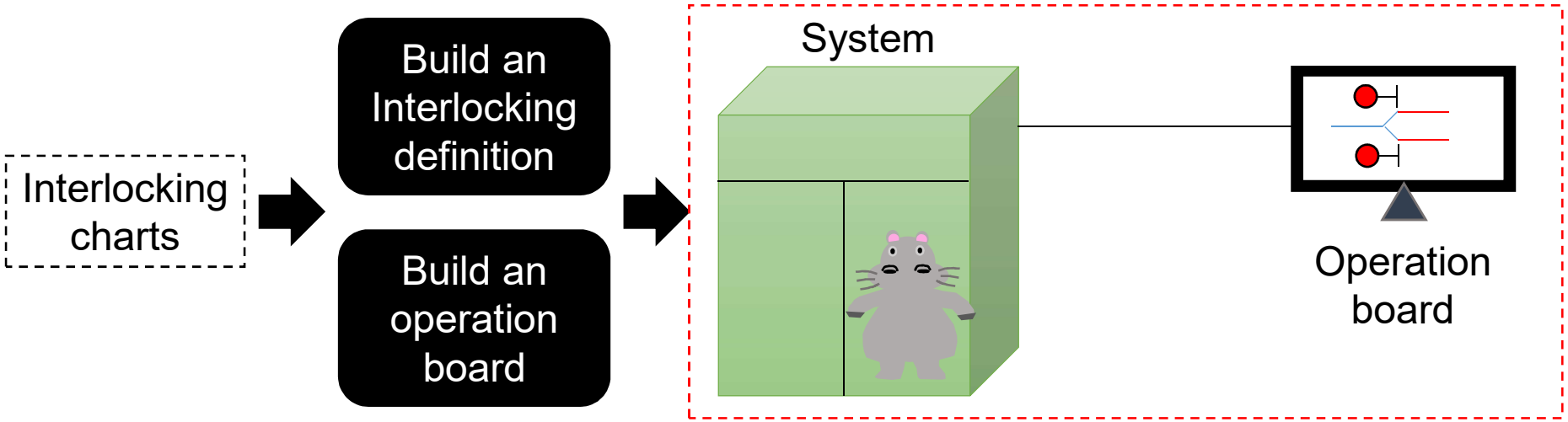
IEC 62278 6.2.3.1 b)
EN 50126-1 7.3.2.1 b)



If Hippo Corp. undertakes interlocking data conversion, will the interface change? The interface of the system itself does not seem to change. But the role seems to change. It can be done manually or by machines?

2-3 Consider these boundaries

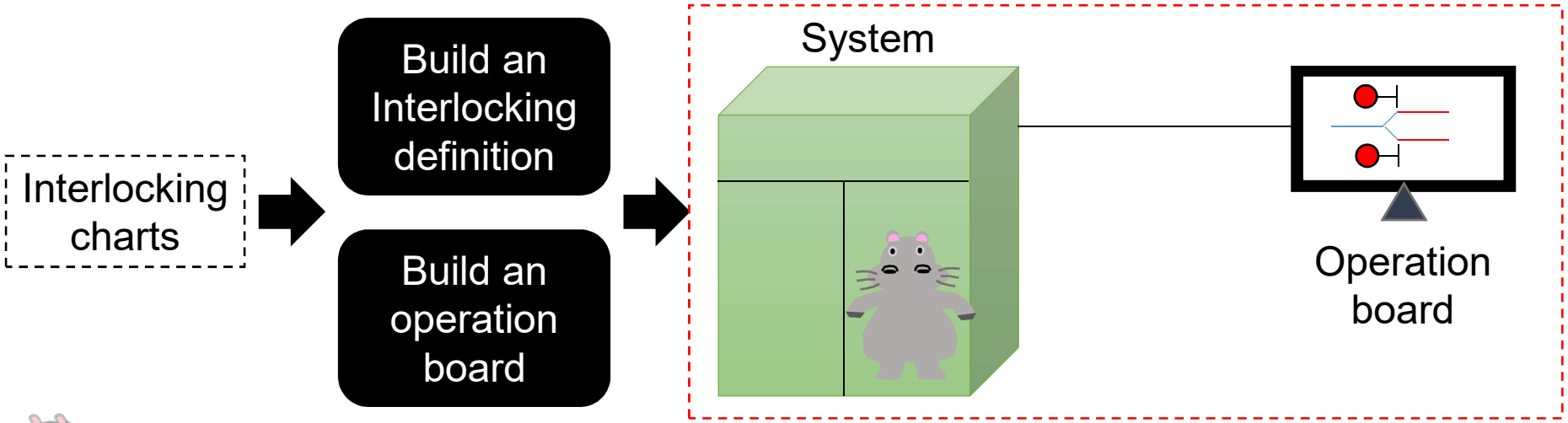
IEC 62278 6.2.3.1 b)
EN 50126-1 7.3.2.1 b)



The required safety requirement level changes depending on the mutual influence of whether this configuration is done manually, by machines, in Hippo Corp., or by another company. I understand that the boundaries and requirements of the system are very important.

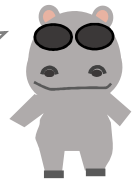
2-3 Consider these boundaries

IEC 62278 6.2.3.1 b)
EN 50126-1 7.3.2.1 b)



What if the interlocking definition is vague and of no practical use? I feel like it's dangerous.

In that case, the president will be dismissed. If this interlocking definition was built by Piggy Corp. with poor quality, we might suffer a disadvantage.



Do something, Kabao!

……

2-1 Define the system objective

2-2 Define the system mission profile, that is, numerical targets

2-3 In preparation for RAMS analysis

2-3-1 Define the system boundary

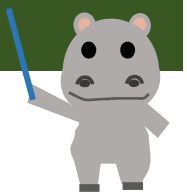
2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system

2-3-3 Define the scope of system hazard analysis

2-4 Evaluate the items that may affect RAM and grasp a feeling for them

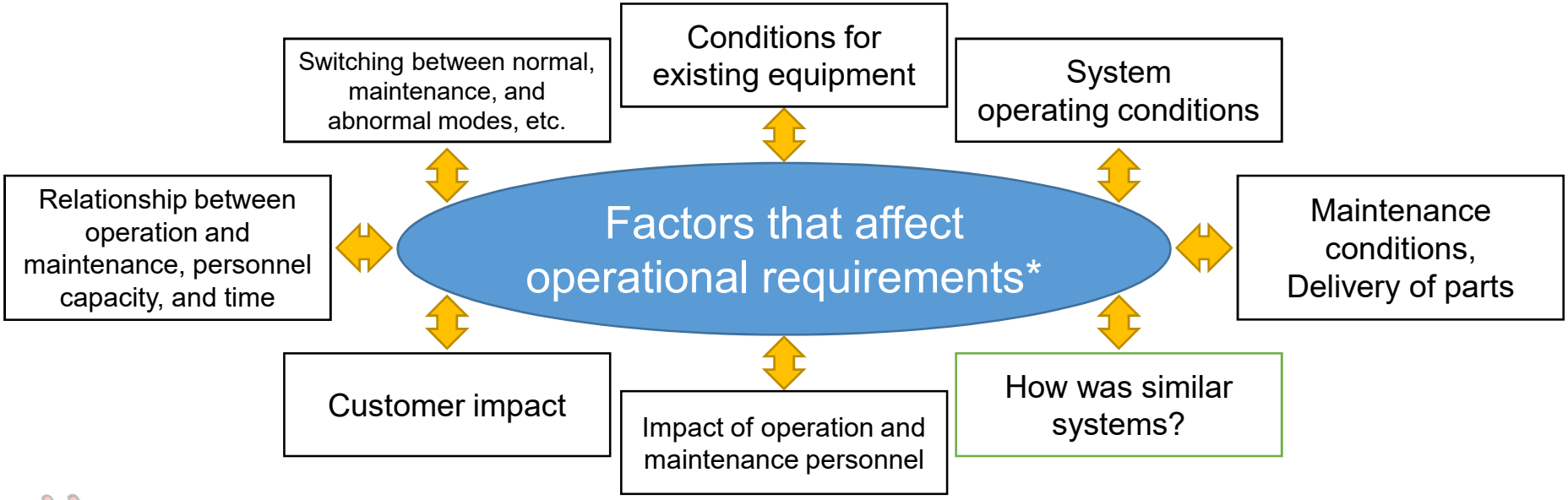
2-5 Detect hazards and grasp a feeling for them

2-6 Establish the initial RAM Plan and Safety Plan for the system



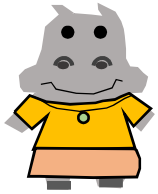
2-3 Operational requirements that affect the system

IEC 62278 6.2.3.1 c)
EN 50126-1 7.3.2.1 c)



It's similar to the scope of consideration of company management.
I'm counting on you to do a great job, Kabao. If you double your restraint time and make up for it, we can double the scale of our corporation's management.

I feel thin. I will quit my job.



If you clarify these clauses, you will be able to determine the operational requirements and see the difference from the system you are currently thinking about.

* IEC 62278 Application conditions
EN 50126 Operational requirements

2-3 Operational requirements that affect the system

IEC 62278 6.2.3.1 c)
EN 50126-1 7.3.2.1 c)

The interlocking system basically operates continuously until it is replaced.

Well, that's right. (Absolutely bad things happen...)

This means that Hippo Corp. will take responsibility if it breaks down by the time we replace it.

We can't guarantee that. (What's this old man saying?)

In reality, it is used for maintenance trains even in the middle of the night

Switching between normal, maintenance, and abnormal modes, etc.

Conditions for existing equipment

System operating conditions

So, it must be completely no-maintenance and non-stop for 20 years!

Am I wrong?

Relationship between operation and maintenance, personnel capacity, and time

Most operators do not prefer to work only at night

Operational requirements*
= operates 24 hours a day for 20 years

Maintenance conditions, Delivery of parts

It's unnecessary because it is a premise that the system will not break

Customer impact

Trains cannot be stopped in the middle of the day

Impact of operation and maintenance personnel

It is unknown when the special trains will run

How was similar systems?

It has always been the case

* IEC 62278 Application conditions
EN 50126 Operational requirements

2-3 Operational requirements that affect the system

IEC 62278 6.2.3.1 c)
EN 50126-1 7.3.2.1 c)

I've got it. I let our technology team do it with the feeling of jumping off the stage of Kiyomizu.

Your answer was what I expected, Kabao. You are an example of a good salesperson.

We are also doing business. I'm very sorry, but is it okay to charge an additional 200%?

What are you talking about? It's cheaper to do the inspection every three years as before.

Thank you for your understanding. You are an example of Kansai people.

After all, the operational requirements that affect the system have been decided after comprehensively taking into consideration the matters such as costs, labor, and safety, depending on whether to allocate more to the machine requirements or to the human resources.

We should keep a record of this in accordance with the RAMS standard so that we can better understand why we made this decision later, and it will be useful when reviewing.

2-1 Define the system objective

2-2 Define the system mission profile, that is, numerical targets

2-3 In preparation for RAMS analysis

2-3-1 Define the system boundary

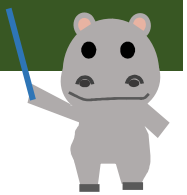
2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system

2-3-3 Define the scope of system hazard analysis

2-4 Evaluate the items that may affect RAM and grasp a feeling for them

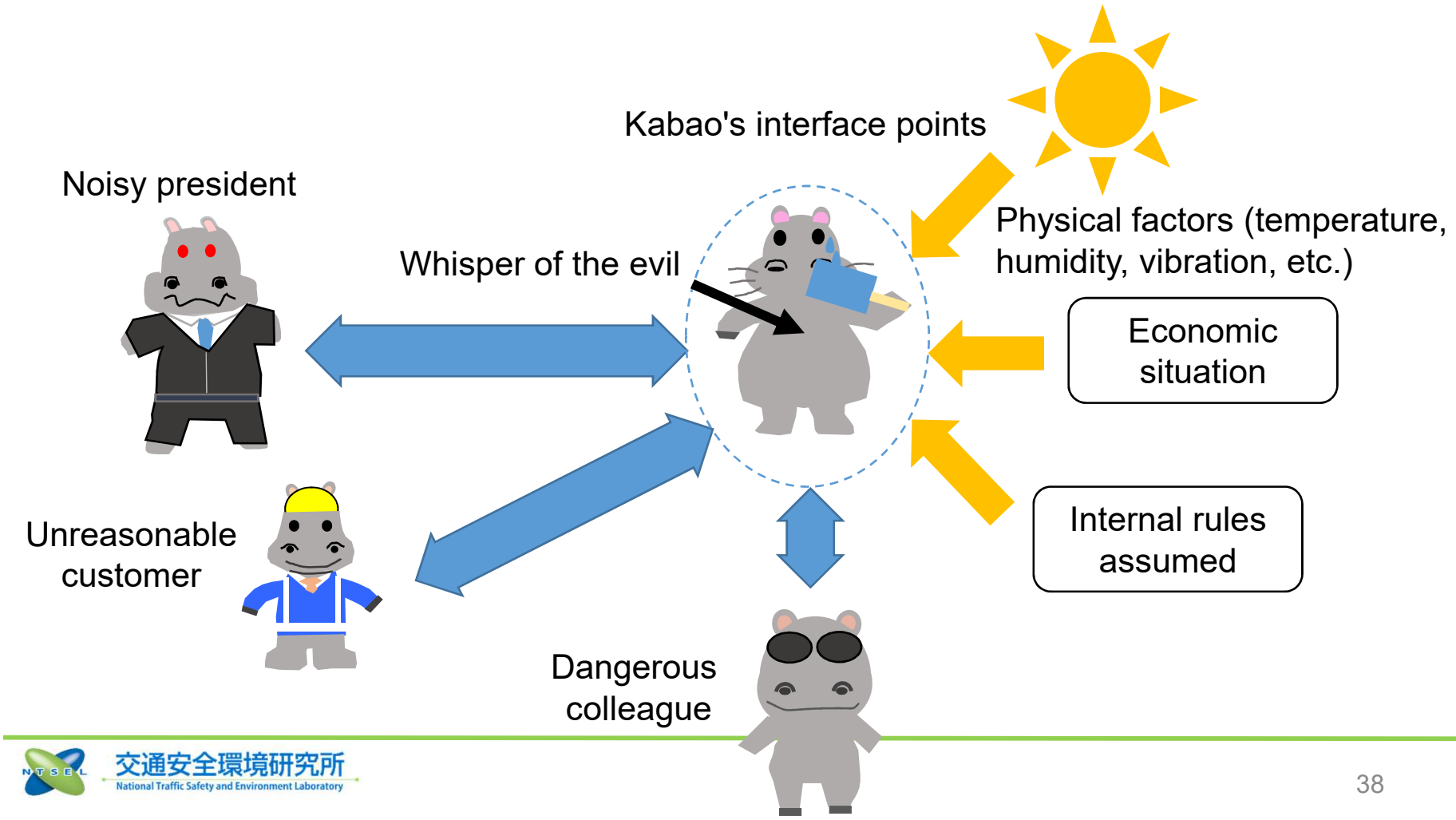
2-5 Detect hazards and grasp a feeling for them

2-6 Establish the initial RAM Plan and Safety Plan for the system



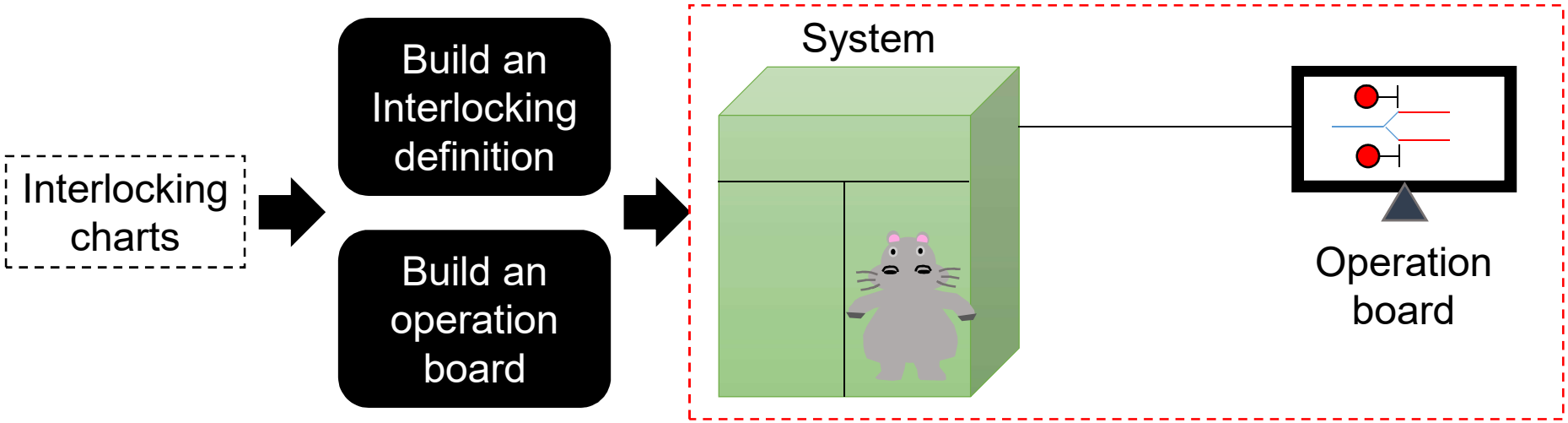
2-3 Define the scope of hazard / risk analysis

Determine the scope of hazard that causes Kabao to get fired to conduct risk analysis



IEC 62278 6.2.3.1 d)

2-3 Define the scope of hazard / risk analysis



What should we do with this black part?

2-3 Define the scope of hazard / risk analysis and consider whether to target the system

IEC 62278 6.2.3.1 d)
IEC 62278 6.1.3.2 b)

From the president's point of view, before designing, we have to think about where the safety might be adversely affected and decide how much we will do for it. Below are plans A, B and C.

Plan A

Since we are not in charge of data creation, we Hippo Corp. will not take any responsibility for malfunction caused by data error. If the data is incorrect, the interlocking operation will not work properly and may have a life-threatening effect.

Let Kabao say this. Somehow, I have a feeling that we might lose the order.

Such safe use conditions are called Safety Related Application Conditions (SRAC).

Plan B

Please leave the data creation to us. We will make equipment that automatically converts from the interlocking chart.

The safety of the converter needs to be considered. Can we do it?

Plan C

We will strengthen the data creation system and create data manually (by hippos' legs?).

I feel like Hippo Railway will take advantage of the situation. It's troublesome.

EN50126-1 7.3.2.1 e)

2-3 Know the difference

To be honest, it's rare to build a system from scratch.
We want to make use of what we have done so far and decide the ranges of mission profile and analysis only for the difference.

e) identification of the system and related documents, including assumptions made about particular functions or subsystems that are different from an existing reference version, explicitly stating and justifying the deviations.

In identifying the system and clarifying the related materials, EN 50126 is supposed to include how it differs from the existing one.
(It is not specified in IEC standard.)

After all, "a man who understands the difference" is important.

No one knows about such old coffee TV commercials.

2-1 Define the system objective

2-2 Define the system mission profile, that is, numerical targets

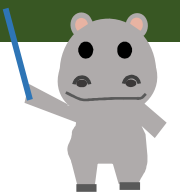
2-3 In preparation for RAMS analysis

- 2-3-1 Define the system boundary
- 2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system
- 2-3-3 Define the scope of system hazard analysis

2-4 Evaluate the items that may affect RAM and grasp a feeling for them

2-5 Detect hazards and grasp a feeling for them

2-6 Establish the initial RAM Plan and Safety Plan for the system



IEC 62278 6.2.3.2 a)

2-4,5 Grasp the risky part of the system in RAMS

From the president's point of view, I would like to grasp in advance how much failure the system can tolerate, and then, think about estimation, construction period, staffing, and safety.

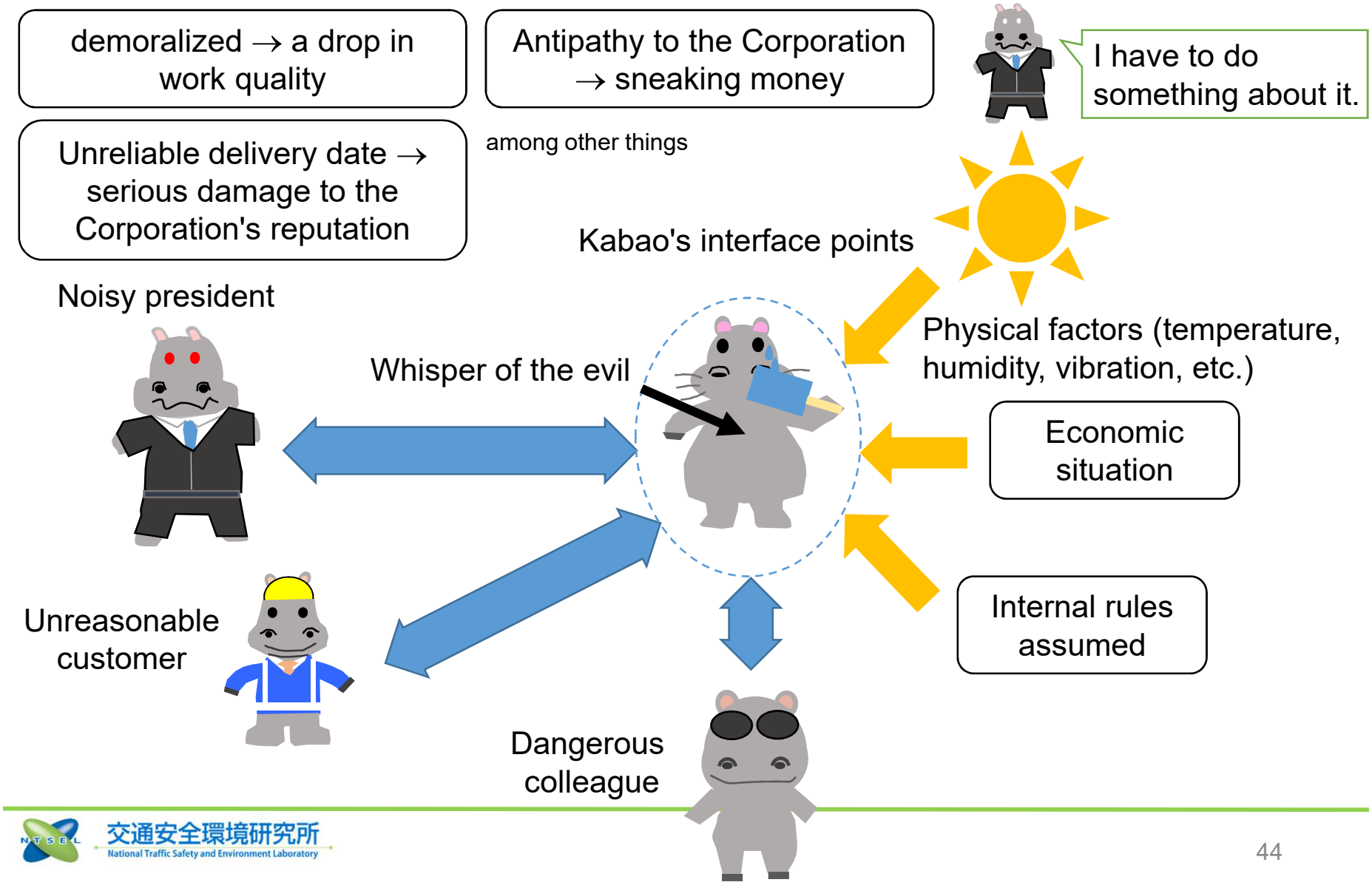
Well, that's right for those who are responsible for management. You have to spend a lot of money and time on the risky subject. This is called preliminary RAM analysis, and regarding safety, it is called preliminary hazard analysis. It's very important.

Hey, Kabao, did you understand? It's hazard prediction. Get some money from Hippo Railway for this.

There is no sweet company that will give you money by saying, "Please give us money because it's risky". We definitely have to say the reason properly.

2-4,5 Consider what unfavorable behavior Kabao will do in this situation.

IEC 62278 6.2.3.2 a)



IEC 62278 6.2.3.2 a), b)

2-4,5 Consider the events that affect RAMS

Data accuracy
Unauthorized access

Restricted investment amount
Culture of safety

Adverse human effects

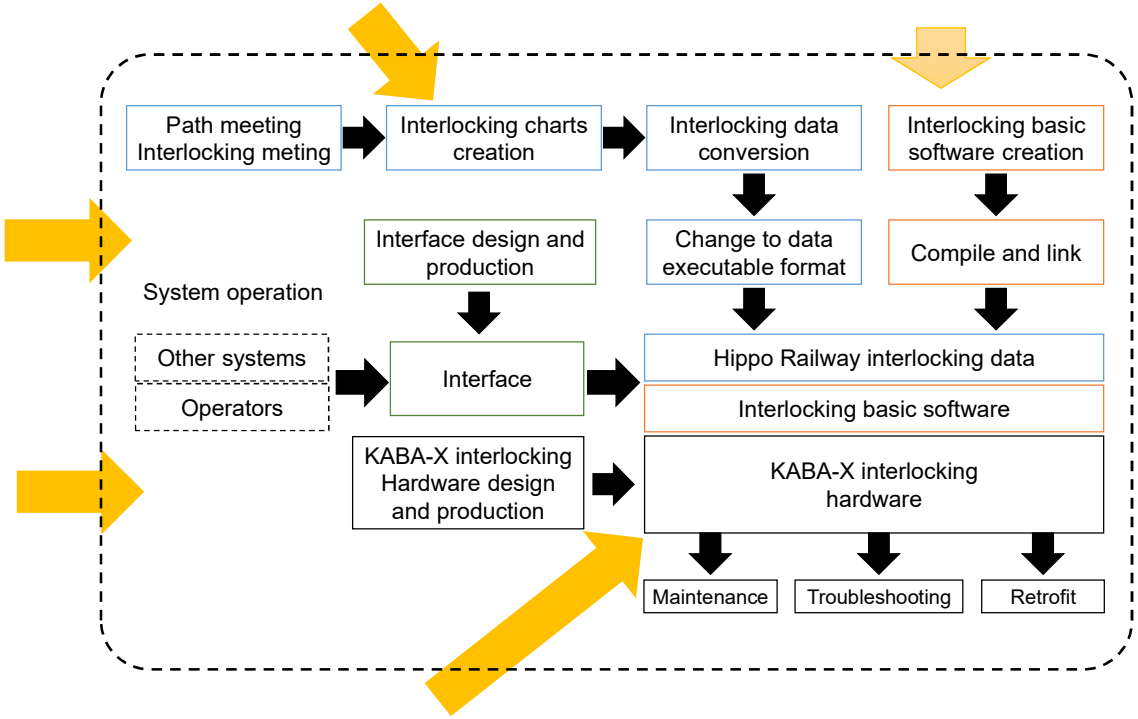
Noisy president

Geek who doesn't make according to specifications

Unreasonable customer

Sales staff who forgets to say the important thing

Adverse effects from other systems / hacking



Physical factors (temperature, humidity, vibration, etc.)

IEC 62278 6.2.3.2 a)

2-4,5 How do you analyze it even though the contents have not been decided?

From the president's point of view, it's natural that I want to grasp the things that are likely to pose various risks.

But the contents of the system have not been decided yet. How do you analyze it? Isn't risk analysis the phase 3?

If you feel motivated, you can do anything.

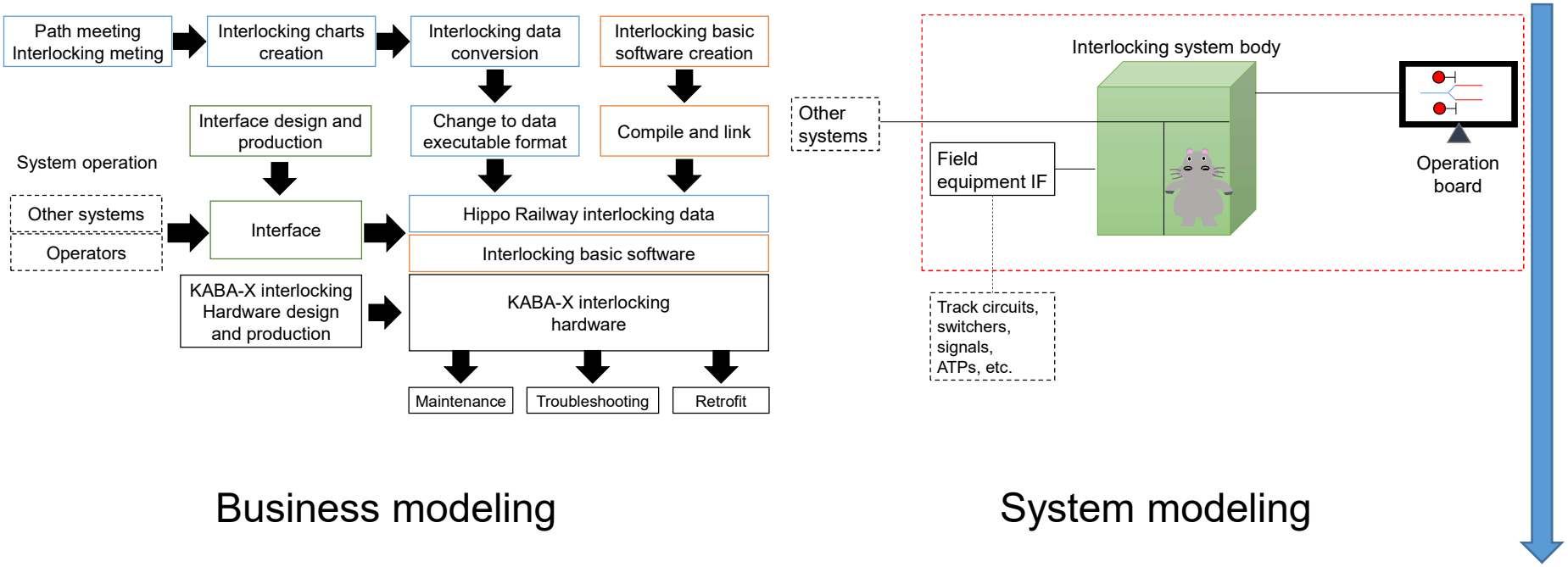
It's nonsense!

So, what should we really do?

IEC 62278 6.2.3.2 a)

2-4,5 How about thinking this way?

Model business and system as far as we know



Business modeling

System modeling

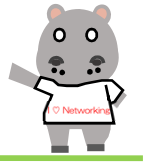
Imagine what happens if the information order / flow is wrong, the information does not come, or is delayed

2-4,5 Summarize the affected events, their consequences, and the need for action

IEC 62278 6.2.3.2 a)

Events	Impact	Adverse effects	Necessity of measures	ID
The interlocking chart is incorrect	Safety	A false signal display Conversion of different switchers	Necessary because it can lead to loss of life	XXX-001
	Reliability	Signal is not shown	Necessary due to large transportation impact	XXX-002
The interlocking data cannot be created	Reliability	Cannot operate	Necessary due to the impact on the construction schedule	XXX-003
The interlocking data is delayed	Reliability	Delayed delivery	Necessary due to the impact on the construction schedule	XXX-004
The interlocking data is incorrect	Safety	A false signal display Conversion of different switchers	Necessary because it can lead to loss of life	XXX-005
The order of creating interlocking charts and interlocking data is different	Safety	A false signal display due to different versions, etc.	Necessary because it can lead to loss of life	XXX-006
The rest is omitted.				

I was paying attention only to the unsafe transition due to a system failure, but it seems that it is not the only problem.



2-1 Define the system objective

2-2 Define the system mission profile, that is, numerical targets

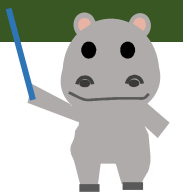
2-3 In preparation for RAMS analysis

- 2-3-1 Define the system boundary
- 2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system
- 2-3-3 Define the scope of system hazard analysis

2-4 Evaluate the items that may affect RAM and grasp a feeling for them

2-5 Detect hazards and grasp a feeling for them

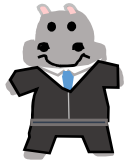
2-6 Establish the initial RAM Plan and Safety Plan for the system



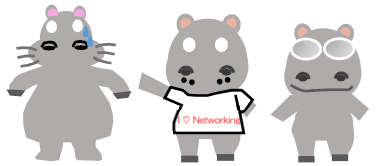
I will explain about the RAM Plan.

IEC 62278 6.2.3.3, 6.2.3.4
EN 50126-1 7.3.2.2, 7.3.2.3

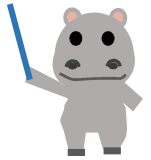
2-6 From the discussions so far



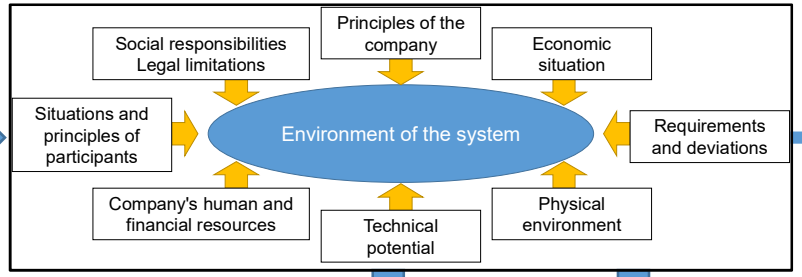
Hey, you guys! We had a lot of discussions, but if we don't sort it out, my head is going to explode. I wonder if it's time to decide what kind of policy we need. It seems like you don't want to do it.



At this phase, we are supposed to put together a plan related to RAMS.

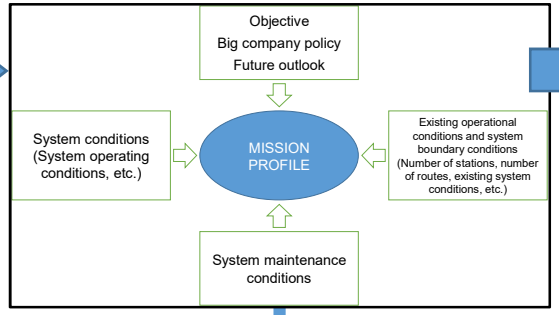


Objective (function, etc.)

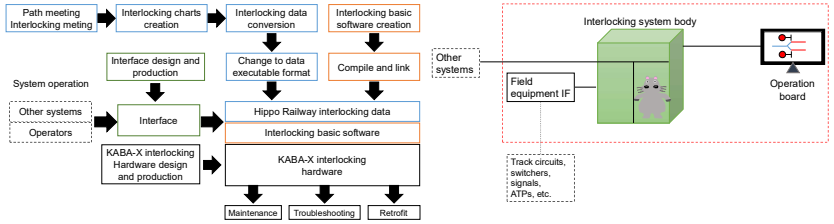


Understanding the surrounding situation

Clarification of mission



Clarification of the scope of risk analysis



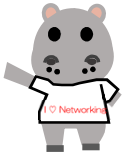
Business modeling

System modeling

RAMS related plans

EN 50126-1 7.3.2.2

2-6 What is a RAM Plan*?



The president told me to do it, but what should I write?

Write about management planning, and reliability, availability, and maintainability analyses and their planning.

That president would say "what I mean, that is, management," and is that really okay?

I am the final decision-maker! I'm the CEO. I will decide. Hippos only need one boss.

* In IEC 62278, the RAM Plan is not defined, but is defined as the RAM Programme in phase 4. However, as long as the Safety Plan, which is a plan for safety, is formulated in phase 2, it seems natural to formulate the RAM Plan in the same way, so I brought it here in response to EN 50126. IEC 62278 decides to create a RAMS policy (6.2.3.3) that is consistent with the Safety Plan before developing the RAM Programme.

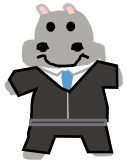
2-6 What is a Safety Plan?

IEC62278 6.2.3.4
EN 50126-1 7.3.2.3

I have a sharp intuition. A Safety Plan is a safe version of the RAM Plan. Am I right?

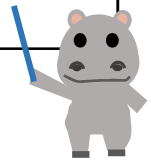
(I think it's strange if you don't understand that.)
You are right! You are amazing!

So, what kind of safety plans does Hippo Corp. have?



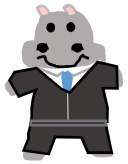
I've been told by Hippo Railway to prepare it every time, but it's hard to get it right. It's about time to make something like "This is the safety of Hippo Corp.", but I don't know what to write.

IEC 62278 defines the Safety Plan as follows:
documented set of time scheduled activities, resources and events serving to implement the organisational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project



EN 50126-1 Annex A. 3

2-6 What should we write specifically?



As the CEO, I want to give specific instructions to my subordinates.

I don't want to say too much, but it's in EN 50126-1 Table A.1.

1. Pre-Acquisition
   - Evaluate RAMS targets of specific application
2. Feasibility Study
   - Evaluate RAMS requirements
   - Evaluate past data and experience of RAMS
   - Identify influence on Safety imposed by specific application
3. Invitation for Tenders
   - Perform preliminary RAMS analysis (Worst case)
   - Apportion system RAMS requirements
   - Perform system hazard & safety risk analysis
   - Perform RAM related risk analysis
   - Prepare for future RAMS data assessment
   - Clause by clause comments concerning RAMS
   - (The following is omitted.)

It lists things that need to be planned as above.

EN 50126-1 Annex A. 3

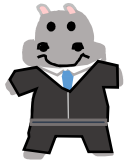
2-6 Points to keep in mind for railway operators

In my case as a railway operator, what should I pay attention to?

How about just assuming the opposite of the role in the material above?

1. Pre-Acquisition → Concept stage in railway operators
   - Evaluate RAMS targets of specific application
   - → Determine RAMS targets of the specific application system
2. Feasibility Study → System definition and terms of use
   - Evaluate RAMS requirements → Examine the validity of mission profile from RAMS perspective
   - Evaluate past data and experience of RAMS
   - → Extract survey targets and survey contents of similar systems
   - Identify influence on Safety imposed by specific application
   - → Extract survey targets and survey contents of existing systems
3. Invitation for Tenders
   - Manufacturer evaluation method
4. After contract
   - Evaluation method of manufacturer's management system
   - Safety analysis method and evaluation method
   - Maintenance method
   - Acceptance and testing system
   - Refurbishment and replacement plans

2-6 What about the structure or reference materials?



When it comes to planning, we have to think about the structure and the documents we have to prepare. It should be in the RAMS standard.

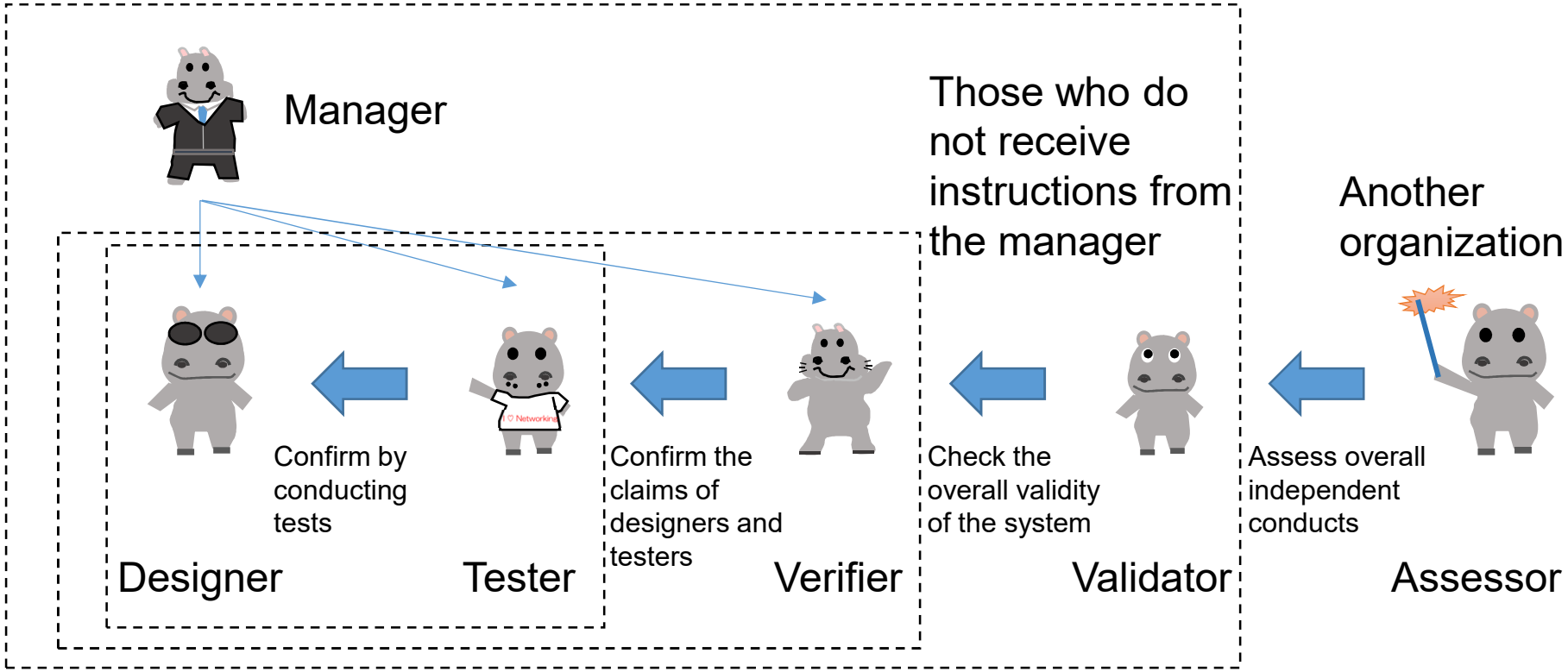
I don't want to say too much, but IEC 62278 doesn't cover that much.

That means I have to make the hacking Hippo or Kabami, the executive engineer, think about it. "You guys, think about the structure and the documents."

Please refer to each technical standard.

2-6 Example of the structure

IEC 62425 5.3.3
EN 50126-2 7.2



Establish an appropriate system, necessary abilities, and education in a form that meets safety levels, quality control regulations and standards. IEC 62278 has no example of the structure that is often defined by referring to other standards.

2-6 Example of reference documents to prepare (Mainly hardware safety)

IEC 62278 6.2.3.4 e), g)
EN 50126-1 7.3.2.3 e)
IEC 62425 5.3.2
IEC 62279 Ed.2 5.3

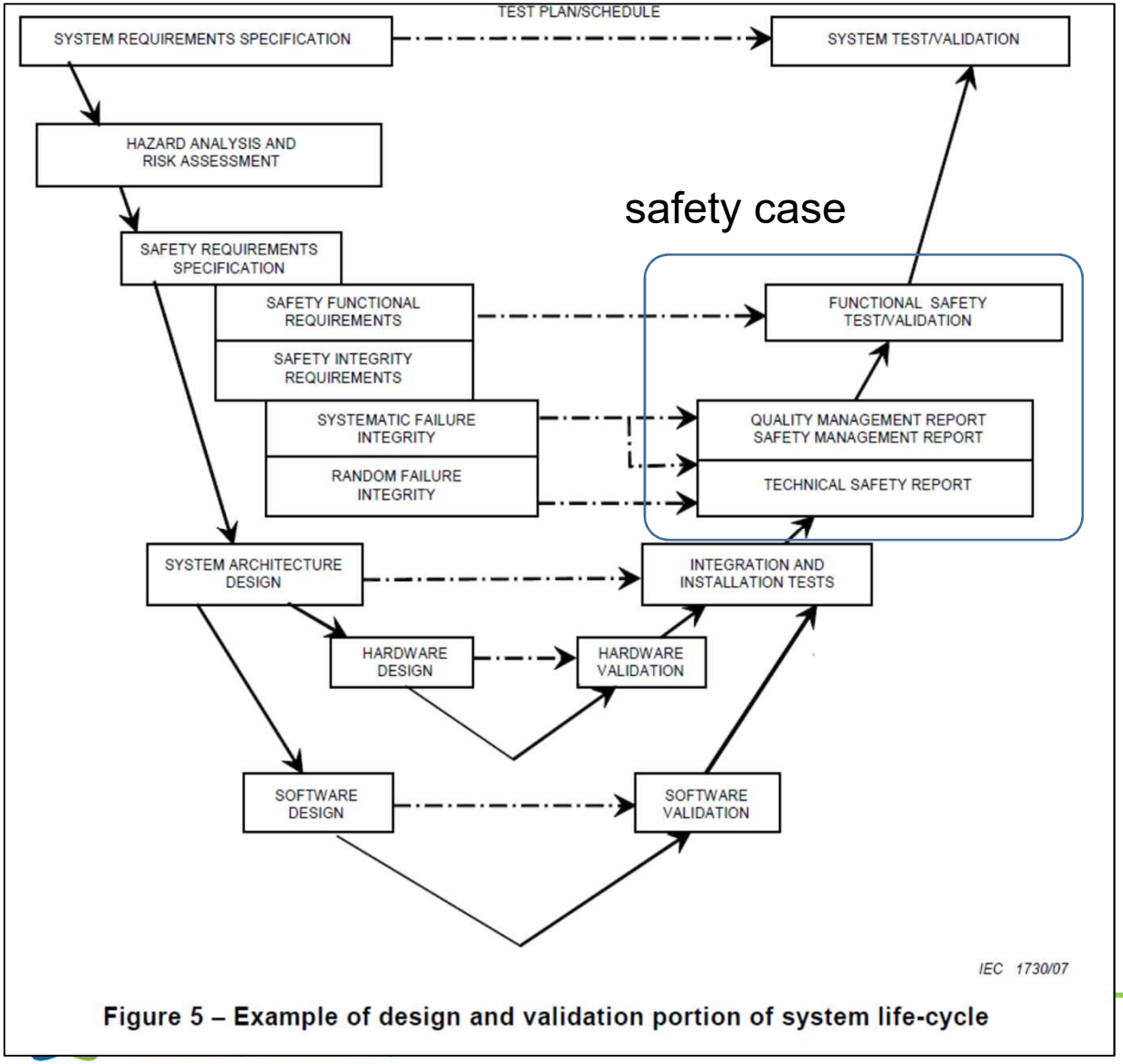
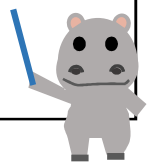


Figure 5 – Example of design and validation portion of system life-cycle

It shows the items to be performed from system requirements specification to comprehensive tests in IEC 62425.
At each phase, it is stated that the requirements / requirements verification, test plan / test plan verification, test implementation / its verification, and the creation of a safety case that is a summary of safety.



2-6 Example of reference documents to prepare (Mainly software safety)

IEC 62278 6.2.3.4 e), g)
EN 50126-1 7.3.2.3 e)
IEC 62425 5.3.2
IEC 62279 Ed.2 5.3

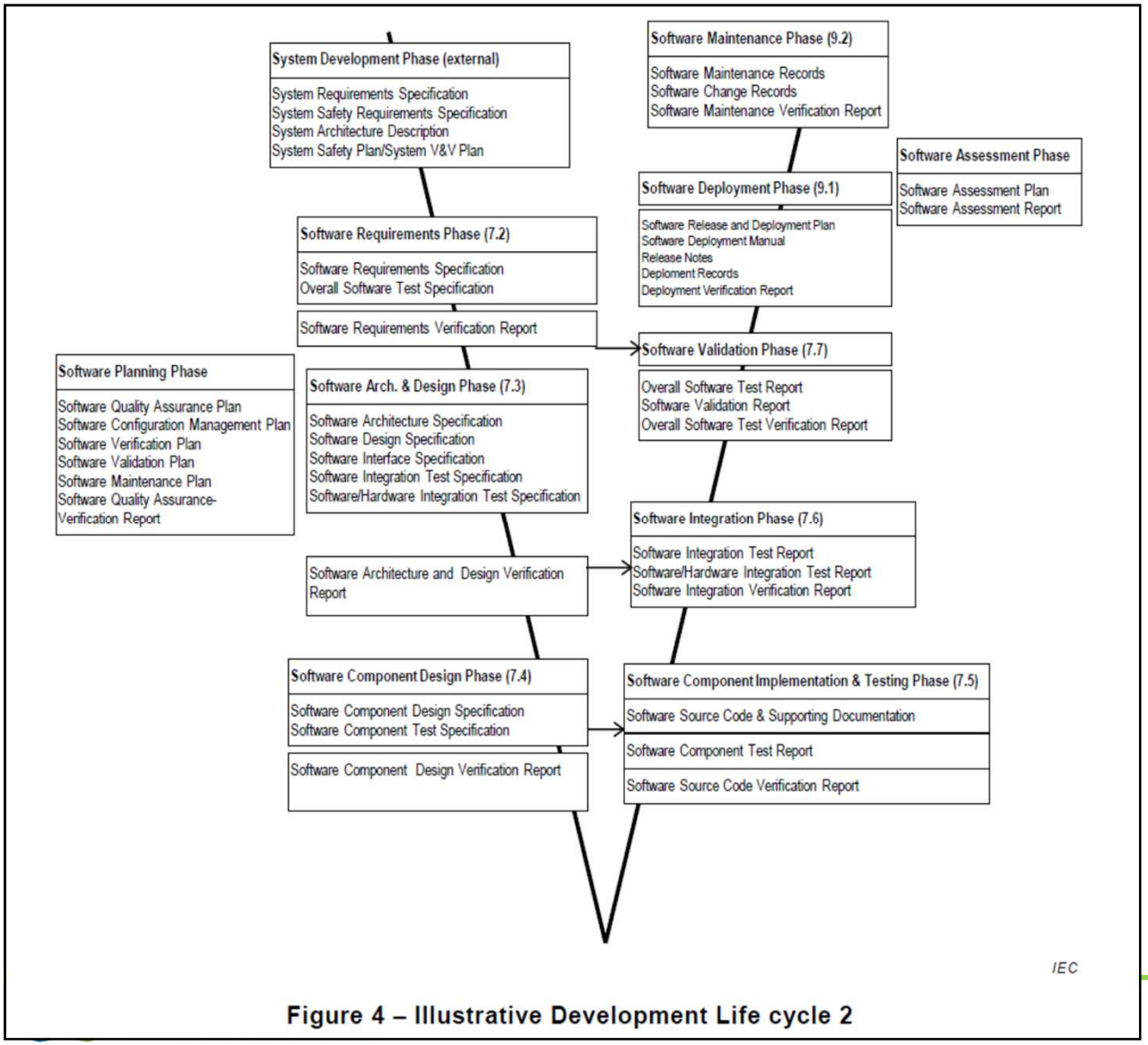
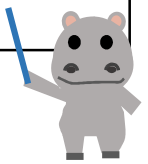


Figure 4 – Illustrative Development Life cycle 2

It shows the items to be performed from system requirements specification to maintenance from the viewpoint of software in IEC 62279.
It states what documents are needed at each phase.



Conclusion

2-1 Define the system objective

Objectives are not clearly stated in the standard, but define the purpose of the system.

2-2 Define the system mission profile, that is, numerical targets

It cannot be made without numerical values that achieve the purpose, and it cannot be analyzed and evaluated.

2-3 In preparation for RAMS analysis

2-3-1 Define the system boundary

2-3-2 Establish the scope of operational requirements (operation, maintenance, external equipment, etc.) influencing the characteristics of the system

2-3-3 Define the scope of system hazard analysis

If you do not decide how far you will be in charge of the system, you will not be able to analyze and evaluate it.

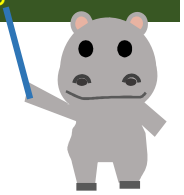
2-4 Evaluate the items that may affect RAM and grasp a feeling for them

2-5 Detect hazards and grasp a feeling for them

Grasp the emphasis when building the system. Also, get a rough idea of the safety features.

2-6 Establish the initial RAM Plan and Safety Plan for the system

You can't do anything without a plan. Formulate the necessary plan according to the purpose of the system, numerical goals, surrounding background, scope of responsibility, safety functions, etc.



Next time preview

- Finally, I will explain about safety analysis.