Defining the specifications

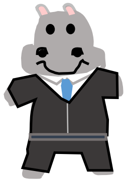
—Both specifications and confirmation are important—

(RAMS Phase 4)

Mori Takashi

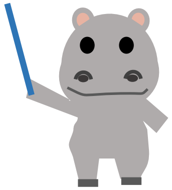
National Traffic, Safety and Environment Laboratory,
National Agency for Automobile and Land Transport Technology, Japan

Actors

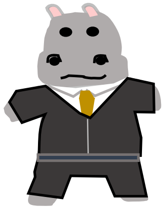


President of Hippo Corp.
Motto: Technology and inspiration

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



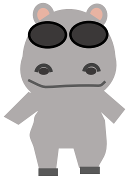
anonymous Hippo
Unknown Consultant
Motto: Knowledge is power!



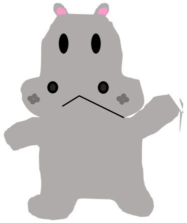
Prof. Ohkaba
Motto: Software must be in good order.

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

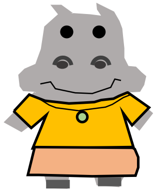
Otakaba
Engineer, Hippo Corp.
Motto: No fun, No engineering!



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!"

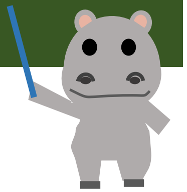


Kabami
Executive Engineer, Hippo Corp.
Motto: Let's work together.

What is required at this phase

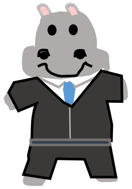
4-1 Specify the overall RAMS requirements for the system

4-2 Specify the overall acceptance criteria for RAMS for the system

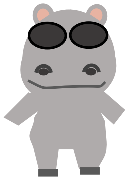


IEC 62278 6.4.3.1
EN 50126-1 7.5.2

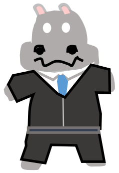
4-1 What are system requirements?



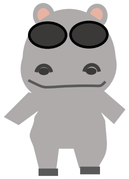
Folks, we have completed the risk analysis, what next?



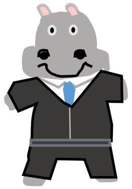
Then, I ask, what was the risk analysis for?



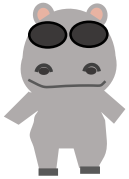
It's about... knowing the risks and using them to run the business!



That is not an explanation. If you know what are hazards, why don't you make use of the system's requirements to find out what you need to do?



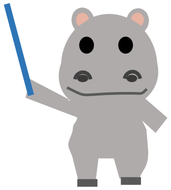
You know exactly what I mean. That's what I wanted to say!



(It's an absolute lie. Lying eyes.)

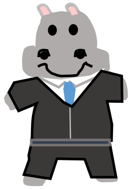
4-1 What are RAMS requirements and system requirements?

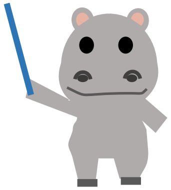
IEC 62278 6.4.3.1
EN 50126-1 7.5.2



What are the system requirements for the Hippo Corp. interlocking system "KABA-X Interlocking"?

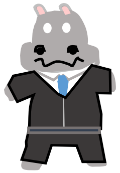
Well, Its system is to switch switchers and present the signals according to the station master's operation. In case of wrong input, the order is invalidated.

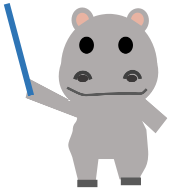




Is there anything else? Can you make that system with that?

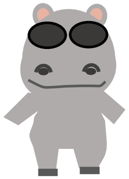
Think and act for yourself – that's Hippo Corp. We don't want staff who have to listen to everything before they work.





It's nice to be free. But can engineers design with it?

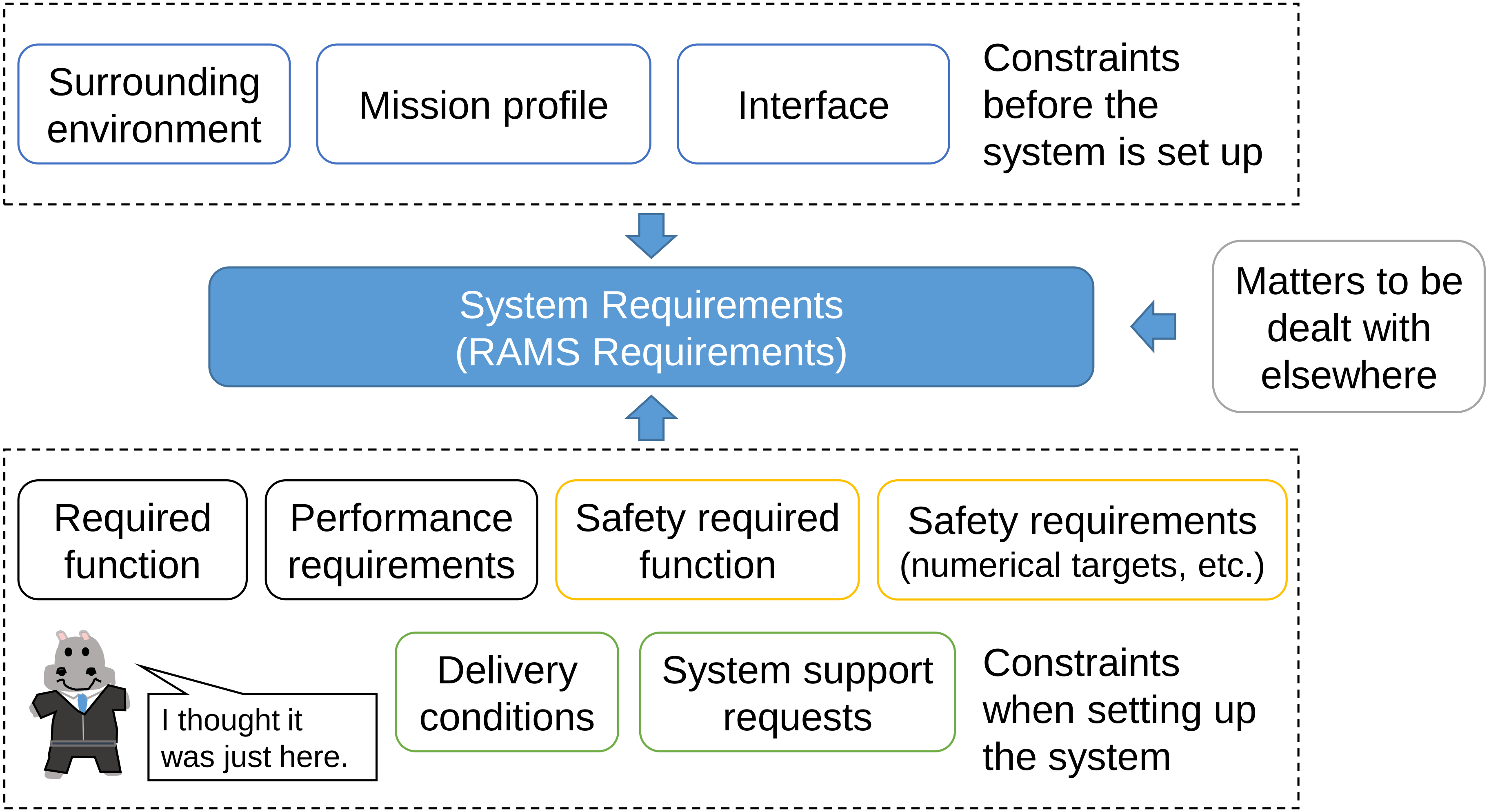
I'll build what I think is the best! If the boss says I'm autonomous, I'm not responsible for the budget, but I'll spend as much money as I want to design it.



4-1 What are RAMS requirements and system requirements?

IEC 62278 6.4.3.1

EN 50126-1 7.5.2



Surrounding environment

Mission profile

Interface

Constraints before the system is set up

System Requirements (RAMS Requirements)

Matters to be dealt with elsewhere

Required function

Performance requirements

Safety required function

Safety requirements (numerical targets, etc.)

I thought it was just here.

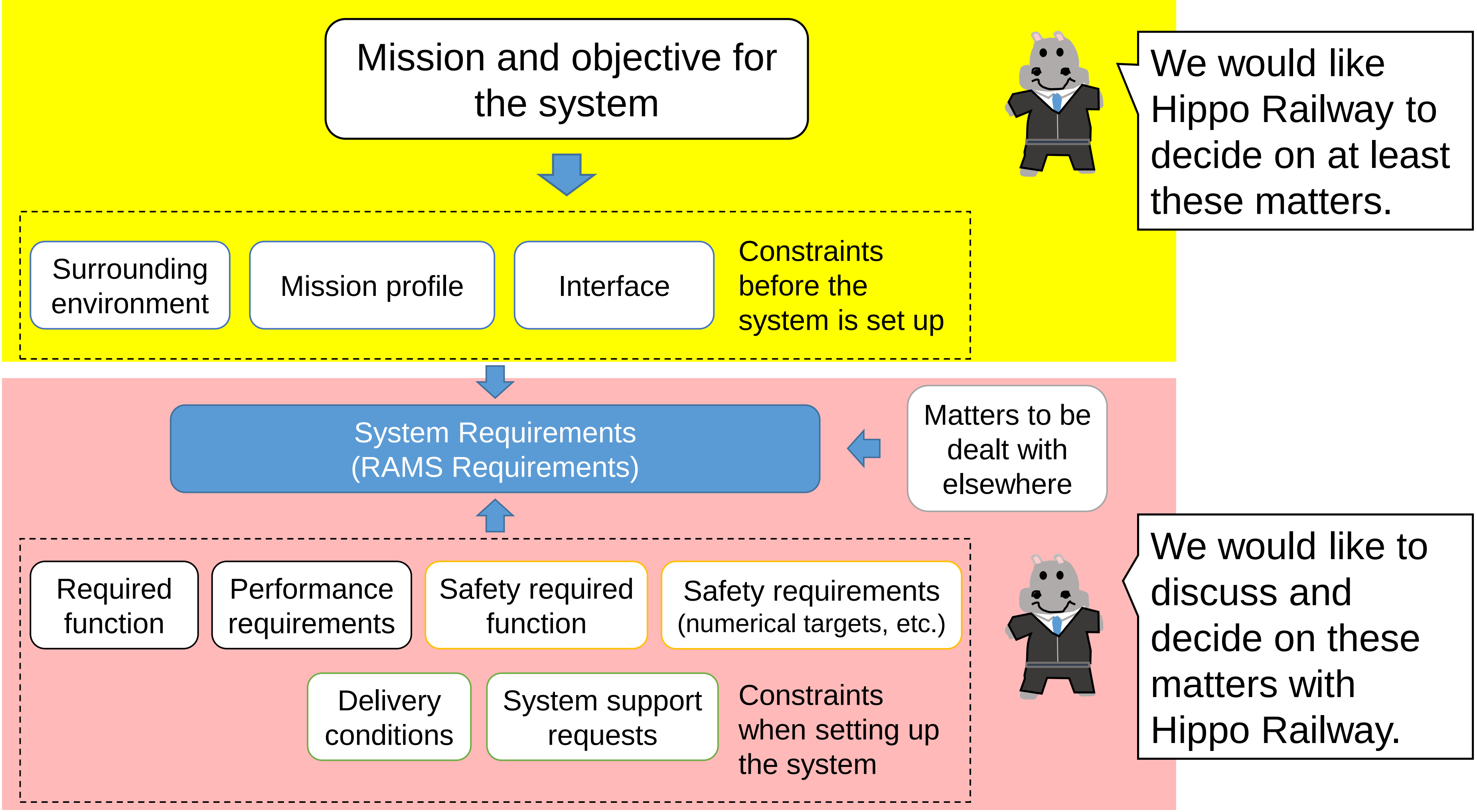
Delivery conditions

System support requests

Constraints when setting up the system

4-1 Role of railway operators

IEC 62278 6.4.3.1
EN 50126-1 7.5.2



Mission and objective for the system

Surrounding environment

Mission profile

Interface

Constraints before the system is set up

System Requirements (RAMS Requirements)

Matters to be dealt with elsewhere

Required function

Performance requirements

Safety required function

Safety requirements (numerical targets, etc.)

Delivery conditions

System support requests

Constraints when setting up the system

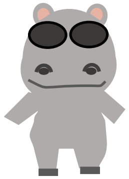
We would like Hippo Railway to decide on at least these matters.

We would like to discuss and decide on these matters with Hippo Railway.

4-1 Precise and complete definitions

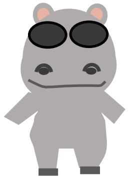
IEC 62278 6.4.3.1

EN 50126-1 7.5.2



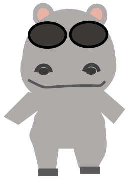
I'll make something good! If customers use it, they will cry and be happy.

There are likely to be a lot of features that I haven't heard about when I do the test.



Customers are selfish anyway. I've programmed it to include everything they're likely to say. I'll do it even if they don't tell me. That's the Hacking Hippo philosophy!

But there's no way to test a function you haven't heard about. You can't ship without testing.



There are no bugs in my software. No testing is needed.

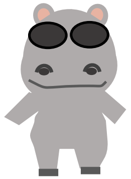
……..

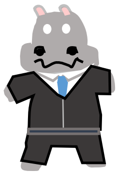
4-1 What do the standards say?

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2

But the RAMS standard doesn't say specifically how the specifications are to be detailed and exhaustive.

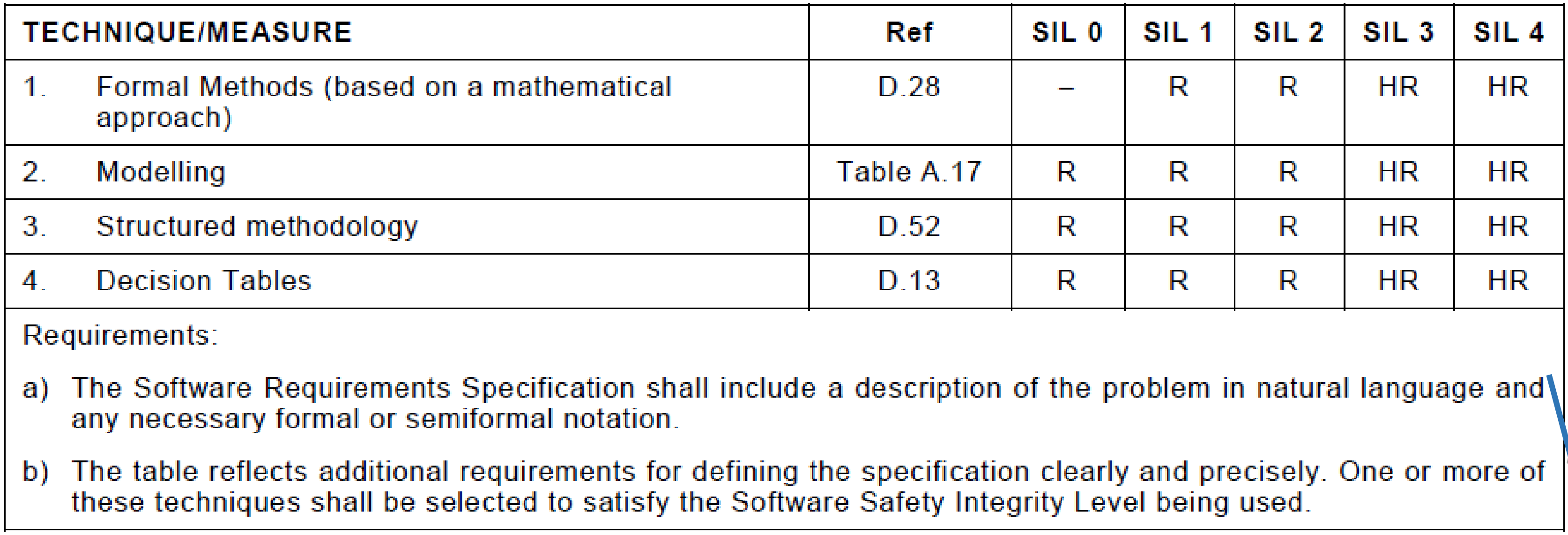
I'll do what it doesn't say. That's what Hacking Hippo is all about!





Even if you can do it, it's not good for anyone else. That's not good.

Software Requirements Specification (Table A.2) / IEC 62279

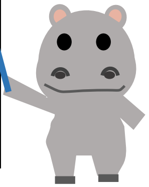


TECHNIQUE/MEASURE	Ref	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. Formal Methods (based on a mathematical approach)	D.28	–	R	R	HR	HR
2. Modelling	Table A.17	R	R	R	HR	HR
3. Structured methodology	D.52	R	R	R	HR	HR
4. Decision Tables	D.13	R	R	R	HR	HR

Requirements:

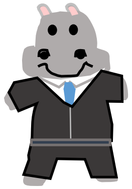
a) The Software Requirements Specification shall include a description of the problem in natural language and any necessary formal or semiformal notation.

b) The table reflects additional requirements for defining the specification clearly and precisely. One or more of these techniques shall be selected to satisfy the Software Safety Integrity Level being used.



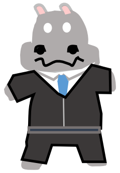
4-1 Example of requirement function modelling

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2



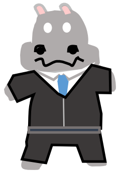
Kabao, explain your mission in working with Hippo Railway to secure profits.

Uh, I always think about sales activities, you know. I visit and talk to Hippo Railway everyday.



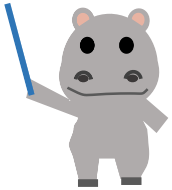
That's why I'm saying what we're going to do to ensure profits. Effort is important, but the outcome is profit. What are the required functions to secure profits?

I'm doing my best.



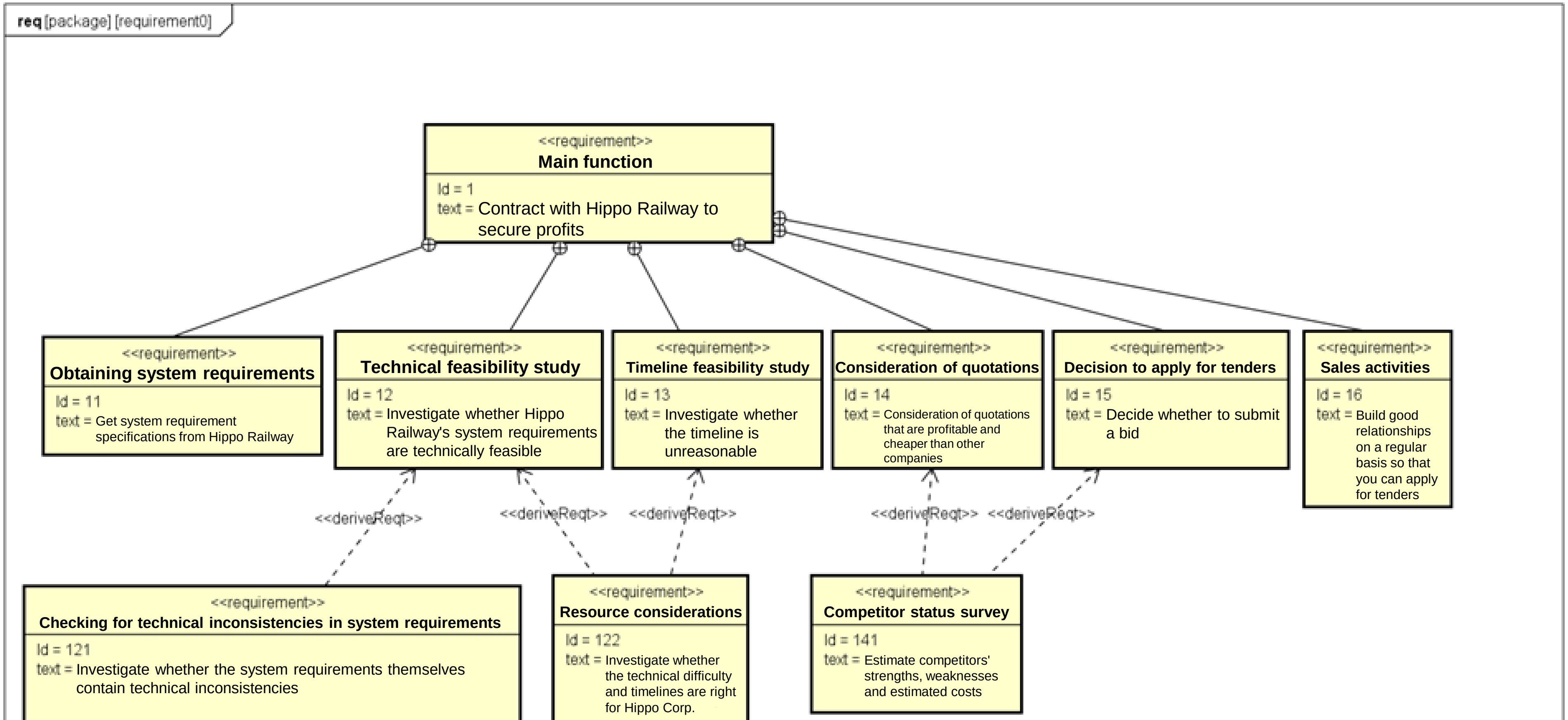
Huh. So you don't understand after all. That's the problem.

Now let’s model the required functions to secure profit.



4-1 Example of requirement function modelling

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2



req [package] [requirement0]

<<requirement>>
Main function
Id = 1
text = Contract with Hippo Railway to secure profits

<<requirement>>
Obtaining system requirements
Id = 11
text = Get system requirement specifications from Hippo Railway

<<requirement>>
Technical feasibility study
Id = 12
text = Investigate whether Hippo Railway's system requirements are technically feasible

<<requirement>>
Timeline feasibility study
Id = 13
text = Investigate whether the timeline is unreasonable

<<requirement>>
Consideration of quotations
Id = 14
text = Consideration of quotations that are profitable and cheaper than other companies

<<requirement>>
Decision to apply for tenders
Id = 15
text = Decide whether to submit a bid

<<requirement>>
Sales activities
Id = 16
text = Build good relationships on a regular basis so that you can apply for tenders

<<deriveReqt>>

<<deriveReqt>>

<<deriveReqt>>

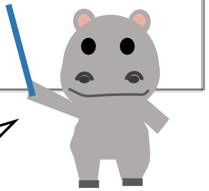
<<deriveReqt>>

<<deriveReqt>>

<<requirement>>
Checking for technical inconsistencies in system requirements
Id = 121
text = Investigate whether the system requirements themselves contain technical inconsistencies

<<requirement>>
Resource considerations
Id = 122
text = Investigate whether the technical difficulty and timelines are right for Hippo Corp.

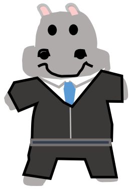
<<requirement>>
Competitor status survey
Id = 141
text = Estimate competitors' strengths, weaknesses and estimated costs



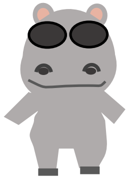
Example of SysML notation

4-1 Benefits of modelling

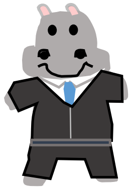
IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2



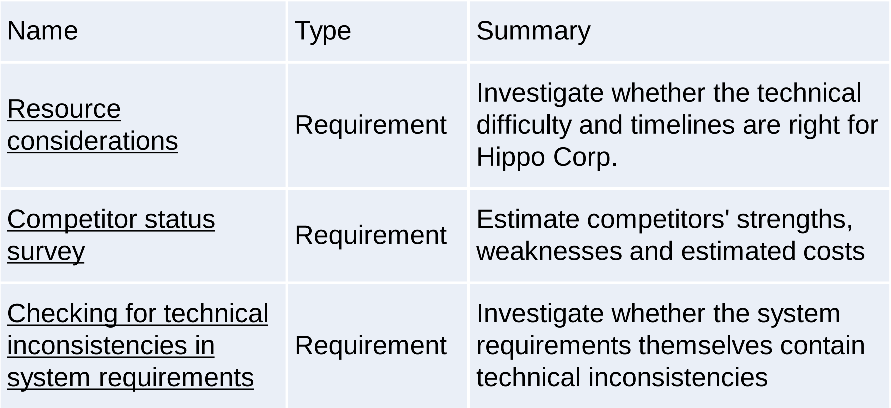
It is true that the definition could be written without missing anything, but I can't quite see the benefit.



That's less ambiguous and more comprehensive than writing in natural sentences.
Do you know, boss? These modelling tools convert to some extent to tabular and natural text.

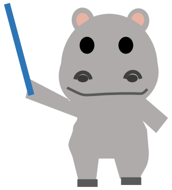


Then it wouldn't be duplicating efforts.



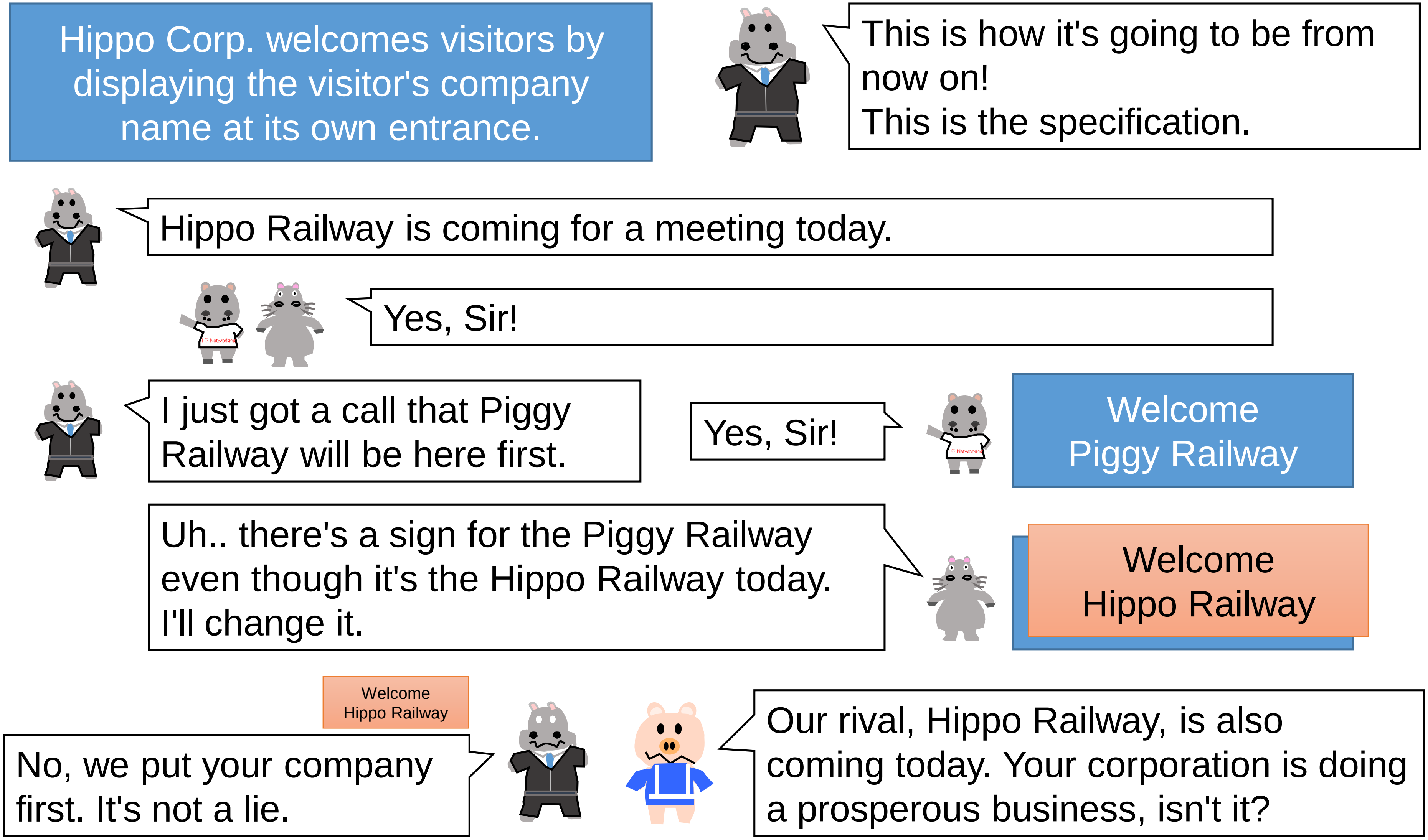
Name	Type	Summary
Resource considerations	Requirement	Investigate whether the technical difficulty and timelines are right for Hippo Corp.
Competitor status survey	Requirement	Estimate competitors' strengths, weaknesses and estimated costs
Checking for technical inconsistencies in system requirements	Requirement	Investigate whether the system requirements themselves contain technical inconsistencies

You also get this kind of output. If I add more various UML diagrams, the skeleton of the source code is also generated automatically.



4-1 Formal method

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2



Hippo Corp. welcomes visitors by displaying the visitor's company name at its own entrance.

This is how it's going to be from now on!
This is the specification.

Hippo Railway is coming for a meeting today.

Yes, Sir!

I just got a call that Piggy Railway will be here first.

Yes, Sir!

Welcome
Piggy Railway

Uh.. there's a sign for the Piggy Railway even though it's the Hippo Railway today. I'll change it.

Welcome
Hippo Railway

Welcome
Hippo Railway

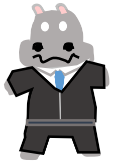
No, we put your company first. It's not a lie.

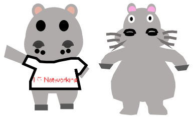
Our rival, Hippo Railway, is also coming today. Your corporation is doing a prosperous business, isn't it?

4-1 Formal method

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2

Hey! You guys! You almost stopped my heart.

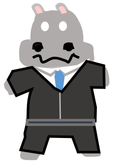


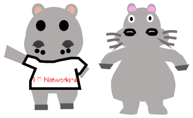


We did it right according to the specifications.

Hippo Corp. welcomes visitors
by displaying the visitor's company name at its own entrance.

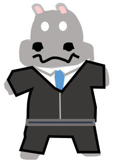
You can't do it in the wrong order.

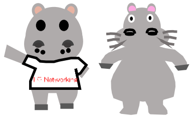




We are sorry about that, but that's not in the specifications.

I can't write every single case. You have to use common sense.





Well, yes, but the programme only works as you are told, so if we were to be a corporation with lax specifications, we would go bankrupt.

4-1 Formal method

IEC 62278 6.4.3.1
EN 50126-1 7.5.2
IEC 62279 Table A.2

Formal method:
The specification can be defined precisely by defining the specification in unambiguous language, defining test cases and conducting tests. It also allows for the automatic generation of parts of software code, which may improve productivity.

```
active proctype otakaba()
      {
      printf ("Piggy Railway¥n")
      }
active proctype kabao()
      {
      printf ("Hippo Railway¥n")
      }
```

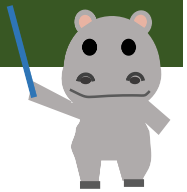
Example of Promela definitions, with Otakaba signposting for Piggy Railway and Kabao signposting for Hippo Railway.

If this is analysed with the model checking tool SPIN, all cases are listed.
(In this example, first Otakaba chooses Piggy Railway, then Kabao chooses Hippo Railway and vice versa. It can be seen that the behaviour is not uniquely determined).

4-2 Specify the overall acceptance criteria for RAMS for the system

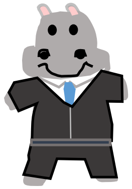
4-1 Specify the overall RAMS requirements for the system

4-2 Specify the overall acceptance criteria for RAMS for the system



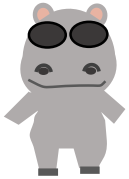
IEC 62278 6.4.3.2
EN 50126-1 7.5.4

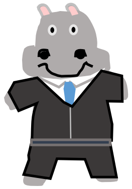
4-2 How to accept requirements?



Acceptance of requirements? If I'm OK with that, then it's OK. I'm the rulebook!

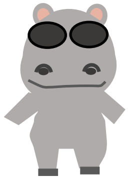
Try that bullishness once in front of , the Manager of Electric Dept. of Hippo Railway.
I don't think he will buy our products again.

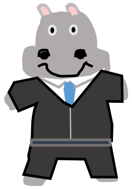




Our dearest Hippo Railway. What you say is absolutely true. There's no doubt about it.

(It's an absolute lie. Lying eyes.)



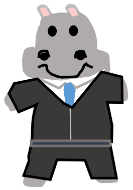


Kabao, take the premium baseball tickets to the manager of Hippo Railway. It's the yellow team. Don't take the orange team's.

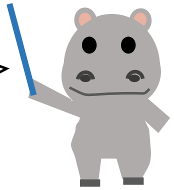
You know, that guy, he's a crazy fan of the yellow team, but he would never accept something like that.
I get scolded a lot when I bring it to him. There will be no more talk of system acceptance.

4-2 How to accept requirements?

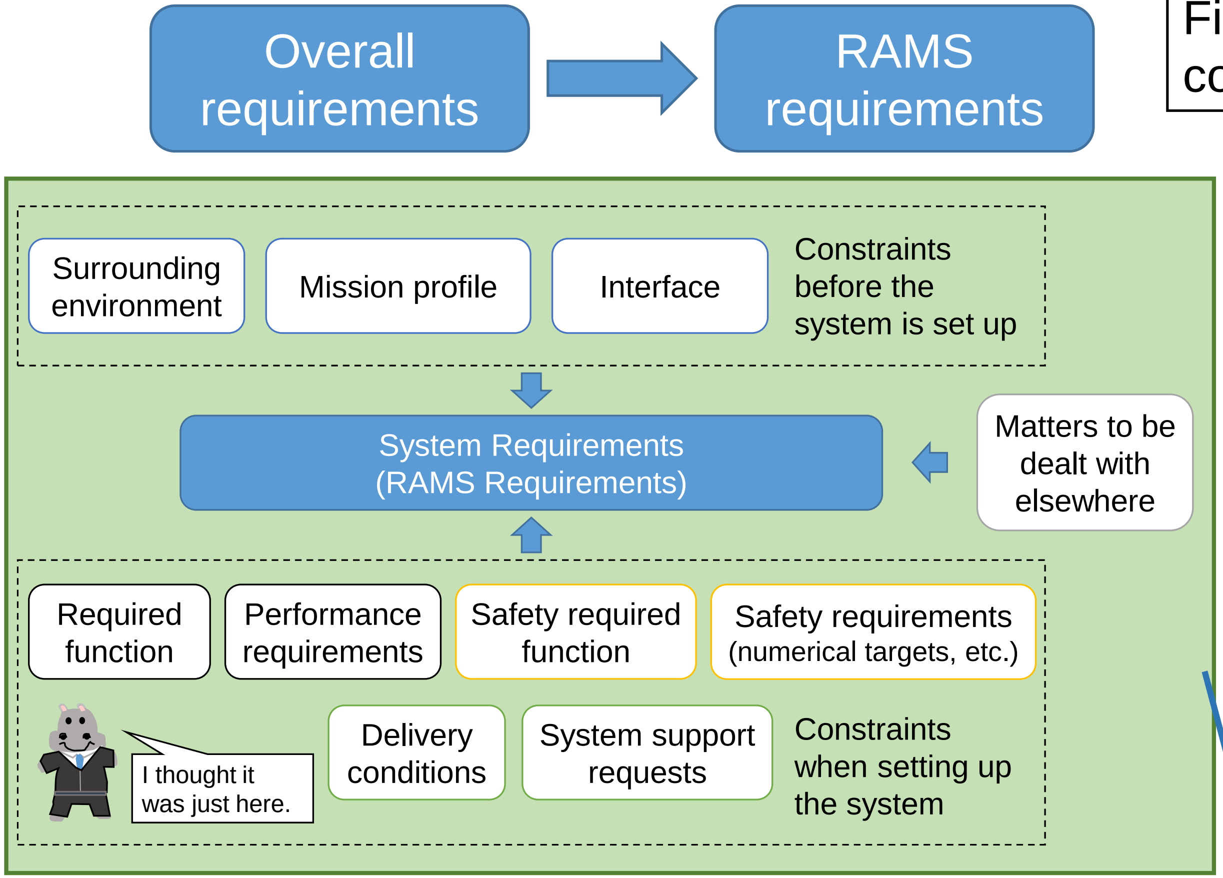
IEC 62278 6.4.3.2
EN 50126-1 7.5.4



What exactly does the standard say about acceptance?



First, check for consistency.



Overall requirements → RAMS requirements

Surrounding environment

Mission profile

Interface

Constraints before the system is set up

System Requirements (RAMS Requirements)

Matters to be dealt with elsewhere

Required function

Performance requirements

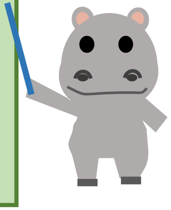
Safety required function

Safety requirements (numerical targets, etc.)

Delivery conditions

System support requests

Constraints when setting up the system



It's about whether these things are properly taken into account.

4-2 How to accept requirements?

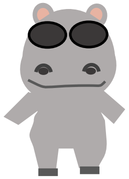
IEC 62278 6.4.3.2
EN 50126-1 7.5.4

Establish the acceptance criteria

↓

Demonstration and acceptance process for the overall RAMS requirements facilitated by the RAMS validation plan, which should include

- a description of the target system
- the RAMS validation (≈ test) principles based on the system requirements including RAMS requirements
- the RAMS tests and analysis for the validation
- the validation management structure
- the validation sequence and schedule
- procedures for dealing with non-conformance

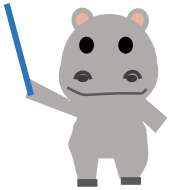


There are no mistakes in my code; Kabao's sales are full of mistakes.

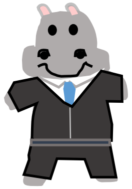
That's terrible.

IEC 62278 6.4.3.2
EN 50126-1 7.5.4

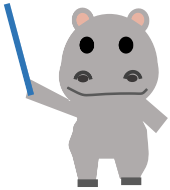
4-2 How will the tests be conducted?



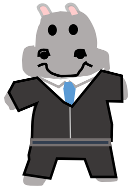
Testing is very important for validation, but how do you test Hippo Corp. interlocking system "KABA-X Interlocking"?



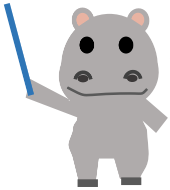
Yes! The test coverage is most important. So we're testing all the interlocking conditions of all the pathways.



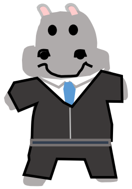
Excellent. Black box testing. And what happens when there are some modifications?



We'll test the interlocking conditions of all paths, with or without modifications, again on a round-the-clock basis. That is the quality of Hippo Corp.!



That's great! But doesn't it cost a lot of money? I think it will take a lot of time.

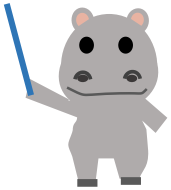


Our safety-first philosophy is more valuable than time and money. Right, Kabao?

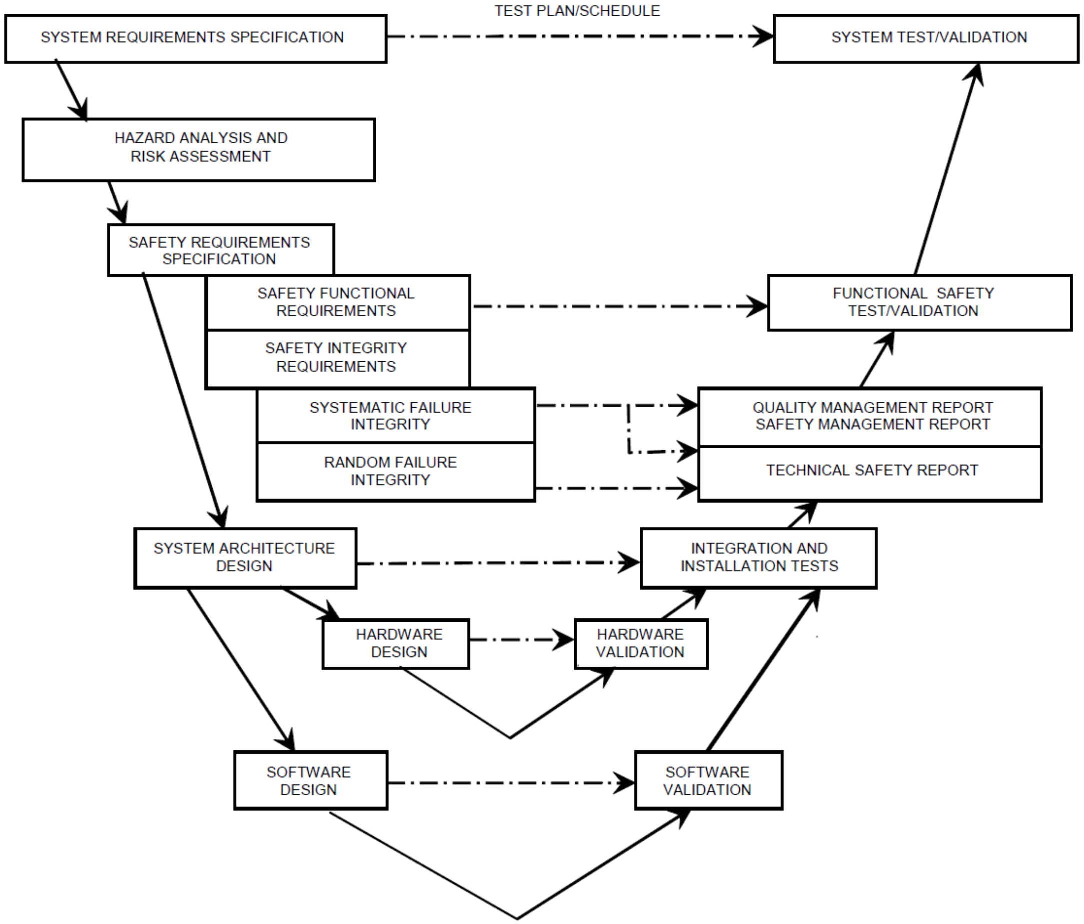
But Hippo Railway says that our refurbishment is expensive.

4-2 Hierarchical tests

IEC 62278 6.4.3.2
IEC 62425 5.3.2
IEC 62279 5.3.2.1
EN 50126-1 7.5.4

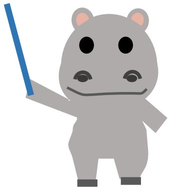


How about hierarchical tests to determine the content?

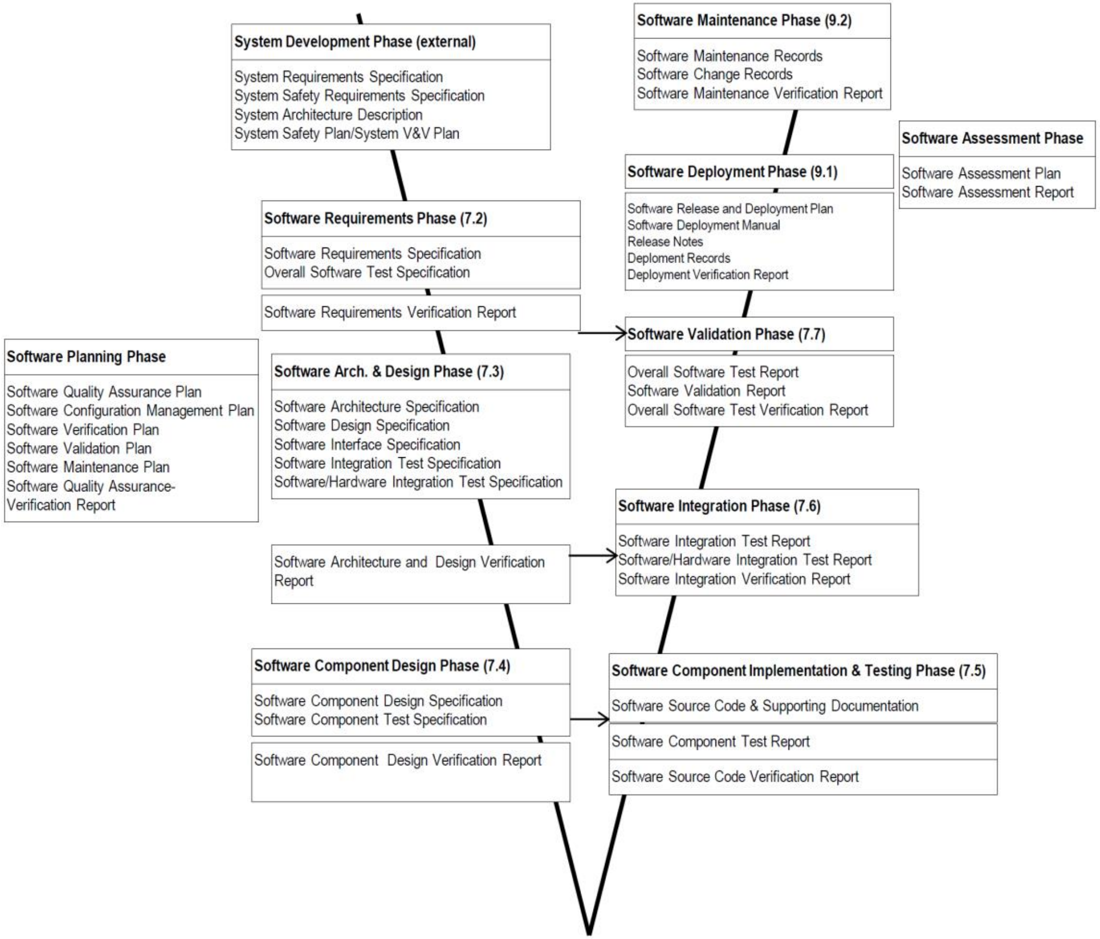

TEST PLAN/SCHEDULE
SYSTEM REQUIREMENTS SPECIFICATION
SYSTEM TEST/VALIDATION
HAZARD ANALYSIS AND RISK ASSESSMENT
SAFETY REQUIREMENTS SPECIFICATION
SAFETY FUNCTIONAL REQUIREMENTS
SAFETY INTEGRITY REQUIREMENTS
FUNCTIONAL SAFETY TEST/VALIDATION
SYSTEMATIC FAILURE INTEGRITY
RANDOM FAILURE INTEGRITY
QUALITY MANAGEMENT REPORT
SAFETY MANAGEMENT REPORT
TECHNICAL SAFETY REPORT
SYSTEM ARCHITECTURE DESIGN
INTEGRATION AND INSTALLATION TESTS
HARDWARE DESIGN
HARDWARE VALIDATION
SOFTWARE DESIGN
SOFTWARE VALIDATION

4-2 Hierarchical tests

IEC 62278 6.4.3.2
IEC 62425 5.3.2
IEC 62279 5.3.2.1
EN 50126-1 7.5.4



This is the case when limited to the software part.



System Development Phase (external)
System Requirements Specification
System Safety Requirements Specification
System Architecture Description
System Safety Plan/System V&V Plan

Software Requirements Phase (7.2)
Software Requirements Specification
Overall Software Test Specification
Software Requirements Verification Report

Software Planning Phase
Software Quality Assurance Plan
Software Configuration Management Plan
Software Verification Plan
Software Validation Plan
Software Maintenance Plan
Software Quality Assurance-Verification Report

Software Arch. & Design Phase (7.3)
Software Architecture Specification
Software Design Specification
Software Interface Specification
Software Integration Test Specification
Software/Hardware Integration Test Specification
Software Architecture and Design Verification Report

Software Component Design Phase (7.4)
Software Component Design Specification
Software Component Test Specification
Software Component Design Verification Report

Software Component Implementation & Testing Phase (7.5)
Software Source Code & Supporting Documentation
Software Component Test Report
Software Source Code Verification Report

Software Integration Phase (7.6)
Software Integration Test Report
Software/Hardware Integration Test Report
Software Integration Verification Report

Software Validation Phase (7.7)
Overall Software Test Report
Software Validation Report
Overall Software Test Verification Report

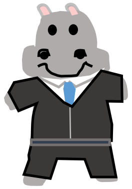
Software Deployment Phase (9.1)
Software Release and Deployment Plan
Software Deployment Manual
Release Notes
Deploment Records
Deployment Verification Report

Software Maintenance Phase (9.2)
Software Maintenance Records
Software Change Records
Software Maintenance Verification Report

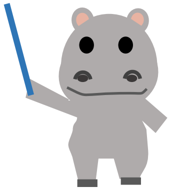
Software Assessment Phase
Software Assessment Plan
Software Assessment Report

4-2 Do we only have to do the overall test?

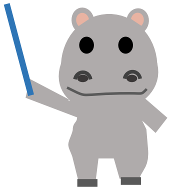
IEC 62278 6.4.3.2
EN 50126-1 7.5.4



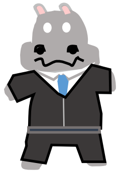
As long as it works properly as an interlocking system, why not do a complete test of the entire interlocking function at Station A?



But Station A may only be using some of the features of the software module, and testing of features not used at Station A will be omitted.

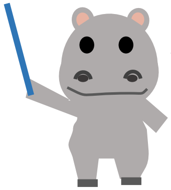


In terms of hardware, if the station is bigger than Station A, you might add an interface card. What about those kinds of tests?



Hey, Otakaba! I hope you've done these tests properly. Think of all the things you'll have to do.

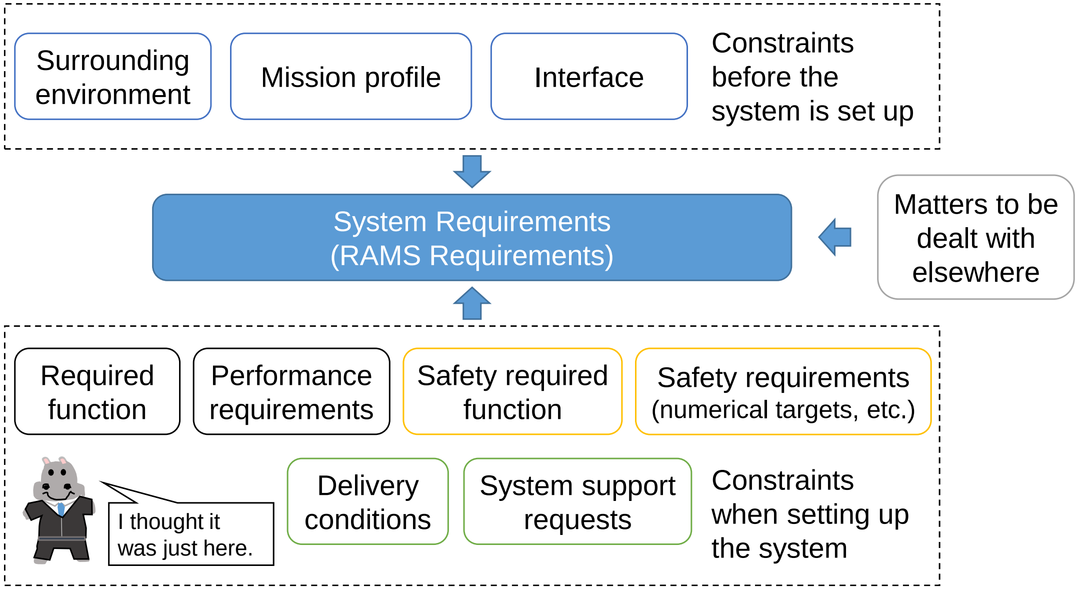
I did them because I knew you would say that.



That is why hierarchical testing is necessary.

Conclusion

- System requirements are not only functional requirements.
- An exhaustive approach of determining requirements is preferred. Modelling is one method; the formal method may also be necessary in the future.
- System acceptance is not only about final testing. The final acceptance test is carried out after the checks at each stage have been completed.


Surrounding environment
Mission profile
Interface
Constraints before the system is set up
System Requirements (RAMS Requirements)
Matters to be dealt with elsewhere
Required function
Performance requirements
Safety required function
Safety requirements (numerical targets, etc.)
I thought it was just here.
Delivery conditions
System support requests
Constraints when setting up the system

Next

See you on 21 October 2021.