FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

BORIS GLOGER®

Agile Process Framework for Projects in the Safety Critical Field

Dr. Hans Tschürtz
Christoph Schmiedinger

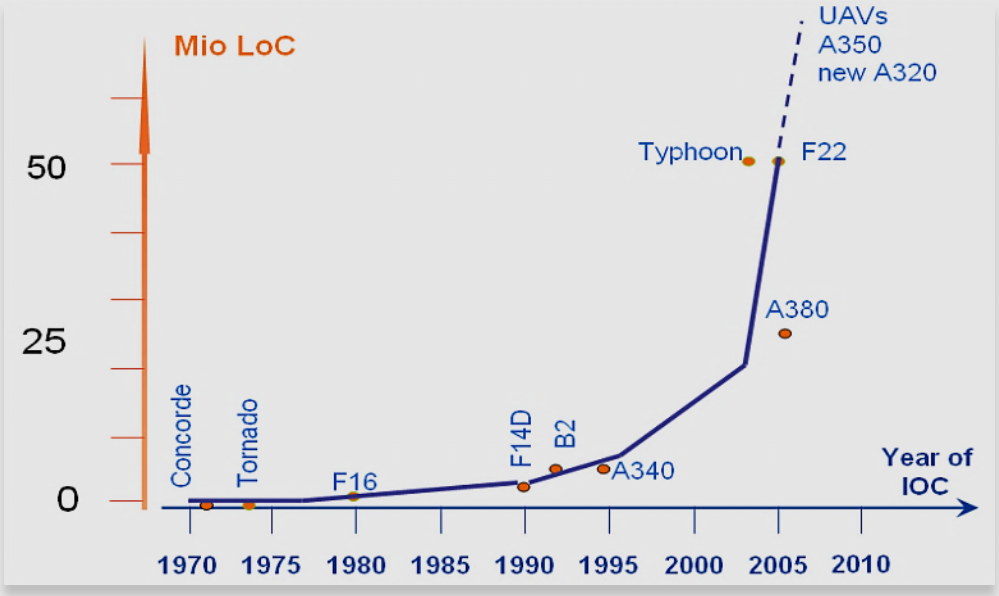
Introduction

> Change in the domain of safety-critical applications
  > Safety compliance, quality, and reliability are a matter of course
  > Increasing focus on functional requirements
  > Demand of more flexibility

> Safety specifications recommend sequential development models
  > IEC 61508, ISO 26262, …
  > Prejudices against agile approaches

Problem Statement 1/3

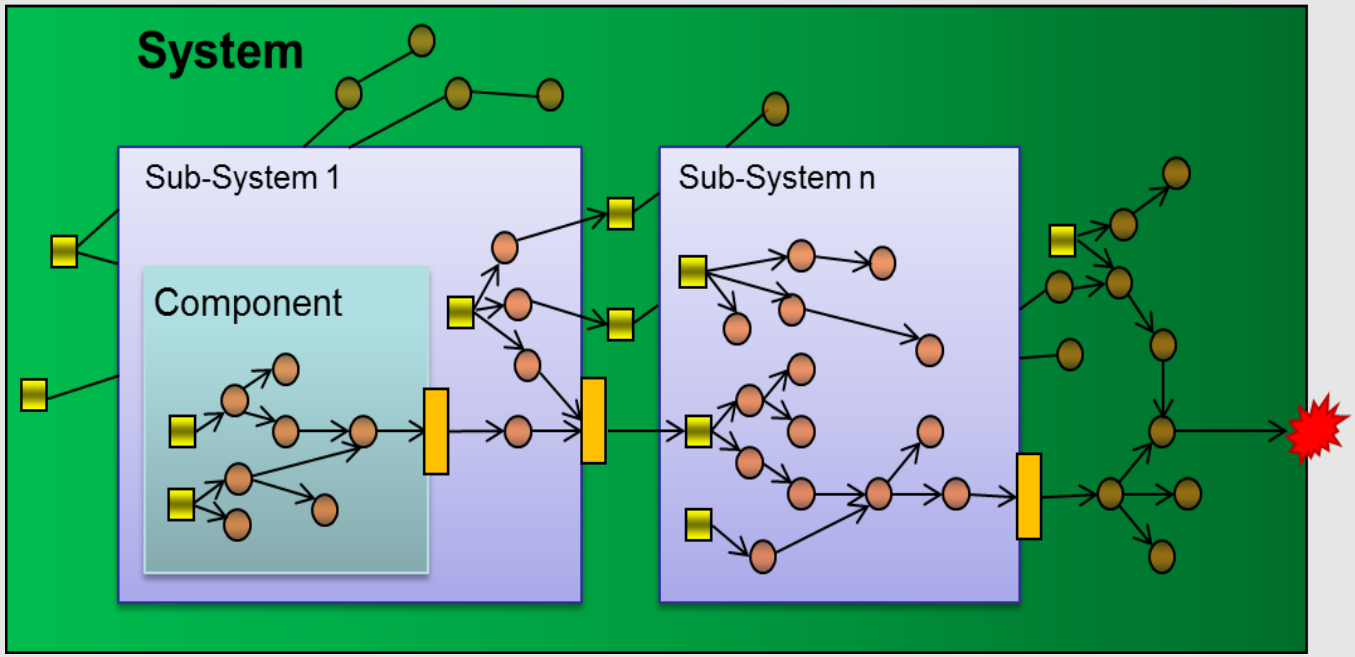
> Complexity of technical systems increases exponentially
> Growing number of computer-based control devices that are mutually strongly coupled (Tight Coupling)
> More and more control functions and featured are realised with software



Problem Statement 2/3

> Number of inherent faults and errors increases, as well as the number of system conditions

> Incidents and accidents occur, caused by the interaction of several causes



Problem Statement 3/3

> „Seldom does a single hazard cause an accident. More often, an accident occurs as the result of a sequence of causes termed initiating and contributory hazards."
[FAA System Safety Handbook]

> "[…] the probability of any one specific combination of failures will be extremely low, but as experience shows, this is precisely what leads to major accidents."
[Holzmann: Conquering Complexity]

> "System failure can come from the interaction of sub-systems deficiencies which individually do not produce an end system failure but may do in combination."
[Sundaram P., Hartfelder D.: Rigor in Automotive Safety Critical System Development]

→ Increasing system complexity and tight coupling leads to non-predictable system states that can lead to

System Accidents *(Change in the nature of Accidents)*

Caused by "Flawed Requirements"

What do we need?

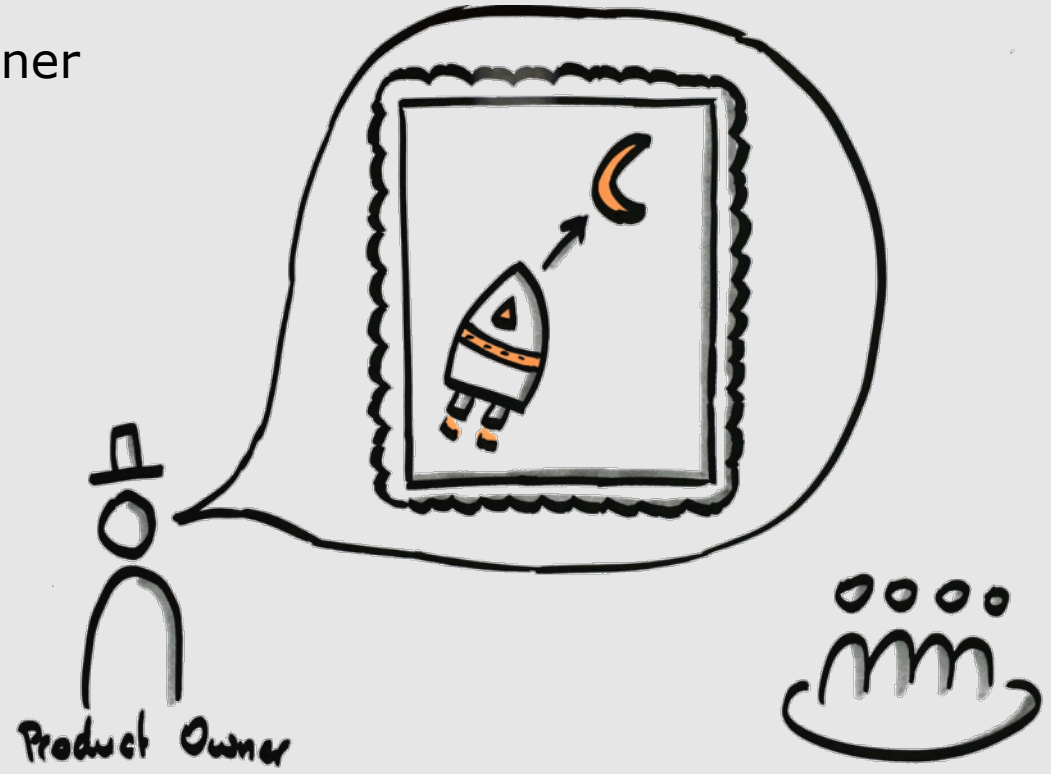
> A flexible approach that meets new challenges while suitable for managing complex systems
  > Identification of hazards in early stages
  > Continuous evaluation of the development direction
  > Preventive avoidance of hazards instead of controlling them
  > Possibility for changes in every development stage

> Skilled people that have
  > knowledge in engineering disciplines and safety
  > the ability to imagine a holistic picture of the whole system on organisational and on engineering level

But now: let's start!

Project Goals

> It's all about a vision
  > ... and the underlying constraints
> Role of the product owner
  > Visionary

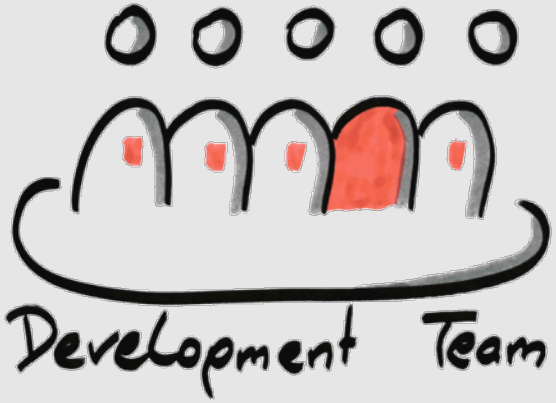


How to achieve?

> Need for a cross-functional agile team

> Cross-functional means that the team needs all the skills to build a potentially shippable product
  > In a safety-critical environment this calls for a team member who is a safety expert (e.g. a safety engineer)
  > Safety is like quality a matter of all team members

> The product is only valuable if it is safe
  > Therefore this assurance has to be made in every iteration



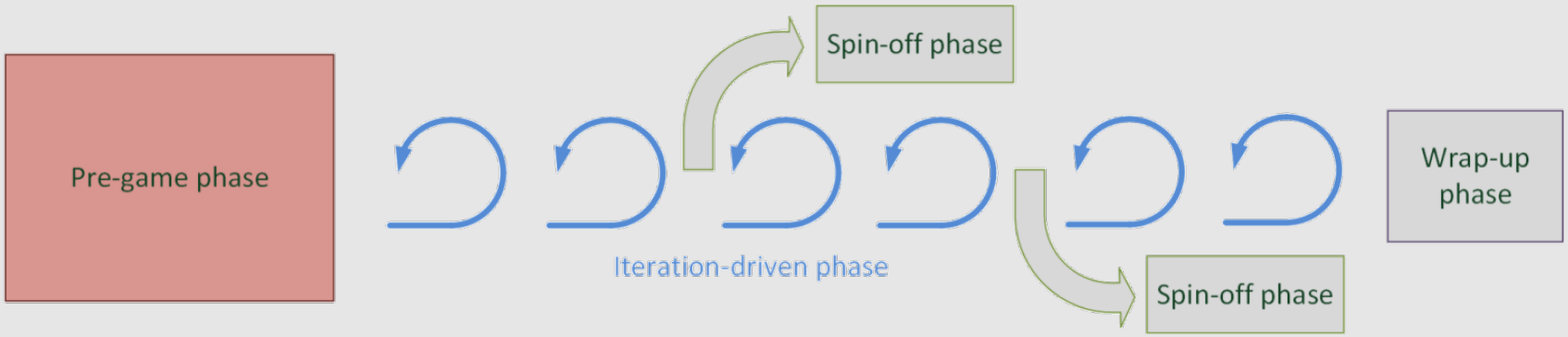
Skills of the safety expert

> Knowledge of relevant norms and standards (e.g. ISO 26262)

> Knowledge of safety and hazard analyse methods

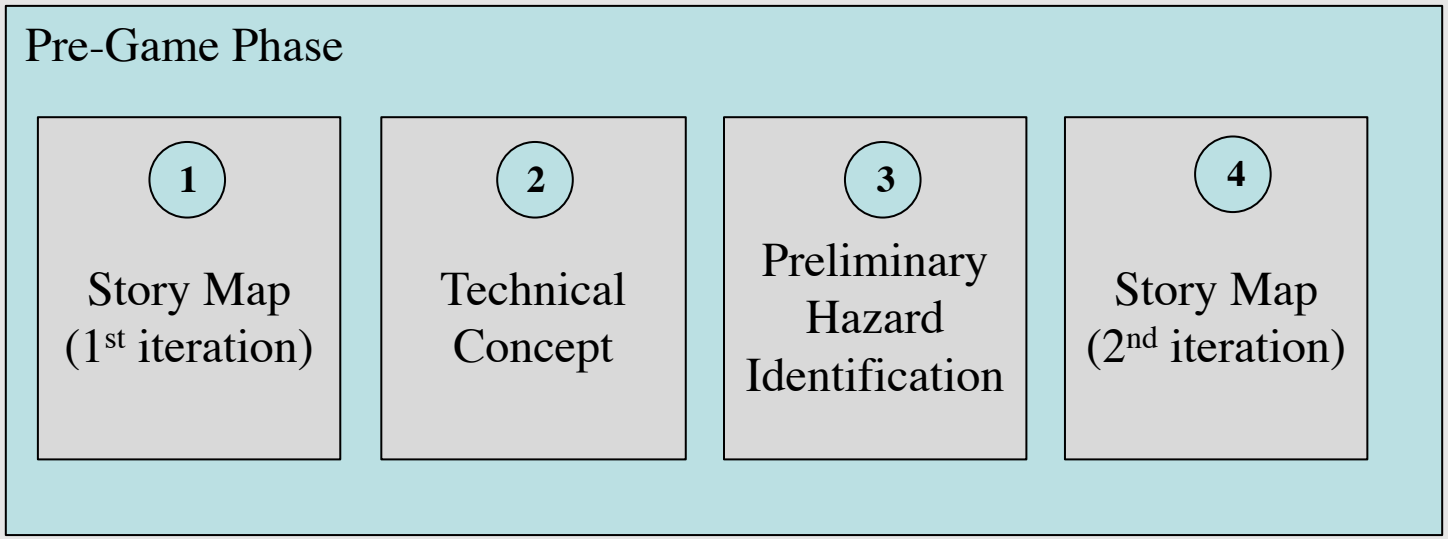
> ....

Lifecycle Model



The "Pre-Game" Phase

> Every good project needs a solid foundation
  > ... but we don't believe that months of analysing and designing is the right approach



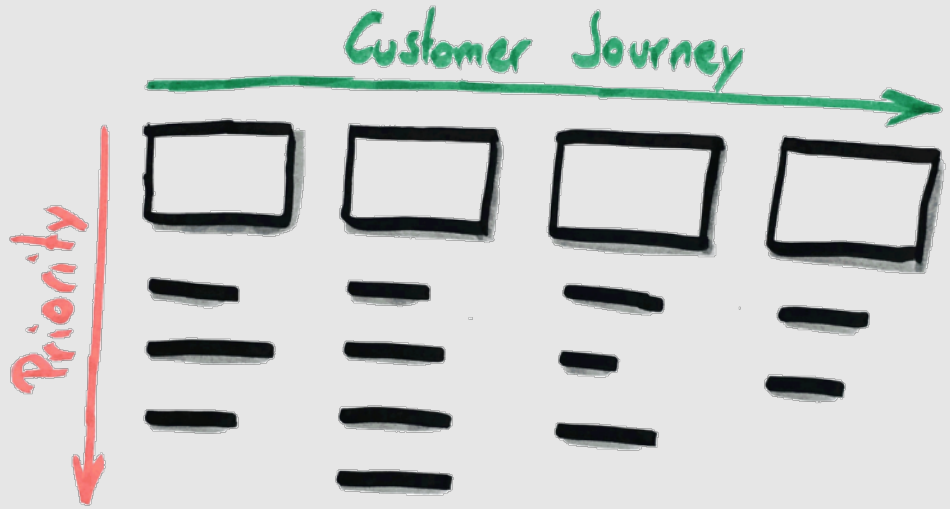
"Pre-Game" Phase – Organisational Set-up

> Involvement of all experts (at minimum the whole development team)
  > Optional: additional experts of various disciplines
> Concentrated workshop-atmosphere
> Off-site in order to ensure the necessary focus

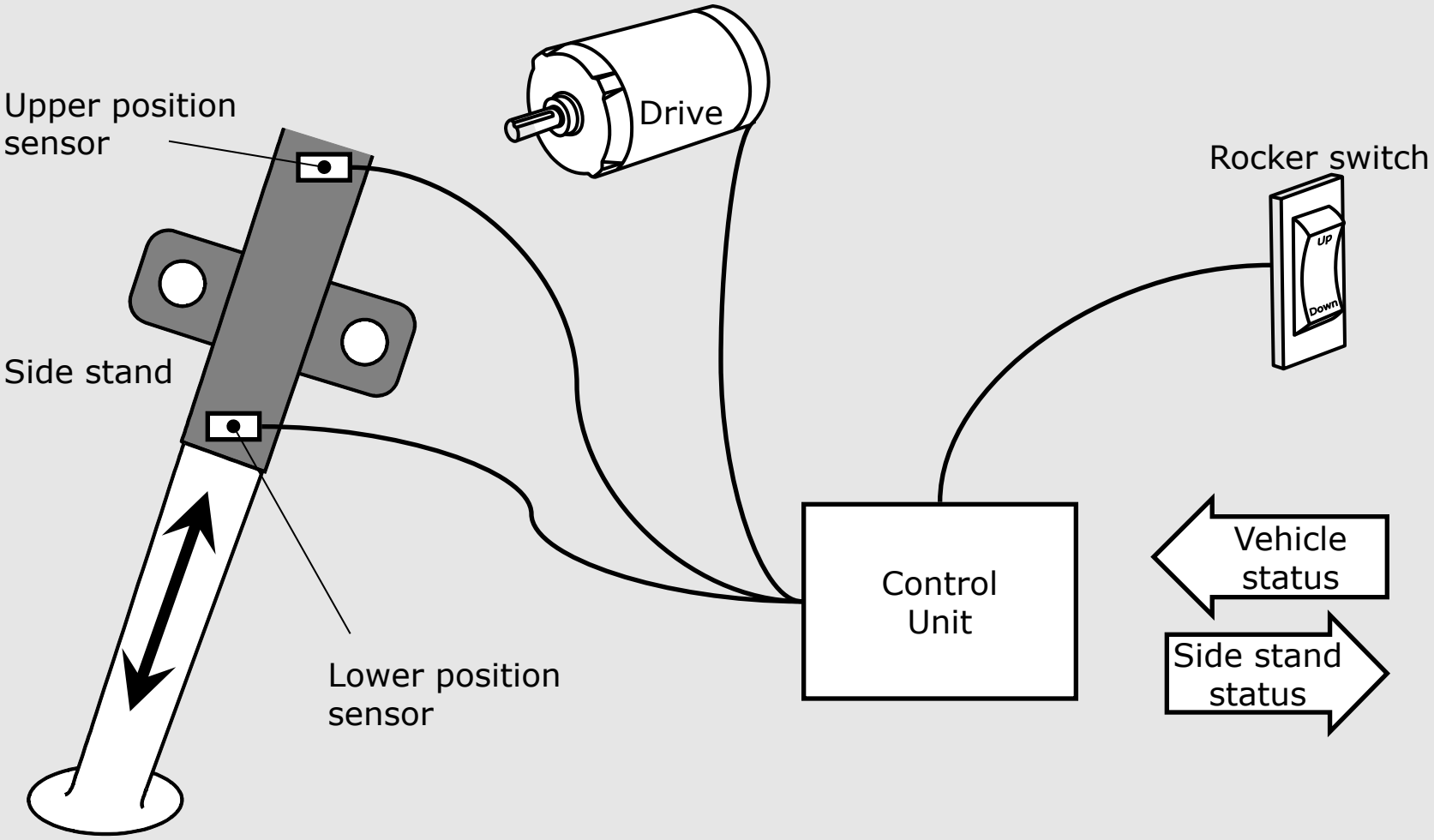
Pre-Game Phase
Step 1

Story Map (1st iteration)

> Modelling of a customer journey
    > ... or a process-/ state-oriented sequence of steps
> Define containers
> Define high-level functionalities



Exercise – Side Stand Control



Exercise – Legal requirements

> Council Directive 93/31/EEC
on stands for two-wheel motor vehicles

> The vehicle shall be designed in such a way that it cannot be propelled by its engine when the prop stand is extended.

> The side stand shall not retract automatically if the angle of lean is altered unexpectedly or the vehicle is being left unattended in its parking position.

Pre-Game Phase
Step 2

Technical Concept

> Input: Story Map

> Use of the Shell Model

> Modelling of a system architecture
    > Interfaces, controller, drivers, sensors, actors, …

Preliminary Hazard Identification

Pre-Game Phase
Step 3

> Input: Technical concept and hazard checklist (if available)

> Activities
  > Identify hazards and their possible causes
  > Assign risk to causes
  > Identify Automotive Safety Integrity Level (ASIL)
  > Specify countermeasures when risk is too high

> Output: Safety Concept (including safety requirements)

FFA (Functional Failure Analysis) – Overview

> Deviations of a system from its intended functions / behaviour are considered

> Combinations of FFA guidewords produce the deviations, which are postulated for the system

> Identification of the theoretical causes and effects resulting from those deviations

> Usually restricted on borders of the (sub-)system under consideration

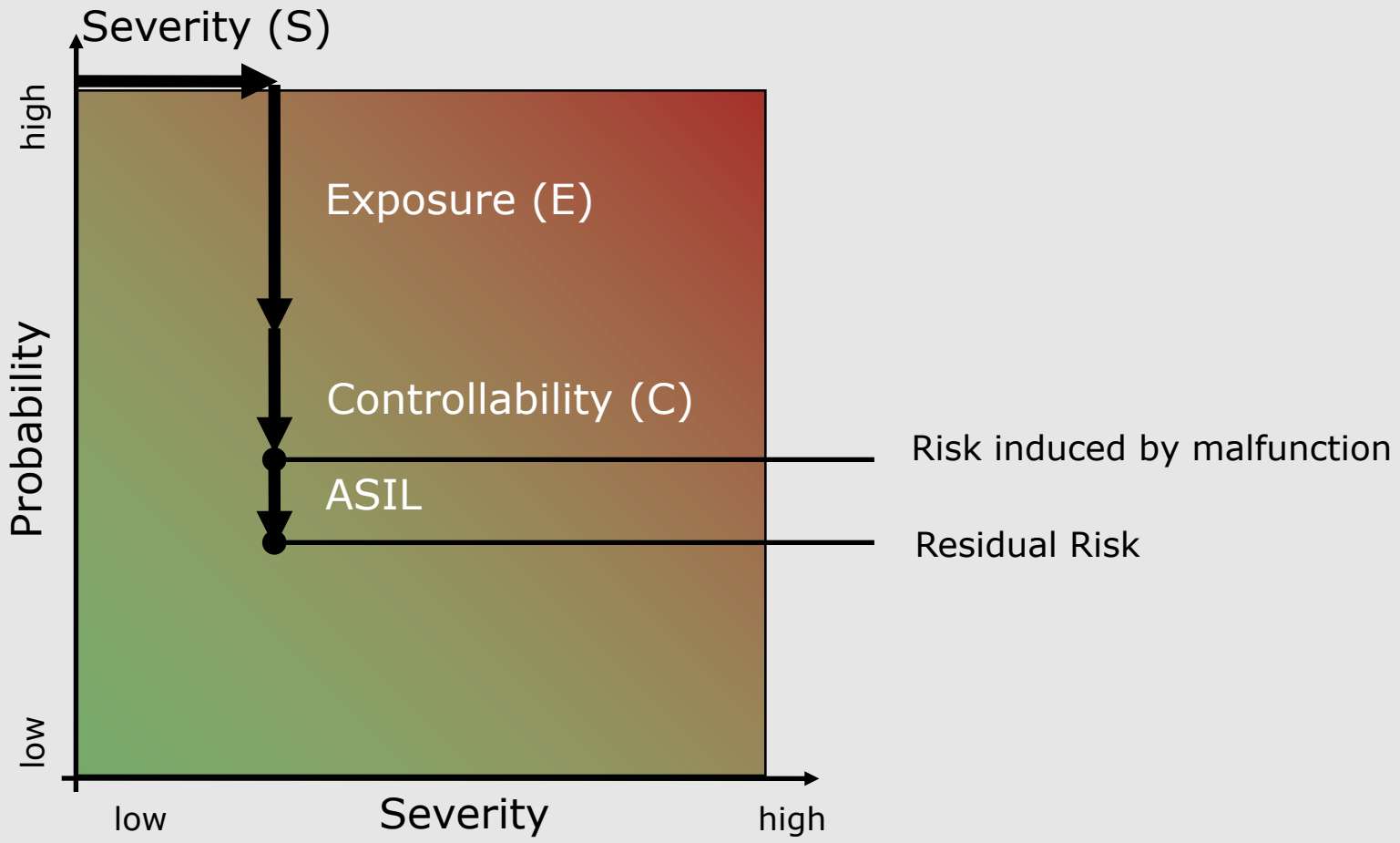
FFA Guideword	Meaning
Omission	Function not provided when required
Commission	Function provided when not intended
Incorrect	Function provided incorrectly

Function	Provided	Not Provided
Required	✓	×
Not intended	×	✓
Incorrectly	×	✓

FFA Example – Power Window

Function	Guideword	Effect
1. Power window closes	Omission	window does not close
	Commission	window closes unintentionally (without request)
	Incorrect	window closes insufficiently or jitters
2. <function>	Omission	…
	Commission	…
	Incorrect	…
3. <function>	Omission	…
	Commission	…
	Incorrect	…

Risk Evaluation According to ISO 26262

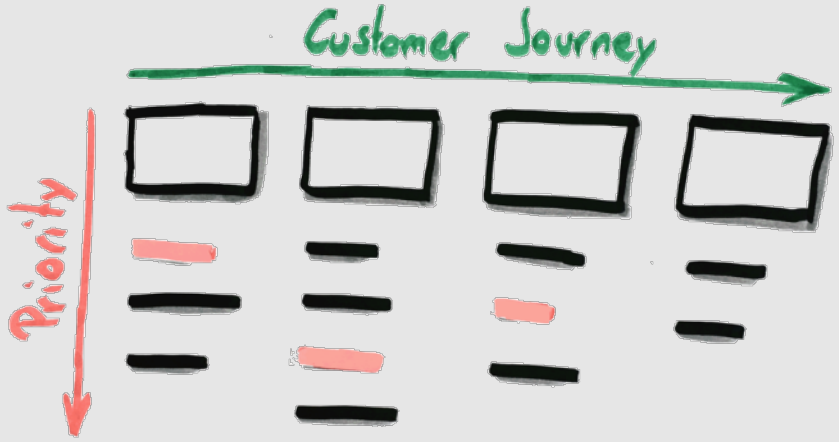


Pre-Game Phase
Step 4

Story Map (2nd iteration)

> Update of the recently created story map based on new insights
  > Especially safety measures must be represented

> Story map is the foundation for the first product backlog
  > Modelling of the first user stories for the first 2-3 iterations

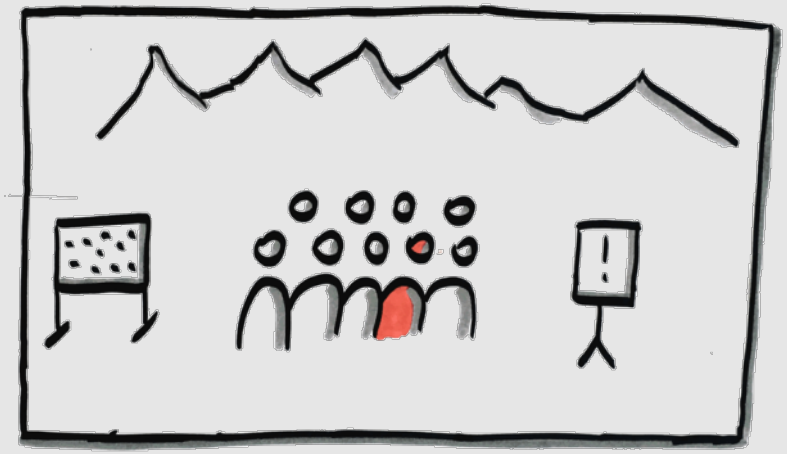


The Foundation is laid

… but what's next?

"Iteration"-Driven Phase

> The team(s) start their sprints by implementing user story after user story



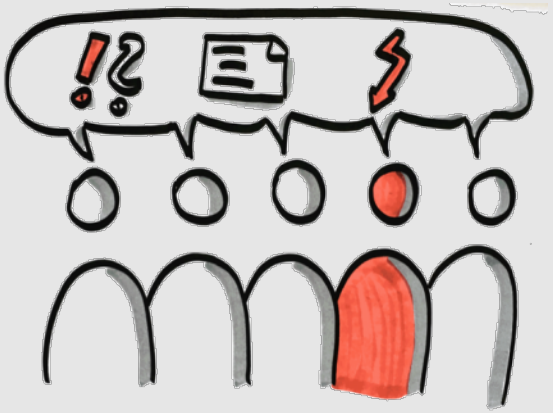
"Pre-Game" Phase

"Iteration-Driven" Phase

Impact Assessment

> Every new user story requires an impact assessment
  > What is the impact of the new functionality on the safety concept?
  > Are there new hazards introduced?

> First impacts can be identified during the conversation of user stories in the backlog refinement meeting, in sprint planning I or II



Iteration Work

> Within the iteration all the necessary actions are performed
  > Update of the safety concept (safety case, ...)
  > Derive of new safety requirements/measures

> Definition of Done
  > Helpful „tool" in order to verify if all necessary actions have been taken
    > Example items
      > Impact Assessment
      > Specific safety analysis
      > Update of safety/design documents
      > Automated tests
      > Tracing of documentation items

Assurance

Preconditions and Success Factors

> Agile model needs a great deal of discipline

> Well organized way of working

> Interdisciplinary development teams

> Preliminary workshop activities are crucial for the success of the project

> Transition of the organisation to agile approaches

> Responsible usage of modern technical practices

Learning Outcomes

> Efficient pre-project Workshop
    > Story Mapping, Shell Modelling and Safety Analyses

> Interdisciplinary Teams
    > Need for safety engineer

> Impact Assessment & Definition of Done
    > It's all about discipline

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

> VIENNA INSTITUTE FOR SAFETY & SYSTEMS ENGINEERING

BORIS GLOGER®

Thank you for your attention.

Safe Systems for a Safer World!

> Christoph Schmiedinger christoph.schmiedinger@borisgloger.com

> Dr. Hans Tschürtz hans.tschuertz@fh-campuswien.ac.at