



LAAS-CNRS



MODEL-BASED RISK ANALYSIS OF HUMAN-ROBOT INTERACTIONS AND SAFETY ARGUMENT CONSTRUCTION

Quynh Anh DO HOANG

Jérémie GUIOCHET

Mohamed KAÂNICHE

David POWELL

qdohoang@laas.fr

Model-based Safety Assessment Workshop
ISAE Campus de Rangueil – Toulouse March 15,16 2011

Summary

- Human-robot interaction: MIRAS project
- Model-based risk analysis: HAZOP-UML
- Safety argument construction using GSN

A Rehabilitation Robot: The MIRAS Robot

The MIRAS project :

A robotic strolling assistance

- **GOAL**

- Assists patient in standing up, walking and sitting down
- For people suffering from gait and orientation problems

- **MEANS**

- Motorised base and moving handlebar
- Sensors to detect patient's position and health condition



MIRAS : Multimodal Interactive Robot for Assistance in Strolling

Building a safe system...

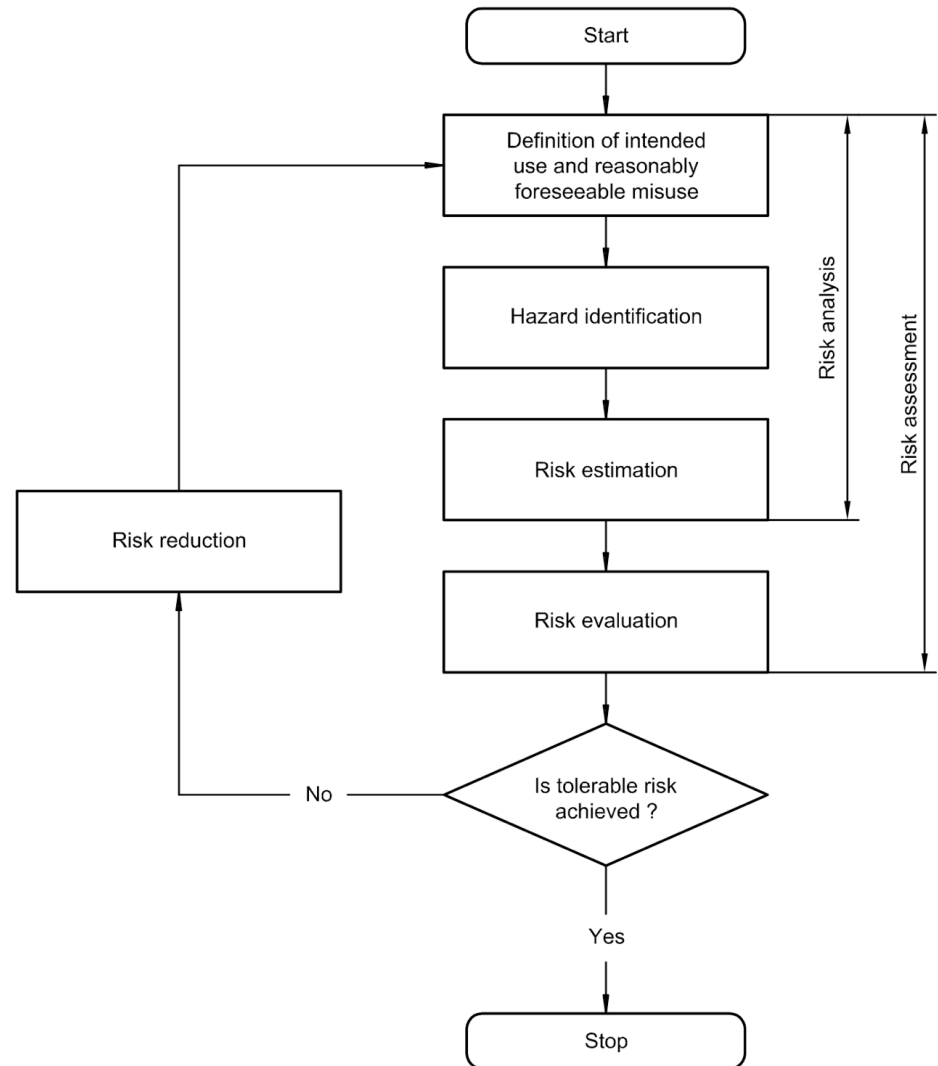
- Building a zero-risk system...
 - Totally correct specification
 - All hazardous situations predicted
 - All hazardous situations correctly handled
 - Totally correct design and implementation
- ... is actually impossible
 - *Justified confidence* that the specification covers the most hazardous situations
 - *Justified confidence* that the design includes adequate protection techniques
 - *Justified confidence* that the system is correctly implemented

Building a safe system...

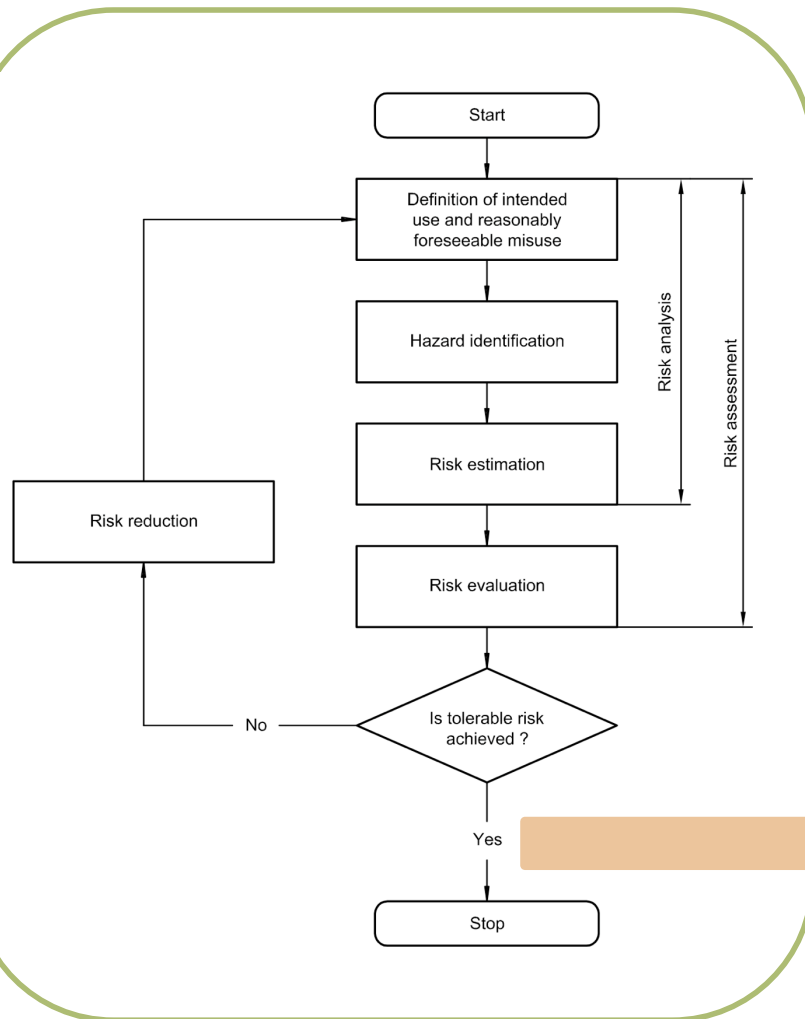
- **Safety**: absence of unacceptable risk [ISO-Guide51]
- **Risk management**: systematic application of management policies, procedures and practices to the task of analysing, evaluating, controlling and monitoring risk [ISO 14971]

Risk management process

- ISO/IEC Guides 51 & 73
- ISO/FDIS 14971



Risk management process



Argumentation process

- **Safety case** : A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment. [1]



[1] U.K Ministry of Defence, Defence Standard 00-56 Issue 4: Safety Management Requirements for Defence Systems. HMSO, 2007

Systematic model-based approach

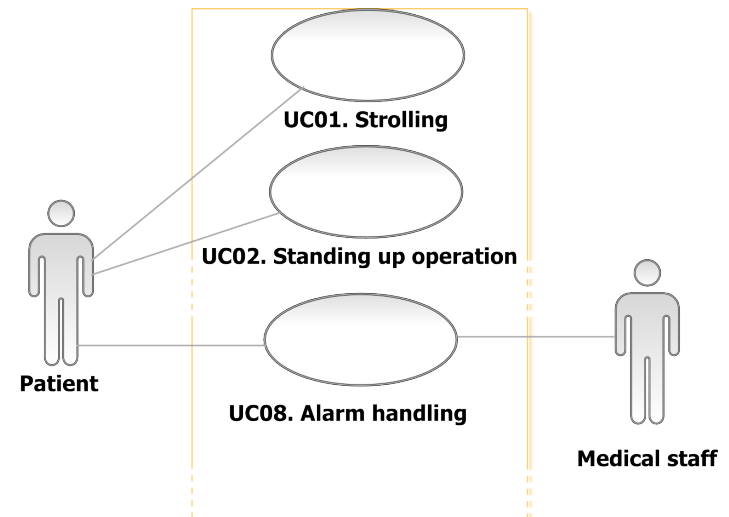
Model-based risk assessment

- Adapt the classical risk management process by using **UML** (Unified Modelling Language) to model the system, including the user
- Why UML ?
 - *De facto* standard
 - Use case, sequence diagram and statechart are easily understandable by non-experts (transdisciplinary models)
 - Diagrams can also be used for development process
 - Models include the user

Unified Modeling Language

- **Use cases**

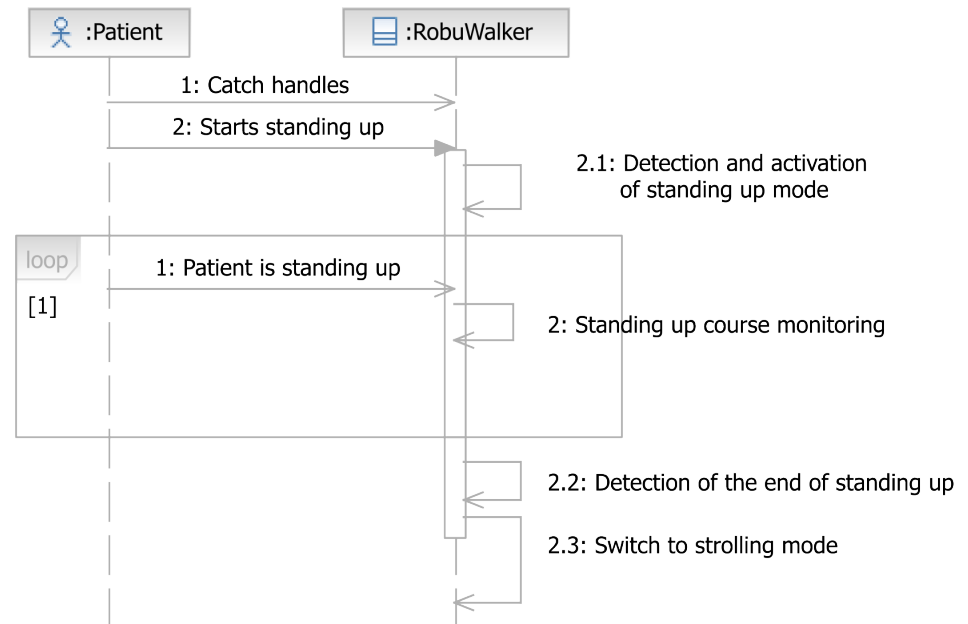
- Describe the intended use of the robot
- Completed with conditions

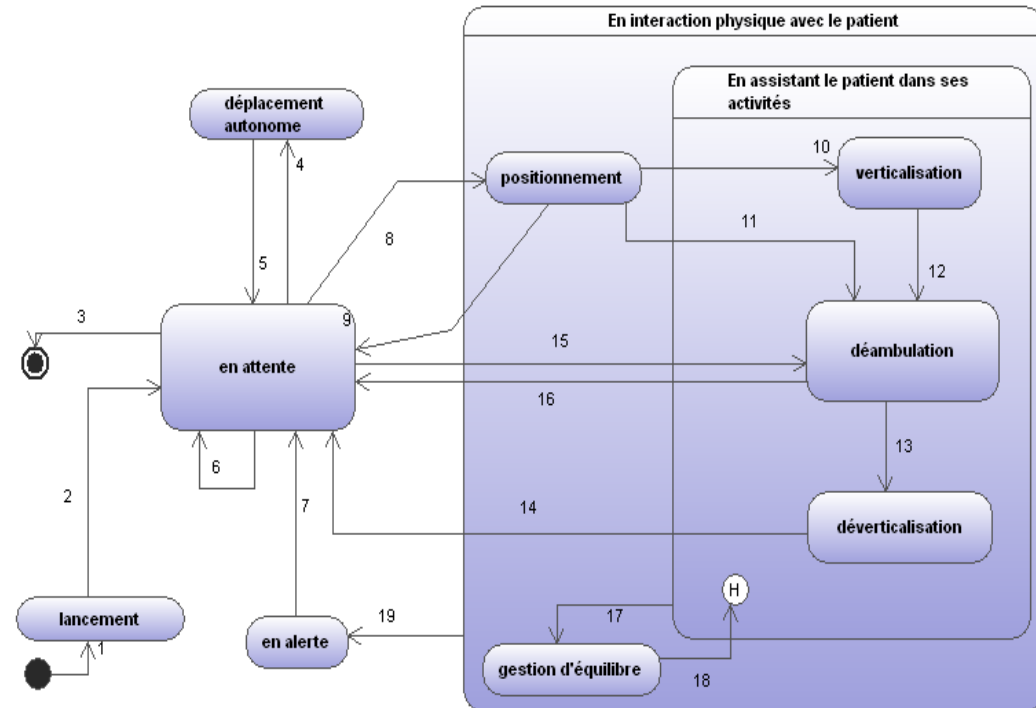


Unified Modeling Language

- Sequence diagrams

- Describe nominal scenarios corresponding to the use cases
- Messages are either actions (self-messages) or interactions

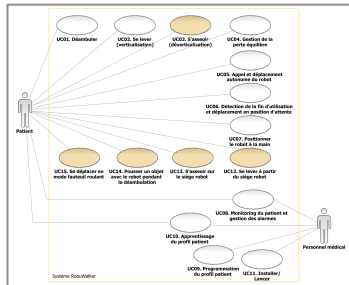




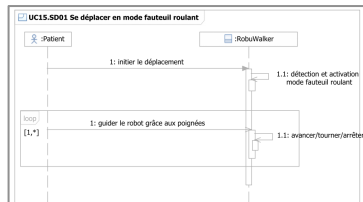
UML Models

HAZOP Guidewords

Risk analysis HAZOP-UML



Use Case Diagram

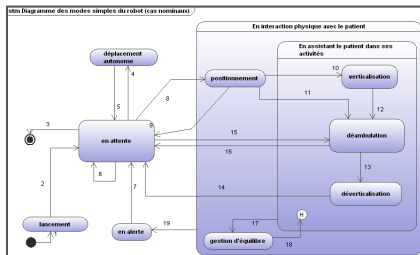


Sequence Diagram



Guideword	Signification
No / None	Complete negation of the design
More than	Quantitative increase
Less than	Quantitative decrease
As well as	All the design intention is achieved together with additions
Part of	Only some of the design intention is achieved
Reverse	The logical opposite of the design intention is achieved
Other than	Complete substitution

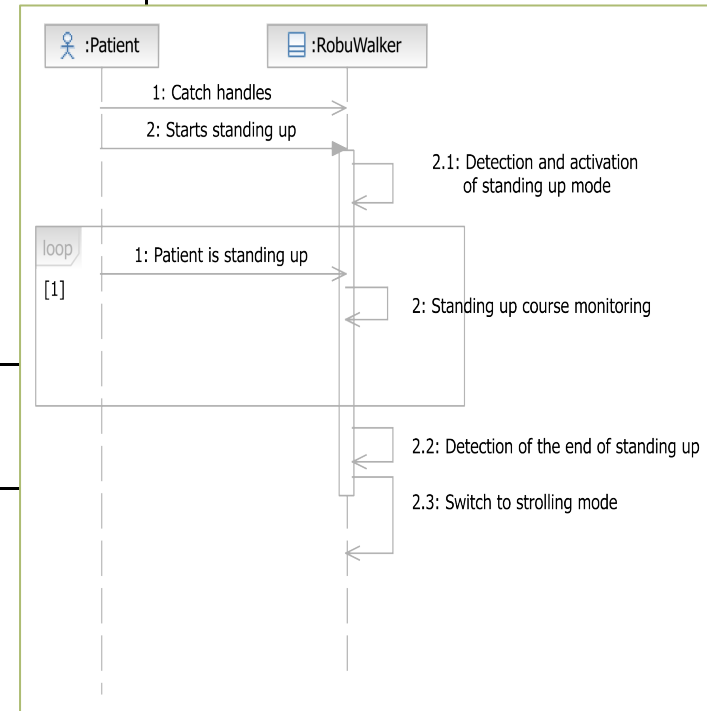
HAZOP - UML							Date: June 2011	
Project: PRODIGES							Prepared by: Othmane Touhami	
HAZOP number: UC4504							Reviewed by: Othmane Touhami	
Title: Sequence Diagram 4 (part) "Take an object from the user's hand"							Approved by:	
Intention (Safety)	Guideword	Deviation	Is the Cause Effect in Real World?	Severity	Possible Cause	Integrity level Requirements	New Safety Requirements	Remarks
Receive and prepare order (robot)	More than	The robot receives several different orders	Yes, Wrong order taken into account	Moderate	Failure of order reception	100% for order reception should be 100%	User education and training	Means for communication between user and robot (e.g. audio/visual signals, messages, user can check interpretation of the robot)
Put the object in gripper (robot)	Before	Since the gripper is open the user can take the object in the robot before the robot is ready	Yes, Wrong order taken into account	Severe	Human error	None	The robot should keep the gripper closed until the arm movement is finished	The procedure in the seq. diag. is to release the robot's gripper to grasp the object. Only then the user can place the object in the robot's gripper. A safer procedure is the robot should keep the gripper closed until arm movement is finished (i.e. moving sequence diagram...)



Statechart

HAZOP-UML

Entity = Sequence Diagram		
Attribute	Guideword	Interpretation
Predecessors / successors during interaction	No	Message is not sent
	Other than	Unexpected message is sent
	As well as	Message is sent as well as another message
	More than	Message sent more often than intended
	Less than	Message sent less often than intended
	Before	Message sent before intended
	After	Message sent after intended
	Part of	Only a part of a set of messages is sent
Message timing	Reverse	Reverse order of expected messages
	As well as	Message sent at correct time and also at incorrect time
	Early	Message sent earlier than intended time
Sender / receiver objects	Later	Message sent later than intended time
	No	Message sent to but never received by intended object
	Other than	Message sent to wrong object
	As well as	Message sent to correct object and also an incorrect object
	Reverse	Source and destination objects are reversed
	More	Message sent to more objects than intended
	Less	Message sent to fewer objects than intended



Example of HAZOP-UML application

Project : PHRIENDS HAZOP number : UC4/SD4 Entity : Sequence Diagram 4 (sd4) "Take an object from the user's hand"								Date: June-01-2008 Prepared by: Ofaina Taofifenua Revised by: Jérémie Guiochet Approved by:	
Element (attribute)	Guide word	Deviation	a. Use Case Effect b. Real World Effect	Severity	Possible Causes	Integrity level Requirements	New Safety Requirements	Remarks	Hazard Number
Receive and interpret order (pred/succ)	More than / as well as	The robot receives several different orders	a. Wrong order taken into account b. Wrong task, bad synchronization between robot and user, could result in collision	Moderate	Failure of H/W for order reception Human error	H/W for order reception should be SIL1	User education and training Define a protocol for communication between user and robot (e.g. acknowledgment messages, user can check interpretation of the order)	Means for communication between robot and user needs to be defined for the PHRIENDS use case (speech, graphical HMI, vision, etc.)	
Put the object in the gripper (pred/succ)	Before	Since the gripper is open the user can give the object to the robot before the latter is ready	a. Bad synchronization between user and robot can cause collision b. The object can fall / The arm and human can collide	Severe	Human error	None	The robot should keep the gripper closed until the arm movement is finished	The procedure in the seq. diag. is as follows: the robot opens its gripper then the robot arm moves towards the user hand. Only then the user can place the object in the robot gripper. A safer procedure is: the robot should keep the gripper closed until arm movement is finished -> modify sequence diagram	2, 19, 20

Results in the MIRAS project

- **First iteration of the process**

- 11 use cases, 12 sequence diagrams
- 297 interpreted deviations
- 13 hazards identified
- 29 recommendations for design modifications

➔ New specification and design of the robot



- **Second iteration of the process on the new UML model**

- 1 modified use case, 4 new use cases, 4 new sequence diagrams
- 215 interpreted deviations
- 1 new hazard identified
- 28 new recommendations for design modifications


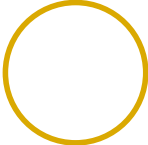



Hazard list

HN	Description	PHA	Use Case Diagram	Sequence Diagram	Statechart
HN1	Incorrect posture of patient during movement	2	4	3	4
HN2	Patient fall during robot use		29	27	30
HN3	Robot shutdown during use : patient is not assisted	1	2		5
HN4	Patient fall without alarm or with a late alarm		11	13	32
HN5	Physiological problem of the patient without alarm or with a late alarm		15	10	
HN6	Patient fall caused by the robot	10	51	37	10
HN7	Failure to switch to safe mode when a problem is detected, the robot keeps moving		8		
HN8	Robot parts catching patient or clothes	3	5	4	
HN9	Collision between the robot (or robot part) and the patient	2	14	14	
HN10	Collision between the robot and a person other than the patient		5	14	2
HN11	Disturbance of medical staff during an intervention		1		
HN12	Patient loses her balance	11	1	70	1
HN13	Patient fatigue	12	1	53	21
HN14	Patient injury caused by sudden movements of robot while carrying the patient			3	

Safety case construction using GSN

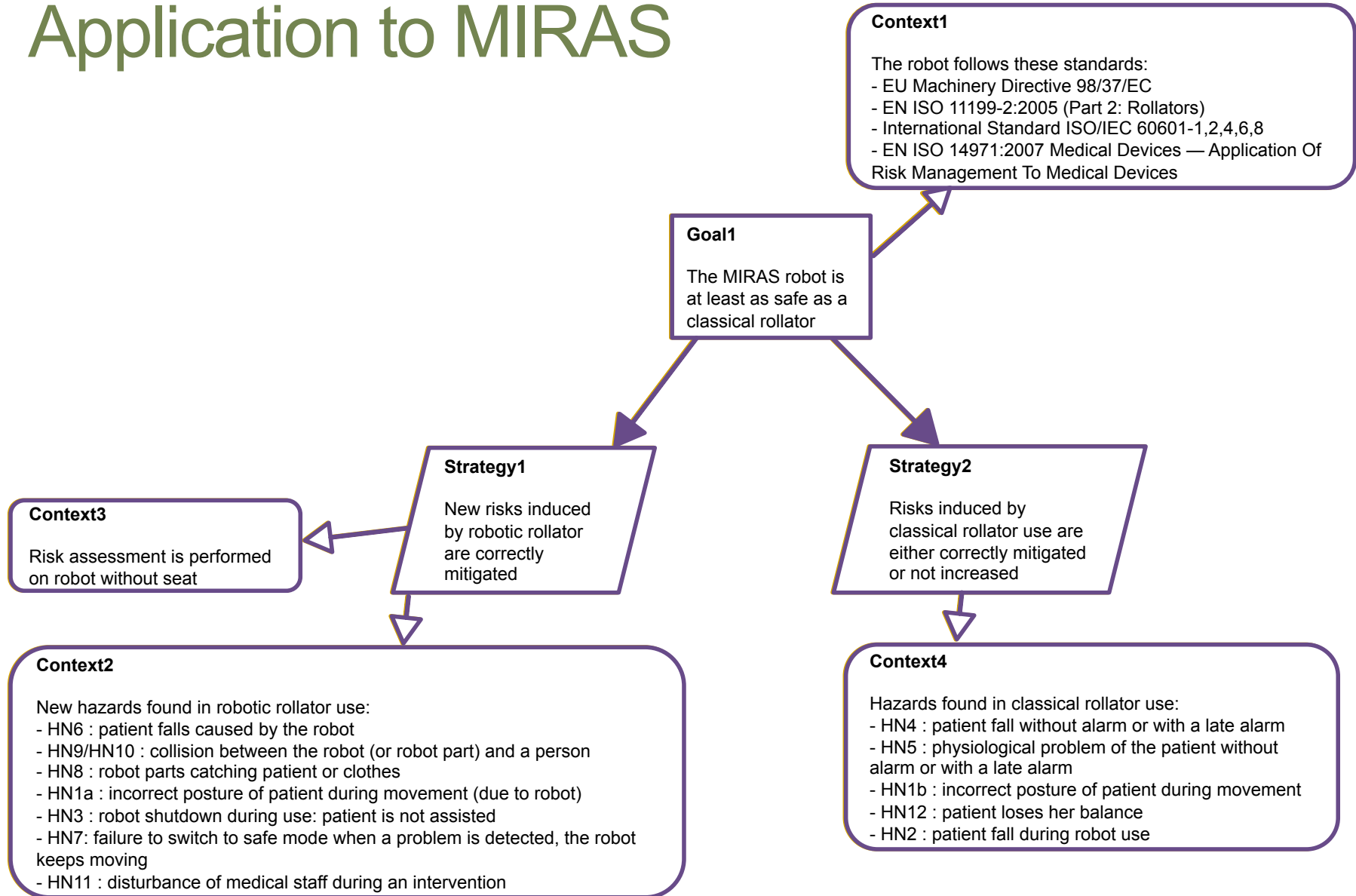
- **Goal Structuring Notation**
 - A graphical notation developed at University of York
 - Mostly used in safety cases
- **Argument elements**
 - Requirement
 - Claim
 - Evidence
 - Context

Goal Structuring Notation

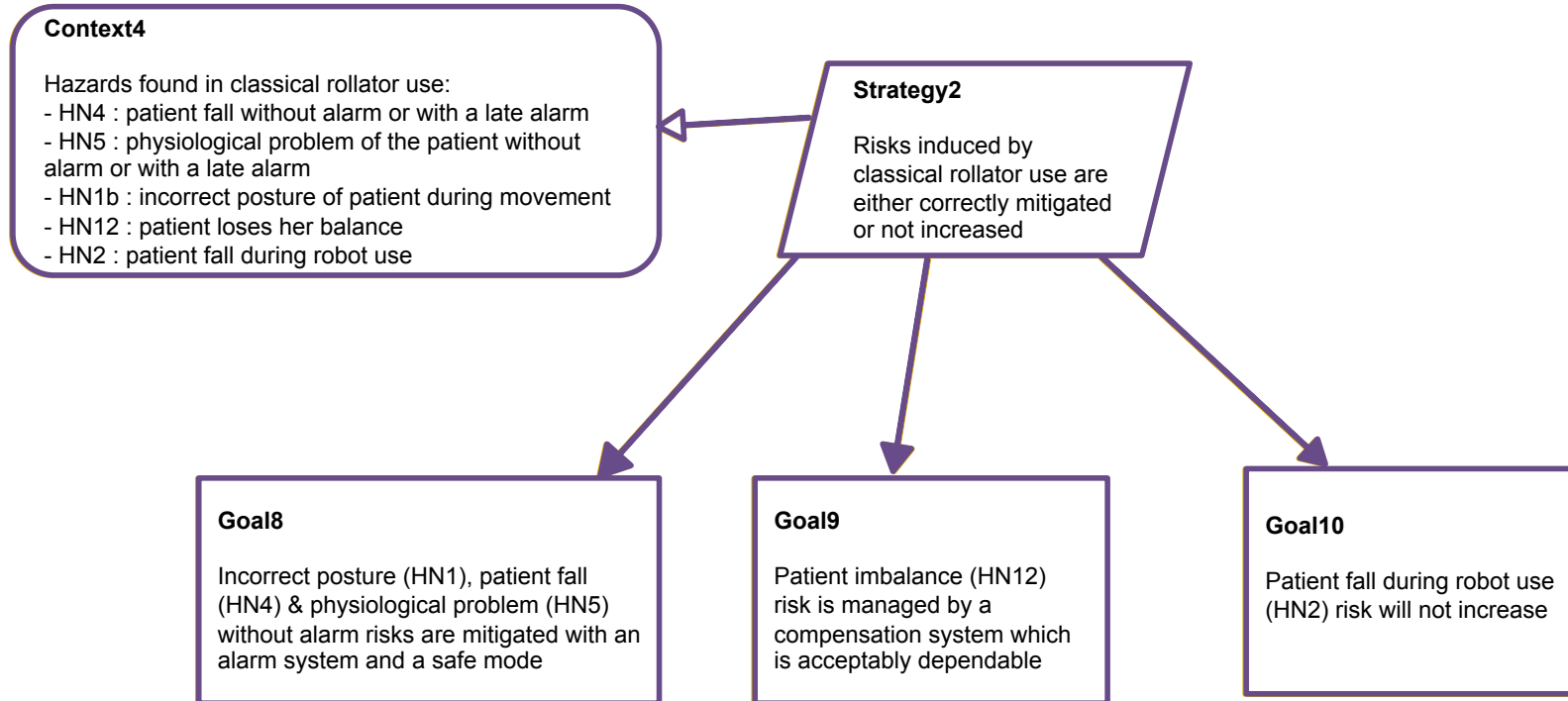
« To show how goals  are broken down into sub-goals,
and eventually supported by evidence (solutions) 
whilst making clear the strategies  adopted,
the rationale for the approach (assumptions, justifications) 
and the context  in which goals are stated. » [2]

[2] T. P. Kelly & R. A Weaver, *The Goal Structuring Notation – A Safety Argument Notation*, Dependable Systems and Network Workshop on Assurance Case, July 2004

Application to MIRAS



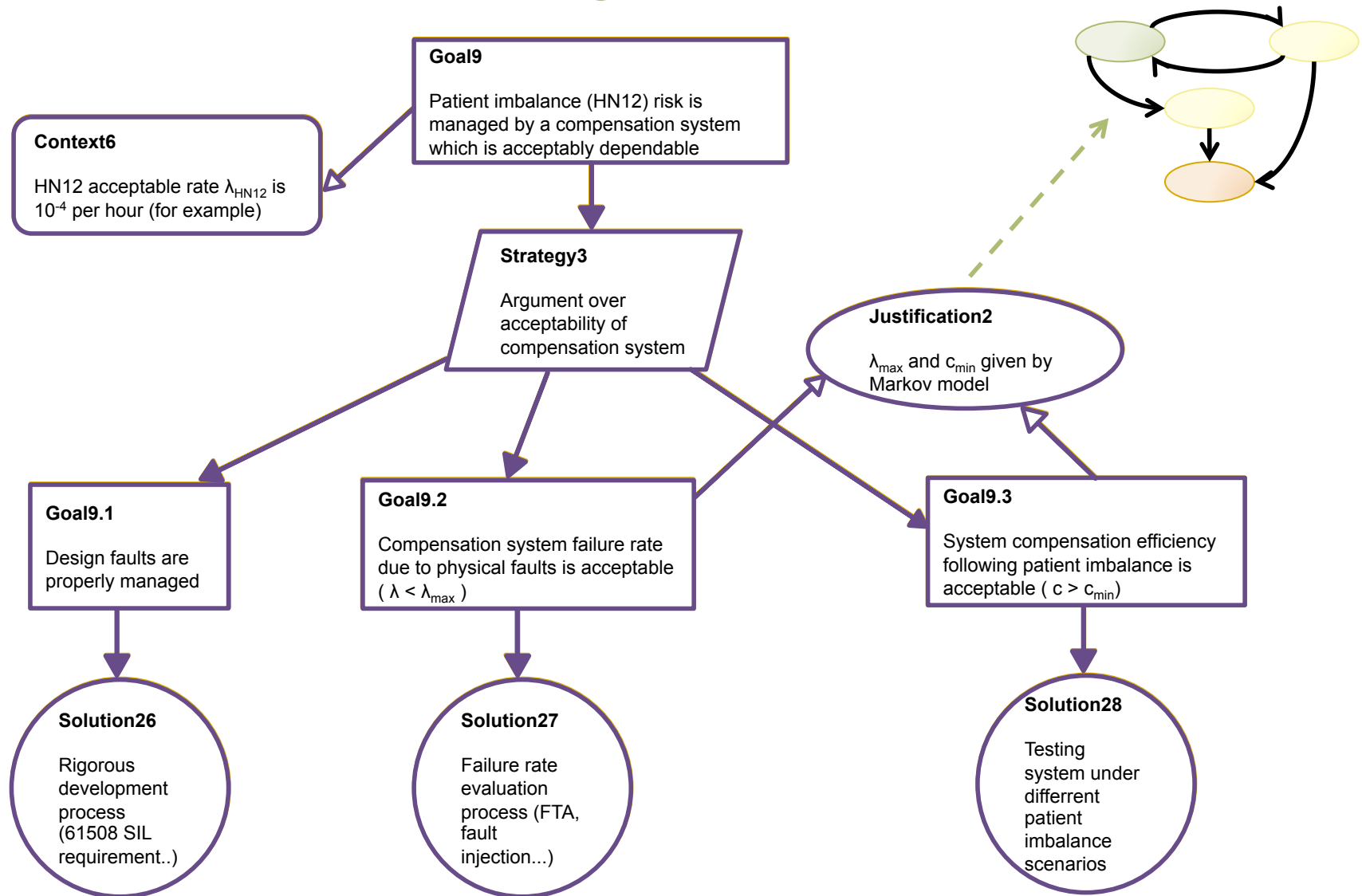
Development of a strategy



How did we treat HN12 ?

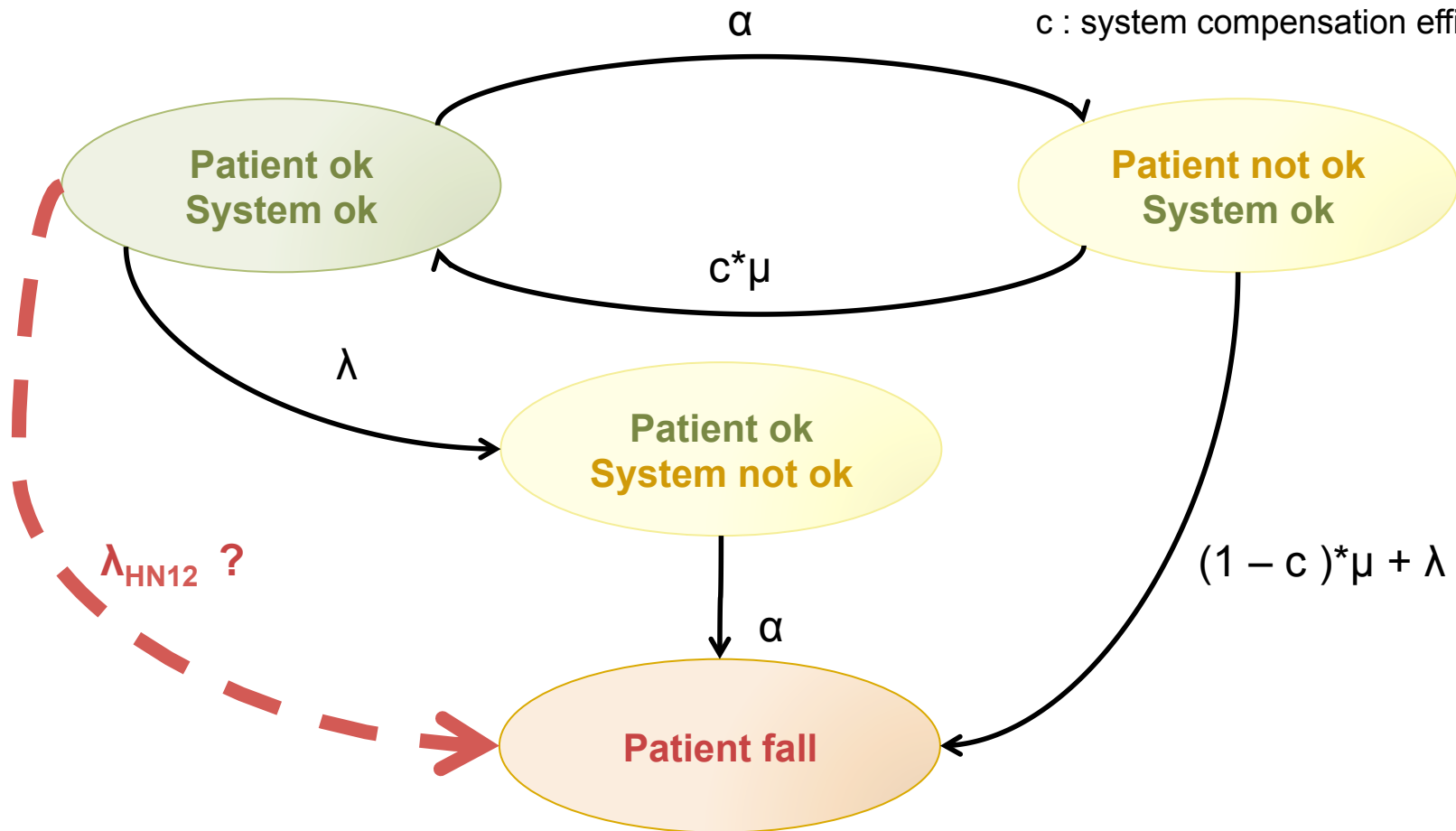
- What is HN12 ?
 - The patient loses her balance
- MIRAS assistance
 - Moves back or forward to help patient to find her balance
- What is the hazard ?
 - Loss of balance not detected in time
 - Improper compensation

Development of a goal



Markov model

λ : system failure rate
 α : loss of balance rate
 μ : compensation rate
 c : system compensation efficiency



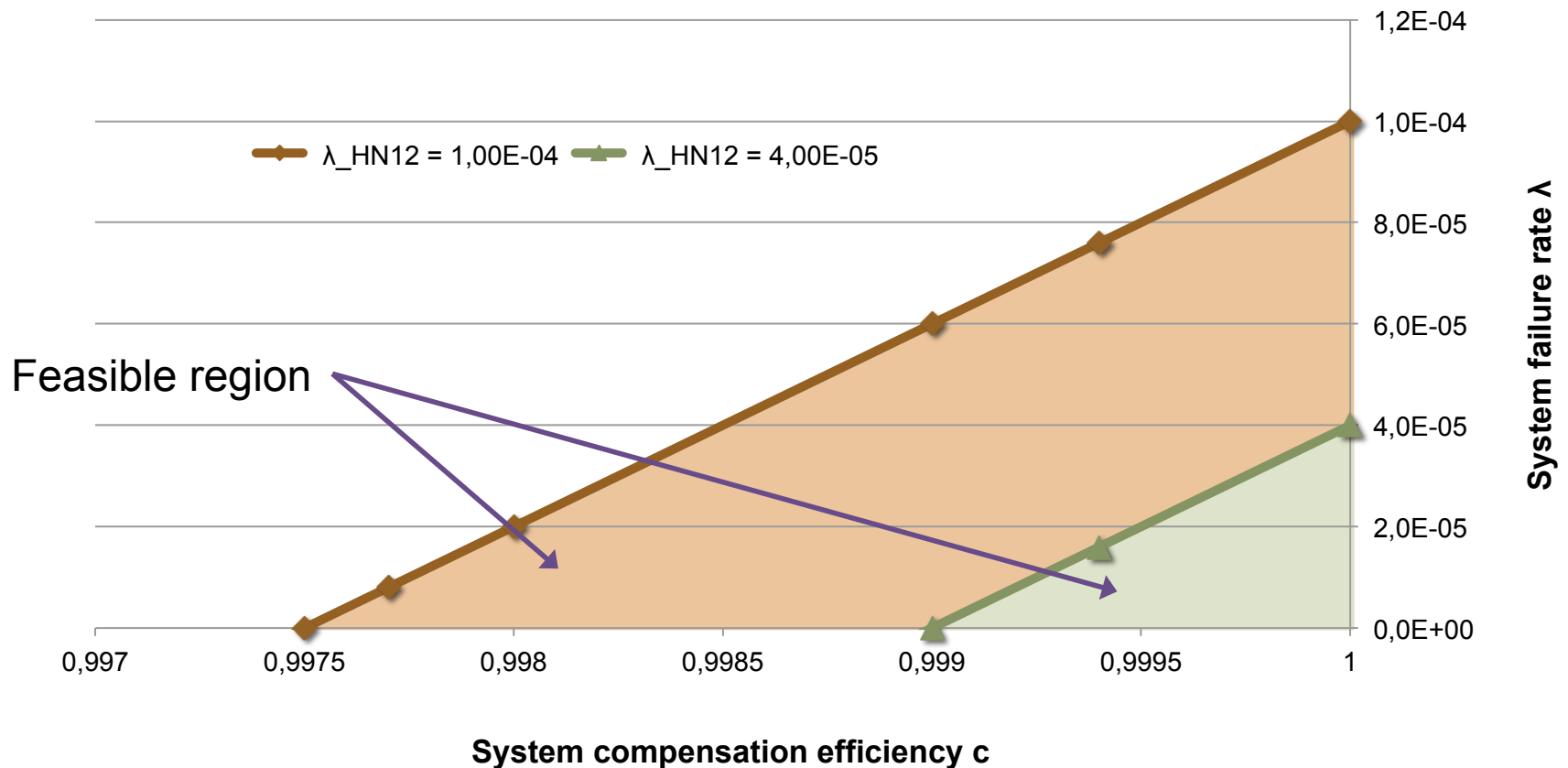
$$\lambda_{HN12} \approx \lambda + (1 - c) * \alpha$$

$\lambda \approx 10^{-4}$ per hour
 $\alpha \approx 4 * 10^{-2}$ per hour (1 fall per day)
 $\mu \approx 60$ per hour (compensation in 1 minute)

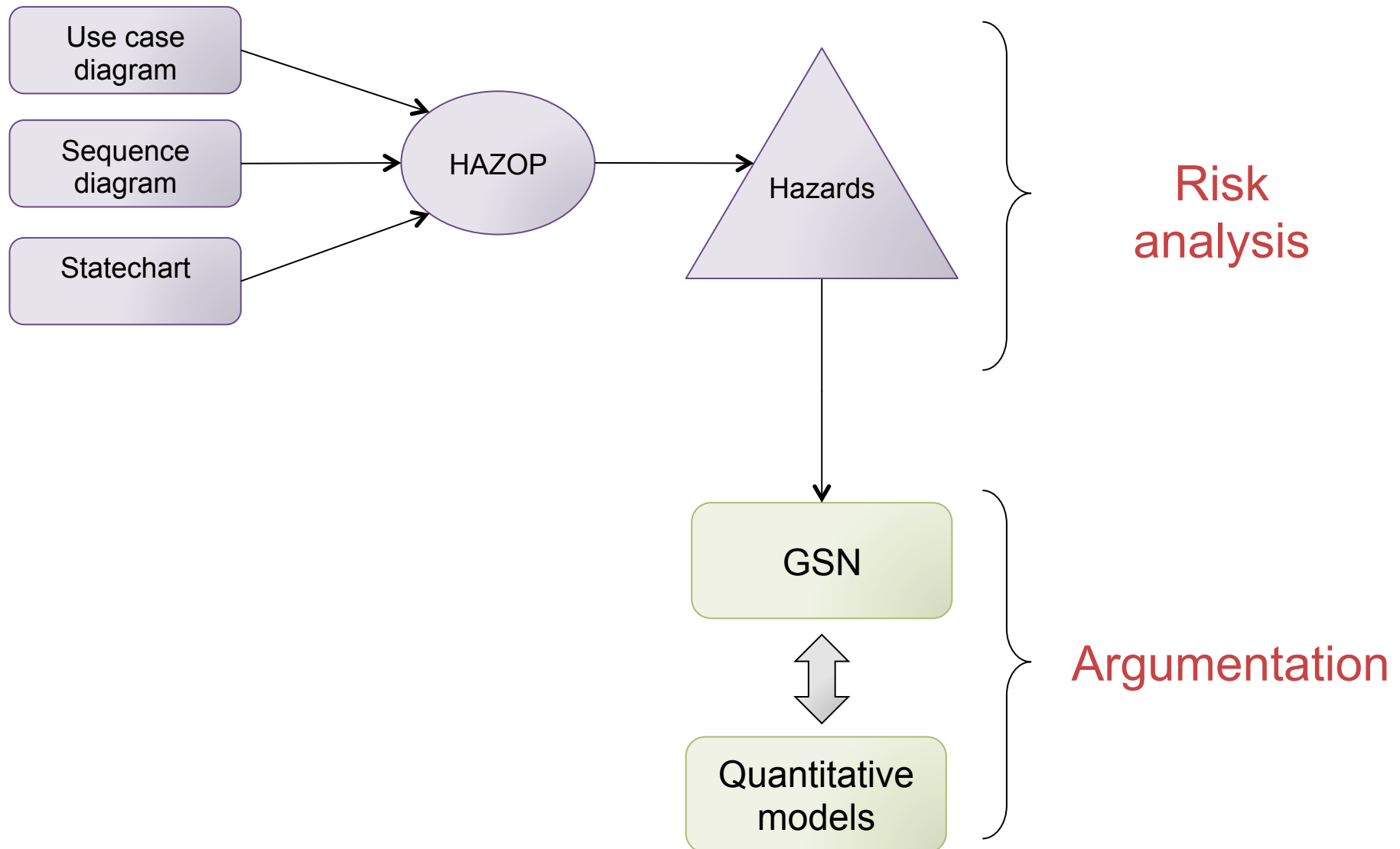
Which values of c_{\min} and λ_{\max} ?

$$\lambda \approx \lambda_{\text{HN12}} - (1 - c) \cdot \alpha$$

$$\alpha \approx 4 \cdot 10^{-2} \text{ per hour}$$



UML models



Thank you for your attention !



LAAS-CNRS



MODEL-BASED RISK ANALYSIS OF HUMAN-ROBOT INTERACTIONS AND SAFETY ARGUMENT CONSTRUCTION

Quynh Anh DO HOANG

Jérémie GUIOCHET

Mohamed KAÂNICHE

David POWELL

qdohoang@laas.fr

Model-based Safety Assessment Workshop
ISAE Campus de Rangueil – Toulouse March 15,16 2011