MEDICUSSY

Risk assessment for medical devices

Motivation & Context

Medical devices domain characteristics

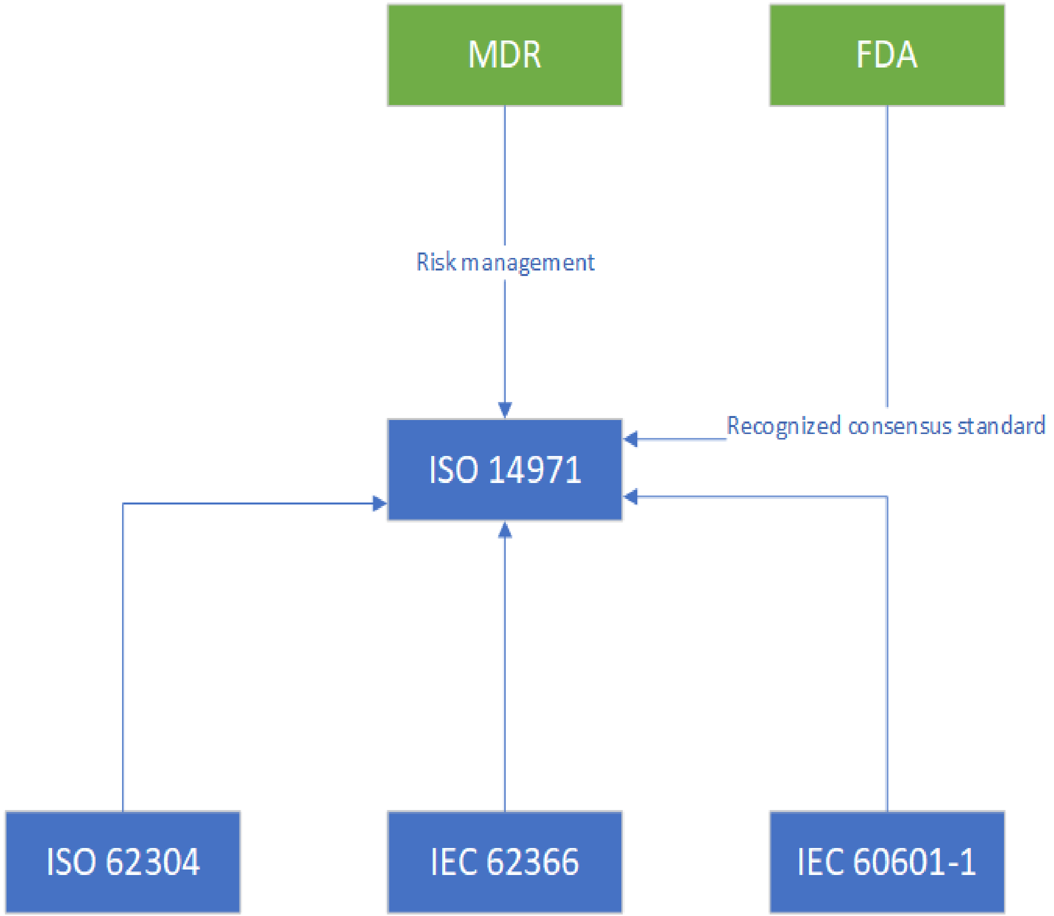
- Significant documentation effort to gain certification
- Today, document driven development approach
- Risk management (RM) activities are a cost driver
- Lack of standardized methods and practices to qualify medical equipment
- RM information-wise decoupled from engineering

Objectives

- Provide standard based method implementation for RM
- Enable integration of RM into engineering activities
- Comply with RAAML language and philosophy
- Enable MBSE

Related standards

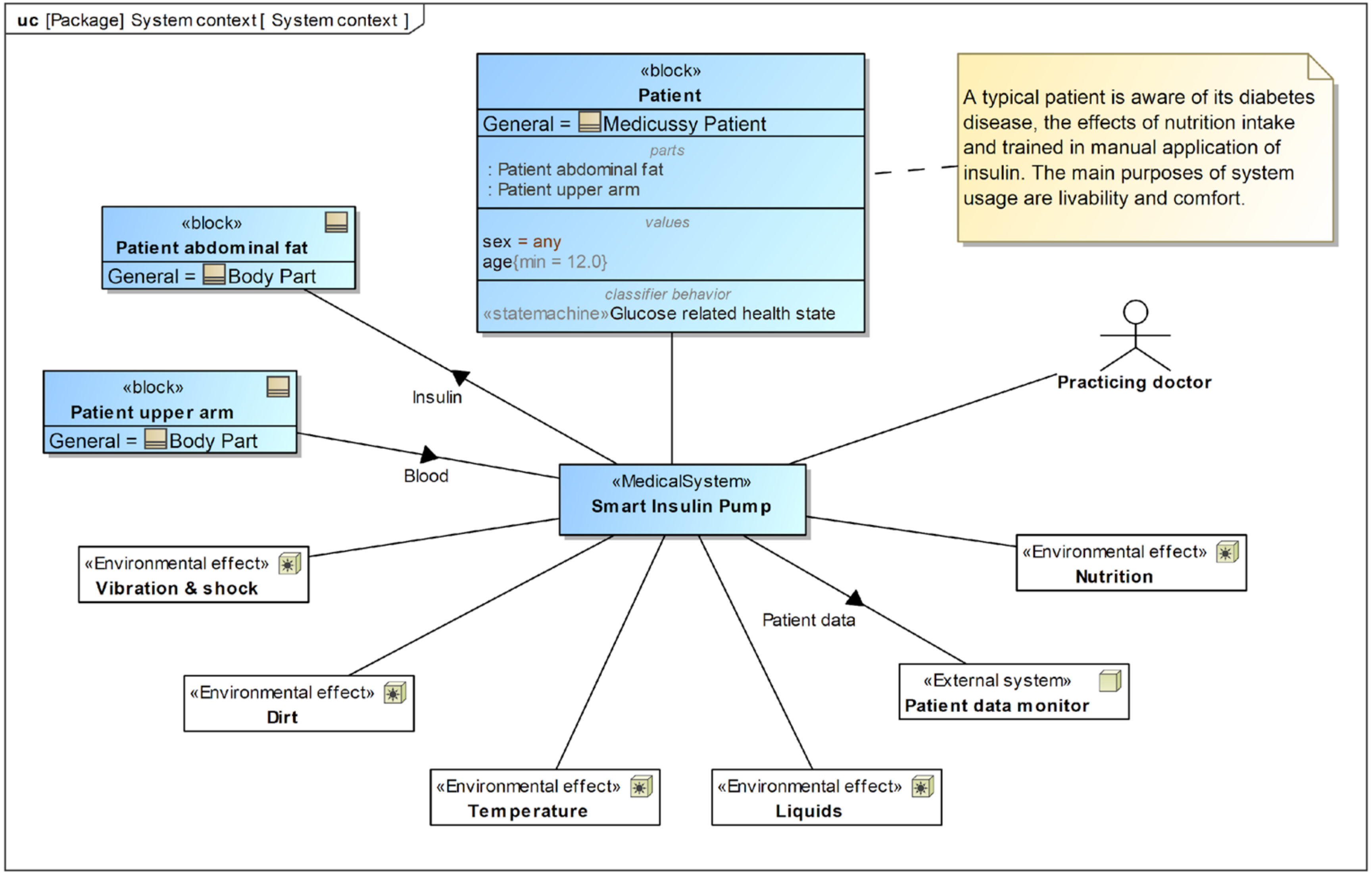
- ISO 14971:2019 – medical devices – Application of risk management to medical devices
- IEC 62304:2006 Medical devices software – Software lifecycle processes
- IEC 62366:2015 Medical devices - Part 1: Application of usability engineering to medical devices
- IEC 60601:2006 - Medical electrical equipment – Part 1: General requirements for basic safety and essential performance
- RAAML Version 1.0
- SysML Version 1.6
- UML Version 2.5.1



Example

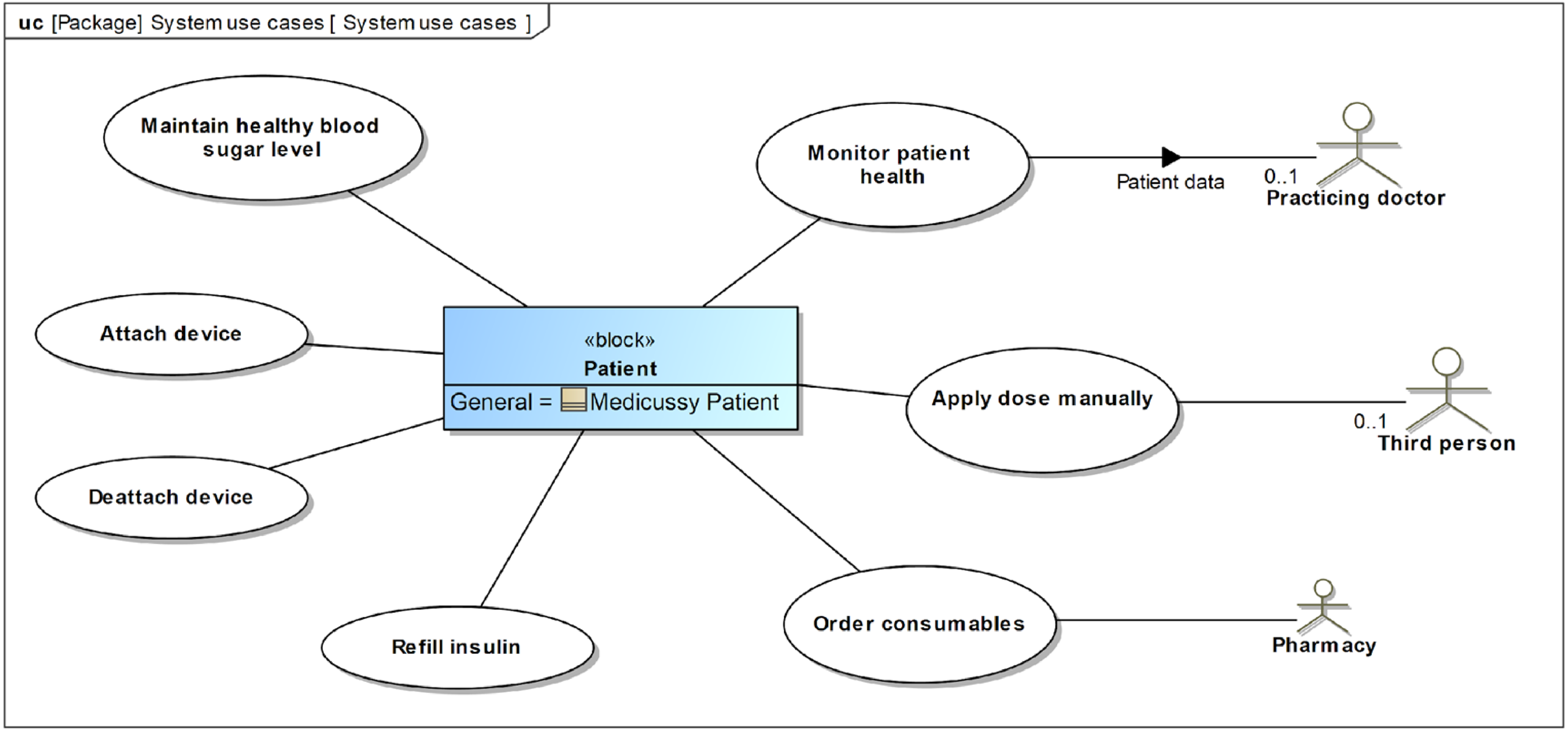
Medicussy in action

Define the system boundary

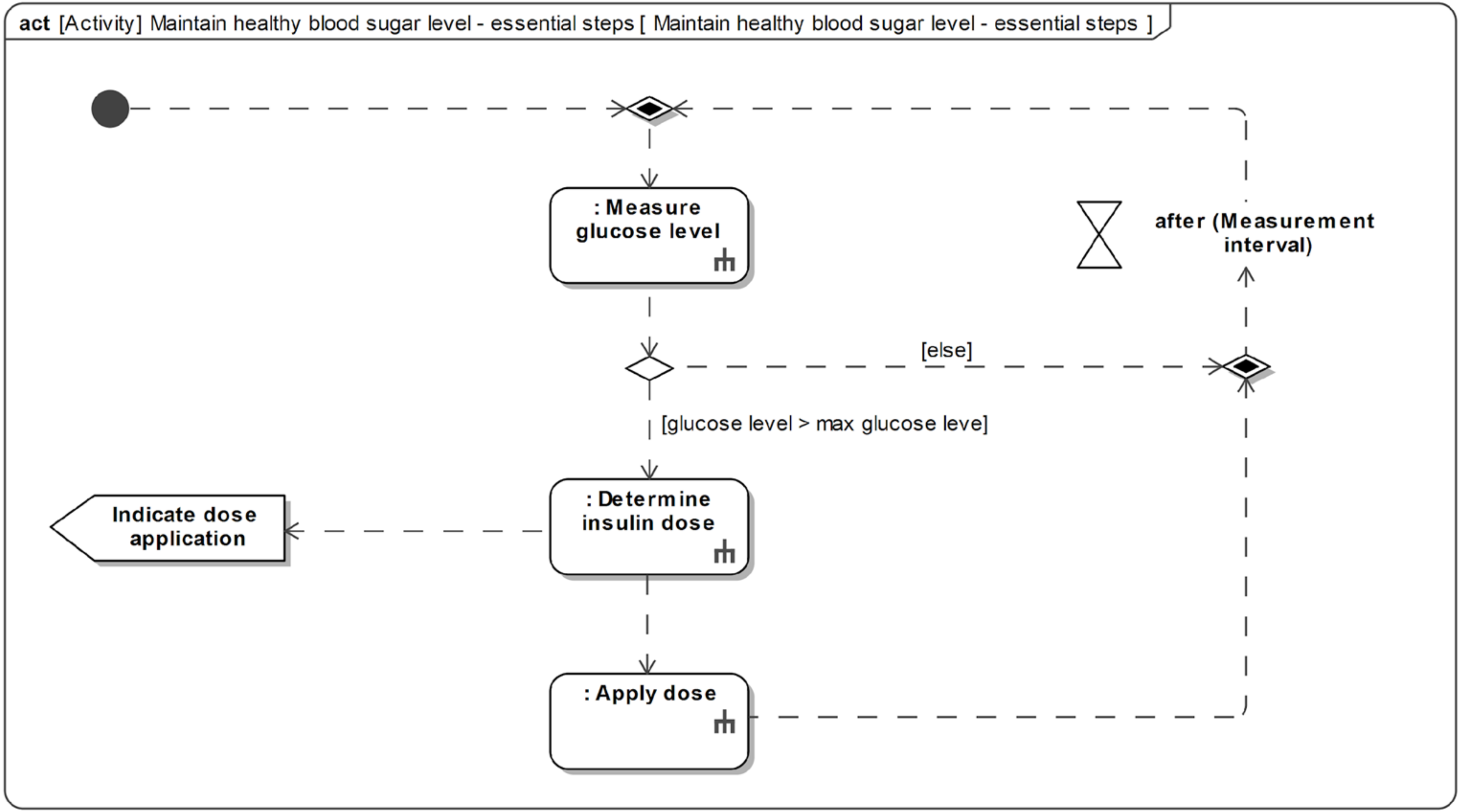


- The blue colored blocks are specializations of Medicussy library items

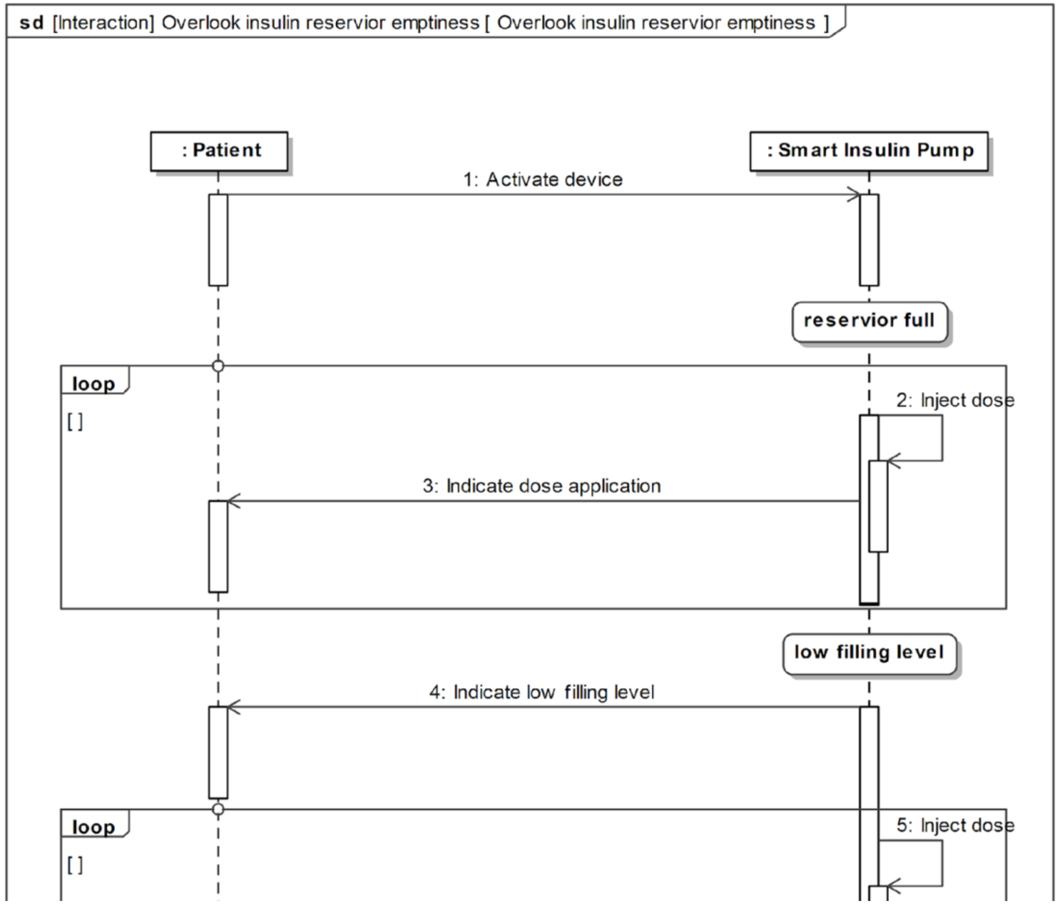
Usability analysis - normal use

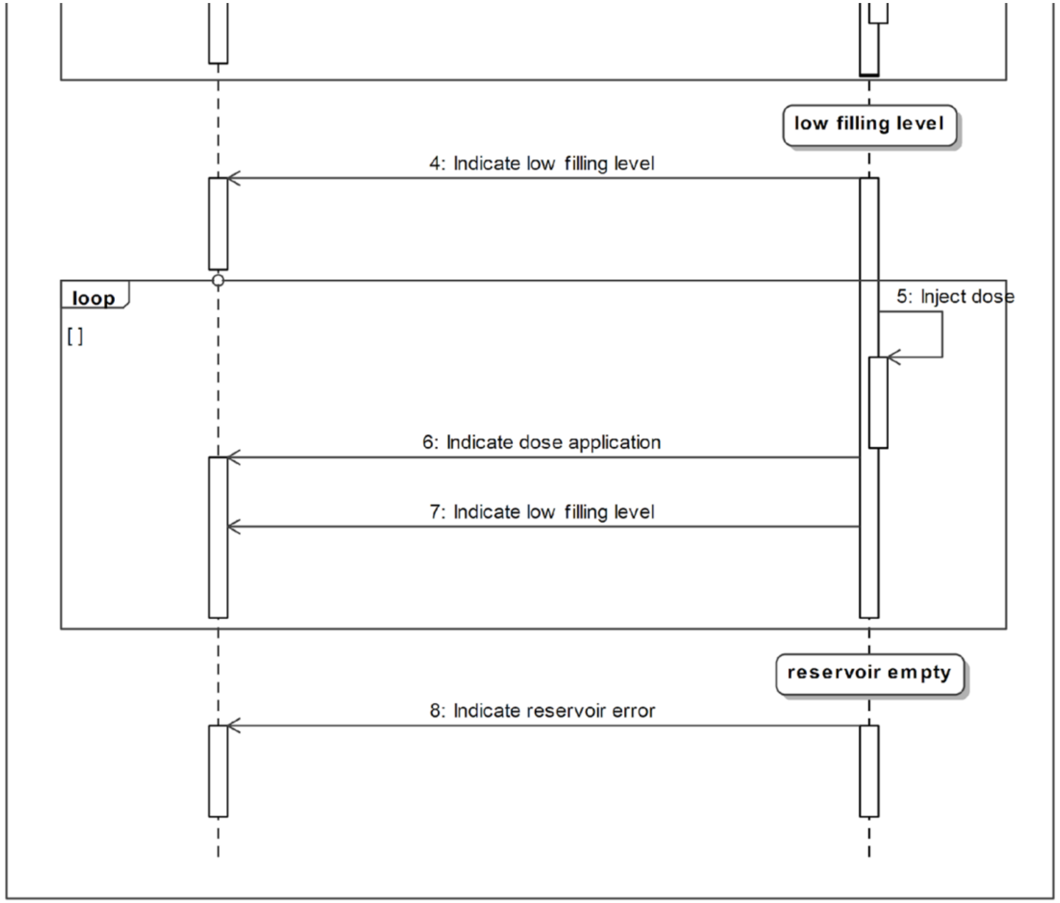


Usability analysis - normal use

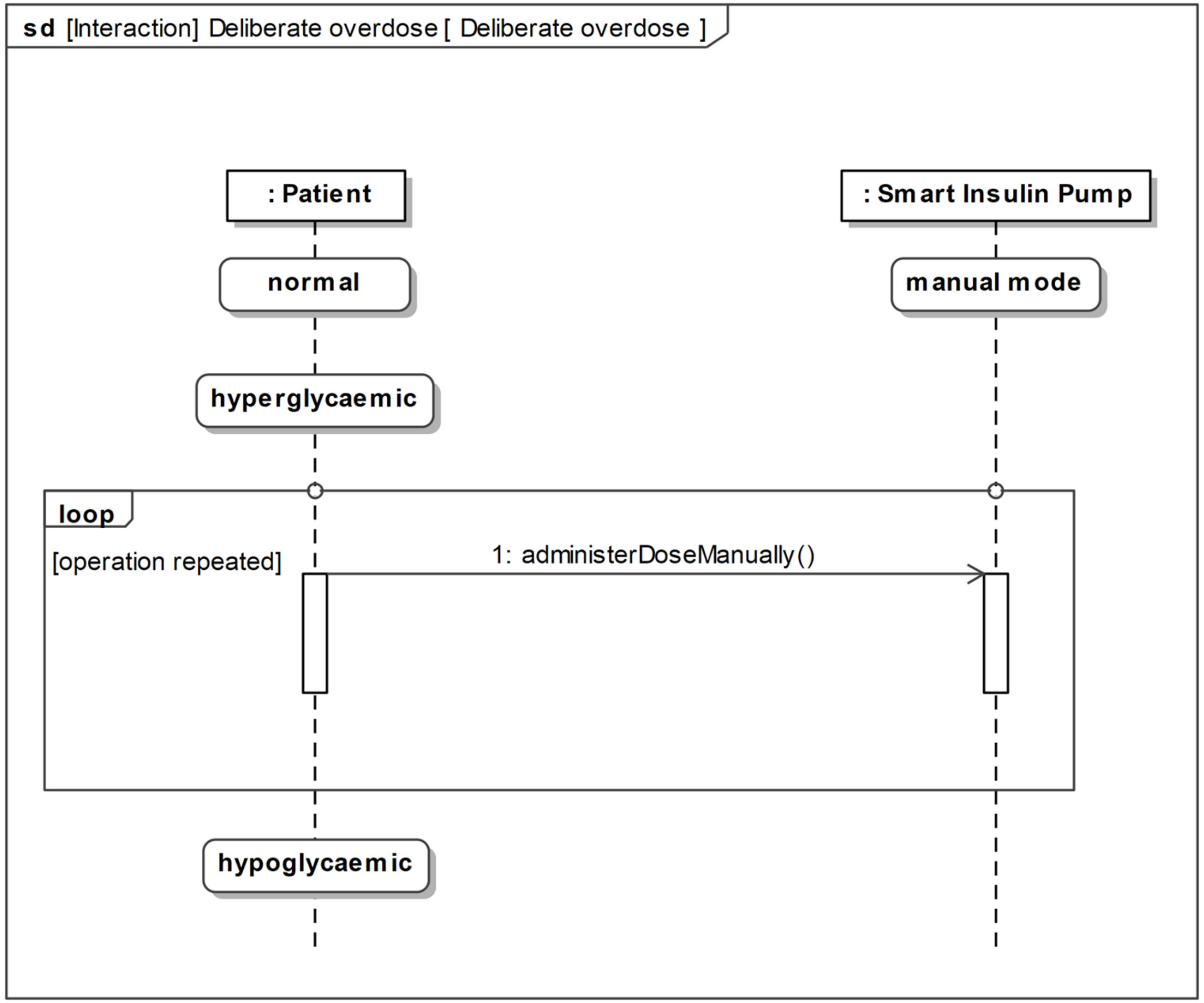

act [Activity] Maintain healthy blood sugar level - essential steps [Maintain healthy blood sugar level - essential steps]
: Measure glucose level
after (Measurement interval)
[else]
[glucose level > max glucose leve]
Indicate dose application
: Determine insulin dose
: Apply dose

Usability analysis - use errors


sd [Interaction] Overlook insulin reservior emptiness [Overlook insulin reservior emptiness]
: Patient
: Smart Insulin Pump
1: Activate device
reservior full
loop
[ ]
2: Inject dose
3: Indicate dose application
low filling level
4: Indicate low filling level
loop
[ ]
5: Inject dose


low filling level
4: Indicate low filling level
loop
[ ]
5: Inject dose
6: Indicate dose application
7: Indicate low filling level
reservoir empty
8: Indicate reservoir error

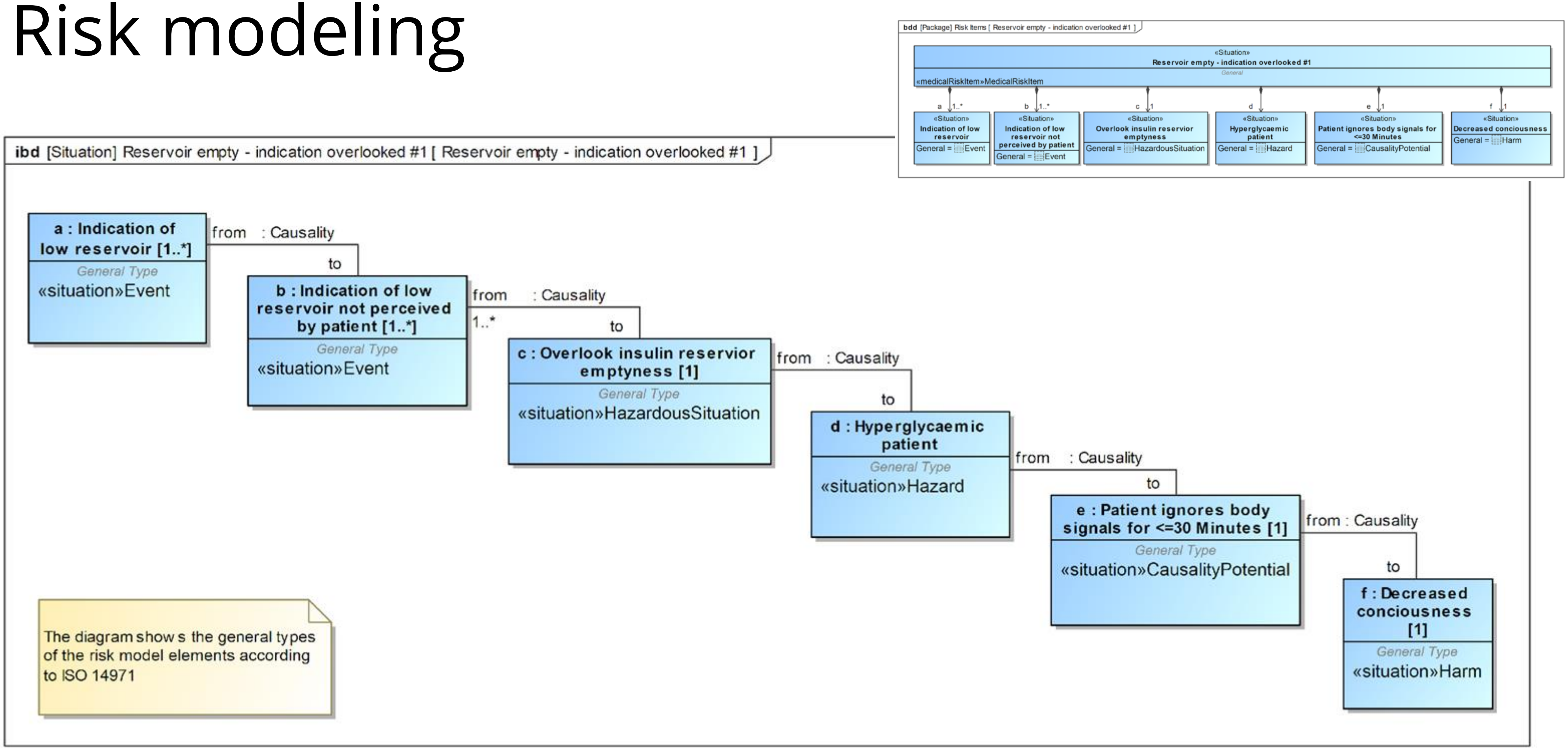
Usability analysis - abnormal use



Abnormal use is defined as “conscious, deliberate act [..] that is counter to or violates NORMAL USE

Source: ISO 62366:2015

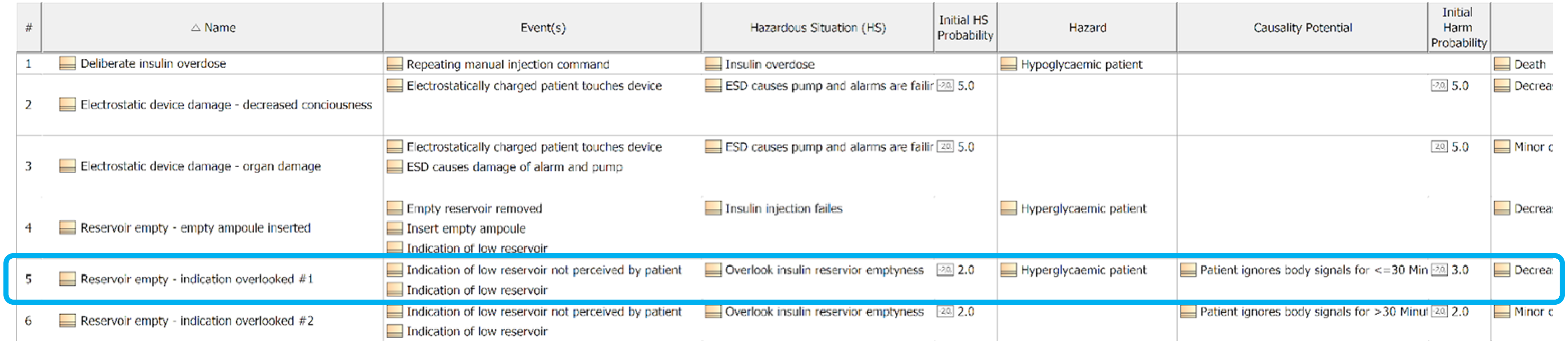
Risk modeling



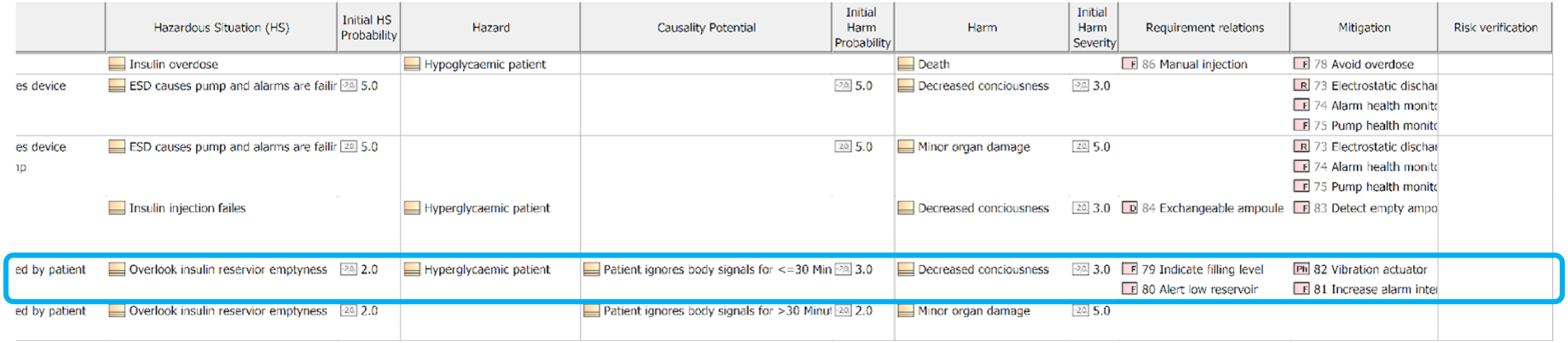
bdd [Package] Risk Items [Reservoir empty - indication overlooked #1]
«Situation»
Reservoir empty - indication overlooked #1
General
«medicalRiskItem»MedicalRiskItem
a 1..*
b 1..*
c 1
d
e 1
f 1
«Situation»
Indication of low reservoir
General = Event
«Situation»
Indication of low reservoir not perceived by patient
General = Event
«Situation»
Overlook insulin reservior emptyness
General = HazardousSituation
«Situation»
Hyperglycaemic patient
General = Hazard
«Situation»
Patient ignores body signals for <=30 Minutes
General = CausalityPotential
«Situation»
Decreased conciousness
General = Harm
ibd [Situation] Reservoir empty - indication overlooked #1 [Reservoir empty - indication overlooked #1]
a : Indication of low reservoir [1..*]
General Type
«situation»Event
from : Causality
to
b : Indication of low reservoir not perceived by patient [1..*]
General Type
«situation»Event
from : Causality
1..*
to
c : Overlook insulin reservior emptyness [1]
General Type
«situation»HazardousSituation
from : Causality
to
d : Hyperglycaemic patient
General Type
«situation»Hazard
from : Causality
to
e : Patient ignores body signals for <=30 Minutes [1]
General Type
«situation»CausalityPotential
from : Causality
to
f : Decreased conciousness [1]
General Type
«situation»Harm

The diagram shows the general types of the risk model elements according to ISO 14971

Risk analysis matrix



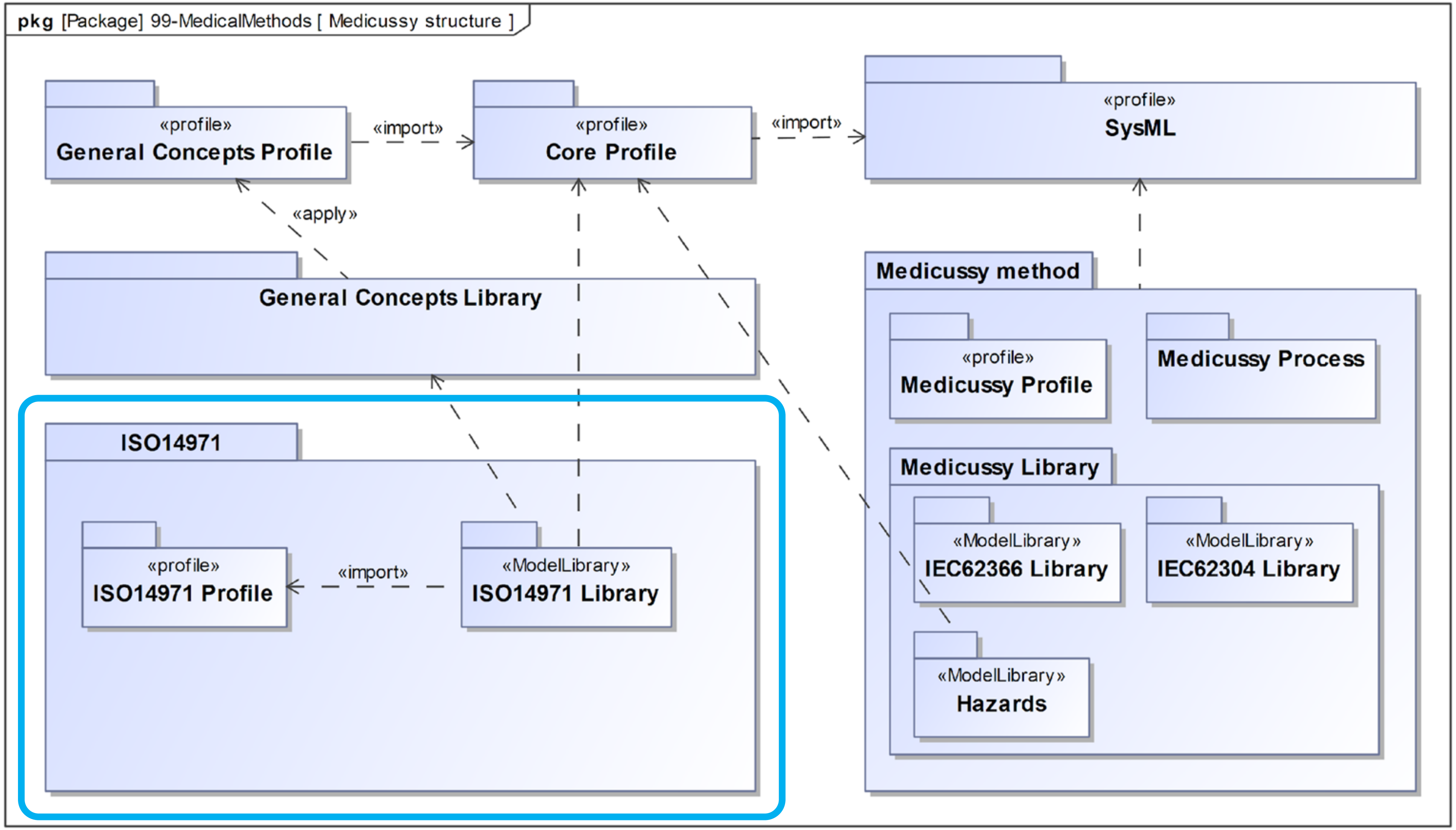
#	△ Name	Event(s)	Hazardous Situation (HS)	Initial HS Probability	Hazard	Causality Potential	Initial Harm Probability	
1	Deliberate insulin overdose	Repeating manual injection command	Insulin overdose		Hypoglycaemic patient			Death
2	Electrostatic device damage - decreased conciousness	Electrostatically charged patient touches device	ESD causes pump and alarms are failir	5.0			5.0	Decrea:
3	Electrostatic device damage - organ damage	Electrostatically charged patient touches device ESD causes damage of alarm and pump	ESD causes pump and alarms are failir	5.0			5.0	Minor c
4	Reservoir empty - empty ampoule inserted	Empty reservoir removed Insert empty ampoule Indication of low reservoir	Insulin injection failes		Hyperglycaemic patient			Decrea:
5	Reservoir empty - indication overlooked #1	Indication of low reservoir not perceived by patient Indication of low reservoir	Overlook insulin reservior emptyness	2.0	Hyperglycaemic patient	Patient ignores body signals for <=30 Min	3.0	Decrea:
6	Reservoir empty - indication overlooked #2	Indication of low reservoir not perceived by patient Indication of low reservoir	Overlook insulin reservior emptyness	2.0		Patient ignores body signals for >30 Minu	2.0	Minor c



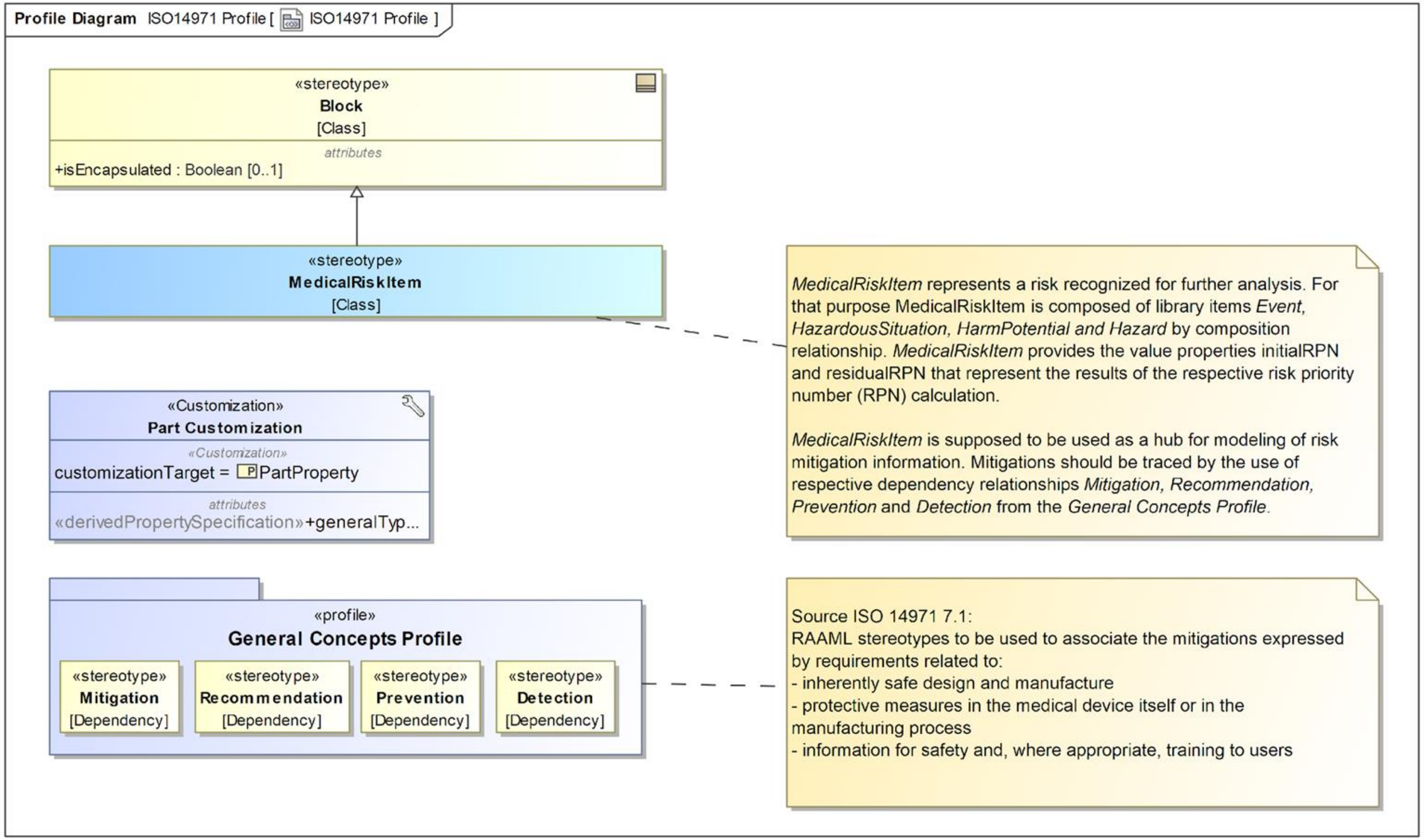
	Hazardous Situation (HS)	Initial HS Probability	Hazard	Causality Potential	Initial Harm Probability	Harm	Initial Harm Severity	Requirement relations	Mitigation	Risk verification
	Insulin overdose		Hypoglycaemic patient			Death		F 86 Manual injection	F 78 Avoid overdose	
es device	ESD causes pump and alarms are failir	5.0			5.0	Decreased conciousness	3.0		R 73 Electrostatic dischar F 74 Alarm health monitc F 75 Pump health monitc	
es device ıp	ESD causes pump and alarms are failir	5.0			5.0	Minor organ damage	5.0		R 73 Electrostatic dischar F 74 Alarm health monitc F 75 Pump health monitc	
	Insulin injection failes		Hyperglycaemic patient			Decreased conciousness	3.0	D 84 Exchangeable ampoule	F 83 Detect empty ampo	
ed by patient	Overlook insulin reservior emptyness	2.0	Hyperglycaemic patient	Patient ignores body signals for <=30 Min	3.0	Decreased conciousness	3.0	F 79 Indicate filling level F 80 Alert low reservoir	Ph 82 Vibration actuator F 81 Increase alarm inte	
ed by patient	Overlook insulin reservior emptyness	2.0		Patient ignores body signals for >30 Minu	2.0	Minor organ damage	5.0			

ISO 14971 Profile & Library

Medicussy structure



ISO 14971 Profile



MedicalRiskItem represents a risk recognized for further analysis. For that purpose MedicalRiskItem is composed of library items *Event, HazardousSituation, HarmPotential and Hazard* by composition relationship. *MedicalRiskItem* provides the value properties initialRPN and residualRPN that represent the results of the respective risk priority number (RPN) calculation.

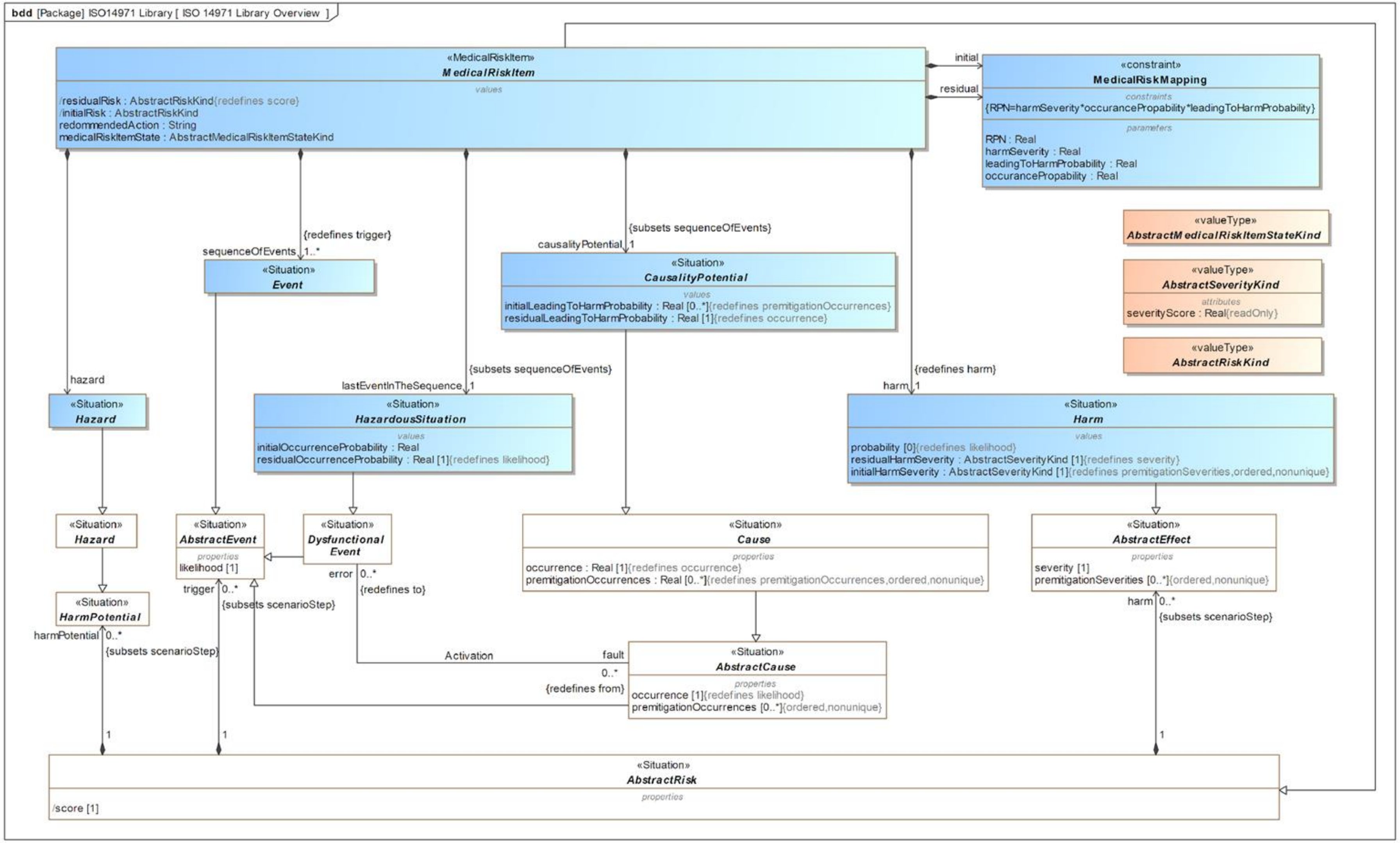
MedicalRiskItem is supposed to be used as a hub for modeling of risk mitigation information. Mitigations should be traced by the use of respective dependency relationships *Mitigation, Recommendation, Prevention* and *Detection* from the *General Concepts Profile*.

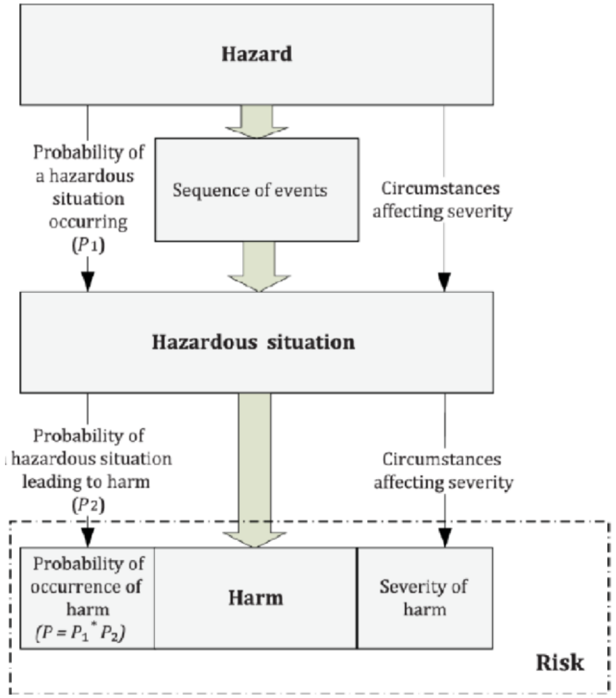
Source ISO 14971 7.1:
RAAML stereotypes to be used to associate the mitigations expressed by requirements related to:
- inherently safe design and manufacture
- protective measures in the medical device itself or in the manufacturing process
- information for safety and, where appropriate, training to users

MedicalRiskItem is not a normative term within ISO 14971.

The ISO 14971 profile introduces the stereotype MedicalRiskItem in order to manage risk in the model analogue to RAAML FMEA implementation.

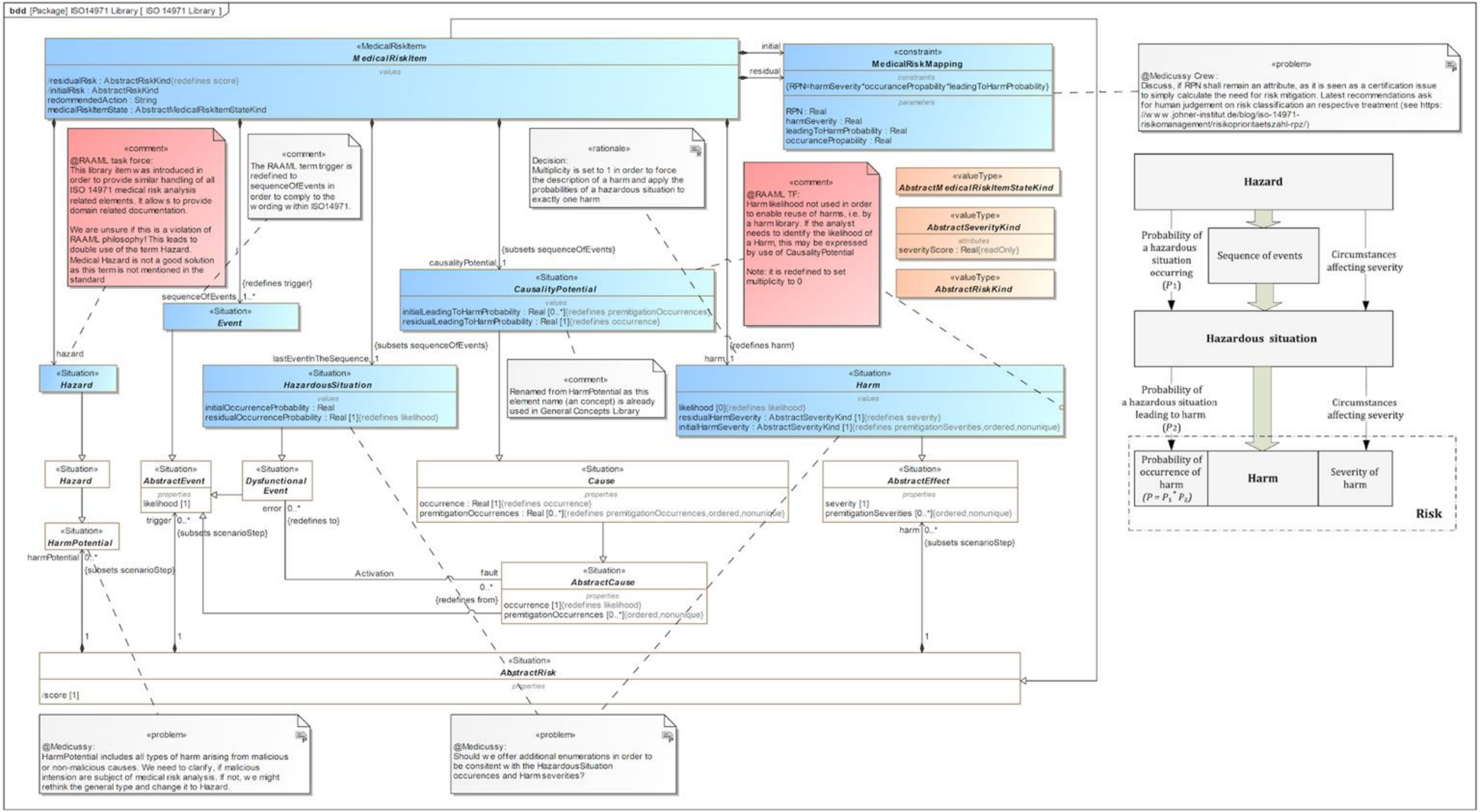
ISO 14971 Library


bdd [Package] ISO14971 Library [ISO 14971 Library Overview]
«MedicalRiskItem»
MedicalRiskItem
values
/residualRisk : AbstractRiskKind{redefines score}
/initialRisk : AbstractRiskKind
redommendedAction : String
medicalRiskItemState : AbstractMedicalRiskItemStateKind
initial
residual
«constraint»
MedicalRiskMapping
constraints
{RPN=harmSeverity*occuranceProbability*leadingToHarmProbability}
parameters
RPN : Real
harmSeverity : Real
leadingToHarmProbability : Real
occuranceProbability : Real
«valueType»
AbstractMedicalRiskItemStateKind
«valueType»
AbstractSeverityKind
attributes
severityScore : Real{readOnly}
«valueType»
AbstractRiskKind
{redefines trigger}
sequenceOfEvents 1..*
«Situation»
Event
{subsets sequenceOfEvents}
causalityPotential 1
«Situation»
CausalityPotential
values
initialLeadingToHarmProbability : Real [0..*]{redefines premitigationOccurrences}
residualLeadingToHarmProbability : Real [1]{redefines occurrence}
hazard
«Situation»
Hazard
{subsets sequenceOfEvents}
lastEventInTheSequence 1
«Situation»
HazardousSituation
values
initialOccurrenceProbability : Real
residualOccurrenceProbability : Real [1]{redefines likelihood}
{redefines harm}
harm 1
«Situation»
Harm
values
probability [0]{redefines likelihood}
residualHarmSeverity : AbstractSeverityKind [1]{redefines severity}
initialHarmSeverity : AbstractSeverityKind [1]{redefines premitigationSeverities,ordered,nonunique}
«Situation»
Hazard
«Situation»
AbstractEvent
properties
likelihood [1]
«Situation»
Dysfunctional Event
error 0..*
{redefines to}
trigger 0..*
{subsets scenarioStep}
«Situation»
Cause
properties
occurrence : Real [1]{redefines occurrence}
premitigationOccurrences : Real [0..*]{redefines premitigationOccurrences,ordered,nonunique}
«Situation»
AbstractEffect
properties
severity [1]
premitigationSeverities [0..*]{ordered,nonunique}
harm 0..*
{subsets scenarioStep}
«Situation»
HarmPotential
harmPotential 0..*
{subsets scenarioStep}
Activation
fault
0..*
{redefines from}
«Situation»
AbstractCause
properties
occurrence [1]{redefines likelihood}
premitigationOccurrences [0..*]{ordered,nonunique}
1
1
1
«Situation»
AbstractRisk
properties
/score [1]


Hazard
Probability of a hazardous situation occurring (P_1)
Sequence of events
Circumstances affecting severity
Hazardous situation
Probability of hazardous situation leading to harm (P_2)
Circumstances affecting severity
Probability of occurrence of harm ($P = P_1 * P_2$)
Harm
Severity of harm
Risk

Source: ISO 14971:2019 Annex C

Open issues


bdd [Package] ISO14971 Library [ISO 14971 Library]
«MedicalRiskItem»
MedicalRiskItem
values
/residualRisk : AbstractRiskKind{redefines score}
/initialRisk : AbstractRiskKind
redommendedAction : String
medicalRiskItemState : AbstractMedicalRiskItemStateKind
initial
residual
«constraint»
MedicalRiskMapping
constraints
{RPN=harmSeverity*occuranceProbability*leadingToHarmProbability}
parameters
RPN : Real
harmSeverity : Real
leadingToHarmProbability : Real
occuranceProbability : Real
«valueType»
AbstractMedicalRiskItemStateKind
«valueType»
AbstractSeverityKind
attributes
severityScore : Real{readOnly}
«valueType»
AbstractRiskKind
{subsets sequenceOfEvents}
causalityPotential 1
«Situation»
CausalityPotential
values
initialLeadingToHarmProbability : Real [0..*]{redefines premitigationOccurrences}
residualLeadingToHarmProbability : Real [1]{redefines occurrence}
{redefines trigger}
sequenceOfEvents 1..*
«Situation»
Event
hazard
«Situation»
Hazard
{subsets sequenceOfEvents}
lastEventInTheSequence 1
«Situation»
HazardousSituation
values
initialOccurrenceProbability : Real
residualOccurrenceProbability : Real [1]{redefines likelihood}
{redefines harm}
harm 1
«Situation»
Harm
values
likelihood [0]{redefines likelihood}
residualHarmSeverity : AbstractSeverityKind [1]{redefines severity}
initialHarmSeverity : AbstractSeverityKind [1]{redefines premitigationSeverities,ordered,nonunique}
«Situation»
Hazard
«Situation»
AbstractEvent
properties
likelihood [1]
«Situation»
Dysfunctional Event
error 0..*
{redefines to}
trigger 0..*
{subsets scenarioStep}
«Situation»
HarmPotential
harmPotential 0..*
{subsets scenarioStep}
«Situation»
Cause
properties
occurrence : Real [1]{redefines occurrence}
premitigationOccurrences : Real [0..*]{redefines premitigationOccurrences,ordered,nonunique}
«Situation»
AbstractEffect
properties
severity [1]
premitigationSeverities [0..*]{ordered,nonunique}
harm 0..*
{subsets scenarioStep}
Activation
fault
0..*
{redefines from}
«Situation»
AbstractCause
properties
occurrence [1]{redefines likelihood}
premitigationOccurrences [0..*]{ordered,nonunique}
1
1
1
«Situation»
AbstractRisk
properties
/score [1]
Hazard
Sequence of events
Probability of a hazardous situation occurring (P_1)
Circumstances affecting severity
Hazardous situation
Probability of a hazardous situation leading to harm (P_2)
Circumstances affecting severity
Probability of occurrence of harm ($P = P_1 * P_2$)
Harm
Severity of harm
Risk

«comment»
@RAAML task force:
This library item was introduced in order to provide similar handling of all ISO 14971 medical risk analysis related elements. It allows to provide domain related documentation.

We are unsure if this is a violation of RAAML philosophy! This leads to double use of the term Hazard. Medical Hazard is not a good solution as this term is not mentioned in the standard

«comment»
The RAAML term trigger is redefined to sequenceOfEvents in order to comply to the wording within ISO14971.

«rationale»
Decision:
Multiplicity is set to 1 in order to force the description of a harm and apply the probabilities of a hazardous situation to exactly one harm

«comment»
@RAAML TF:
Harm likelihood not used in order to enable reuse of harms, i.e. by a harm library. If the analyst needs to identify the likelihood of a Harm, this may be expressed by use of CausalityPotential

Note: it is redefined to set multiplicity to 0

«problem»
@Medicussy Crew :
Discuss, if RPN shall remain an attribute, as it is seen as a certification issue to simply calculate the need for risk mitigation. Latest recommendations ask for human judgement on risk classification an respective treatment (see https://www.johner-institut.de/blog/iso-14971-risikomanagement/risikoprioritaetszahl-rpz/)

«comment»
Renamed from HarmPotential as this element name (an concept) is already used in General Concepts Library

«problem»
@Medicussy:
HarmPotential includes all types of harm arising from malicious or non-malicious causes. We need to clarify, if malicious intension are subject of medical risk analysis. If not, we might rethink the general type and change it to Hazard.

«problem»
@Medicussy:
Should we offer additional enumerations in order to be consitent with the HazardousSituation occurences and Harm severities?

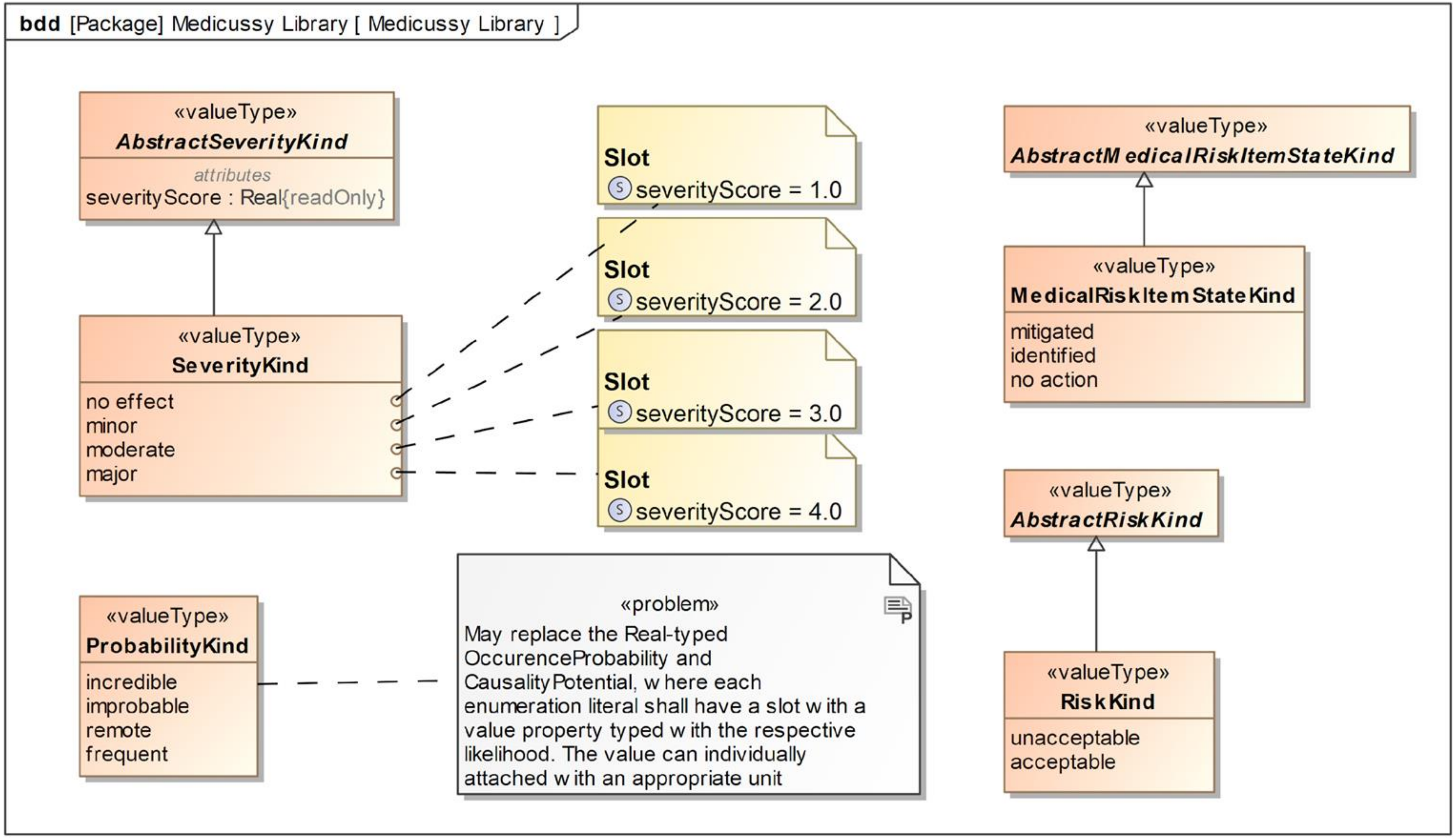
General questions

- Recommendations how to share with the community?
- Do you see this project as relevant future RAAML extension?
- Smart modeling with library driven approach, especially:
  - Creating risk model compositions
  - Automatic generalization
  - Redefine assistance

Implementation

Potential addons to support risk management method implementation

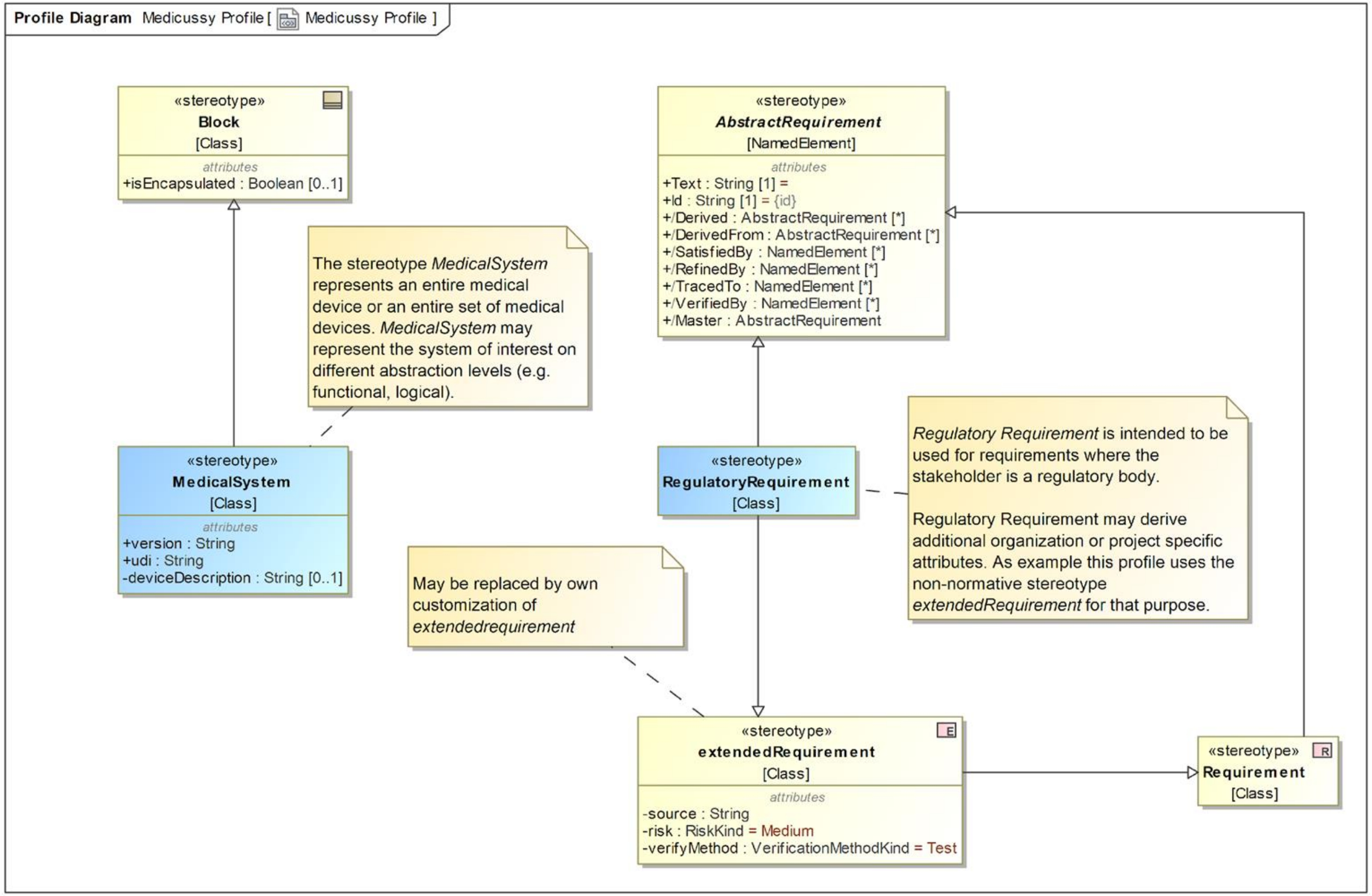
Medicussy Library



May replace the Real-typed OccurenceProbability and CausalityPotential, where each enumeration literal shall have a slot with a value property typed with the respective likelihood. The value can individually attached with an appropriate unit

Selected library items that are introduced to support medical system analysis in accordance to applicable ISO 14971

Medicussy Profile



Profile Diagram Medicussy Profile [Medicussy Profile]

«stereotype»
Block
[Class]
attributes
+isEncapsulated : Boolean [0..1]

«stereotype»
AbstractRequirement
[NamedElement]
attributes
+Text : String [1] =
+Id : String [1] = {id}
+/Derived : AbstractRequirement [*]
+/DerivedFrom : AbstractRequirement [*]
+/SatisfiedBy : NamedElement [*]
+/RefinedBy : NamedElement [*]
+/TracedTo : NamedElement [*]
+/VerifiedBy : NamedElement [*]
+/Master : AbstractRequirement

The stereotype *MedicalSystem* represents an entire medical device or an entire set of medical devices. *MedicalSystem* may represent the system of interest on different abstraction levels (e.g. functional, logical).

«stereotype»
MedicalSystem
[Class]
attributes
+version : String
+udi : String
-deviceDescription : String [0..1]

«stereotype»
RegulatoryRequirement
[Class]

Regulatory Requirement is intended to be used for requirements where the stakeholder is a regulatory body.

Regulatory Requirement may derive additional organization or project specific attributes. As example this profile uses the non-normative stereotype *extendedRequirement* for that purpose.

May be replaced by own customization of *extendedrequirement*

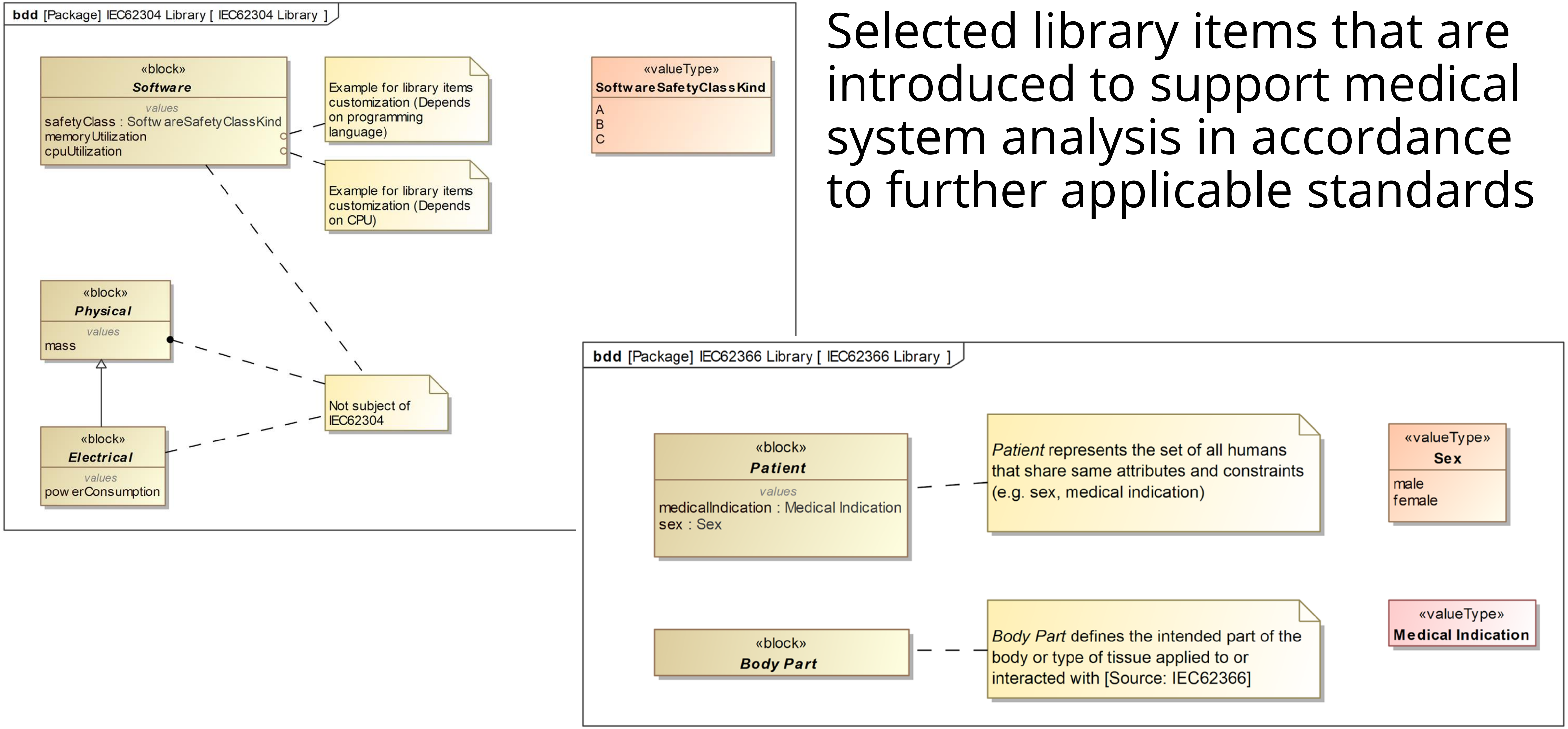
«stereotype»
extendedRequirement
[Class]
attributes
-source : String
-risk : RiskKind = Medium
-verifyMethod : VerificationMethodKind = Test

«stereotype»
Requirement
[Class]

Selected stereotypes that are introduced to support medical system analysis

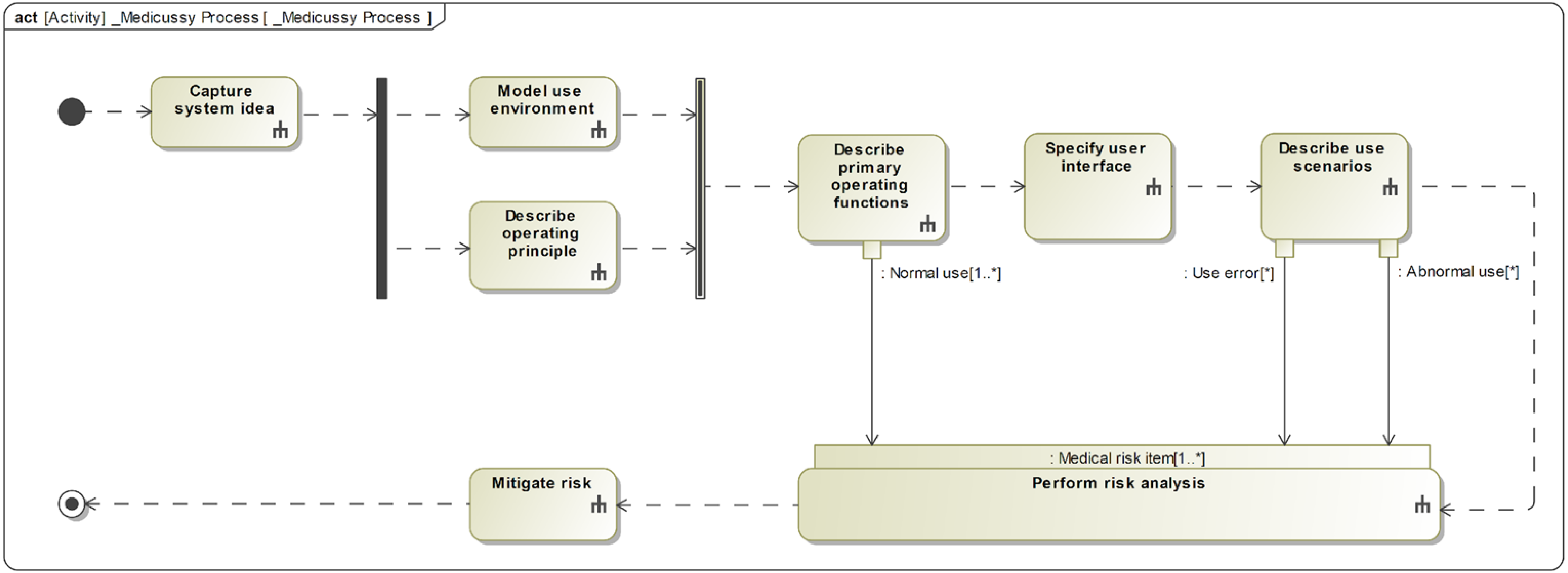
IEC 62304 & IEC 62366 Library

Selected library items that are introduced to support medical system analysis in accordance to further applicable standards



bdd [Package] IEC62304 Library [IEC62304 Library]
«block»
Software
values
safetyClass : SoftwareSafetyClassKind
memoryUtilization
cpuUtilization
Example for library items customization (Depends on programming language)
Example for library items customization (Depends on CPU)
«valueType»
SoftwareSafetyClassKind
A
B
C
«block»
Physical
values
mass
«block»
Electrical
values
powerConsumption
Not subject of IEC62304
bdd [Package] IEC62366 Library [IEC62366 Library]
«block»
Patient
values
medicalIndication : Medical Indication
sex : Sex
Patient represents the set of all humans that share same attributes and constraints (e.g. sex, medical indication)
«valueType»
Sex
male
female
«block»
Body Part
Body Part defines the intended part of the body or type of tissue applied to or interacted with [Source: IEC62366]
«valueType»
Medical Indication

Risk management process – initial analysis


act [Activity] _Medicussy Process [_Medicussy Process]
Capture system idea
Model use environment
Describe operating principle
Describe primary operating functions
Specify user interface
Describe use scenarios
: Normal use[1..*]
: Use error[*]
: Abnormal use[*]
: Medical risk item[1..*]
Perform risk analysis
Mitigate risk