Assurance Case Report

generated on 02.06.2014 at 13:34

by Brian Larson (blarson)

on server: tct.nor-sta.eu

Project name: **Open PCA Pump Assurance Case**

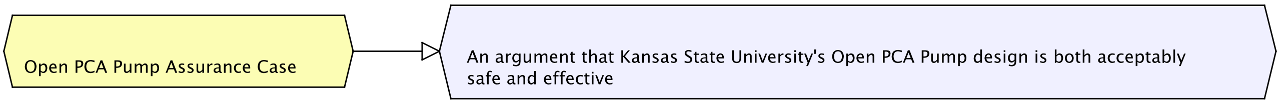
Folder: **pcapac**

Project description:

This assurance case was created to be part of exemplary medical device design artifacts, demonstrating application of best practices by Kansas State University for the US Food and Drug Administration's Scholar-in-Residence program through the National Science Foundation (#0932289, #1239543). As such, this assurance case links to the other artifacts, requirements and design.

List of sections:

1. Open PCA Pump Assurance Case

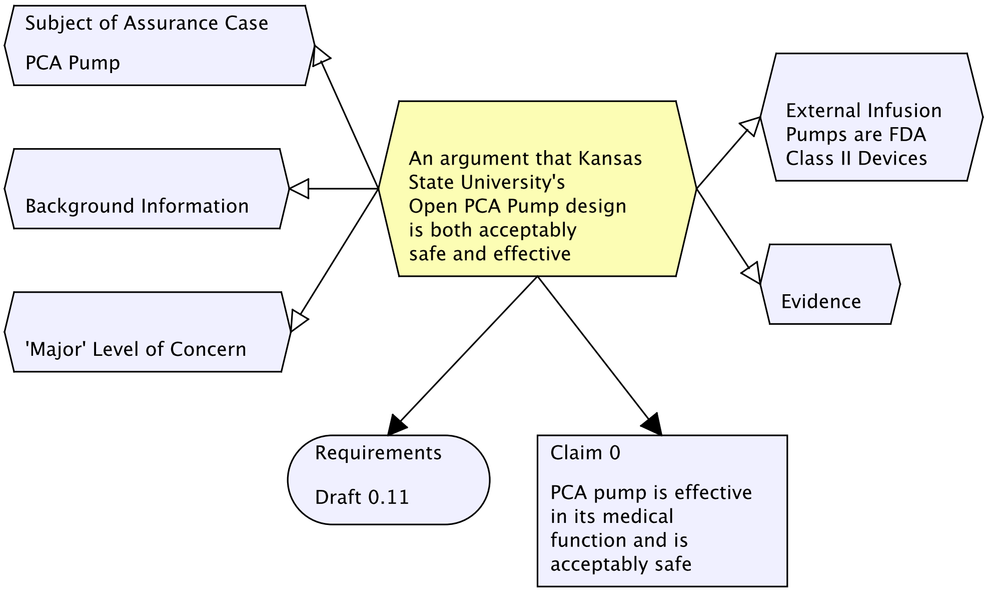

Open PCA Pump Assurance Case
An argument that Kansas State University's Open PCA Pump design is both acceptably safe and effective

Open PCA Pump Assurance Case

An argument that Kansas State University's Open PCA Pump design is both acceptably safe and effective

See details in section 2

2. An argument that Kansas State University's Open PCA Pump design is both acceptably safe and effective


Subject of Assurance Case
PCA Pump
Background Information
'Major' Level of Concern
An argument that Kansas State University's Open PCA Pump design is both acceptably safe and effective
External Infusion Pumps are FDA Class II Devices
Evidence
Requirements
Draft 0.11
Claim 0
PCA pump is effective in its medical function and is acceptably safe

An argument that Kansas State University's Open PCA Pump design is both acceptably safe and effective

This Open PCA Pump assurance case is an exemplary medical device design artifact created as part of the NSF/FDA Scholar in Residence program. It is intended to show a convincing argument that would be part of a submission for FDA medical device approval.

An assurance case should be developed concurrently with device design, starting at the beginning of the project by engineers, not thrown together by Regulatory Affairs during submission preparation.

This assurance case should be considered to be mid-project, necessarily incomplete, with placeholders for test reports and clinical trials. An actual assurance case would continue to be refined and expanded until complete, with references to all the reports and data needed to support asserted facts and claims.

Ideally preparation of an assurance case would be the responsibility of a seasoned, experienced system engineer, with contributions from the entire engineering team with contributions from marketing, regulatory affairs, research, clinical trials, and potential users. Tracing of the argument down to facts from requirements, architecture, verification and validation will be superb training for novice engineers.

Subject of Assurance Case: PCA Pump

The scope of this Open PCA Pump Assurance Case is a hypothetical patient-controlled analgesia pump, its requirements developed according to FAA's Requirements Engineering Management Handbook, and its architectural model in the Architecture Analysis and Design Language.

Requirements: Draft 0.11

Evidence: ICE-PCArequirements.pdf

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 11. Requirements Reference

Background Information

See details in section 3

'Major' Level of Concern

See details in section 4

External Infusion Pumps are FDA Class II Devices

See details in section 6

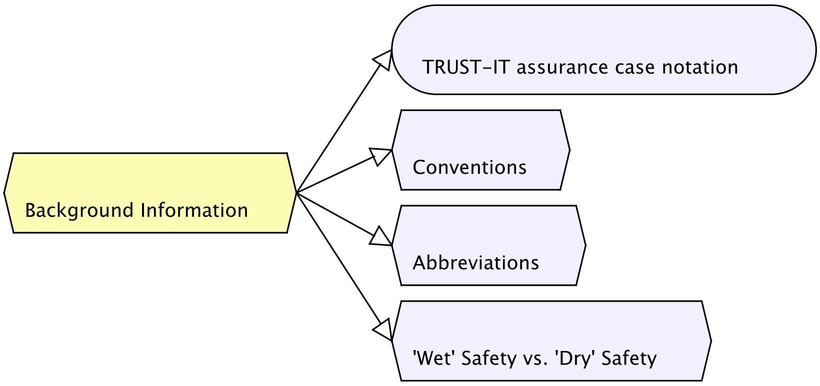
Claim 0: PCA pump is effective in its medical function and is acceptably safe

See details in section 7

Evidence

See details in section 115

3. Background Information


Background Information
TRUST-IT assurance case notation
Conventions
Abbreviations
'Wet' Safety vs. 'Dry' Safety

Background Information

TRUST-IT assurance case notation

Basics of TRUST-IT notation are explained in attached document.

[*note: how you can get the document?*
1) select the "Evidence" bar below
2) click the "Open Evidence" button
A short summary of NOR-STA/TRUST-IT notation will open a .pdf in another tab of your browser.
]

Evidence:	TRUST-IT notation.pdf
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Conventions

All references placed under "Evidence" information node. Then multiple parts of the assurance case can reference the same evidence.

Abbreviations

AADL - Architecture Analysis and Design Language
BLESS - Behavior Language for Embedded Systems with Software
FHA - Functional Hazard Assessment
FMEA - Failure Modes and Effects Analysis
FTA - Fault Tree Analysis
KVO - Keep Vein Open (rate)
OSATE - Open-Source AADL Tool Environment
PCA - Patient-Controlled Analgesic (pump)
RDAL - Requirements Definition and Analysis Language
SFT - System Feature Test
VTBI - Volume To Be Infused

'Wet' Safety vs. 'Dry' Safety

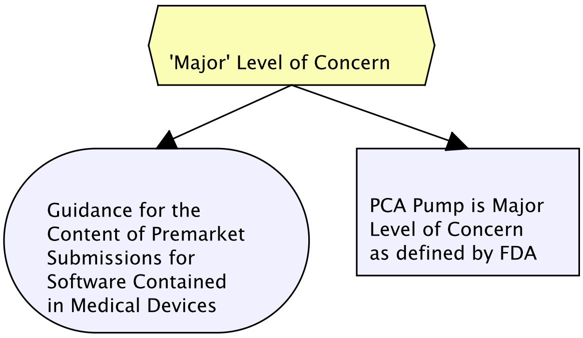
'Wet' safety concerns improper use. 'Dry' safety concerns the device itself.
Achieving safety in practice requires both, but the skills necessary are vastly different.

Wet safety involves human factors and institutional processes that are necessarily subjective. Dry safety can be definitively engineered.

Whenever possible, wet safety hazards should be mitigated by dry safety means. For the Open PCA Pump, hazards due to improper prescription entry are mitigated by reading the prescription from the drug container with a scanner, followed by authentication. Similarly, clinician authorization is enforced by authenticating clinician badges, but the hospital itself must assure that those so authorized are indeed capable, competent, and trained.

Nevertheless, engineered dry safety can never overcome all wet safety hazards. Those think they're being revelatory in pointing this out become tedious and annoying.

4. 'Major' Level of Concern


'Major' Level of Concern
Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices
PCA Pump is Major Level of Concern as defined by FDA

'Major' Level of Concern

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

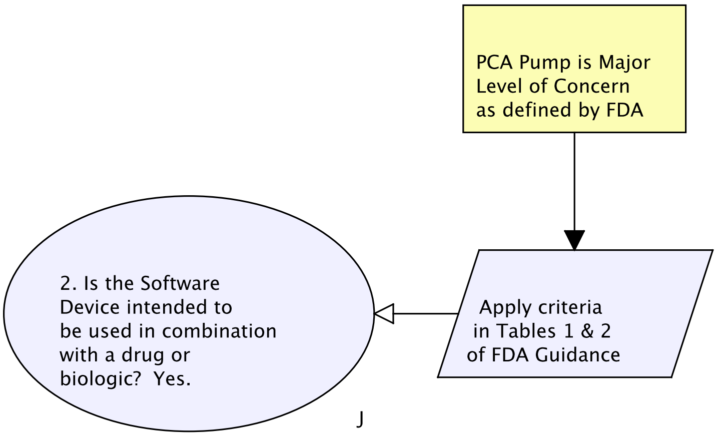
Evidence: FDAHazardAnalysis.pdf#page=8

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA Pump is Major Level of Concern as defined by FDA

See details in section 5

5. PCA Pump is Major Level of Concern as defined by FDA


PCA Pump is Major Level of Concern as defined by FDA
Apply criteria in Tables 1 & 2 of FDA Guidance
2. Is the Software Device intended to be used in combination with a drug or biologic? Yes.
J

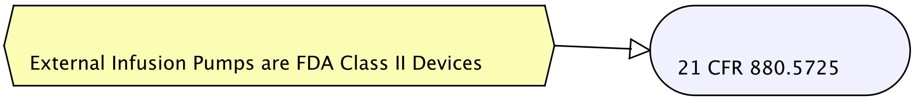
PCA Pump is Major Level of Concern as defined by FDA

Apply criteria in Tables 1 & 2 of FDA Guidance

2. Is the Software Device intended to be used in combination with a drug or biologic? Yes.

Second question of Table 1 in FDA Guidance

6. External Infusion Pumps are FDA Class II Devices



External Infusion Pumps are FDA Class II Devices

1.

19 § 880.5725 Infusion pump

2.

20 (a) Identification. An infusion pump is a device used in a health care facility to pump fluids

3.

21 into a patient in a controlled manner. The device may use a piston pump, a roller pump, or

4.

22 a peristaltic pump and may be powered electrically or mechanically. The device may also

5.

23 operate using a constant force to propel the fluid through a narrow tube which determines

6.

24 the flow rate. The device may include means to detect a fault condition, such as air in, or

7.

25 blockage of, the infusion line and to activate an alarm.

8.

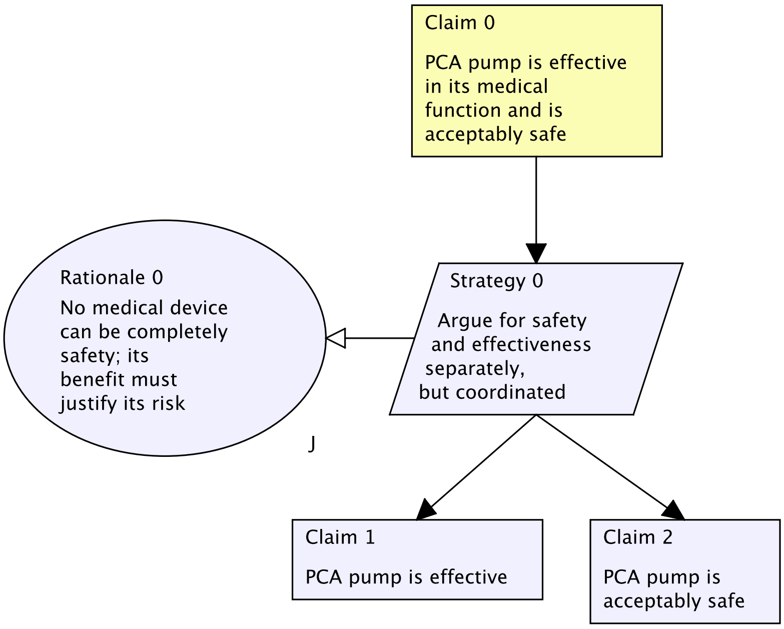
26 (b) Classification. Class II (performance standards).

21 CFR 880.5725

Evidence: IPGenera Guidance.pdf#page=5

Repository: NOR-STA SVN PCAPAC - NOR-STA

7. Claim 0: PCA pump is effective in its medical function and is acceptably safe


Claim 0
PCA pump is effective in its medical function and is acceptably safe
Rationale 0
No medical device can be completely safety; its benefit must justify its risk
J
Strategy 0
Argue for safety and effectiveness separately, but coordinated
Claim 1
PCA pump is effective
Claim 2
PCA pump is acceptably safe

Claim 0: PCA pump is effective in its medical function and is acceptably safe

This is the principal claim of the assurance case. It corresponds to evaluation criteria of medical devices used by US Food and Drug Administration to determine approval.

Strategy 0: Argue for safety and effectiveness separately, but coordinated

Rationale 0: No medical device can be completely safety; its benefit must justify its risk

If you had an ailment that kills 99% of those diagnosed within a year, a drug or device that kills half of those who get it, but extends normal mortality for five years for the others, will be justified.

A PCA pump cures nothing. It merely reduces the pain caused by something else. As such, the acceptable risk of using a PCA pump is very low, but not zero.

Therefor, PCA pump must be exceptionally safe, chasing down and mitigating every possible hazard

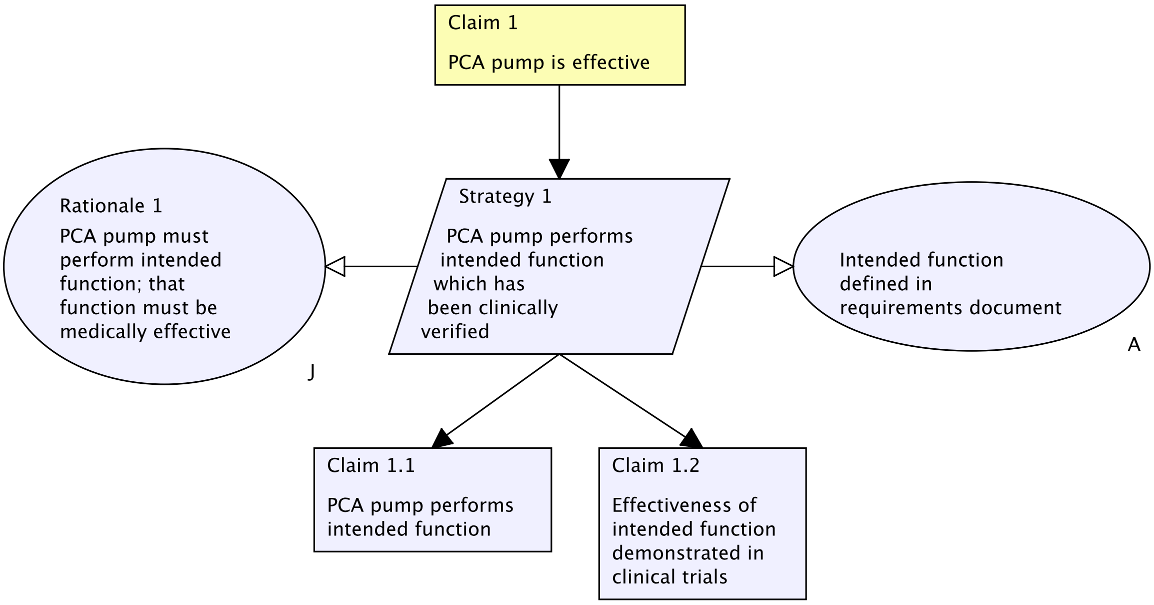
Claim 1: PCA pump is effective

See details in section 8

Claim 2: PCA pump is acceptably safe

See details in section 19

8. Claim 1: PCA pump is effective


Claim 1
PCA pump is effective
Rationale 1
PCA pump must perform intended function; that function must be medically effective
J
Strategy 1
PCA pump performs intended function which has been clinically verified
Intended function defined in requirements document
A
Claim 1.1
PCA pump performs intended function
Claim 1.2
Effectiveness of intended function demonstrated in clinical trials

Claim 1: PCA pump is effective

Strategy 1: PCA pump performs intended function which has been clinically verified

Rationale 1: PCA pump must perform intended function; that function must be medically effective

Intended function defined in requirements document

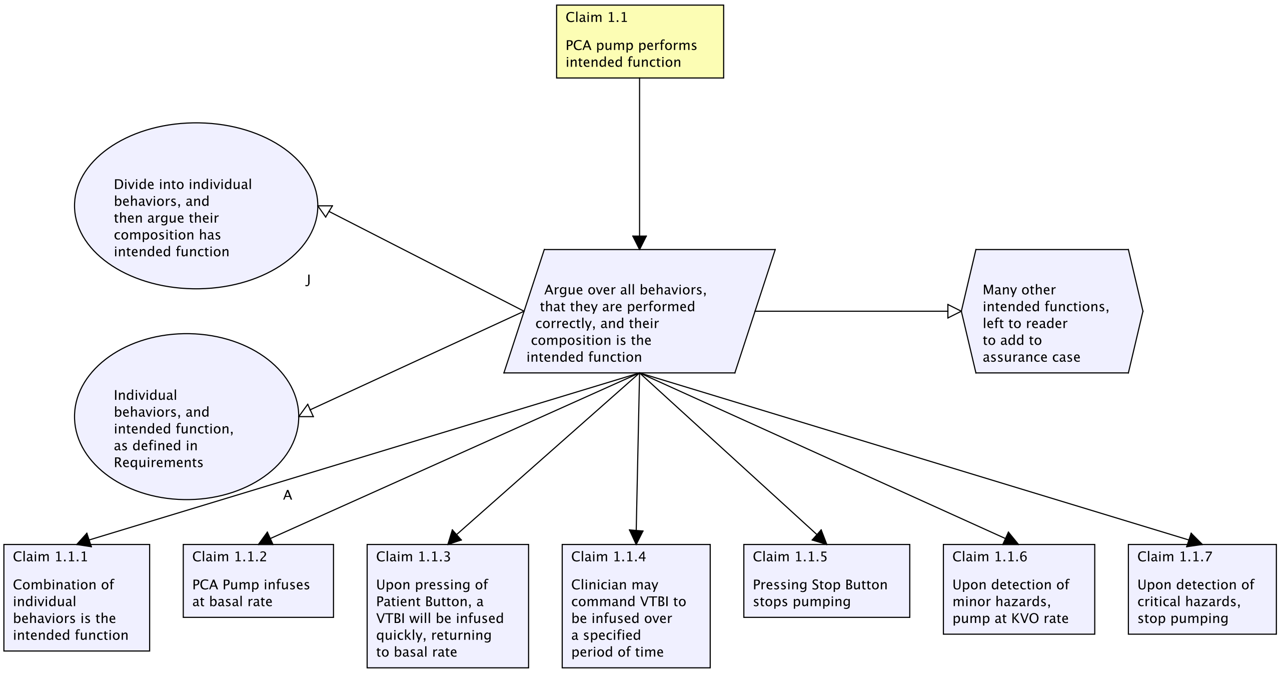
Claim 1.1: PCA pump performs intended function

See details in section 9

Claim 1.2: Effectiveness of intended function demonstrated in clinical trials

See details in section 18

9. Claim 1.1: PCA pump performs intended function


Claim 1.1
PCA pump performs intended function
Divide into individual behaviors, and then argue their composition has intended function
J
Argue over all behaviors, that they are performed correctly, and their composition is the intended function
Many other intended functions, left to reader to add to assurance case
Individual behaviors, and intended function, as defined in Requirements
A
Claim 1.1.1
Combination of individual behaviors is the intended function
Claim 1.1.2
PCA Pump infuses at basal rate
Claim 1.1.3
Upon pressing of Patient Button, a VTBI will be infused quickly, returning to basal rate
Claim 1.1.4
Clinician may command VTBI to be infused over a specified period of time
Claim 1.1.5
Pressing Stop Button stops pumping
Claim 1.1.6
Upon detection of minor hazards, pump at KVO rate
Claim 1.1.7
Upon detection of critical hazards, stop pumping

Claim 1.1: PCA pump performs intended function

Argue over all behaviors, that they are performed correctly, and their composition is the intended function

Divide into individual behaviors, and then argue their composition has intended function

Individual behaviors, and intended function, as defined in Requirements

Claim 1.1.1: Combination of individual behaviors is the intended function

See details in section 10

Claim 1.1.2: PCA Pump infuses at basal rate

See details in section 12

Claim 1.1.3: Upon pressing of Patient Button, a VTBI will be infused quickly, returning to basal rate

See details in section 13

Claim 1.1.4: Clinician may command VTBI to be infused over a specified period of time

See details in section 14

Claim 1.1.5: Pressing Stop Button stops pumping

See details in section 15

Claim 1.1.6: Upon detection of minor hazards, pump at KVO rate

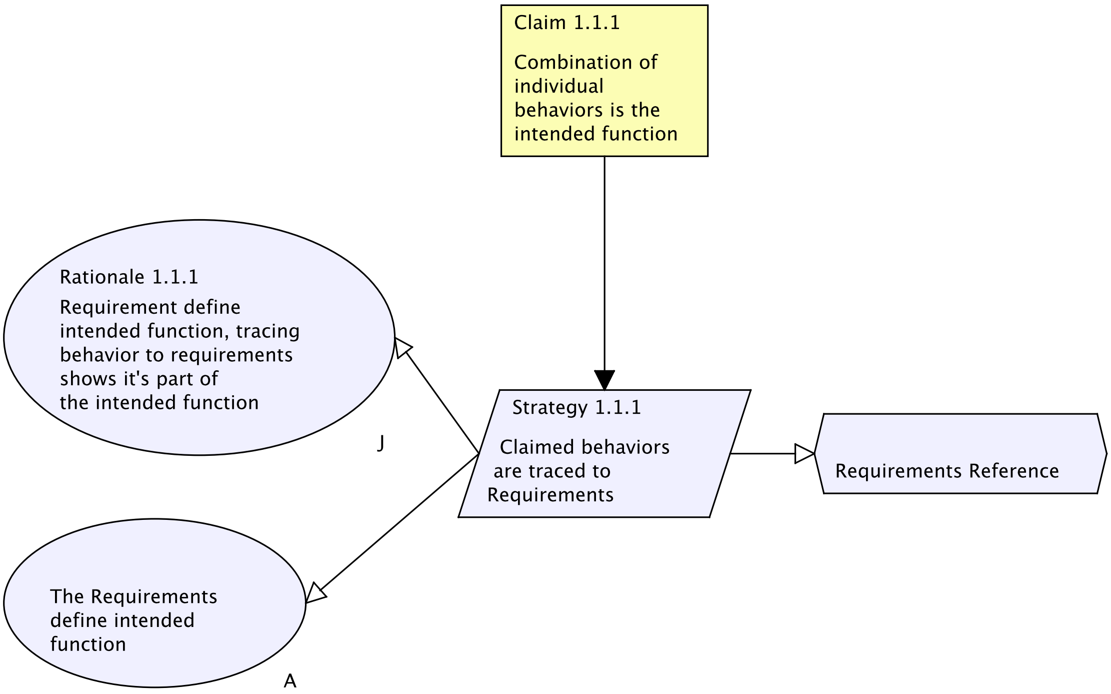
See details in section 16

Claim 1.1.7: Upon detection of critical hazards, stop pumping

See details in section 17

Many other intended functions, left to reader to add to assurance case

10. Claim 1.1.1: Combination of individual behaviors is the intended function


Claim 1.1.1
Combination of individual behaviors is the intended function
Rationale 1.1.1
Requirement define intended function, tracing behavior to requirements shows it's part of the intended function
J
Strategy 1.1.1
Claimed behaviors are traced to Requirements
Requirements Reference
The Requirements define intended function
A

Claim 1.1.1: Combination of individual behaviors is the intended function

This is combination of features, not components. For the PCA pump,

- pump drug at prescribed rate
- give extra bolus upon patient request, except if possibly unsafe
- authenticate patient, prescription, and attending clinician (the operator)
- display current pump rate
- allow clinician to administer extra bolus upon discretion, except if possibly unsafe

Strategy 1.1.1: Claimed behaviors are traced to Requirements

The Requirements defines the "intended function" for the PCA pump.

All this says is that, all the claims following (1.1.2 to 1.1.7+) trace to Requirements. Therefore the behaviors claimed are indeed the intended function of the PCA pump

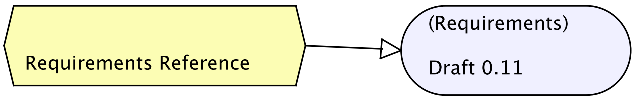
Rationale 1.1.1: Requirement define intended function, tracing behavior to requirements shows it's part of the intended function

The Requirements define intended function

Requirements Reference

See details in section 11

11. Requirements Reference



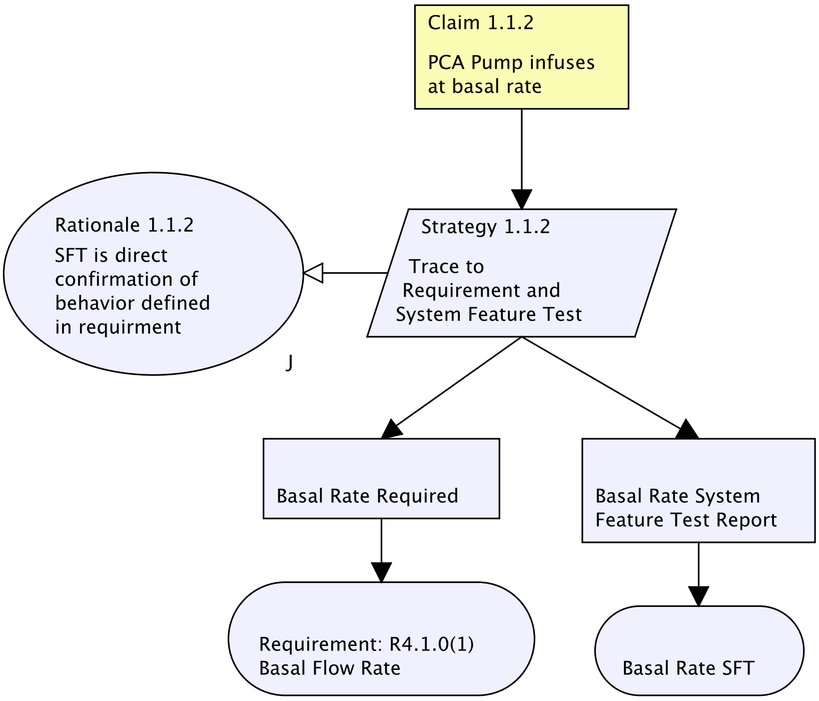
Requirements Reference

(Requirements) Draft 0.11

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link to description in section: 2

12. Claim 1.1.2: PCA Pump infuses at basal rate


Claim 1.1.2
PCA Pump infuses at basal rate
Rationale 1.1.2
SFT is direct confirmation of behavior defined in requirment
J
Strategy 1.1.2
Trace to Requirement and System Feature Test
Basal Rate Required
Basal Rate System Feature Test Report
Requirement: R4.1.0(1) Basal Flow Rate
Basal Rate SFT

Claim 1.1.2: PCA Pump infuses at basal rate

When properly programmed, by authenticated clinician.
Background (normal) rate of infusion.

Strategy 1.1.2: Trace to Requirement and System Feature Test

Rationale 1.1.2: SFT is direct confirmation of behavior defined in requirment

Basal Rate Required

Requirement: R4.1.0(1) Basal Flow Rate

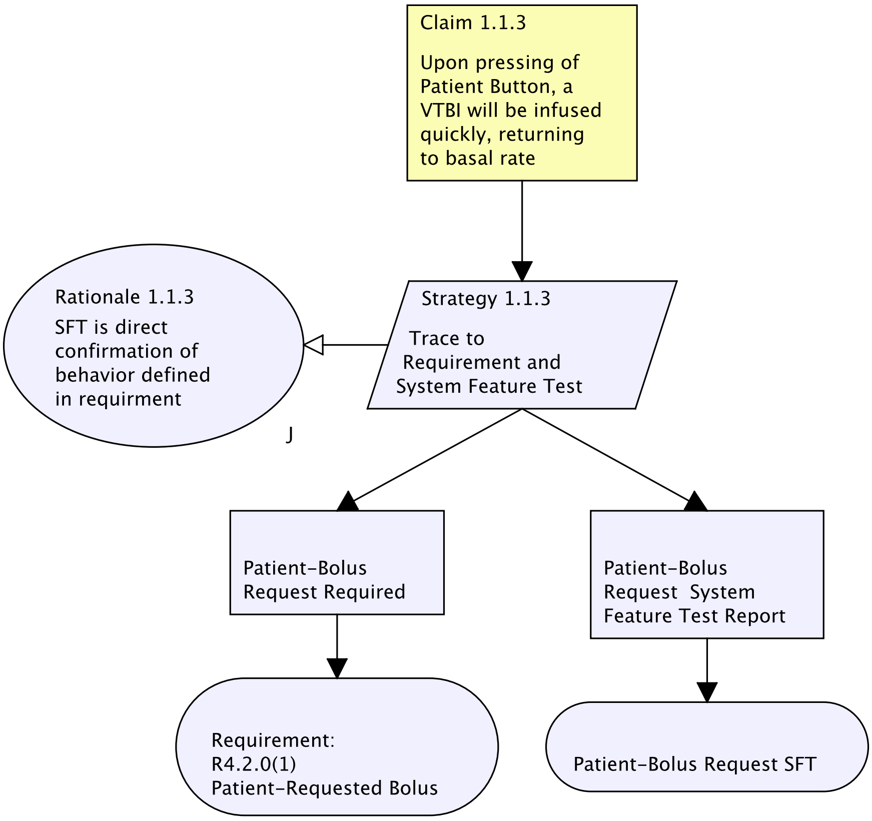
Evidence:	ICE-PCArequirements.pdf#nameddest=basal flow rate
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Basal Rate System Feature Test Report

() Basal Rate SFT

Link to description in section: 116

13. Claim 1.1.3: Upon pressing of Patient Button, a VTBI will be infused quickly, returning to basal rate


Claim 1.1.3
Upon pressing of Patient Button, a VTBI will be infused quickly, returning to basal rate
Rationale 1.1.3
SFT is direct confirmation of behavior defined in requirment
J
Strategy 1.1.3
Trace to Requirement and System Feature Test
Patient-Bolus Request Required
Patient-Bolus Request System Feature Test Report
Requirement: R4.2.0(1) Patient-Requested Bolus
Patient-Bolus Request SFT

Claim 1.1.3: Upon pressing of Patient Button, a VTBI will be infused quickly, returning to basal rate

This is the main function. There are all sorts of safety limitations, but here we're arguing that it performs its normal function.

Strategy 1.1.3: Trace to Requirement and System Feature Test

Rationale 1.1.3: SFT is direct confirmation of behavior defined in requirment

Patient-Bolus Request Required

Requirement: R4.2.0(1) Patient-Requested Bolus

Evidence: ICE-PCArequirements.pdf#nameddest=patient-requested bolus

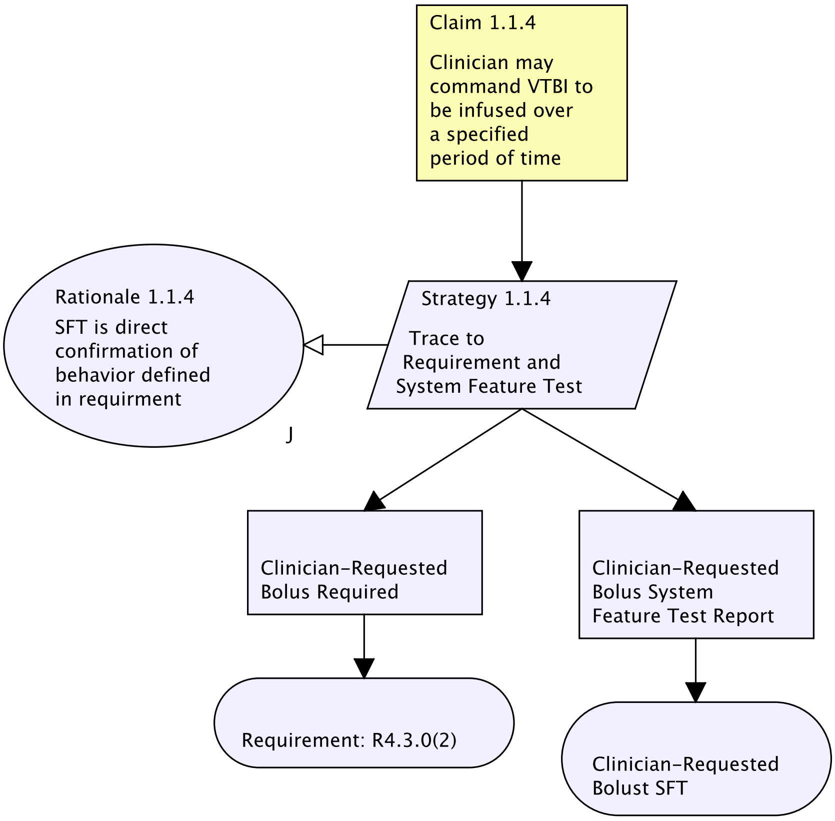
Repository: NOR-STA SVN PCAPAC - NOR-STA

Patient-Bolus Request System Feature Test Report

() Patient-Bolus Request SFT

Link to description in section: 116

14. Claim 1.1.4: Clinician may command VTBI to be infused over a specified period of time


Claim 1.1.4
Clinician may command VTBI to be infused over a specified period of time
Rationale 1.1.4
SFT is direct confirmation of behavior defined in requirment
J
Strategy 1.1.4
Trace to Requirement and System Feature Test
Clinician-Requested Bolus Required
Clinician-Requested Bolus System Feature Test Report
Requirement: R4.3.0(2)
Clinician-Requested Bolust SFT

Claim 1.1.4: Clinician may command VTBI to be infused over a specified period of time

Strategy 1.1.4: Trace to Requirement and System Feature Test

Rationale 1.1.4: SFT is direct confirmation of behavior defined in requirment

Clinician-Requested Bolus Required

Requirement: R4.3.0(2)

Evidence: ICE-PCArequirements.pdf#nameddest=clinician-requested bolus

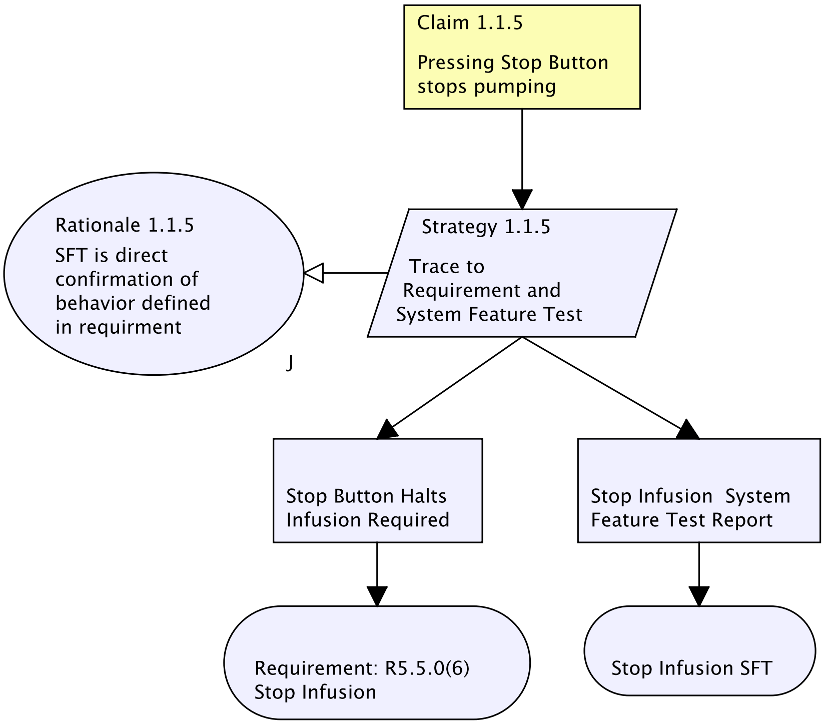
Repository: NOR-STA SVN PCAPAC - NOR-STA

Clinician-Requested Bolus System Feature Test Report

() Clinician-Requested Bolust SFT

Link to description in section: 116

15. Claim 1.1.5: Pressing Stop Button stops pumping


Claim 1.1.5
Pressing Stop Button stops pumping
Rationale 1.1.5
SFT is direct confirmation of behavior defined in requirment
J
Strategy 1.1.5
Trace to Requirement and System Feature Test
Stop Button Halts Infusion Required
Stop Infusion System Feature Test Report
Requirement: R5.5.0(6) Stop Infusion
Stop Infusion SFT

Claim 1.1.5: Pressing Stop Button stops pumping

Strategy 1.1.5: Trace to Requirement and System Feature Test

Rationale 1.1.5: SFT is direct confirmation of behavior defined in requirment

Stop Button Halts Infusion Required

Requirement: R5.5.0(6) Stop Infusion

Evidence: ICE-PCArequirements.pdf#nameddest=stop infusion

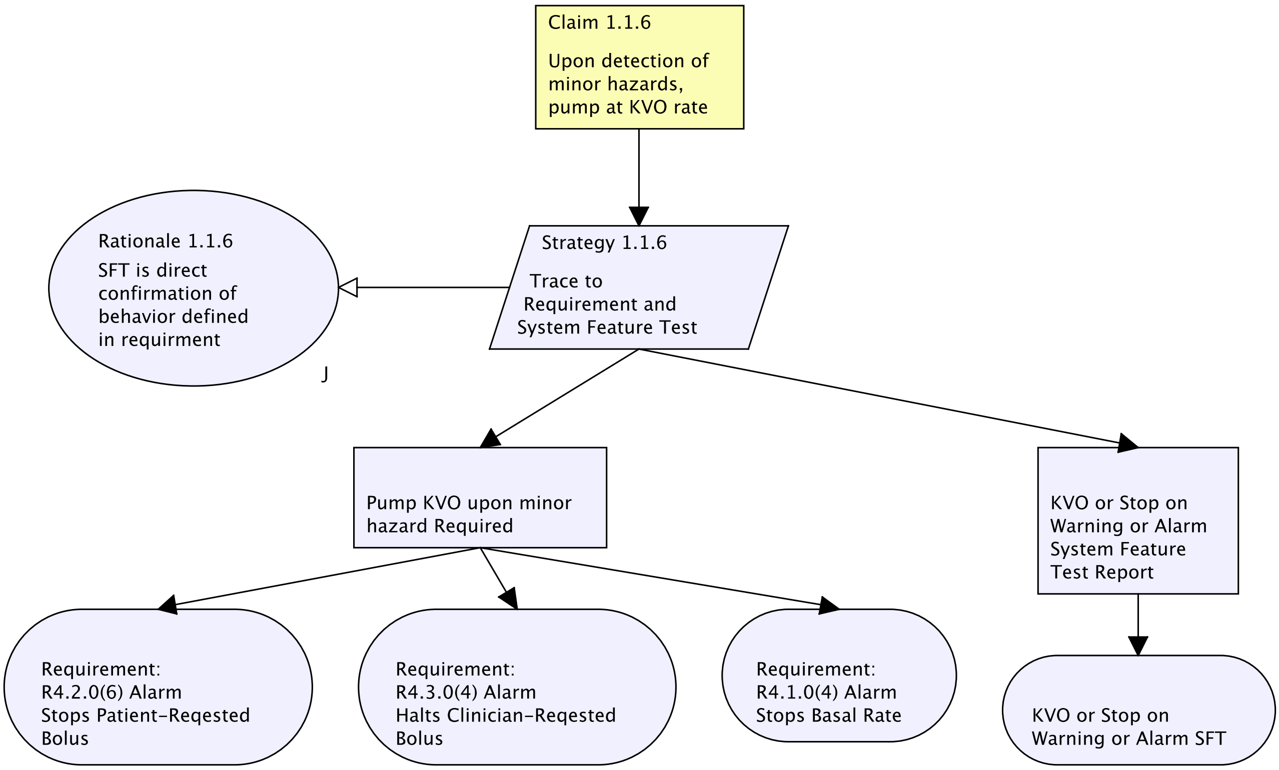
Repository: NOR-STA SVN PCAPAC - NOR-STA

Stop Infusion System Feature Test Report

() Stop Infusion SFT

Link to description in section: 116

16. Claim 1.1.6: Upon detection of minor hazards, pump at KVO rate


Claim 1.1.6
Upon detection of minor hazards, pump at KVO rate
Rationale 1.1.6
SFT is direct confirmation of behavior defined in requirment
J
Strategy 1.1.6
Trace to Requirement and System Feature Test
Pump KVO upon minor hazard Required
KVO or Stop on Warning or Alarm System Feature Test Report
Requirement: R4.2.0(6) Alarm Stops Patient-Reqested Bolus
Requirement: R4.3.0(4) Alarm Halts Clinician-Reqested Bolus
Requirement: R4.1.0(4) Alarm Stops Basal Rate
KVO or Stop on Warning or Alarm SFT

Claim 1.1.6: Upon detection of minor hazards, pump at KVO rate

as specified in Table XX of the Requirements

Strategy 1.1.6: Trace to Requirement and System Feature Test

Rationale 1.1.6: SFT is direct confirmation of behavior defined in requirment

Pump KVO upon minor hazard Required

Requirement: R4.2.0(6) Alarm Stops Patient-Reqested Bolus

Evidence:	ICE-PCArequirements.pdf#nameddest=alarm stops patient-requested bolus
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement: R4.3.0(4) Alarm Halts Clinician-Reqested Bolus

Evidence: ICE-PCArequirements.pdf#nameddest=alarm halts clinician-requested bolus

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R4.1.0(4) Alarm Stops Basal Rate

Evidence: ICE-PCArequirements.pdf#nameddest=alarm stops basal rate

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

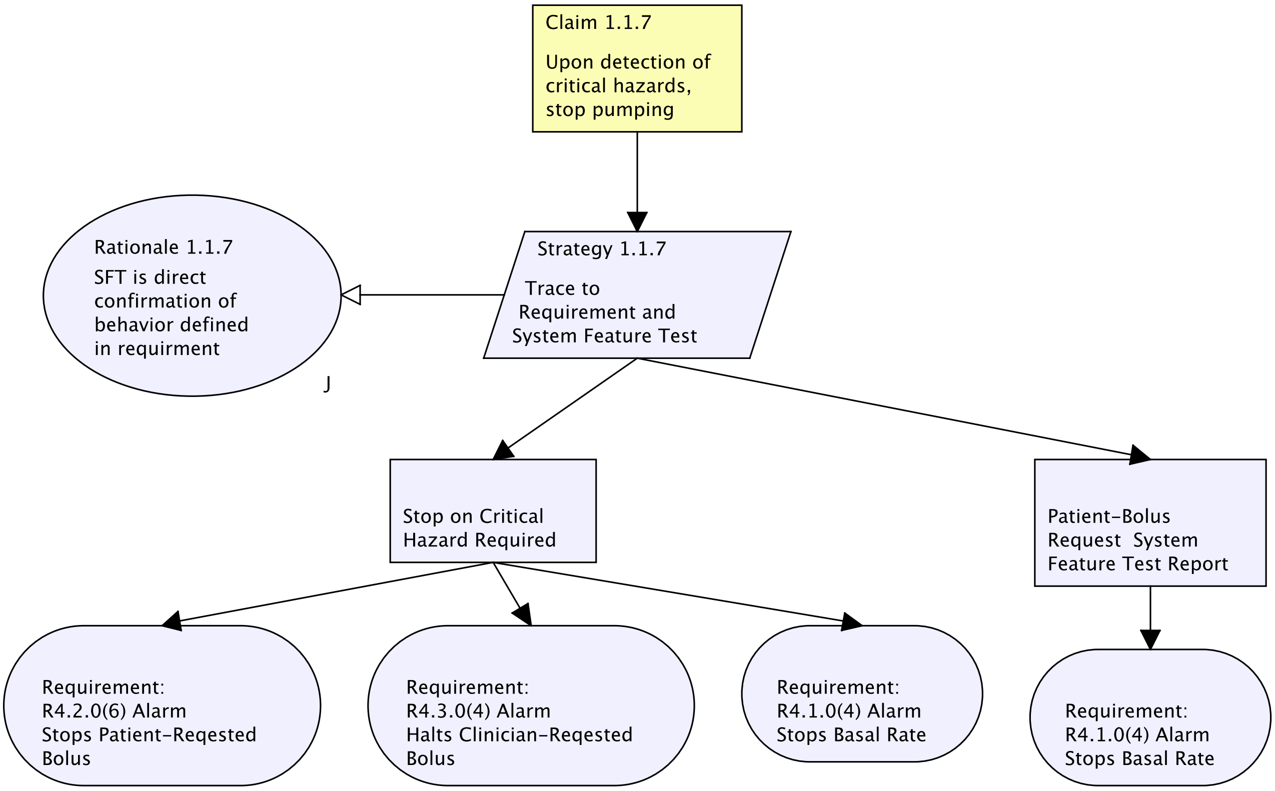
Section 17. Claim 1.1.7: Upon detection of critical hazards, stop pumping

KVO or Stop on Warning or Alarm System Feature Test Report

() KVO or Stop on Warning or Alarm SFT

Link to description in section: 116

17. Claim 1.1.7: Upon detection of critical hazards, stop pumping


Claim 1.1.7
Upon detection of critical hazards, stop pumping
Strategy 1.1.7
Trace to Requirement and System Feature Test
Rationale 1.1.7
SFT is direct confirmation of behavior defined in requirment
J
Stop on Critical Hazard Required
Patient-Bolus Request System Feature Test Report
Requirement: R4.2.0(6) Alarm Stops Patient-Reqested Bolus
Requirement: R4.3.0(4) Alarm Halts Clinician-Reqested Bolus
Requirement: R4.1.0(4) Alarm Stops Basal Rate
Requirement: R4.1.0(4) Alarm Stops Basal Rate

Claim 1.1.7: Upon detection of critical hazards, stop pumping

as specified in Table XX of the Requirements

Strategy 1.1.7: Trace to Requirement and System Feature Test

Rationale 1.1.7: SFT is direct confirmation of behavior defined in requirment

Stop on Critical Hazard Required

Requirement: R4.2.0(6) Alarm Stops Patient-Reqested Bolus

Evidence:	ICE-PCArequirements.pdf#nameddest=alarm stops patient-requested bolus
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement: R4.3.0(4) Alarm Halts Clinician-Reqested Bolus

Evidence:	ICE-PCArequirements.pdf#nameddest=alarm halts clinician-requested bolus
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement: R4.1.0(4) Alarm Stops Basal Rate

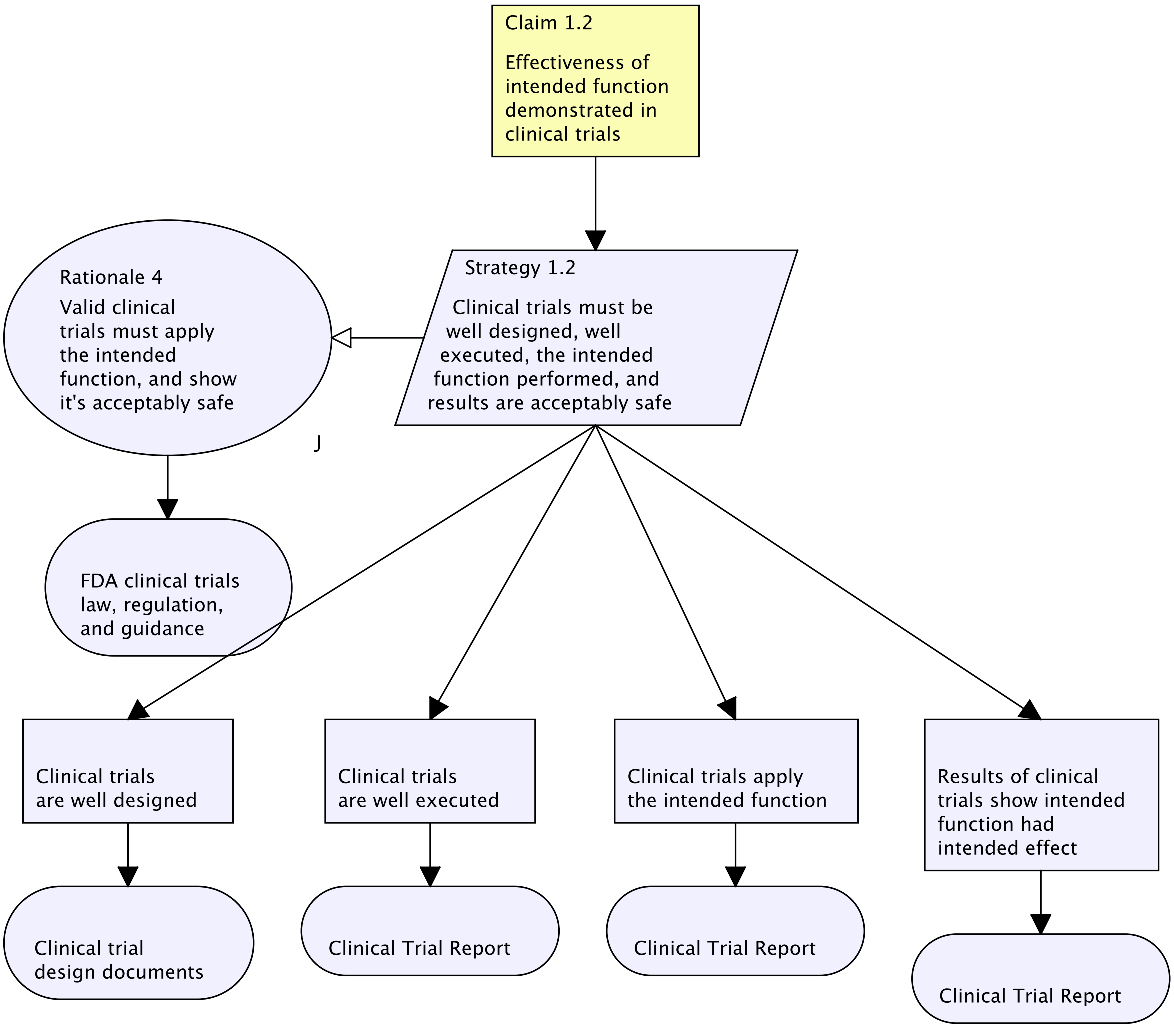
Evidence:	ICE-PCArequirements.pdf#nameddest=alarm stops basal rate
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Patient-Bolus Request System Feature Test Report

() Requirement: R4.1.0(4) Alarm Stops Basal Rate

Link to description in section: 16

18. Claim 1.2: Effectiveness of intended function demonstrated in clinical trials


Claim 1.2
Effectiveness of intended function demonstrated in clinical trials
Rationale 4
Valid clinical trials must apply the intended function, and show it's acceptably safe
Strategy 1.2
Clinical trials must be well designed, well executed, the intended function performed, and results are acceptably safe
J
FDA clinical trials law, regulation, and guidance
Clinical trials are well designed
Clinical trials are well executed
Clinical trials apply the intended function
Results of clinical trials show intended function had intended effect
Clinical trial design documents
Clinical Trial Report
Clinical Trial Report
Clinical Trial Report

Claim 1.2: Effectiveness of intended function demonstrated in clinical trials

Strategy 1.2: Clinical trials must be well designed, well executed, the intended function performed, and results are acceptably safe

Rationale 4: Valid clinical trials must apply the intended function, and show it's acceptably safe

() FDA clinical trials law, regulation, and guidance

Link to description in section: 118

Clinical trials are well designed

() Clinical trial design documents

Link to description in section: 118

Clinical trials are well executed

() Clinical Trial Report

Link to description in section: 118

Clinical trials apply the intended function

() Clinical Trial Report

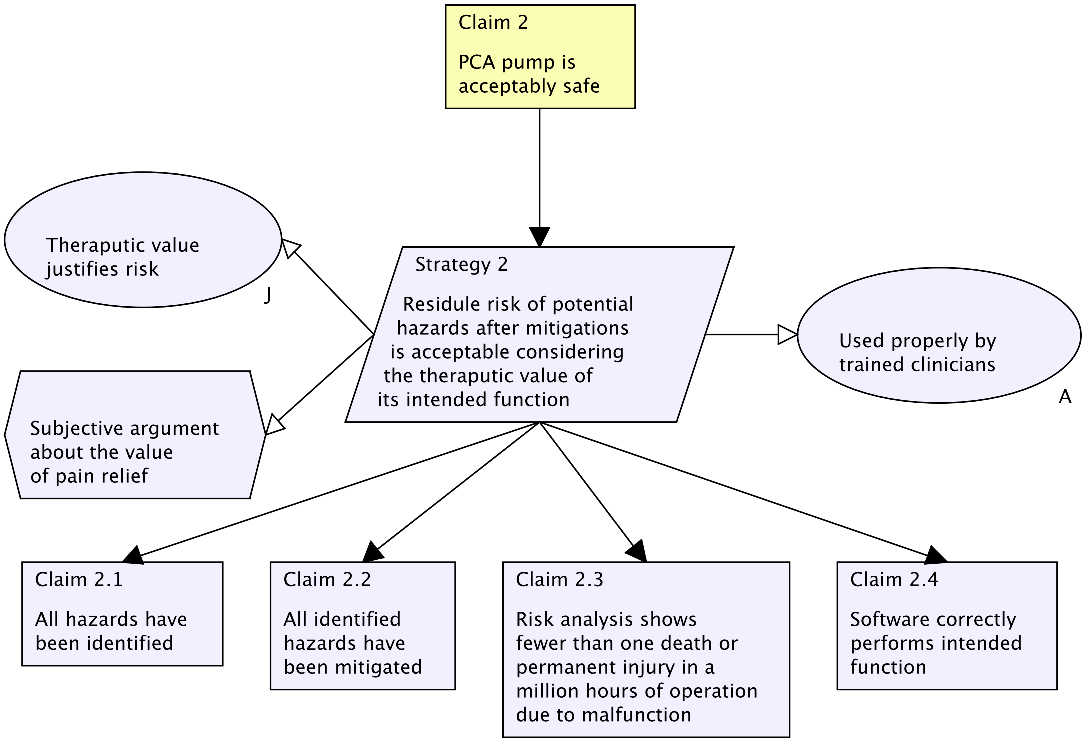
Link to description in section: 118

Results of clinical trials show intended function had intended effect

() Clinical Trial Report

Link to description in section: 118

19. Claim 2: PCA pump is acceptably safe


Claim 2
PCA pump is acceptably safe
Theraputic value justifies risk
J
Strategy 2
Residule risk of potential hazards after mitigations is acceptable considering the theraputic value of its intended function
Used properly by trained clinicians
A
Subjective argument about the value of pain relief
Claim 2.1
All hazards have been identified
Claim 2.2
All identified hazards have been mitigated
Claim 2.3
Risk analysis shows fewer than one death or permanent injury in a million hours of operation due to malfunction
Claim 2.4
Software correctly performs intended function

Claim 2: PCA pump is acceptably safe

Strategy 2: Residule risk of potential hazards after mitigations is acceptable considering the theraputic value of its intended function

Theraputic value justifies risk

This is the central value question to be answered:
"Does the patient benefit warrant potential harm?"

The risk, can (potentially) be estimated, but the benefit is inherently subjective. PCA pumps are frequently used in hospice, to alleviate the suffering the last days of terminal illness. Such patients will accept much more risk than patients recovering from minor surgery.

Subjective argument about the value of pain relief

The subjective argument is unavoidable, must be made, but can be separated from those parts of the assurance case for which objective facts can be ascertained.

Used properly by trained clinicians

FDA guidance for 510(k) approval for infusion pumps was used to guide development of argument that the Open PCA Pump is safe. Many of the hazards identified are errors in use (wet safety), few of which can be addressed by product design (dry safety). Therefore an assertion case about the device itself must assume that it is used according to labeling.

Claim 2.1: All hazards have been identified

See details in section 20

Claim 2.2: All identified hazards have been mitigated

See details in section 21

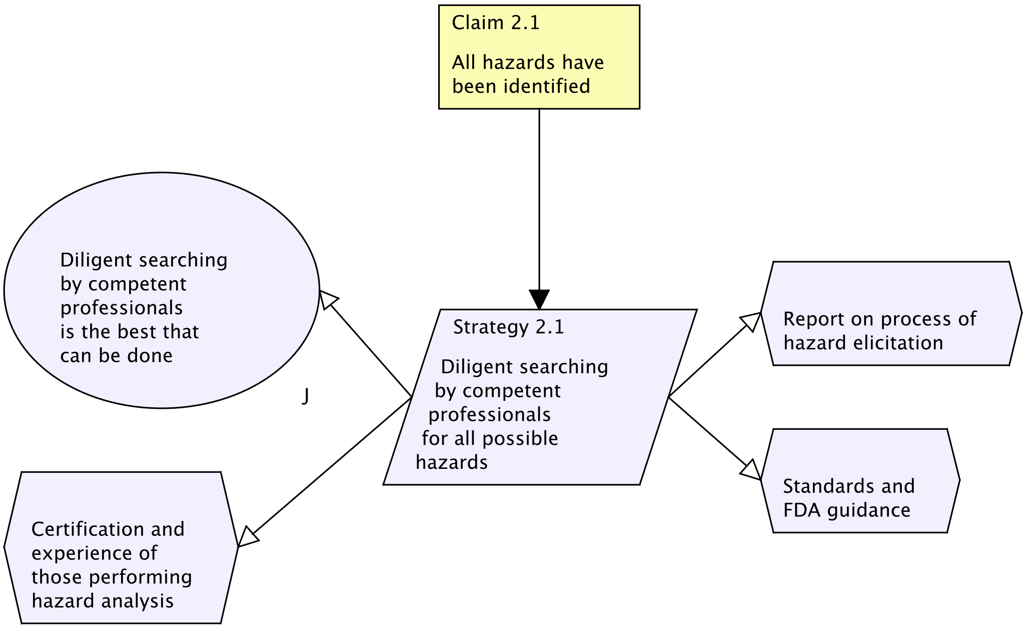
Claim 2.3: Risk analysis shows fewer than one death or permanent injury in a million hours of operation due to malfunction

See details in section 111

Claim 2.4: Software correctly performs intended function

See details in section 112

20. Claim 2.1: All hazards have been identified


Claim 2.1
All hazards have been identified
Diligent searching by competent professionals is the best that can be done
J
Strategy 2.1
Diligent searching by competent professionals for all possible hazards
Report on process of hazard elicitation
Standards and FDA guidance
Certification and experience of those performing hazard analysis

Claim 2.1: All hazards have been identified

Strategy 2.1: Diligent searching by competent professionals for all possible hazards

There can always be hazards, as yet, unknown. Earnestly trying to find all potential hazards is the best anyone can do. The best companies will have process records to show that good people tried to find all hazards.

Diligent searching by competent professionals is the best that can be done

Of course, hazards can be missed, but that all hazards have been identified must be one of the claims, albeit one that can never be fully assured

Certification and experience of those performing hazard analysis

List of individual's names, their degrees and relevant training courses, and summary of relevant experience. Some of the team will be novices; others will be experts with long service.

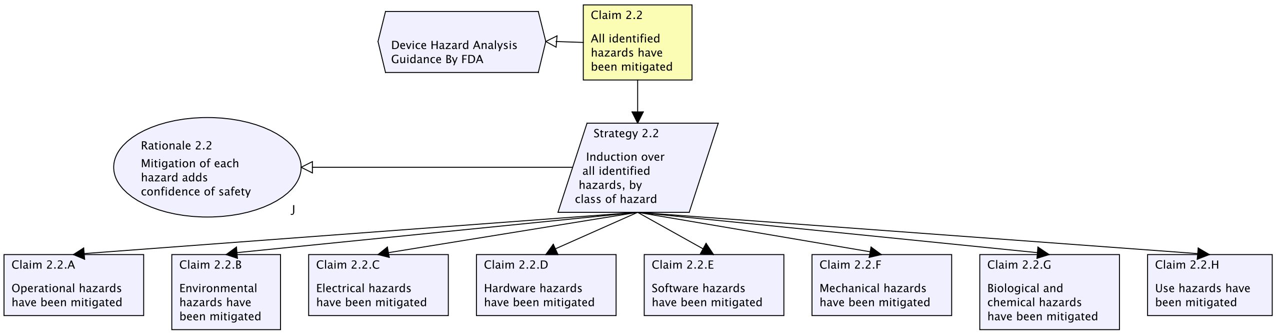
Report on process of hazard elicitation

How was the list of potential hazards compiled?

Standards and FDA guidance

List any external references such as standards or FDA Guidance documents used to identify potential hzards.

21. Claim 2.2: All identified hazards have been mitigated


Device Hazard Analysis Guidance By FDA
Claim 2.2
All identified hazards have been mitigated
Rationale 2.2
Mitigation of each hazard adds confidence of safety
J
Strategy 2.2
Induction over all identified hazards, by class of hazard
Claim 2.2.A
Operational hazards have been mitigated
Claim 2.2.B
Environmental hazards have been mitigated
Claim 2.2.C
Electrical hazards have been mitigated
Claim 2.2.D
Hardware hazards have been mitigated
Claim 2.2.E
Software hazards have been mitigated
Claim 2.2.F
Mechanical hazards have been mitigated
Claim 2.2.G
Biological and chemical hazards have been mitigated
Claim 2.2.H
Use hazards have been mitigated

Claim 2.2: All identified hazards have been mitigated

Strategy 2.2: Induction over all identified hazards, by class of hazard

Grouping hazards makes the argument easier to understand

Rationale 2.2: Mitigation of each hazard adds confidence of safety

See details in section 22

Claim 2.2.A: Operational hazards have been mitigated

See details in section 23

Claim 2.2.B: Environmental hazards have been mitigated

See details in section 42

Claim 2.2.C: Electrical hazards have been mitigated

See details in section 55

Claim 2.2.D: Hardware hazards have been mitigated

See details in section 64

Claim 2.2.E: Software hazards have been mitigated

See details in section 72

Claim 2.2.F: Mechanical hazards have been mitigated

See details in section 81

Claim 2.2.G: Biological and chemical hazards have been mitigated

See details in section 87

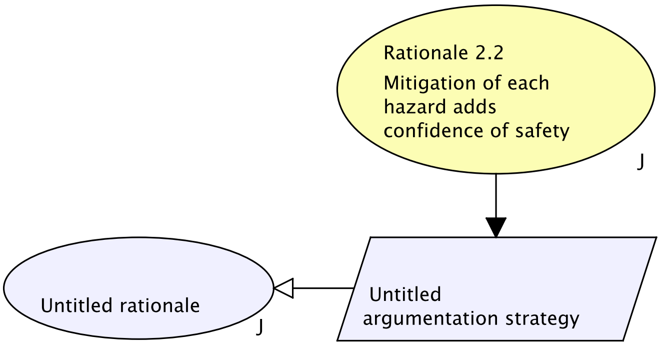
Claim 2.2.H: Use hazards have been mitigated

See details in section 89

Device Hazard Analysis Guidance By FDA

See details in section 110

22. Rationale 2.2: Mitigation of each hazard adds confidence of safety

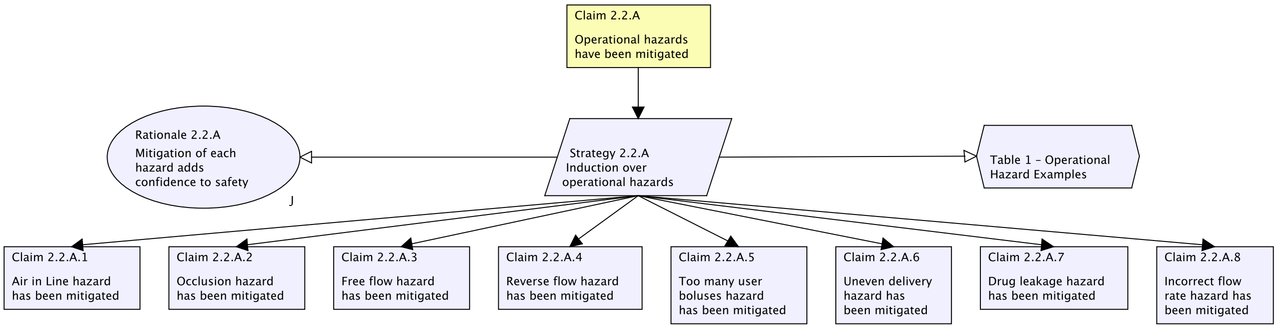

Rationale 2.2
Mitigation of each hazard adds confidence of safety
J
Untitled rationale
J
Untitled argumentation strategy

⚙ Rationale 2.2: Mitigation of each hazard adds confidence of safety

Untitled argumentation strategy

⚙ Untitled rationale

23. Claim 2.2.A: Operational hazards have been mitigated


Claim 2.2.A
Operational hazards have been mitigated
Rationale 2.2.A
Mitigation of each hazard adds confidence to safety
J
Strategy 2.2.A
Induction over operational hazards
Table 1 – Operational Hazard Examples
Claim 2.2.A.1
Air in Line hazard has been mitigated
Claim 2.2.A.2
Occlusion hazard has been mitigated
Claim 2.2.A.3
Free flow hazard has been mitigated
Claim 2.2.A.4
Reverse flow hazard has been mitigated
Claim 2.2.A.5
Too many user boluses hazard has been mitigated
Claim 2.2.A.6
Uneven delivery hazard has been mitigated
Claim 2.2.A.7
Drug leakage hazard has been mitigated
Claim 2.2.A.8
Incorrect flow rate hazard has been mitigated

Claim 2.2.A: Operational hazards have been mitigated

following Table A in guidance

Strategy 2.2.A Induction over operational hazards

Rationale 2.2.A: Mitigation of each hazard adds confidence to safety

Table 1 – Operational Hazard Examples

See details in section 24

Claim 2.2.A.1: Air in Line hazard has been mitigated

See details in section 25

Claim 2.2.A.2: Occlusion hazard has been mitigated

See details in section 29

Claim 2.2.A.3: Free flow hazard has been mitigated

See details in section 34

Claim 2.2.A.4: Reverse flow hazard has been mitigated

See details in section 36

Claim 2.2.A.5: Too many user boluses hazard has been mitigated

See details in section 38

Claim 2.2.A.6: Uneven delivery hazard has been mitigated

See details in section 39

Claim 2.2.A.7: Drug leakage hazard has been mitigated

See details in section 40

Claim 2.2.A.8: Incorrect flow rate hazard has been mitigated

See details in section 41

24. Table 1 – Operational Hazard Examples

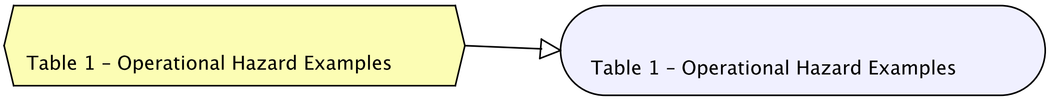


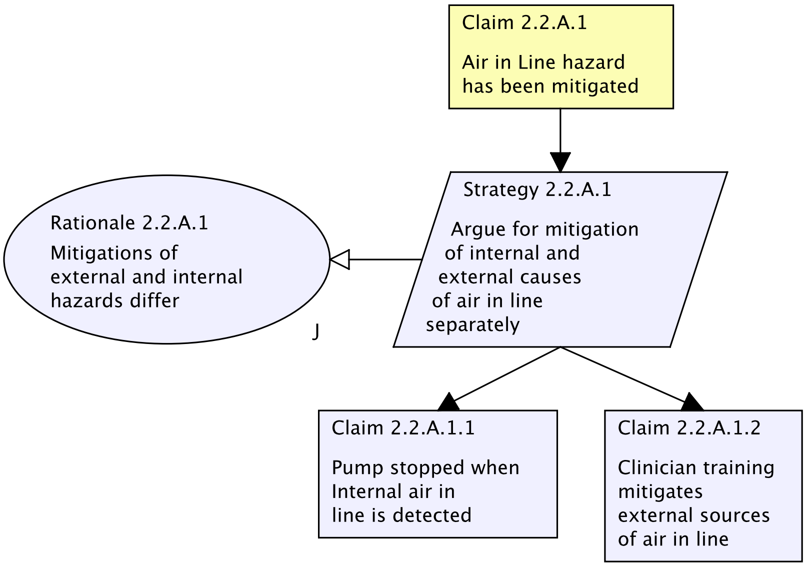
Table 1 - Operational Hazard Examples
Table 1 - Operational Hazard Examples

Table 1 – Operational Hazard Examples

Table 1 – Operational Hazard Examples

Evidence:	IPGenera Guidance.pdf#page=12
Repository:	NOR-STA SVN PCAPAC - NOR-STA

25. Claim 2.2.A.1: Air in Line hazard has been mitigated


Claim 2.2.A.1
Air in Line hazard has been mitigated
Strategy 2.2.A.1
Argue for mitigation of internal and external causes of air in line separately
Rationale 2.2.A.1
Mitigations of external and internal hazards differ
J
Claim 2.2.A.1.1
Pump stopped when Internal air in line is detected
Claim 2.2.A.1.2
Clinician training mitigates external sources of air in line

Claim 2.2.A.1: Air in Line hazard has been mitigated

Strategy 2.2.A.1: Argue for mitigation of internal and external causes of air in line separately

Rationale 2.2.A.1: Mitigations of external and internal hazards differ

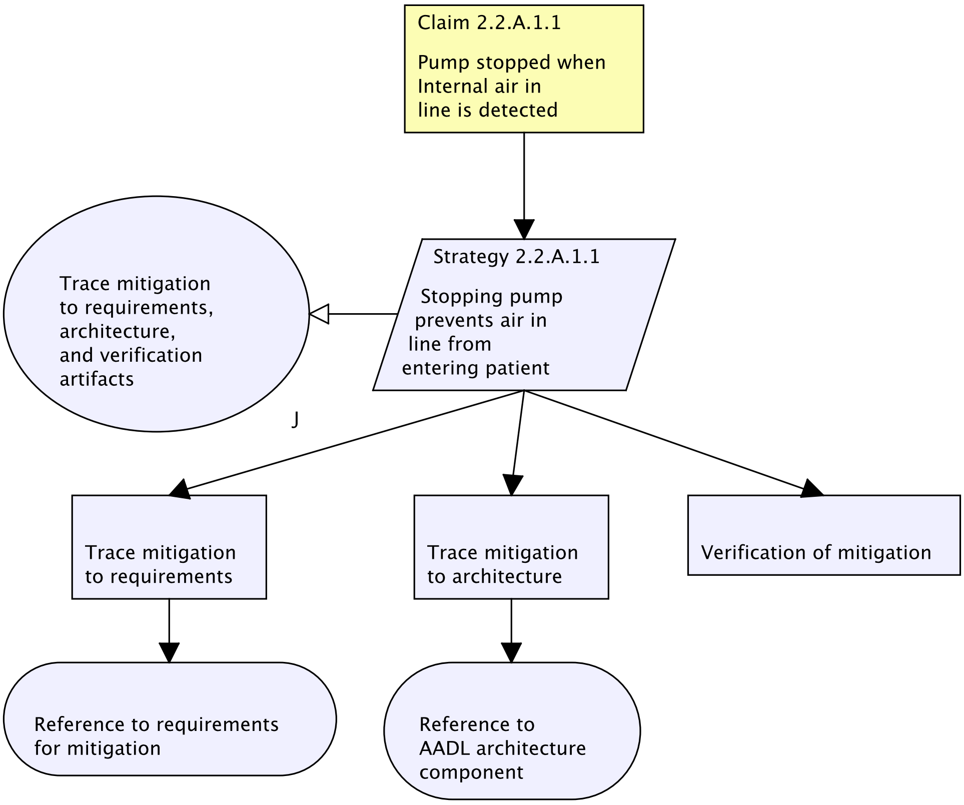
Claim 2.2.A.1.1: Pump stopped when Internal air in line is detected

See details in section 26

Claim 2.2.A.1.2: Clinician training mitigates external sources of air in line

See details in section 28

26. Claim 2.2.A.1.1: Pump stopped when Internal air in line is detected


Claim 2.2.A.1.1
Pump stopped when Internal air in line is detected
Strategy 2.2.A.1.1
Stopping pump prevents air in line from entering patient
Trace mitigation to requirements, architecture, and verification artifacts
J
Trace mitigation to requirements
Trace mitigation to architecture
Verification of mitigation
Reference to requirements for mitigation
Reference to AADL architecture component

Claim 2.2.A.1.1: Pump stopped when Internal air in line is detected

Strategy 2.2.A.1.1: Stopping pump prevents air in line from entering patient

Trace mitigation to requirements, architecture, and verification artifacts

Trace mitigation to requirements

Reference to requirements for mitigation

Evidence:	ICE-PCArequirements.pdf#nameddest=detect air-in-line embolism
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Trace mitigation to architecture

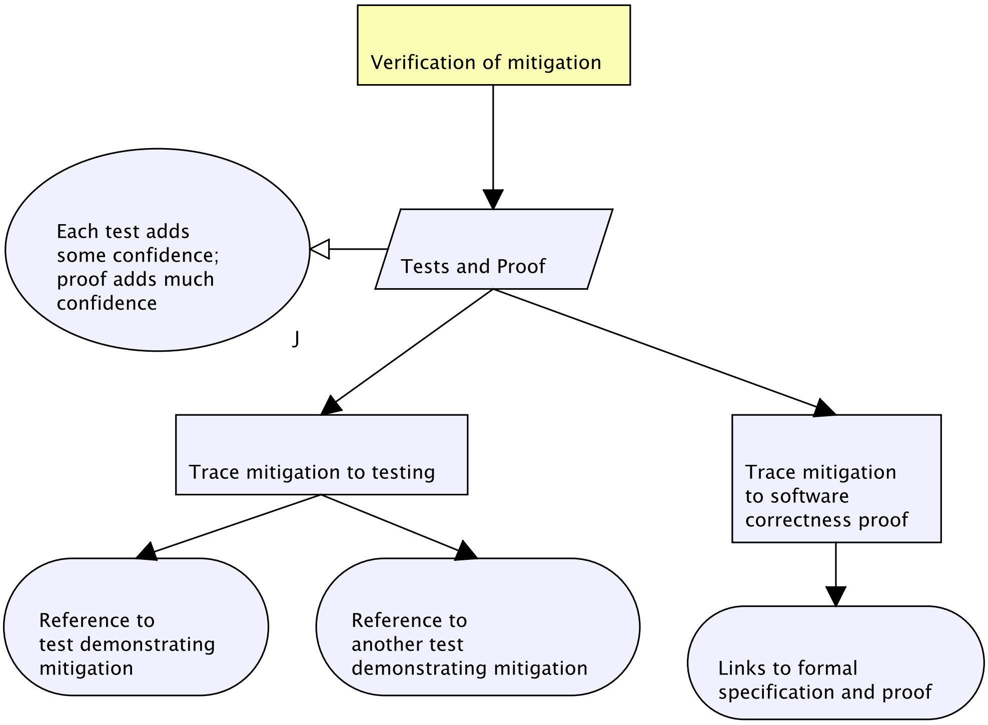
Reference to AADL architecture component

Repository: NOR-STA SVN PCAPAC - NOR-STA

Verification of mitigation

See details in section 27

27. Verification of mitigation


Verification of mitigation
Tests and Proof
Each test adds some confidence; proof adds much confidence
J
Trace mitigation to testing
Trace mitigation to software correctness proof
Reference to test demonstrating mitigation
Reference to another test demonstrating mitigation
Links to formal specification and proof

Verification of mitigation

Tests and Proof

Each test adds some confidence; proof adds much confidence

Trace mitigation to testing

Reference to test demonstrating mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Reference to another test demonstrating mitigation

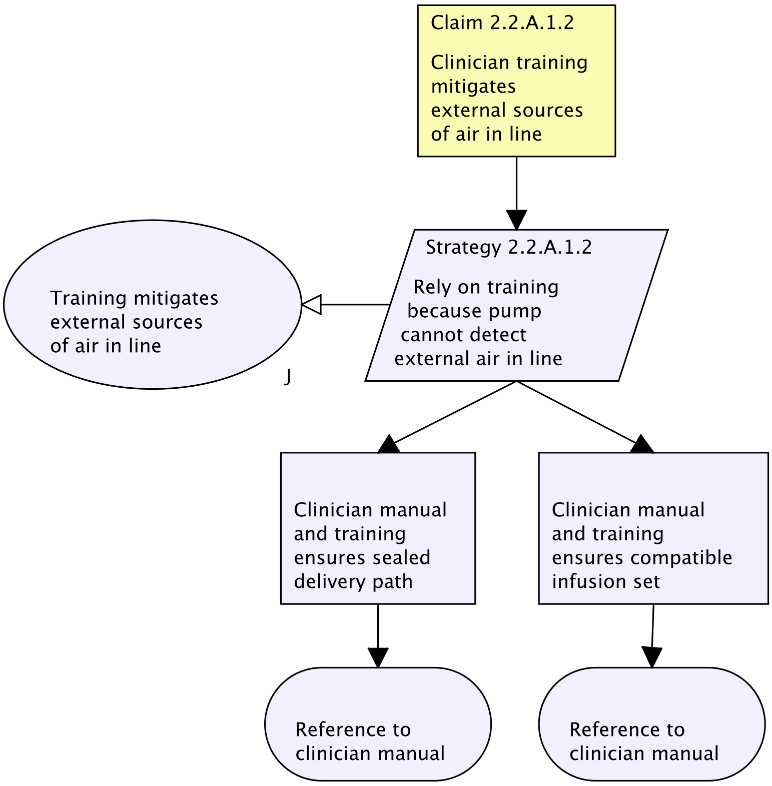
Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace mitigation to software correctness proof

Links to formal specification and proof

Repository: NOR-STA SVN PCAPAC - NOR-STA

28. Claim 2.2.A.1.2: Clinician training mitigates external sources of air in line


Claim 2.2.A.1.2
Clinician training mitigates external sources of air in line
Strategy 2.2.A.1.2
Rely on training because pump cannot detect external air in line
Training mitigates external sources of air in line
J
Clinician manual and training ensures sealed delivery path
Clinician manual and training ensures compatible infusion set
Reference to clinician manual
Reference to clinician manual

Claim 2.2.A.1.2: Clinician training mitigates external sources of air in line

This claim is weak; relies on labeling/training/proper use

Strategy 2.2.A.1.2: Rely on training because pump cannot detect external air in line

Training mitigates external sources of air in line

Clinician manual and training ensures sealed delivery path

Reference to clinician manual

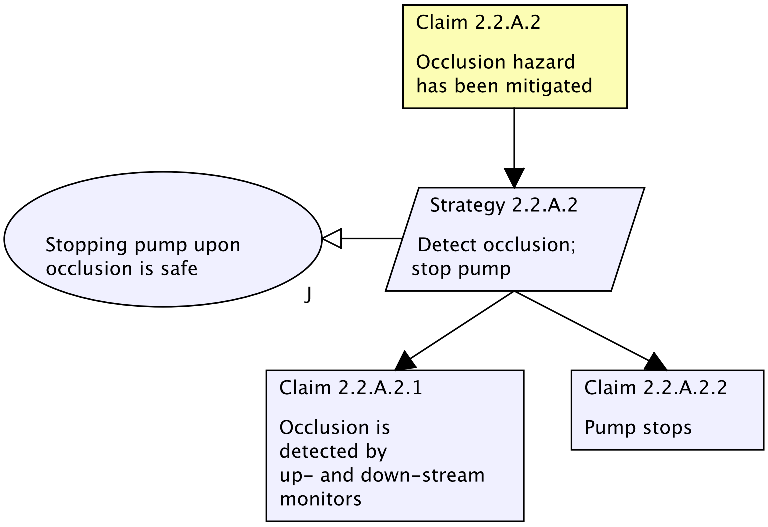
Repository: NOR-STA SVN PCAPAC - NOR-STA

Clinician manual and training ensures compatible infusion set

Reference to clinician manual

Repository: NOR-STA SVN PCAPAC - NOR-STA

29. Claim 2.2.A.2: Occlusion hazard has been mitigated


Claim 2.2.A.2
Occlusion hazard has been mitigated
Strategy 2.2.A.2
Detect occlusion; stop pump
Stopping pump upon occlusion is safe
J
Claim 2.2.A.2.1
Occlusion is detected by up- and down-stream monitors
Claim 2.2.A.2.2
Pump stops

Claim 2.2.A.2: Occlusion hazard has been mitigated

Strategy 2.2.A.2: Detect occlusion; stop pump

Stopping pump upon occlusion is safe

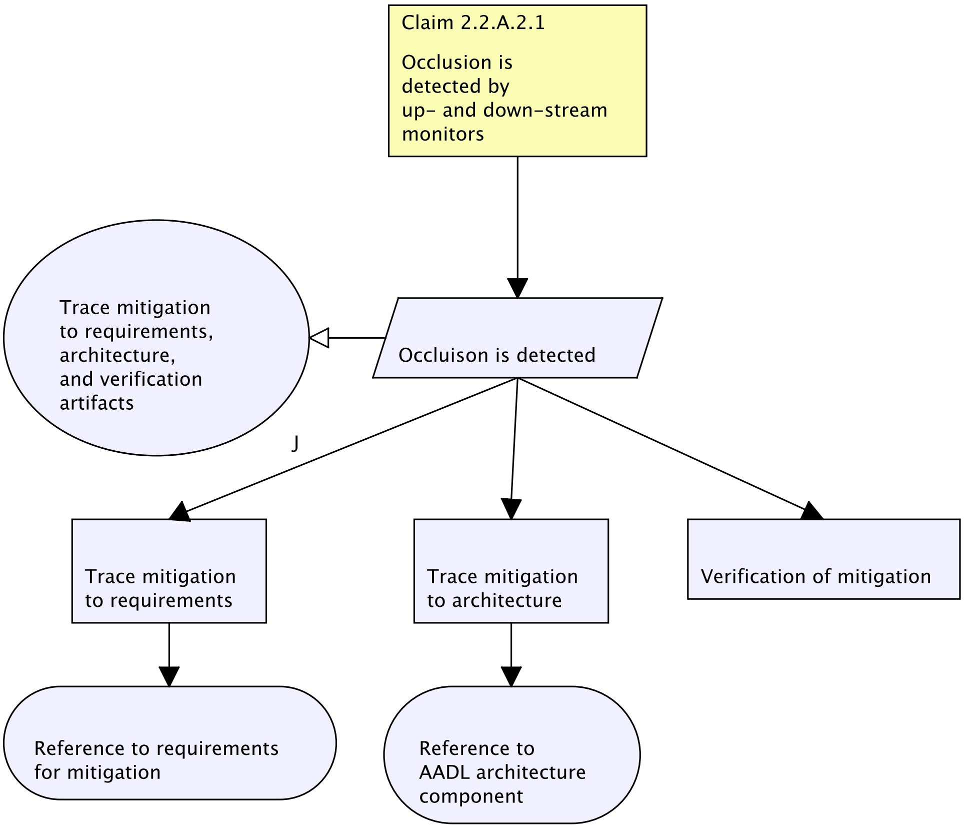
Claim 2.2.A.2.1: Occlusion is detected by up- and down-stream monitors

See details in section 30

Claim 2.2.A.2.2: Pump stops

See details in section 32

30. Claim 2.2.A.2.1: Occlusion is detected by up- and down-stream monitors


Claim 2.2.A.2.1
Occlusion is detected by up- and down-stream monitors
Trace mitigation to requirements, architecture, and verification artifacts
Occluison is detected
J
Trace mitigation to requirements
Trace mitigation to architecture
Verification of mitigation
Reference to requirements for mitigation
Reference to AADL architecture component

Claim 2.2.A.2.1: Occlusion is detected by up- and down-stream monitors

Occluison is detected

Trace mitigation to requirements, architecture, and verification artifacts

Trace mitigation to requirements

Reference to requirements for mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace mitigation to architecture

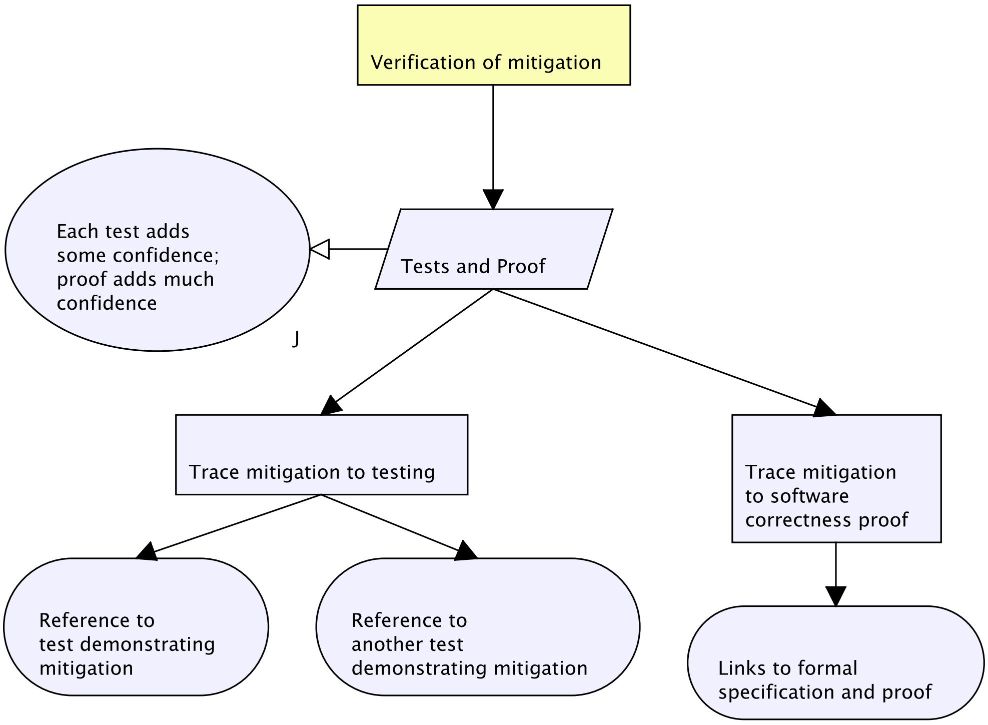
Reference to AADL architecture component

Repository: NOR-STA SVN PCAPAC - NOR-STA

Verification of mitigation

See details in section 31

31. Verification of mitigation


Verification of mitigation
Tests and Proof
Each test adds some confidence; proof adds much confidence
J
Trace mitigation to testing
Trace mitigation to software correctness proof
Reference to test demonstrating mitigation
Reference to another test demonstrating mitigation
Links to formal specification and proof

Verification of mitigation

Tests and Proof

Each test adds some confidence; proof adds much confidence

Trace mitigation to testing

Reference to test demonstrating mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Reference to another test demonstrating mitigation

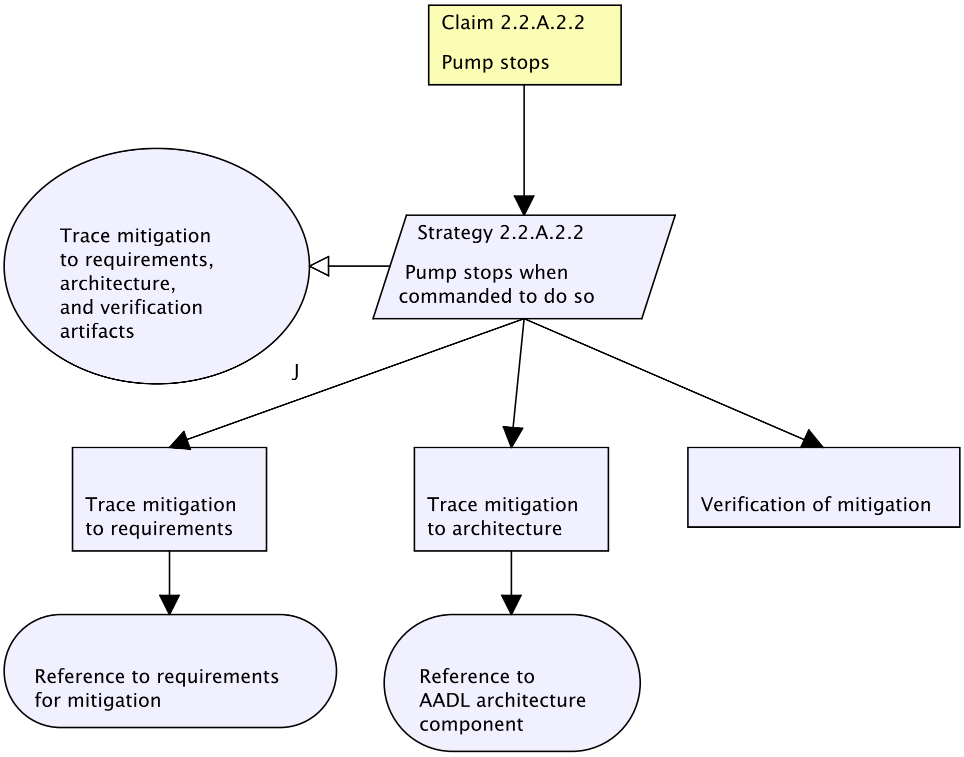
Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace mitigation to software correctness proof

Links to formal specification and proof

Repository: NOR-STA SVN PCAPAC - NOR-STA

32. Claim 2.2.A.2.2: Pump stops


Claim 2.2.A.2.2
Pump stops
Strategy 2.2.A.2.2
Pump stops when commanded to do so
Trace mitigation to requirements, architecture, and verification artifacts
J
Trace mitigation to requirements
Trace mitigation to architecture
Verification of mitigation
Reference to requirements for mitigation
Reference to AADL architecture component

Claim 2.2.A.2.2: Pump stops

Strategy 2.2.A.2.2: Pump stops when commanded to do so

Trace mitigation to requirements, architecture, and verification artifacts

Trace mitigation to requirements

Reference to requirements for mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace mitigation to architecture

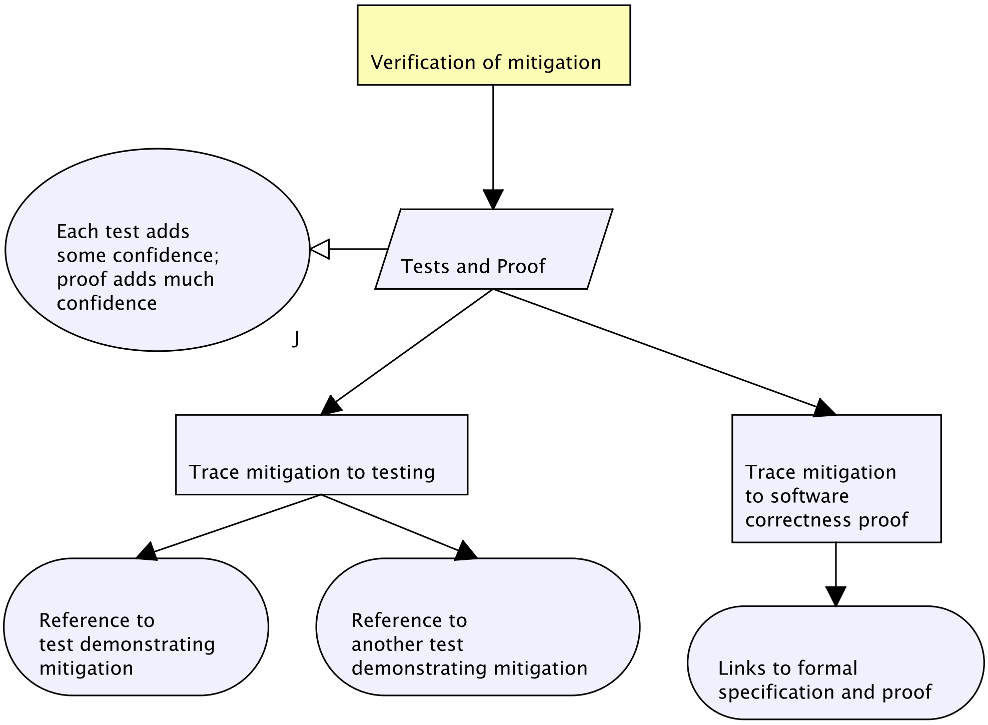
Reference to AADL architecture component

Repository: NOR-STA SVN PCAPAC - NOR-STA

Verification of mitigation

See details in section 33

33. Verification of mitigation


Verification of mitigation
Each test adds some confidence; proof adds much confidence
J
Tests and Proof
Trace mitigation to testing
Trace mitigation to software correctness proof
Reference to test demonstrating mitigation
Reference to another test demonstrating mitigation
Links to formal specification and proof

Verification of mitigation

Tests and Proof

Each test adds some confidence; proof adds much confidence

Trace mitigation to testing

Reference to test demonstrating mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Reference to another test demonstrating mitigation

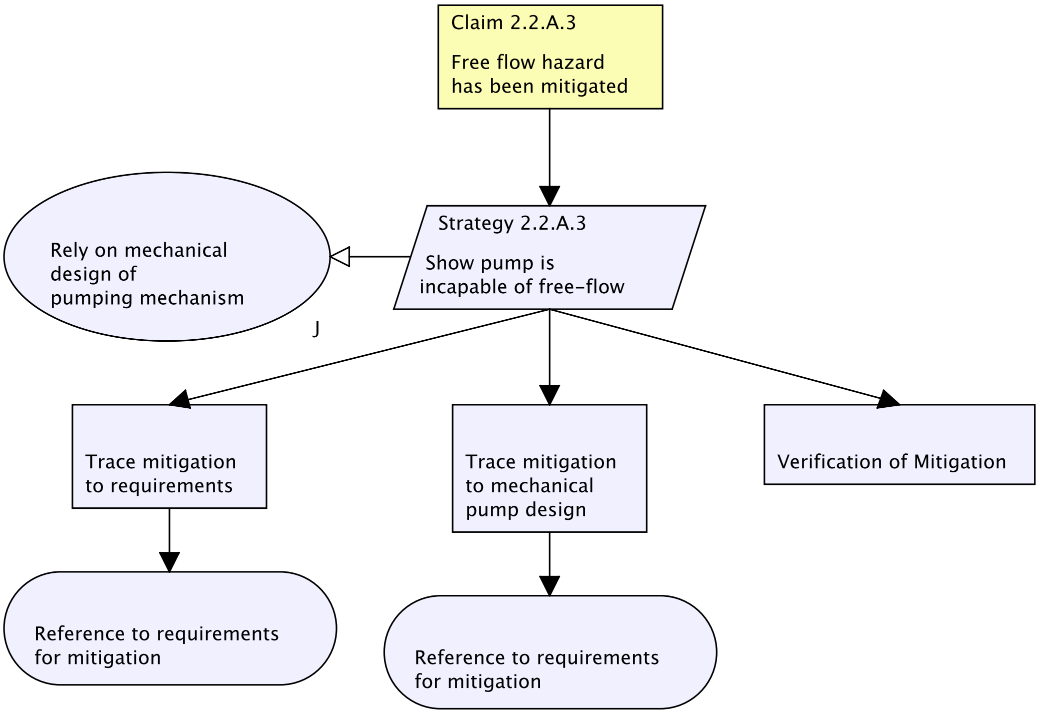
Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace mitigation to software correctness proof

Links to formal specification and proof

Repository: NOR-STA SVN PCAPAC - NOR-STA

34. Claim 2.2.A.3: Free flow hazard has been mitigated


Claim 2.2.A.3
Free flow hazard has been mitigated
Strategy 2.2.A.3
Show pump is incapable of free-flow
Rely on mechanical design of pumping mechanism
J
Trace mitigation to requirements
Trace mitigation to mechanical pump design
Verification of Mitigation
Reference to requirements for mitigation
Reference to requirements for mitigation

Claim 2.2.A.3: Free flow hazard has been mitigated

This hazard only occurs in "hanging bag" infusion pumps that don't actually pump, but instead regulate gravity-fed flow.

Strategy 2.2.A.3: Show pump is incapable of free-flow

Rely on mechanical design of pumping mechanism

Trace mitigation to requirements

Reference to requirements for mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace mitigation to mechanical pump design

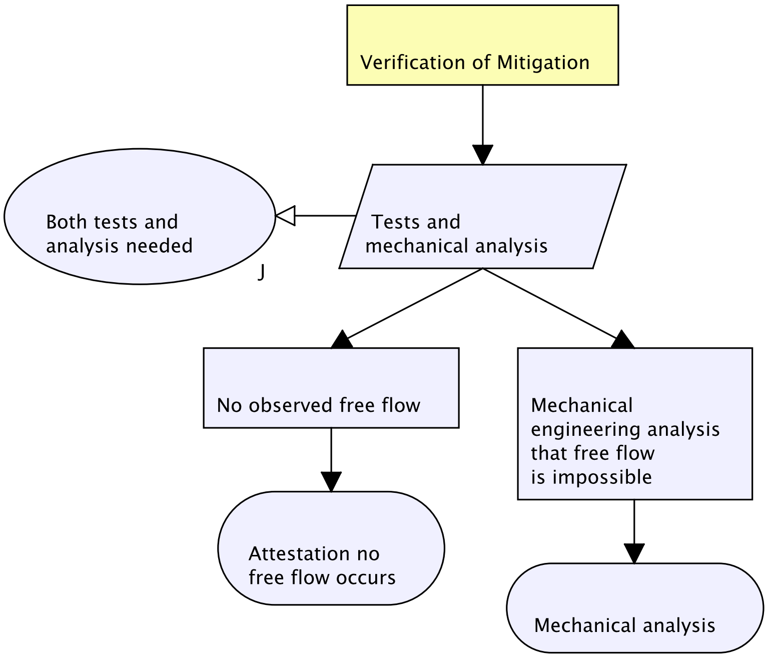
Reference to requirements for mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Verification of Mitigation

See details in section 35

35. Verification of Mitigation


Verification of Mitigation
Both tests and analysis needed
J
Tests and mechanical analysis
No observed free flow
Mechanical engineering analysis that free flow is impossible
Attestation no free flow occurs
Mechanical analysis

Verification of Mitigation

Tests and mechanical analysis

Both tests and analysis needed

Because it is impossible to *prove* a negative (no free flow), observation that flow never occurs must be augmented with mechanical engineering analysis.

No observed free flow

Attestation no free flow occurs

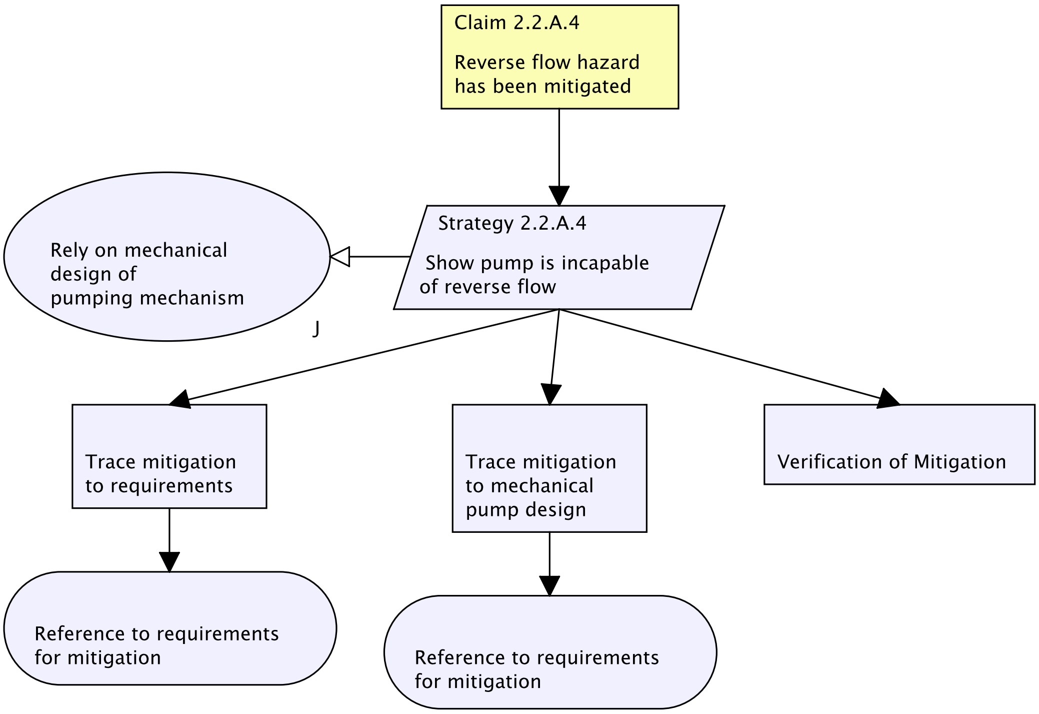
Repository: NOR-STA SVN PCAPAC - NOR-STA

Mechanical engineering analysis that free flow is impossible

Mechanical analysis

Repository: NOR-STA SVN PCAPAC - NOR-STA

36. Claim 2.2.A.4: Reverse flow hazard has been mitigated


Claim 2.2.A.4
Reverse flow hazard has been mitigated
Strategy 2.2.A.4
Show pump is incapable of reverse flow
Rely on mechanical design of pumping mechanism
J
Trace mitigation to requirements
Trace mitigation to mechanical pump design
Verification of Mitigation
Reference to requirements for mitigation
Reference to requirements for mitigation

Claim 2.2.A.4: Reverse flow hazard has been mitigated

Strategy 2.2.A.4: Show pump is incapable of reverse flow

Rely on mechanical design of pumping mechanism

Trace mitigation to requirements

Reference to requirements for mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace mitigation to mechanical pump design

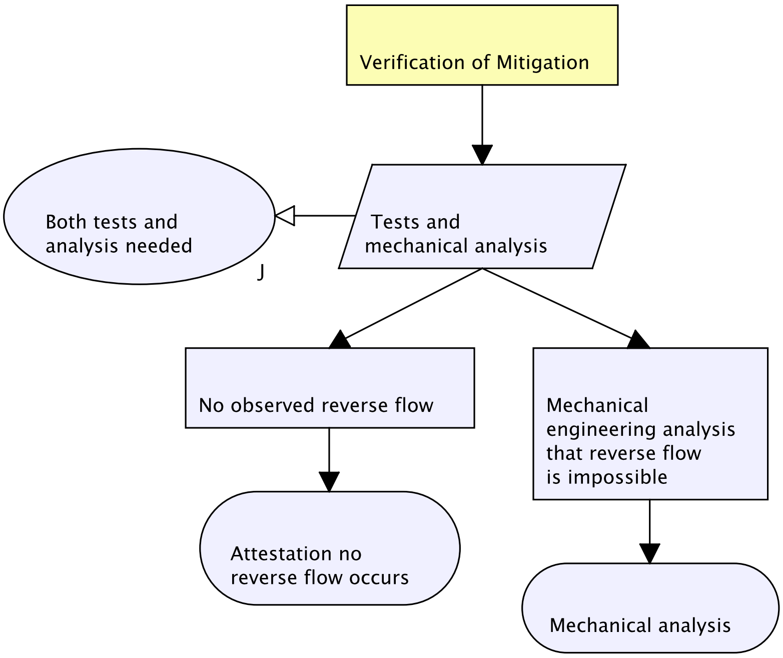
Reference to requirements for mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

Verification of Mitigation

See details in section 37

37. Verification of Mitigation


Verification of Mitigation
Both tests and analysis needed
J
Tests and mechanical analysis
No observed reverse flow
Mechanical engineering analysis that reverse flow is impossible
Attestation no reverse flow occurs
Mechanical analysis

Verification of Mitigation

Tests and mechanical analysis

Both tests and analysis needed

Because it is impossible to *prove* a negative (no free flow), observation that flow never occurs must be augmented with mechanical engineering analysis.

No observed reverse flow

Attestation no reverse flow occurs

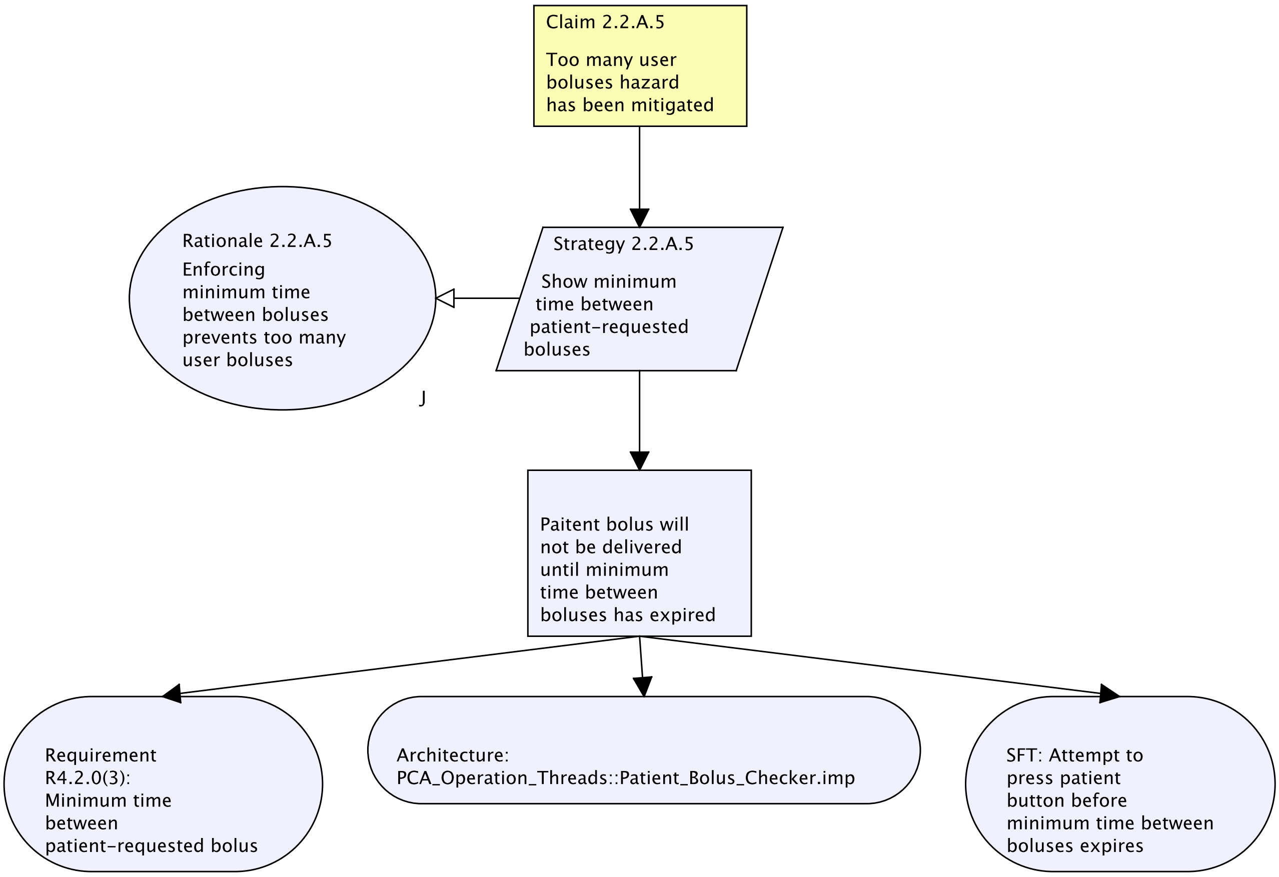
Repository: NOR-STA SVN PCAPAC - NOR-STA

Mechanical engineering analysis that reverse flow is impossible

Mechanical analysis

Repository: NOR-STA SVN PCAPAC - NOR-STA

38. Claim 2.2.A.5: Too many user boluses hazard has been mitigated


Claim 2.2.A.5
Too many user boluses hazard has been mitigated
Rationale 2.2.A.5
Enforcing minimum time between boluses prevents too many user boluses
J
Strategy 2.2.A.5
Show minimum time between patient-requested boluses
Paitent bolus will not be delivered until minimum time between boluses has expired
Requirement R4.2.0(3): Minimum time between patient-requested bolus
Architecture: PCA_Operation_Threads::Patient_Bolus_Checker.imp
SFT: Attempt to press patient button before minimum time between boluses expires

Claim 2.2.A.5: Too many user boluses hazard has been mitigated

Strategy 2.2.A.5: Show minimum time between patient-requested boluses

Rationale 2.2.A.5: Enforcing minimum time between boluses prevents too many user boluses

Paitent bolus will not be delivered until minimum time between boluses has expired

Requirement R4.2.0(3): Minimum time between patient-requested bolus

Evidence: ICE-PCArequirements.pdf#nameddest=minimum time between patient-requested bolus

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Operation_Threads::Patient_Bolus_Checker.imp

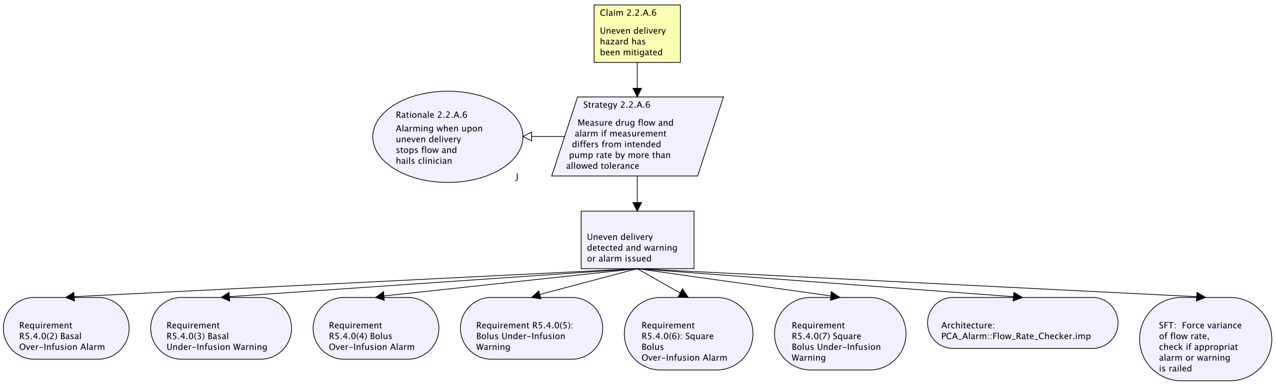
Evidence: PCA_Operation_Threads.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Attempt to press patient button before minimum time between boluses expires

Repository: NOR-STA SVN PCAPAC - NOR-STA

39. Claim 2.2.A.6: Uneven delivery hazard has been mitigated


Claim 2.2.A.6
Uneven delivery hazard has been mitigated
Strategy 2.2.A.6
Measure drug flow and alarm if measurement differs from intended pump rate by more than allowed tolerance
Rationale 2.2.A.6
Alarming when upon uneven delivery stops flow and hails clinician
J
Uneven delivery detected and warning or alarm issued
Requirement R5.4.0(2) Basal Over–Infusion Alarm
Requirement R5.4.0(3) Basal Under–Infusion Warning
Requirement R5.4.0(4) Bolus Over–Infusion Alarm
Requirement R5.4.0(5): Bolus Under–Infusion Warning
Requirement R5.4.0(6): Square Bolus Over–Infusion Alarm
Requirement R5.4.0(7) Square Bolus Under–Infusion Warning
Architecture: PCA_Alarm::Flow_Rate_Checker.imp
SFT: Force variance of flow rate, check if appropriat alarm or warning is railed

Claim 2.2.A.6: Uneven delivery hazard has been mitigated

Strategy 2.2.A.6: Measure drug flow and alarm if measurement differs from intended pump rate by more than allowed tolerance

Rationale 2.2.A.6: Alarming when upon uneven delivery stops flow and hails clinician

Uneven delivery detected and warning or alarm issued

Requirement R5.4.0(2) Basal Over-Infusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=basal over-infusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(3) Basal Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=basal under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(4) Bolus Over-Infusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=bolus over-infusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(5): Bolus Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=bolus under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(6): Square Bolus Over-Infusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=square bolus over-infusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(7) Square Bolus Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=square bolus under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Alarm::Flow_Rate_Checker.imp

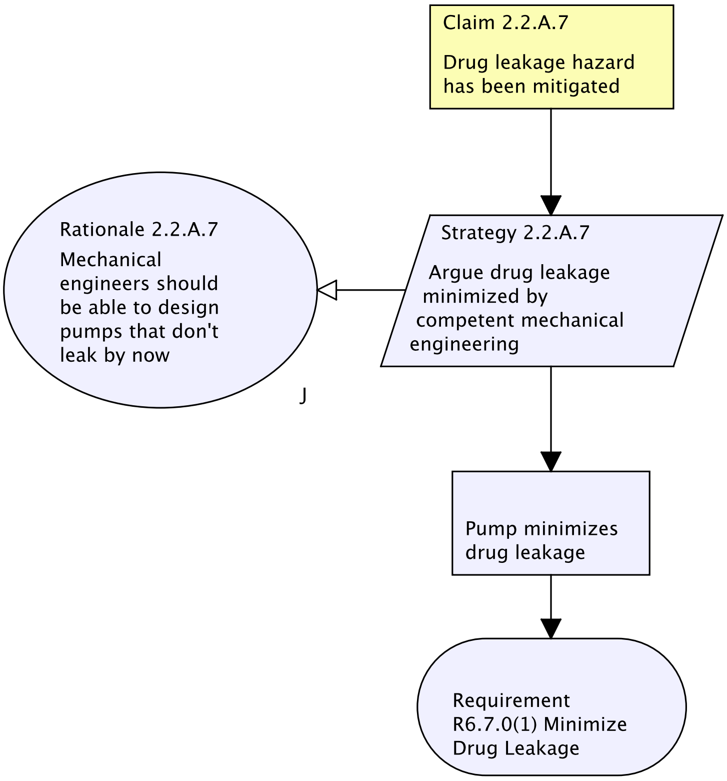
Evidence: PCA_Alarm.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Force variance of flow rate, check if appropriat alarm or warning is railed

Repository: NOR-STA SVN PCAPAC - NOR-STA

40. Claim 2.2.A.7: Drug leakage hazard has been mitigated


Claim 2.2.A.7
Drug leakage hazard has been mitigated
Rationale 2.2.A.7
Mechanical engineers should be able to design pumps that don't leak by now
J
Strategy 2.2.A.7
Argue drug leakage minimized by competent mechanical engineering
Pump minimizes drug leakage
Requirement R6.7.0(1) Minimize Drug Leakage

Claim 2.2.A.7: Drug leakage hazard has been mitigated

Strategy 2.2.A.7: Argue drug leakage minimized by competent mechanical engineering

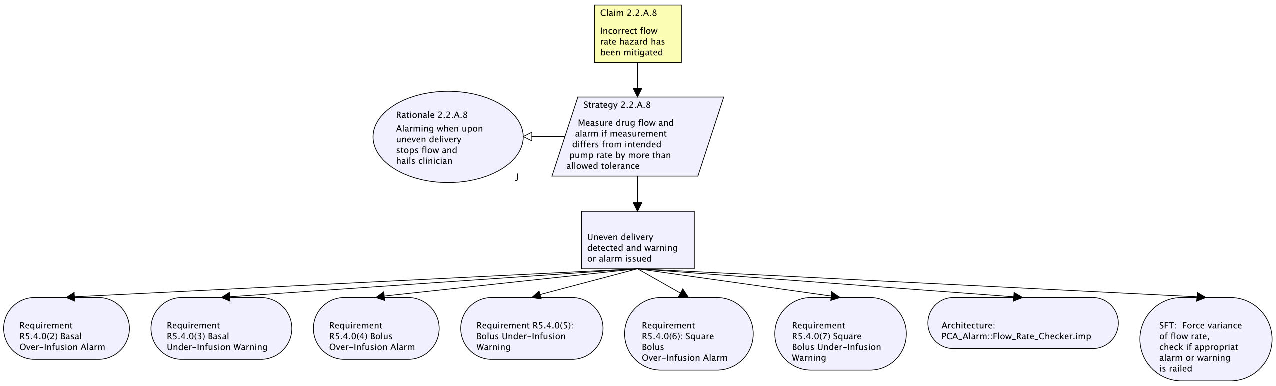
Rationale 2.2.A.7: Mechanical engineers should be able to design pumps that don't leak by now

Pump minimizes drug leakage

Requirement R6.7.0(1) Minimize Drug Leakage

Evidence:	ICE-PCArequirements.pdf#nameddest=minimize drug leakage
Repository:	NOR-STA SVN PCAPAC - NOR-STA

41. Claim 2.2.A.8: Incorrect flow rate hazard has been mitigated


Claim 2.2.A.8
Incorrect flow rate hazard has been mitigated
Strategy 2.2.A.8
Measure drug flow and alarm if measurement differs from intended pump rate by more than allowed tolerance
Rationale 2.2.A.8
Alarming when upon uneven delivery stops flow and hails clinician
J
Uneven delivery detected and warning or alarm issued
Requirement R5.4.0(2) Basal Over-Infusion Alarm
Requirement R5.4.0(3) Basal Under-Infusion Warning
Requirement R5.4.0(4) Bolus Over-Infusion Alarm
Requirement R5.4.0(5): Bolus Under-Infusion Warning
Requirement R5.4.0(6): Square Bolus Over-Infusion Alarm
Requirement R5.4.0(7) Square Bolus Under-Infusion Warning
Architecture: PCA_Alarm::Flow_Rate_Checker.imp
SFT: Force variance of flow rate, check if appropriat alarm or warning is railed

Claim 2.2.A.8: Incorrect flow rate hazard has been mitigated

Strategy 2.2.A.8: Measure drug flow and alarm if measurement differs from intended pump rate by more than allowed tolerance

Rationale 2.2.A.8: Alarming when upon uneven delivery stops flow and hails clinician

Uneven delivery detected and warning or alarm issued

Requirement R5.4.0(2) Basal Over-Infusion Alarm

Evidence:	ICE-PCArequirements.pdf#nameddest=basal over-infusion alarm
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(3) Basal Under-Infusion Warning

Evidence:	ICE-PCArequirements.pdf#nameddest=basal under-infusion warning
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(4) Bolus Over-Infusion Alarm

Evidence:	ICE-PCArequirements.pdf#nameddest=bolus over-infusion alarm
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(5): Bolus Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=bolus under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(6): Square Bolus Over-Infusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=square bolus over-infusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(7) Square Bolus Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=square bolus under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Alarm::Flow_Rate_Checker.imp

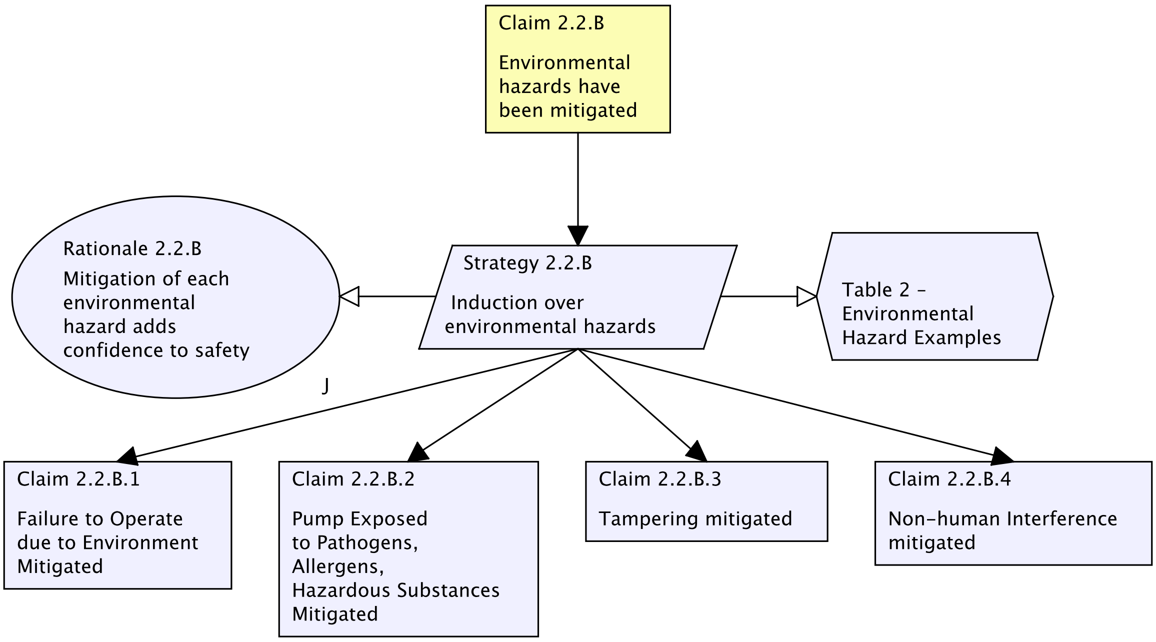
Evidence: PCA_Alarm.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Force variance of flow rate, check if appropriat alarm or warning is railed

Repository: NOR-STA SVN PCAPAC - NOR-STA

42. Claim 2.2.B: Environmental hazards have been mitigated


Claim 2.2.B
Environmental hazards have been mitigated
Rationale 2.2.B
Mitigation of each environmental hazard adds confidence to safety
J
Strategy 2.2.B
Induction over environmental hazards
Table 2 – Environmental Hazard Examples
Claim 2.2.B.1
Failure to Operate due to Environment Mitigated
Claim 2.2.B.2
Pump Exposed to Pathogens, Allergens, Hazardous Substances Mitigated
Claim 2.2.B.3
Tampering mitigated
Claim 2.2.B.4
Non-human Interference mitigated

Claim 2.2.B: Environmental hazards have been mitigated

following Table B in guidance

Strategy 2.2.B: Induction over environmental hazards

Rationale 2.2.B: Mitigation of each environmental hazard adds confidence to safety

Table 2 – Environmental Hazard Examples

See details in section 43

Claim 2.2.B.1: Failure to Operate due to Environment Mitigated

See details in section 44

Claim 2.2.B.2: Pump Exposed to Pathogens, Allergens, Hazardous Substances Mitigated

See details in section 45

Claim 2.2.B.3: Tampering mitigated

See details in section 46

Claim 2.2.B.4: Non-human Interference mitigated

See details in section 51

43. Table 2 – Environmental Hazard Examples

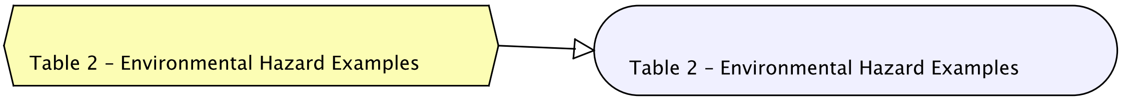


Table 2 – Environmental Hazard Examples
Table 2 – Environmental Hazard Examples

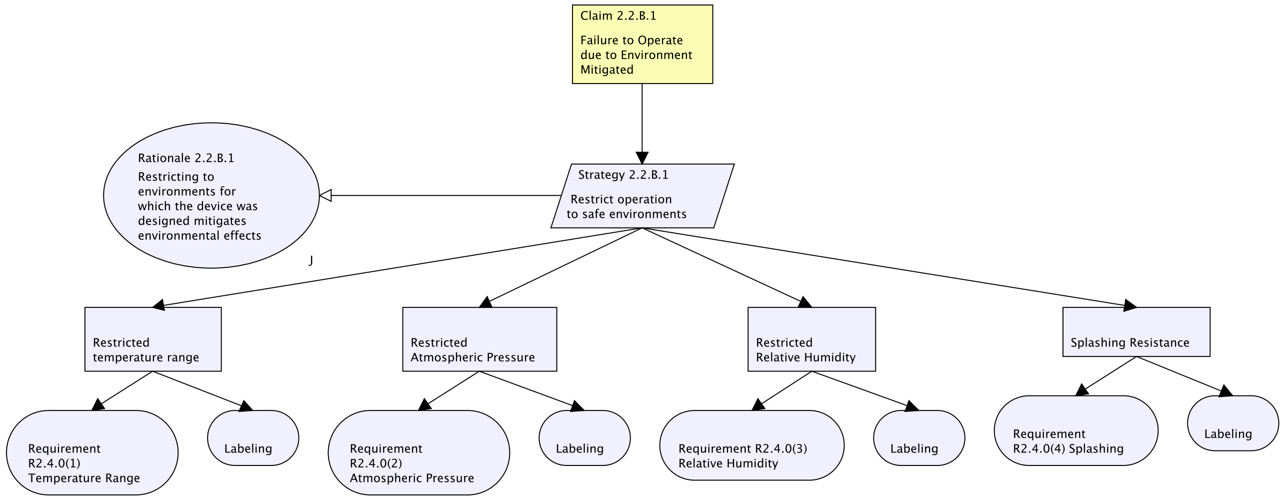
ℹ Table 2 – Environmental Hazard Examples

Table 2 – Environmental Hazard Examples

Evidence: IPGenera Guidance.pdf#page=14

Repository: NOR-STA SVN PCAPAC - NOR-STA

44. Claim 2.2.B.1: Failure to Operate due to Environment Mitigated


Claim 2.2.B.1
Failure to Operate due to Environment Mitigated
Rationale 2.2.B.1
Restricting to environments for which the device was designed mitigates environmental effects
J
Strategy 2.2.B.1
Restrict operation to safe environments
Restricted temperature range
Restricted Atmospheric Pressure
Restricted Relative Humidity
Splashing Resistance
Requirement R2.4.0(1) Temperature Range
Labeling
Requirement R2.4.0(2) Atmospheric Pressure
Labeling
Requirement R2.4.0(3) Relative Humidity
Labeling
Requirement R2.4.0(4) Splashing
Labeling

Claim 2.2.B.1: Failure to Operate due to Environment Mitigated

Corresponding Risk(s) to Health

Overdose Underdose Delay of therapy Electric shock

Potential Cause(s)

Temperature /Humidity/ Air pressure too high or too low

Strategy 2.2.B.1: Restrict operation to safe environments

Rationale 2.2.B.1: Restricting to environments for which the device was designed mitigates environmental effects

Restricted temperature range

Requirement R2.4.0(1) Temperature Range

Evidence: ICE-PCArequirements.pdf#nameddest=temperature range

Repository: NOR-STA SVN PCAPAC - NOR-STA

Labeling

Evidence: ICE-PCArequirements.pdf#nameddest=labeling

Repository: NOR-STA SVN PCAPAC - NOR-STA

Restricted Atmospheric Pressure

Requirement R2.4.0(2) Atmospheric Pressure

Evidence: ICE-PCArequirements.pdf#nameddest=atmospheric pressure

Repository: NOR-STA SVN PCAPAC - NOR-STA

Labeling

Evidence: ICE-PCArequirements.pdf#nameddest=labeling

Repository: NOR-STA SVN PCAPAC - NOR-STA

Restricted Relative Humidity

Requirement R2.4.0(3) Relative Humidity

Evidence: ICE-PCArequirements.pdf#nameddest=relative humidity

Repository: NOR-STA SVN PCAPAC - NOR-STA

Labeling

Evidence: ICE-PCArequirements.pdf#nameddest=labeling

Repository: NOR-STA SVN PCAPAC - NOR-STA

Splashing Resistance

Requirement R2.4.0(4) Splashing

Evidence: ICE-PCArequirements.pdf#nameddest=splashing

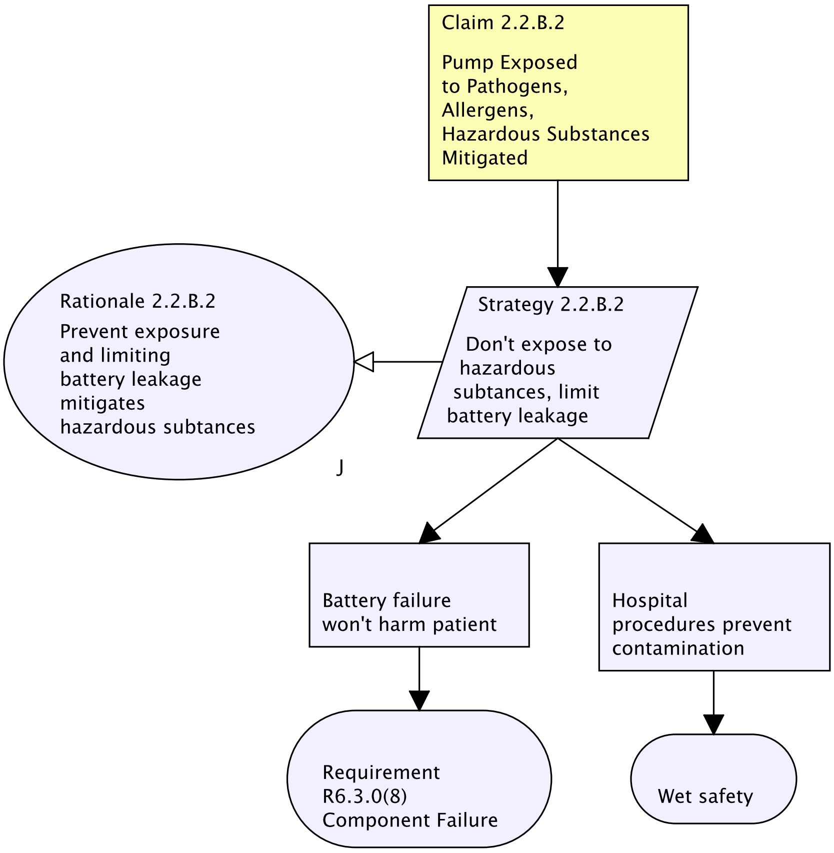
Repository: NOR-STA SVN PCAPAC - NOR-STA

Labeling

Evidence: ICE-PCArequirements.pdf#nameddest=labeling

Repository: NOR-STA SVN PCAPAC - NOR-STA

45. Claim 2.2.B.2: Pump Exposed to Pathogens, Allergens, Hazardous Substances Mitigated


Claim 2.2.B.2
Pump Exposed to Pathogens, Allergens, Hazardous Substances Mitigated
Rationale 2.2.B.2
Prevent exposure and limiting battery leakage mitigates hazardous subtances
J
Strategy 2.2.B.2
Don't expose to hazardous subtances, limit battery leakage
Battery failure won't harm patient
Hospital procedures prevent contamination
Requirement R6.3.0(8) Component Failure
Wet safety

Claim 2.2.B.2: Pump Exposed to Pathogens, Allergens, Hazardous Substances Mitigated

Corresponding Risk(s) to Health

Trauma, Infection,
Allergic response

Potential Cause(s)

Contamination due to spillage / exposure to toxins

Battery leak

Potential Cause(s)

Contamination due to spillage / exposure to toxins

Strategy 2.2.B.2: Don't expose to hazardous subtances, limit battery leakage

Rationale 2.2.B.2: Prevent exposure and limiting battery leakage mitigates hazardous subtances

Battery failure won't harm patient

Requirement R6.3.0(8) Component Failure

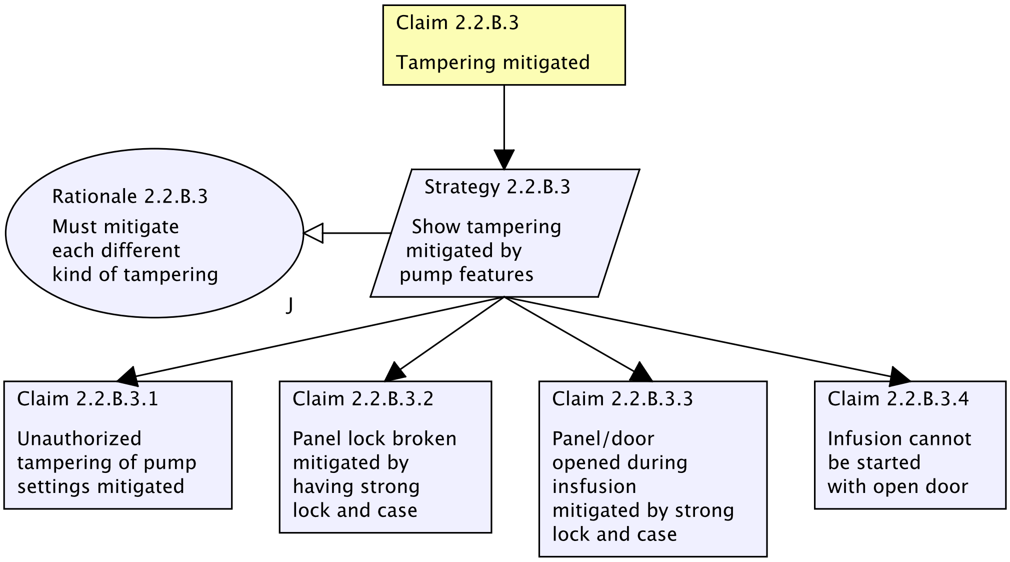
Evidence:	ICE-PCArequirements.pdf#nameddest=component failure
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Hospital procedures prevent contamination

Wet safety

Repository:	NOR-STA SVN PCAPAC - NOR-STA

46. Claim 2.2.B.3: Tampering mitigated


Claim 2.2.B.3
Tampering mitigated
Rationale 2.2.B.3
Must mitigate each different kind of tampering
J
Strategy 2.2.B.3
Show tampering mitigated by pump features
Claim 2.2.B.3.1
Unauthorized tampering of pump settings mitigated
Claim 2.2.B.3.2
Panel lock broken mitigated by having strong lock and case
Claim 2.2.B.3.3
Panel/door opened during insfusion mitigated by strong lock and case
Claim 2.2.B.3.4
Infusion cannot be started with open door

Claim 2.2.B.3: Tampering mitigated

(for example, by a
patient during home use to adjust
drug delivery)

Strategy 2.2.B.3: Show tampering mitigated by pump features

Rationale 2.2.B.3: Must mitigate each different kind of tampering

Claim 2.2.B.3.1: Unauthorized tampering of pump settings mitigated

See details in section 47

Claim 2.2.B.3.2: Panel lock broken mitigated by having strong lock and case

See details in section 48

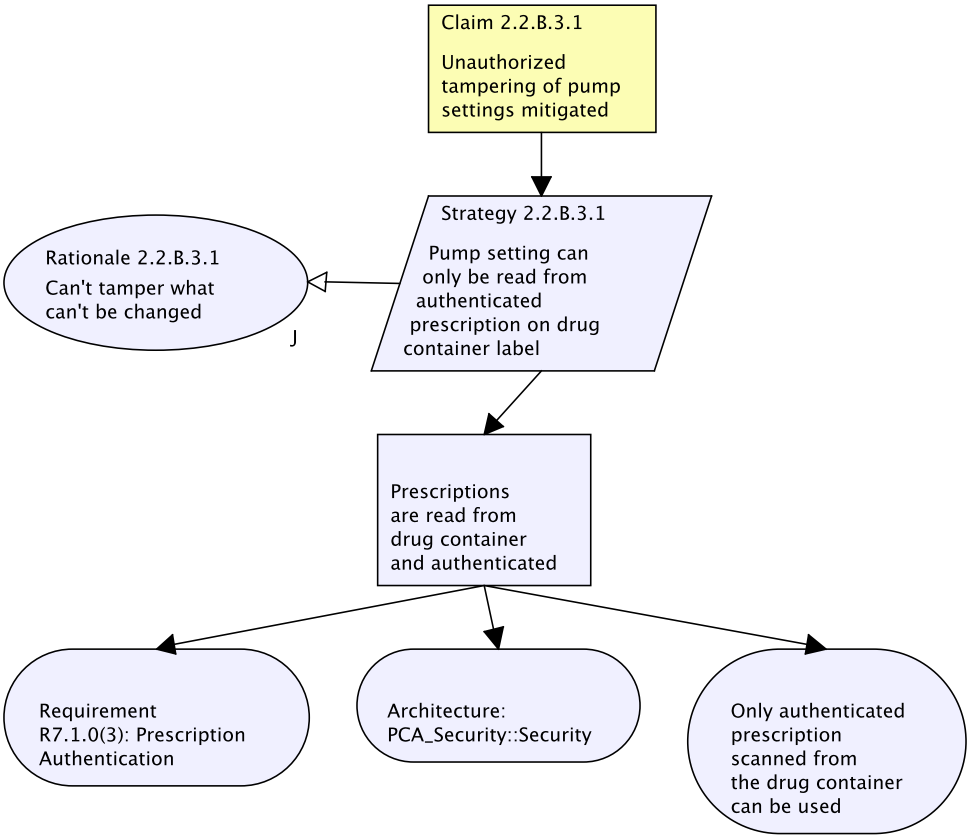
Claim 2.2.B.3.3: Panel/door opened during insfusion mitigated by strong lock and case

See details in section 49

Claim 2.2.B.3.4: Infusion cannot be started with open door

See details in section 50

47. Claim 2.2.B.3.1: Unauthorized tampering of pump settings mitigated


Claim 2.2.B.3.1
Unauthorized tampering of pump settings mitigated
Strategy 2.2.B.3.1
Pump setting can only be read from authenticated prescription on drug container label
Rationale 2.2.B.3.1
Can't tamper what can't be changed
J
Prescriptions are read from drug container and authenticated
Requirement R7.1.0(3): Prescription Authentication
Architecture: PCA_Security::Security
Only authenticated prescription scanned from the drug container can be used

Claim 2.2.B.3.1: Unauthorized tampering of pump settings mitigated

Pump settings defined on hard-to-fake label of drug container,
Authentication of Rx on label
Authentication of Clinician

Strategy 2.2.B.3.1: Pump setting can only be read from authenticated prescription on drug container label

Rationale 2.2.B.3.1: Can't tamper what can't be changed

Prescriptions are read from drug container and authenticated

Requirement R7.1.0(3): Prescription Authentication

Evidence: ICE-PCArequirements.pdf#nameddest=prescription authentication

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Security::Security

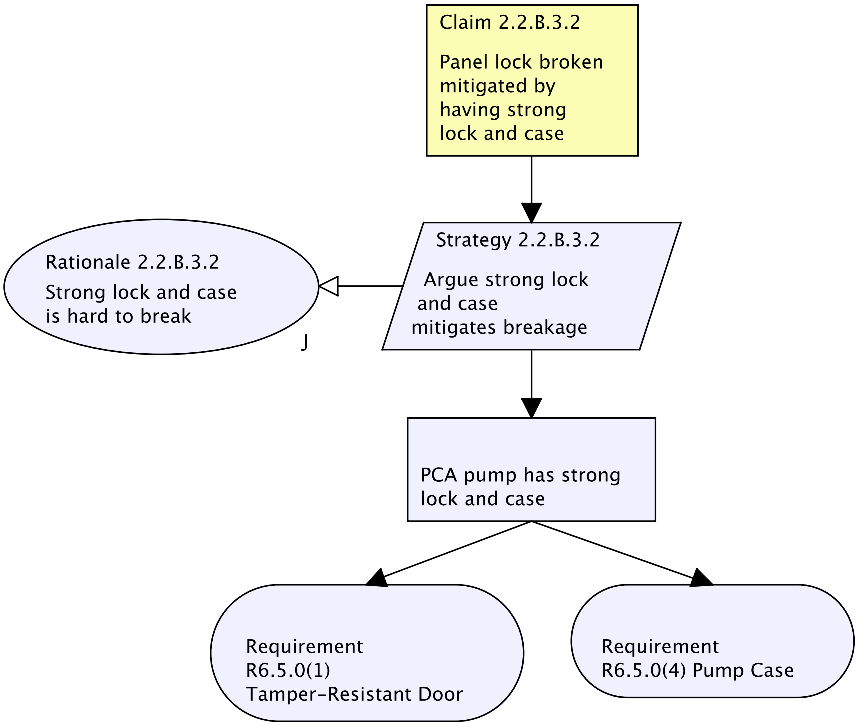
Evidence: PCA_Security.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Only authenticated prescription scanned from the drug container can be used

Repository: NOR-STA SVN PCAPAC - NOR-STA

48. Claim 2.2.B.3.2: Panel lock broken mitigated by having strong lock and case


Claim 2.2.B.3.2
Panel lock broken mitigated by having strong lock and case
Strategy 2.2.B.3.2
Argue strong lock and case mitigates breakage
Rationale 2.2.B.3.2
Strong lock and case is hard to break
J
PCA pump has strong lock and case
Requirement R6.5.0(1) Tamper–Resistant Door
Requirement R6.5.0(4) Pump Case

Claim 2.2.B.3.2: Panel lock broken mitigated by having strong lock and case

Lock must be hard to pick too

Strategy 2.2.B.3.2: Argue strong lock and case mitigates breakage

Rationale 2.2.B.3.2: Strong lock and case is hard to break

PCA pump has strong lock and case

Requirement R6.5.0(1) Tamper-Resistant Door

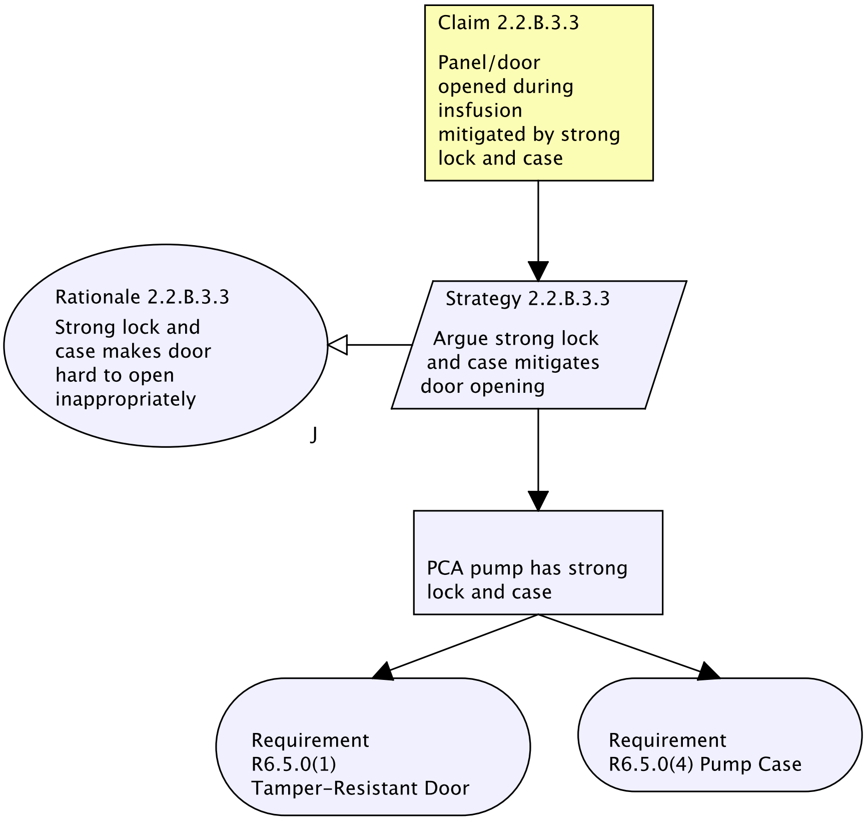
Evidence:	ICE-PCArequirements.pdf#nameddest=tamper-resistant door
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement R6.5.0(4) Pump Case

Evidence: ICE-PCArequirements.pdf#nameddest=pump case

Repository: NOR-STA SVN PCAPAC - NOR-STA

49. Claim 2.2.B.3.3: Panel/door opened during insfusion mitigated by strong lock and case


Claim 2.2.B.3.3
Panel/door opened during insfusion mitigated by strong lock and case
Rationale 2.2.B.3.3
Strong lock and case makes door hard to open inappropriately
J
Strategy 2.2.B.3.3
Argue strong lock and case mitigates door opening
PCA pump has strong lock and case
Requirement R6.5.0(1) Tamper–Resistant Door
Requirement R6.5.0(4) Pump Case

Claim 2.2.B.3.3: Panel/door opened during insfusion mitigated by strong lock and case

Strategy 2.2.B.3.3: Argue strong lock and case mitigates door opening

Rationale 2.2.B.3.3: Strong lock and case makes door hard to open inappropriately

PCA pump has strong lock and case

Requirement R6.5.0(1) Tamper-Resistant Door

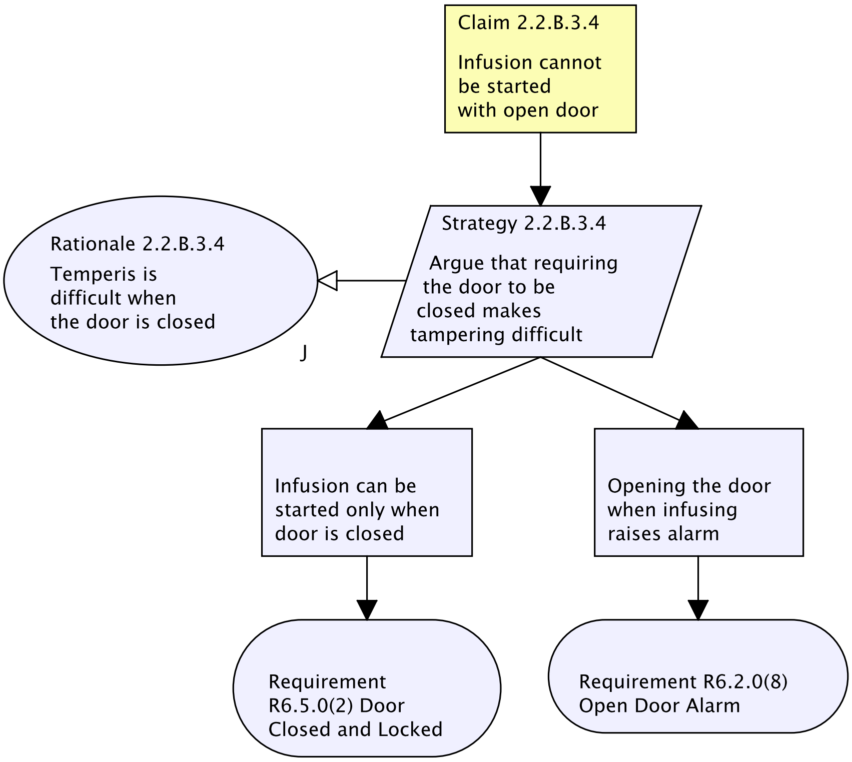
Evidence:	ICE-PCArequirements.pdf#nameddest=tamper-resistant door
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement R6.5.0(4) Pump Case

Evidence: ICE-PCArequirements.pdf#nameddest=pump case

Repository: NOR-STA SVN PCAPAC - NOR-STA

50. Claim 2.2.B.3.4: Infusion cannot be started with open door


Claim 2.2.B.3.4
Infusion cannot be started with open door
Strategy 2.2.B.3.4
Argue that requiring the door to be closed makes tampering difficult
Rationale 2.2.B.3.4
Temperis is difficult when the door is closed
J
Infusion can be started only when door is closed
Opening the door when infusing raises alarm
Requirement R6.5.0(2) Door Closed and Locked
Requirement R6.2.0(8) Open Door Alarm

Claim 2.2.B.3.4: Infusion cannot be started with open door

Trace to use case and architecture

Strategy 2.2.B.3.4: Argue that requiring the door to be closed makes tampering difficult

Rationale 2.2.B.3.4: Temperis is difficult when the door is closed

Infusion can be started only when door is closed

Requirement R6.5.0(2) Door Closed and Locked

Evidence: ICE-PCArequirements.pdf#nameddest=door closed and locked

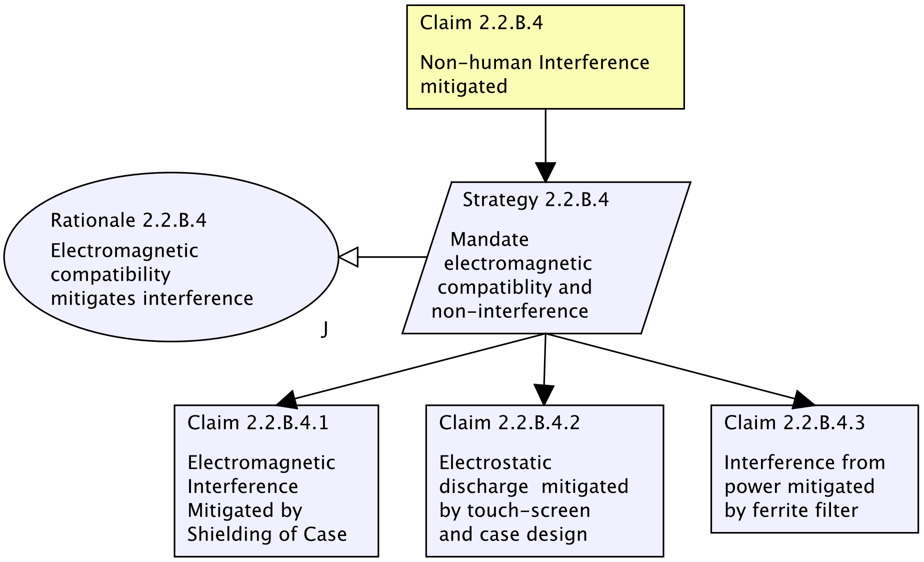
Repository: NOR-STA SVN PCAPAC - NOR-STA

Opening the door when infusing raises alarm

Requirement R6.2.0(8) Open Door Alarm

Evidence:	ICE-PCArequirements.pdf#nameddest=open door alarm
Repository:	NOR-STA SVN PCAPAC - NOR-STA

51. Claim 2.2.B.4: Non-human Interference mitigated


Claim 2.2.B.4
Non-human Interference mitigated
Strategy 2.2.B.4
Mandate electromagnetic compatiblity and non-interference
Rationale 2.2.B.4
Electromagnetic compatibility mitigates interference
J
Claim 2.2.B.4.1
Electromagnetic Interference Mitigated by Shielding of Case
Claim 2.2.B.4.2
Electrostatic discharge mitigated by touch-screen and case design
Claim 2.2.B.4.3
Interference from power mitigated by ferrite filter

Claim 2.2.B.4: Non-human Interference mitigated

Strategy 2.2.B.4: Mandate electromagnetic compatiblity and non-interference

Rationale 2.2.B.4: Electromagnetic compatibility mitigates interference

Claim 2.2.B.4.1: Electromagnetic Interference Mitigated by Shielding of Case

See details in section 52

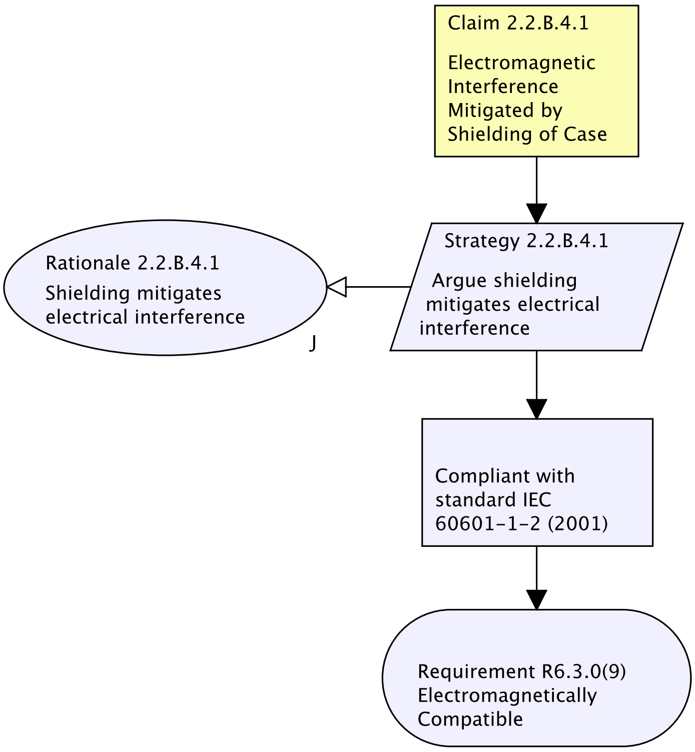
Claim 2.2.B.4.2: Electrostatic discharge mitigated by touch-screen and case design

See details in section 53

Claim 2.2.B.4.3: Interference from power mitigated by ferrite filter

See details in section 54

52. Claim 2.2.B.4.1: Electromagnetic Interference Mitigated by Shielding of Case


Claim 2.2.B.4.1
Electromagnetic Interference Mitigated by Shielding of Case
Strategy 2.2.B.4.1
Argue shielding mitigates electrical interference
Rationale 2.2.B.4.1
Shielding mitigates electrical interference
J
Compliant with standard IEC 60601-1-2 (2001)
Requirement R6.3.0(9) Electromagnetically Compatible

Claim 2.2.B.4.1: Electromagnetic Interference Mitigated by Shielding of Case

This should be added to the requirements

Strategy 2.2.B.4.1: Argue shielding mitigates electrical interference

Rationale 2.2.B.4.1: Shielding mitigates electrical interference

Compliant with standard IEC 60601-1-2 (2001)

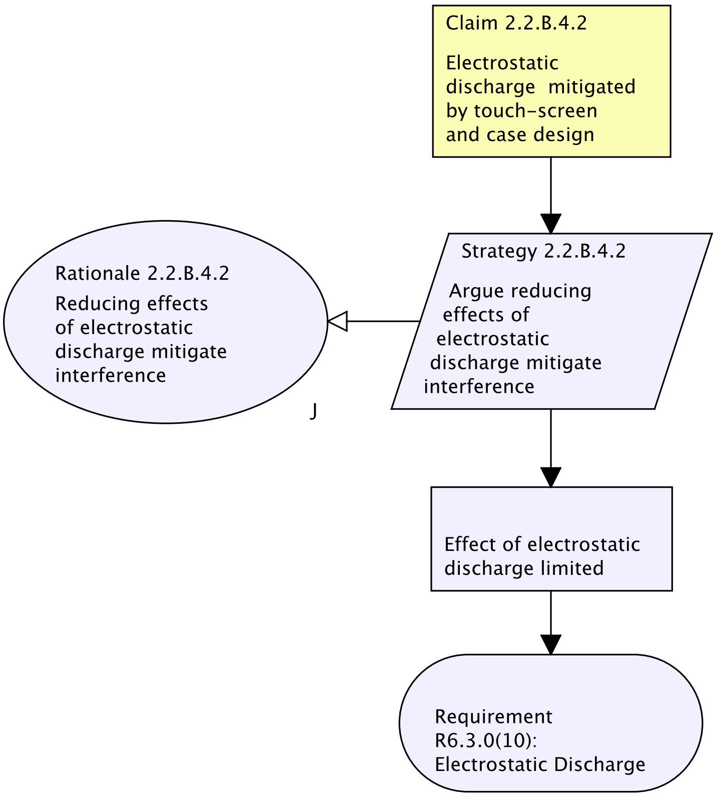
Medical Electrical Equipment, Part 1: General Requirements for Safety, 2. Collateral Standard: Electromagnetic Compatibility - Requirements and Tests

Requirement R6.3.0(9) Electromagnetically Compatible

Evidence: ICE-PCArequirements.pdf#nameddest=electromagnetically compatible

Repository: NOR-STA SVN PCAPAC - NOR-STA

53. Claim 2.2.B.4.2: Electrostatic discharge mitigated by touch-screen and case design


Claim 2.2.B.4.2
Electrostatic discharge mitigated by touch-screen and case design
Strategy 2.2.B.4.2
Argue reducing effects of electrostatic discharge mitigate interference
Rationale 2.2.B.4.2
Reducing effects of electrostatic discharge mitigate interference
J
Effect of electrostatic discharge limited
Requirement R6.3.0(10): Electrostatic Discharge

- **Claim 2.2.B.4.2: Electrostatic discharge mitigated by touch-screen and case design**

- **Strategy 2.2.B.4.2: Argue reducing effects of electrostatic discharge mitigate interference**

- **Rationale 2.2.B.4.2: Reducing effects of electrostatic discharge mitigate interference**

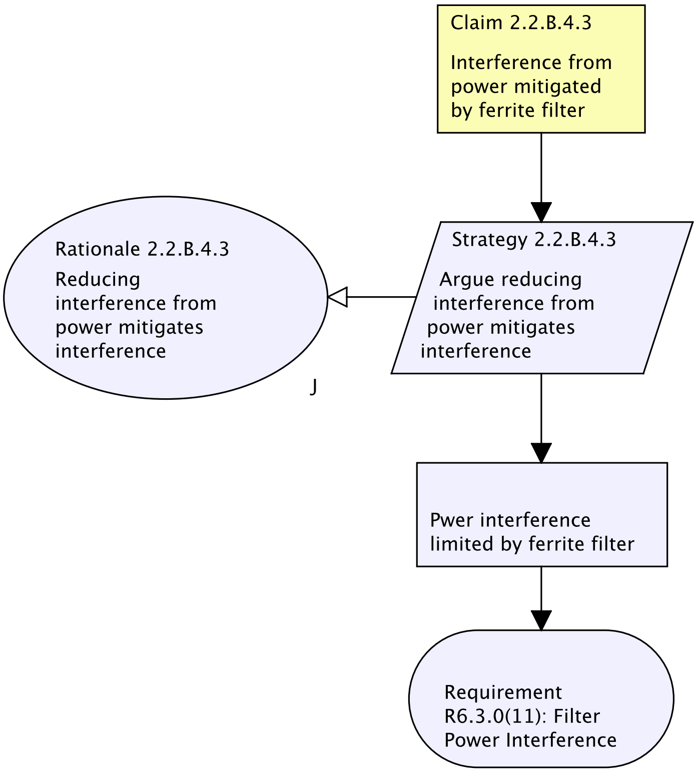
- **Effect of electrostatic discharge limited**

Requirement R6.3.0(10): Electrostatic Discharge

Evidence: ICE-PCArequirements.pdf#nameddest=electrostatic discharge

Repository: NOR-STA SVN PCAPAC - NOR-STA

54. Claim 2.2.B.4.3: Interference from power mitigated by ferrite filter


Claim 2.2.B.4.3
Interference from power mitigated by ferrite filter
Rationale 2.2.B.4.3
Reducing interference from power mitigates interference
J
Strategy 2.2.B.4.3
Argue reducing interference from power mitigates interference
Pwer interference limited by ferrite filter
Requirement R6.3.0(11): Filter Power Interference

Claim 2.2.B.4.3: Interference from power mitigated by ferrite filter

Strategy 2.2.B.4.3: Argue reducing interference from power mitigates interference

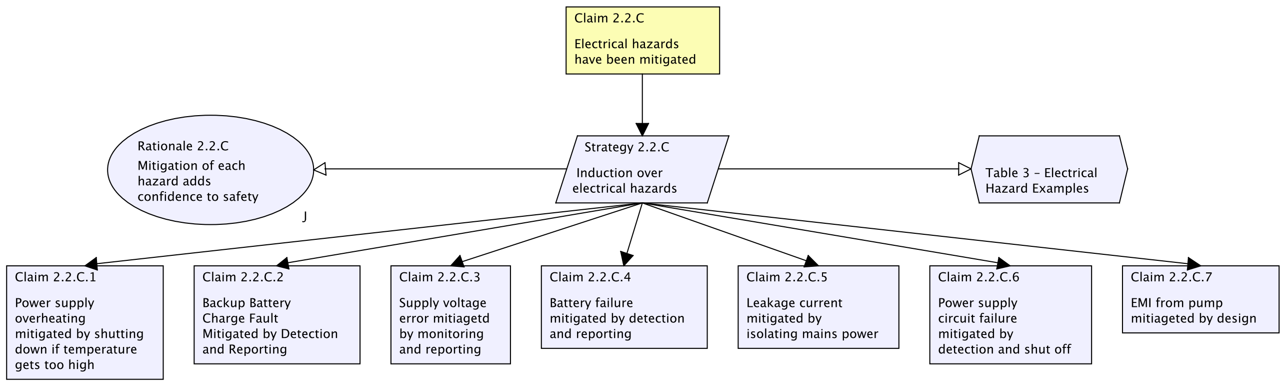
Rationale 2.2.B.4.3: Reducing interference from power mitigates interference

Pwer interference limited by ferrite filter

Requirement R6.3.0(11): Filter Power Interference

Evidence:	ICE-PCArequirements.pdf#nameddest=filter power interference
Repository:	NOR-STA SVN PCAPAC - NOR-STA

55. Claim 2.2.C: Electrical hazards have been mitigated


Claim 2.2.C
Electrical hazards have been mitigated
Rationale 2.2.C
Mitigation of each hazard adds confidence to safety
J
Strategy 2.2.C
Induction over electrical hazards
Table 3 – Electrical Hazard Examples
Claim 2.2.C.1
Power supply overheating mitigated by shutting down if temperature gets too high
Claim 2.2.C.2
Backup Battery Charge Fault Mitigated by Detection and Reporting
Claim 2.2.C.3
Supply voltage error mitiagetd by monitoring and reporting
Claim 2.2.C.4
Battery failure mitigated by detection and reporting
Claim 2.2.C.5
Leakage current mitigated by isolating mains power
Claim 2.2.C.6
Power supply circuit failure mitigated by detection and shut off
Claim 2.2.C.7
EMI from pump mitiageted by design

Claim 2.2.C: Electrical hazards have been mitigated

following Table c in guidance

Strategy 2.2.C: Induction over electrical hazards

Rationale 2.2.C: Mitigation of each hazard adds confidence to safety

Table 3 – Electrical Hazard Examples

See details in section 56

Claim 2.2.C.1: Power supply overheating mitigated by shutting down if temperature gets too high

See details in section 57

Claim 2.2.C.2: Backup Battery Charge Fault Mitigated by Detection and Reporting

See details in section 58

Claim 2.2.C.3: Supply voltage error mitiagetd by monitoring and reporting

See details in section 59

Claim 2.2.C.4: Battery failure mitigated by detection and reporting

See details in section 60

Claim 2.2.C.5: Leakage current mitigated by isolating mains power

See details in section 61

Claim 2.2.C.6: Power supply circuit failure mitigated by detection and shut off

See details in section 62

Claim 2.2.C.7: EMI from pump mitiageted by design

See details in section 63

56. Table 3 – Electrical Hazard Examples

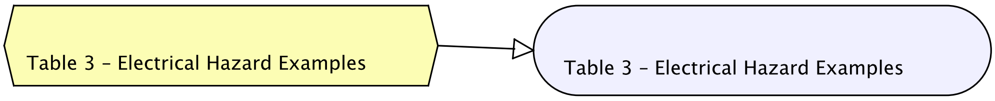


Table 3 – Electrical Hazard Examples
Table 3 – Electrical Hazard Examples

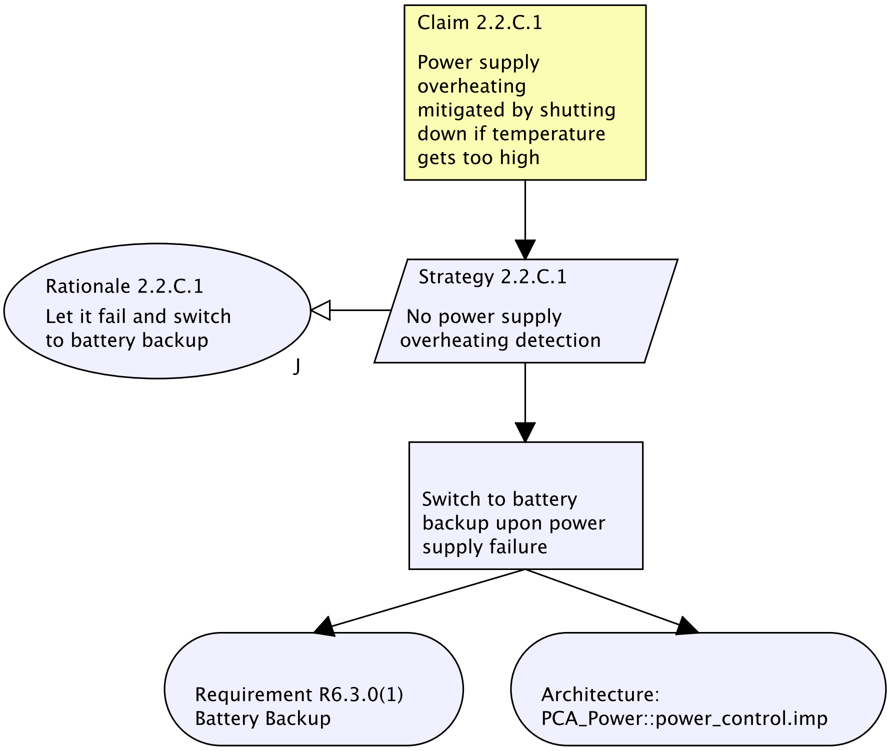
Table 3 – Electrical Hazard Examples

Table 3 – Electrical Hazard Examples

Evidence: IPGenera Guidance.pdf#page=15

Repository: NOR-STA SVN PCAPAC - NOR-STA

57. Claim 2.2.C.1: Power supply overheating mitigated by shutting down if temperature gets too high


Claim 2.2.C.1
Power supply overheating mitigated by shutting down if temperature gets too high
Rationale 2.2.C.1
Let it fail and switch to battery backup
J
Strategy 2.2.C.1
No power supply overheating detection
Switch to battery backup upon power supply failure
Requirement R6.3.0(1) Battery Backup
Architecture: PCA_Power::power_control.imp

Claim 2.2.C.1: Power supply overheating mitigated by shutting down if temperature gets too high

Strategy 2.2.C.1: No power supply overheating detection

Rationale 2.2.C.1: Let it fail and switch to battery backup

Switch to battery backup upon power supply failure

Requirement R6.3.0(1) Battery Backup

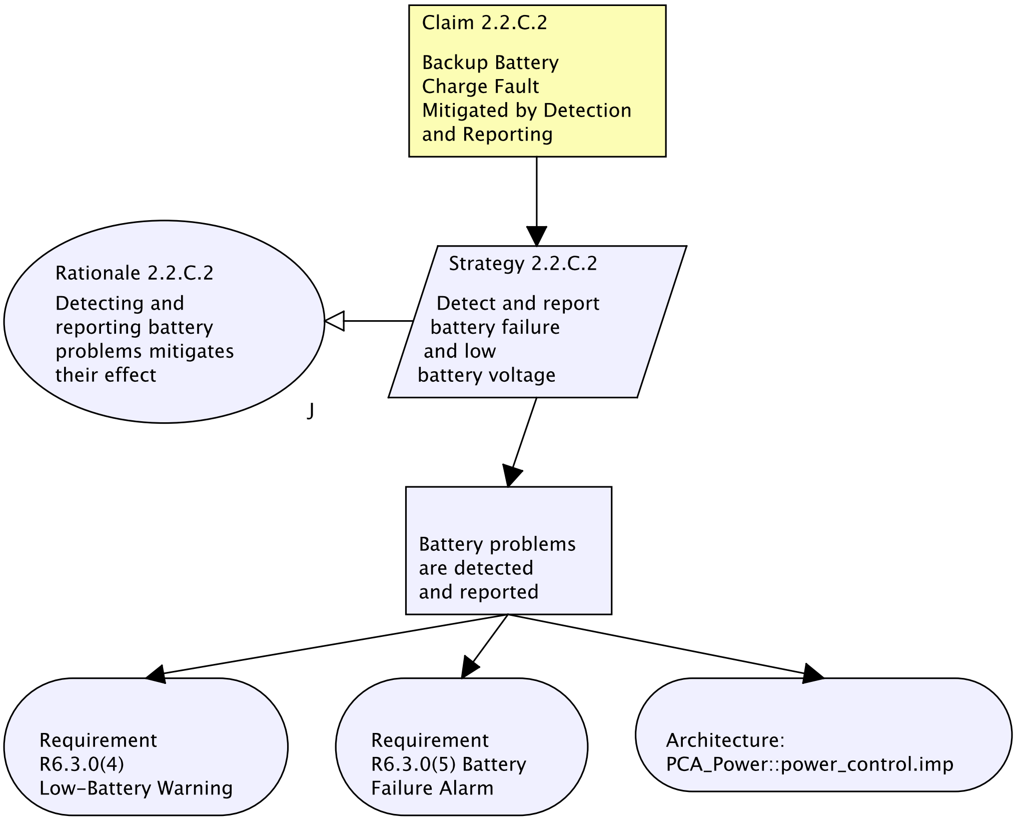
Evidence:	ICE-PCArequirements.pdf#nameddest=battery backup
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Power::power_control.imp

Evidence: PCA_Power.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

58. Claim 2.2.C.2: Backup Battery Charge Fault Mitigated by Detection and Reporting


Claim 2.2.C.2
Backup Battery Charge Fault Mitigated by Detection and Reporting
Rationale 2.2.C.2
Detecting and reporting battery problems mitigates their effect
J
Strategy 2.2.C.2
Detect and report battery failure and low battery voltage
Battery problems are detected and reported
Requirement R6.3.0(4) Low–Battery Warning
Requirement R6.3.0(5) Battery Failure Alarm
Architecture: PCA_Power::power_control.imp

Claim 2.2.C.2: Backup Battery Charge Fault Mitigated by Detection and Reporting

Strategy 2.2.C.2: Detect and report battery failure and low battery voltage

Rationale 2.2.C.2: Detecting and reporting battery problems mitigates their effect

Battery problems are detected and reported

Requirement R6.3.0(4) Low-Battery Warning

Evidence: ICE-PCArequirements.pdf#nameddest=low-battery warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R6.3.0(5) Battery Failure Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=battery failure alarm

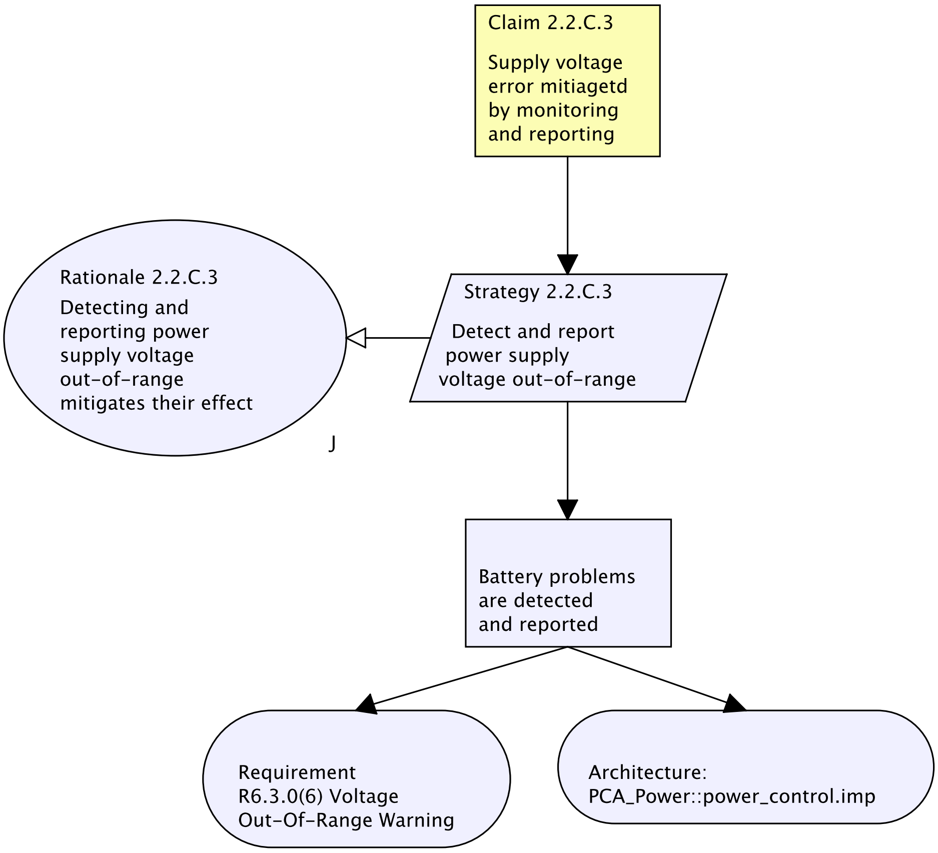
Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Power::power_control.imp

Evidence: PCA_Power.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

59. Claim 2.2.C.3: Supply voltage error mitiagetd by monitoring and reporting



Claim 2.2.C.3
Supply voltage error mitiagetd by monitoring and reporting
Rationale 2.2.C.3
Detecting and reporting power supply voltage out-of-range mitigates their effect
J
Strategy 2.2.C.3
Detect and report power supply voltage out-of-range
Battery problems are detected and reported
Requirement R6.3.0(6) Voltage Out-Of-Range Warning
Architecture: PCA_Power::power_control.imp

Claim 2.2.C.3: Supply voltage error mitiagetd by monitoring and reporting

Strategy 2.2.C.3: Detect and report power supply voltage out-of-range

Rationale 2.2.C.3: Detecting and reporting power supply voltage out-of-range mitigates their effect

Battery problems are detected and reported

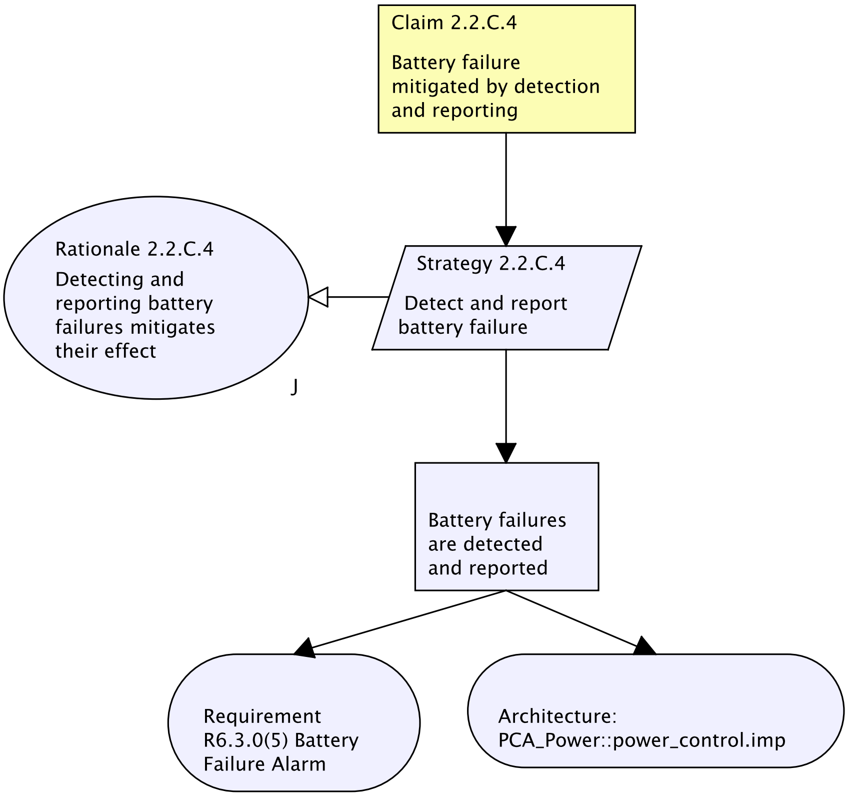
Requirement R6.3.0(6) Voltage Out-Of-Range Warning

Evidence:	ICE-PCArequirements.pdf#nameddest=voltage out-of-range warning
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Power::power_control.imp

Evidence:	PCA_Power.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

60. Claim 2.2.C.4: Battery failure mitigated by detection and reporting


Claim 2.2.C.4
Battery failure mitigated by detection and reporting
Rationale 2.2.C.4
Detecting and reporting battery failures mitigates their effect
J
Strategy 2.2.C.4
Detect and report battery failure
Battery failures are detected and reported
Requirement R6.3.0(5) Battery Failure Alarm
Architecture: PCA_Power::power_control.imp

Claim 2.2.C.4: Battery failure mitigated by detection and reporting

Strategy 2.2.C.4: Detect and report battery failure

Rationale 2.2.C.4: Detecting and reporting battery failures mitigates their effect

Battery failures are detected and reported

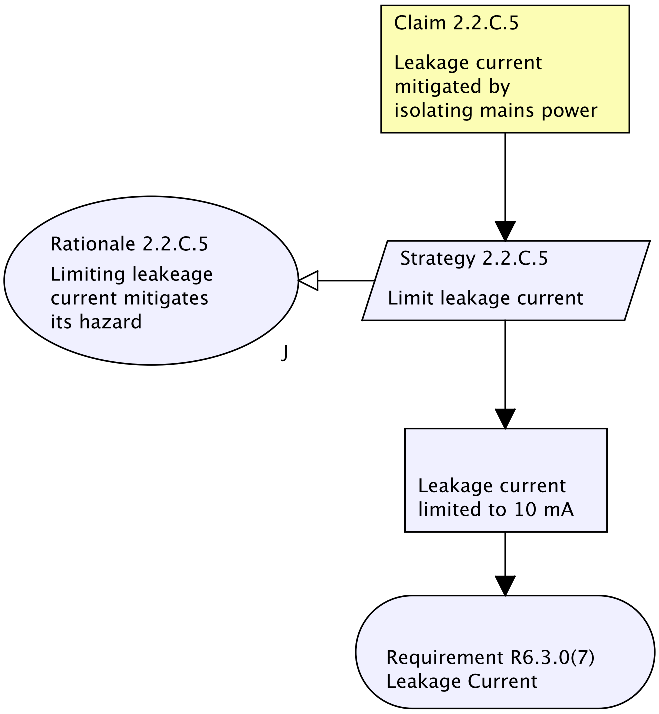
Requirement R6.3.0(5) Battery Failure Alarm

Evidence:	ICE-PCArequirements.pdf#nameddest=battery failure alarm
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Power::power_control.imp

Evidence:	PCA_Power.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

61. Claim 2.2.C.5: Leakage current mitigated by isolating mains power


Claim 2.2.C.5
Leakage current mitigated by isolating mains power
Rationale 2.2.C.5
Limiting leakeage current mitigates its hazard
J
Strategy 2.2.C.5
Limit leakage current
Leakage current limited to 10 mA
Requirement R6.3.0(7) Leakage Current

Claim 2.2.C.5: Leakage current mitigated by isolating mains power

Strategy 2.2.C.5: Limit leakage current

Rationale 2.2.C.5: Limiting leakeage current mitigates its hazard

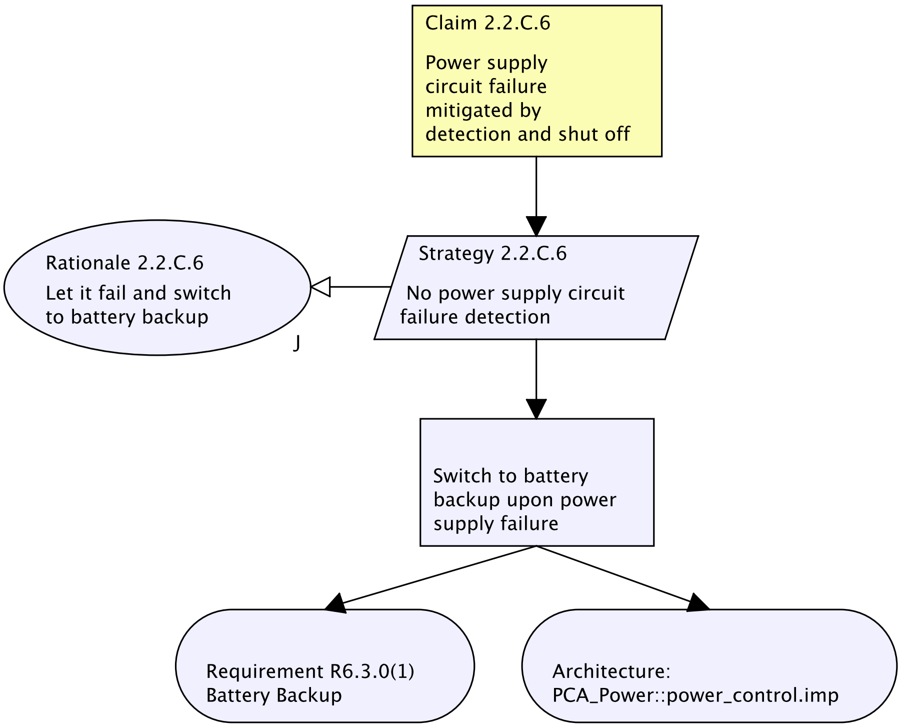
Leakage current limited to 10 mA

Requirement R6.3.0(7) Leakage Current

Evidence: ICE-PCArequirements.pdf#nameddest=leakage current

Repository: NOR-STA SVN PCAPAC - NOR-STA

62. Claim 2.2.C.6: Power supply circuit failure mitigated by detection and shut off


Claim 2.2.C.6
Power supply circuit failure mitigated by detection and shut off
Strategy 2.2.C.6
No power supply circuit failure detection
Rationale 2.2.C.6
Let it fail and switch to battery backup
J
Switch to battery backup upon power supply failure
Requirement R6.3.0(1) Battery Backup
Architecture: PCA_Power::power_control.imp

Claim 2.2.C.6: Power supply circuit failure mitigated by detection and shut off

Strategy 2.2.C.6: No power supply circuit failure detection

Rationale 2.2.C.6: Let it fail and switch to battery backup

Switch to battery backup upon power supply failure

Requirement R6.3.0(1) Battery Backup

Evidence: ICE-PCArequirements.pdf#nameddest=battery backup

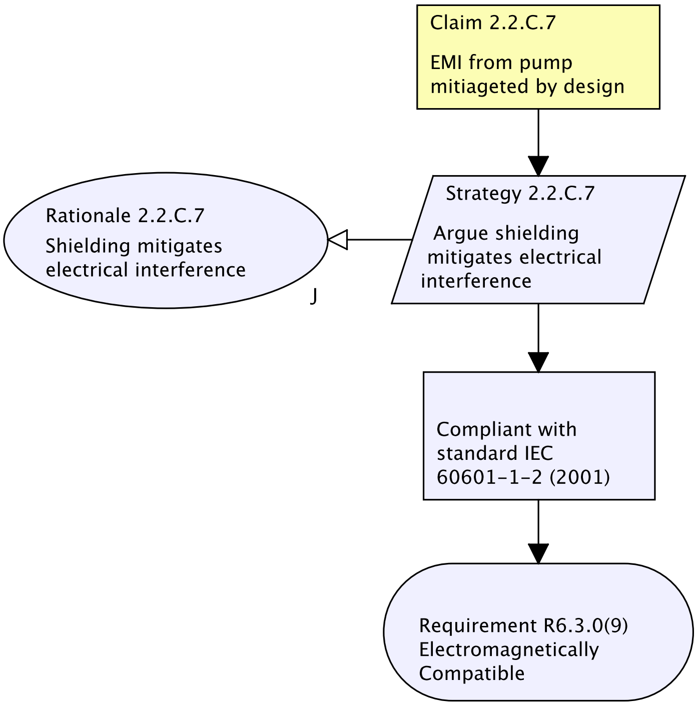
Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Power::power_control.imp

Evidence: PCA_Power.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

63. Claim 2.2.C.7: EMI from pump mitiageted by design


Claim 2.2.C.7
EMI from pump mitiageted by design
Strategy 2.2.C.7
Argue shielding mitigates electrical interference
Rationale 2.2.C.7
Shielding mitigates electrical interference
J
Compliant with standard IEC 60601-1-2 (2001)
Requirement R6.3.0(9) Electromagnetically Compatible

Claim 2.2.C.7: EMI from pump mitiageted by design

and verified by EMI lab testing.

Cite FCC limits on commercial site emissions

Strategy 2.2.C.7: Argue shielding mitigates electrical interference

Rationale 2.2.C.7: Shielding mitigates electrical interference

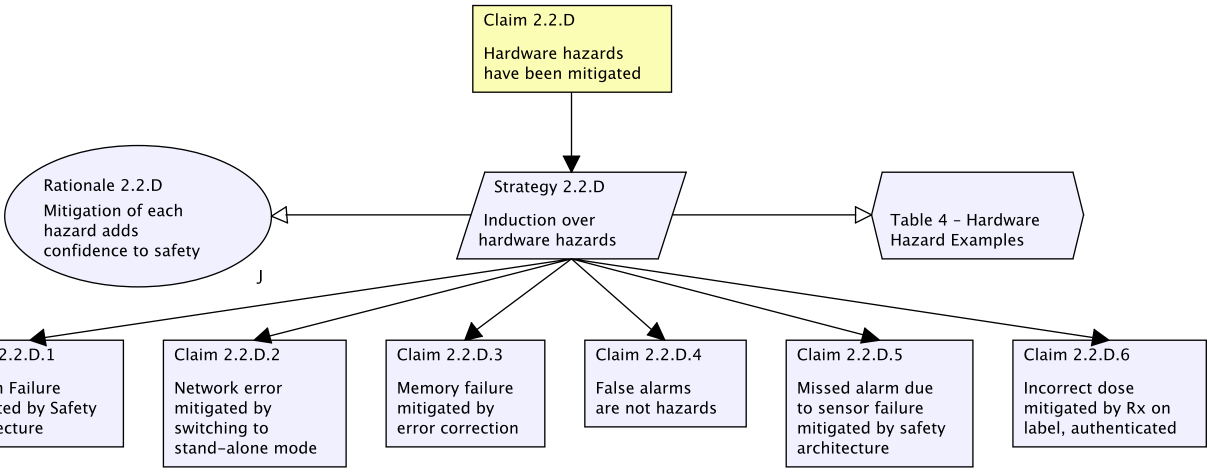
Compliant with standard IEC 60601-1-2 (2001)

Medical Electrical Equipment, Part 1: General Requirements for Safety, 2. Collateral Standard: Electromagnetic Compatibility - Requirements and Tests

Requirement R6.3.0(9) Electromagnetically Compatible

Evidence:	ICE-PCArequirements.pdf#nameddest=electromagnetically compatible
Repository:	NOR-STA SVN PCAPAC - NOR-STA

64. Claim 2.2.D: Hardware hazards have been mitigated


Claim 2.2.D
Hardware hazards have been mitigated
Rationale 2.2.D
Mitigation of each hazard adds confidence to safety
J
Strategy 2.2.D
Induction over hardware hazards
Table 4 – Hardware Hazard Examples
Claim 2.2.D.1
System Failure Mitigated by Safety Architecture
Claim 2.2.D.2
Network error mitigated by switching to stand-alone mode
Claim 2.2.D.3
Memory failure mitigated by error correction
Claim 2.2.D.4
False alarms are not hazards
Claim 2.2.D.5
Missed alarm due to sensor failure mitigated by safety architecture
Claim 2.2.D.6
Incorrect dose mitigated by Rx on label, authenticated

Claim 2.2.D: Hardware hazards have been mitigated

Hardware hazards are those hazards related to the failure of a hardware component of the device.

following Table D in guidance

Strategy 2.2.D: Induction over hardware hazards

Rationale 2.2.D: Mitigation of each hazard adds confidence to safety

Table 4 – Hardware Hazard Examples

See details in section 65

Claim 2.2.D.1: System Failure Mitigated by Safety Architecture

See details in section 66

Claim 2.2.D.2: Network error mitigated by switching to stand-alone mode

See details in section 67

Claim 2.2.D.3: Memory failure mitigated by error correction

See details in section 68

Claim 2.2.D.4: False alarms are not hazards

See details in section 69

Claim 2.2.D.5: Missed alarm due to sensor failure mitigated by safety architecture

See details in section 70

Claim 2.2.D.6: Incorrect dose mitigated by Rx on label, authenticated

See details in section 71

65. Table 4 – Hardware Hazard Examples

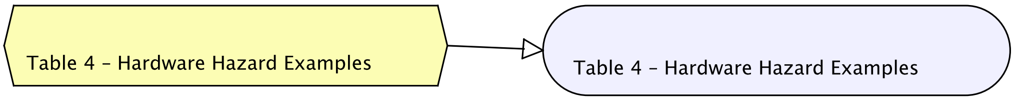


Table 4 – Hardware Hazard Examples
Table 4 – Hardware Hazard Examples

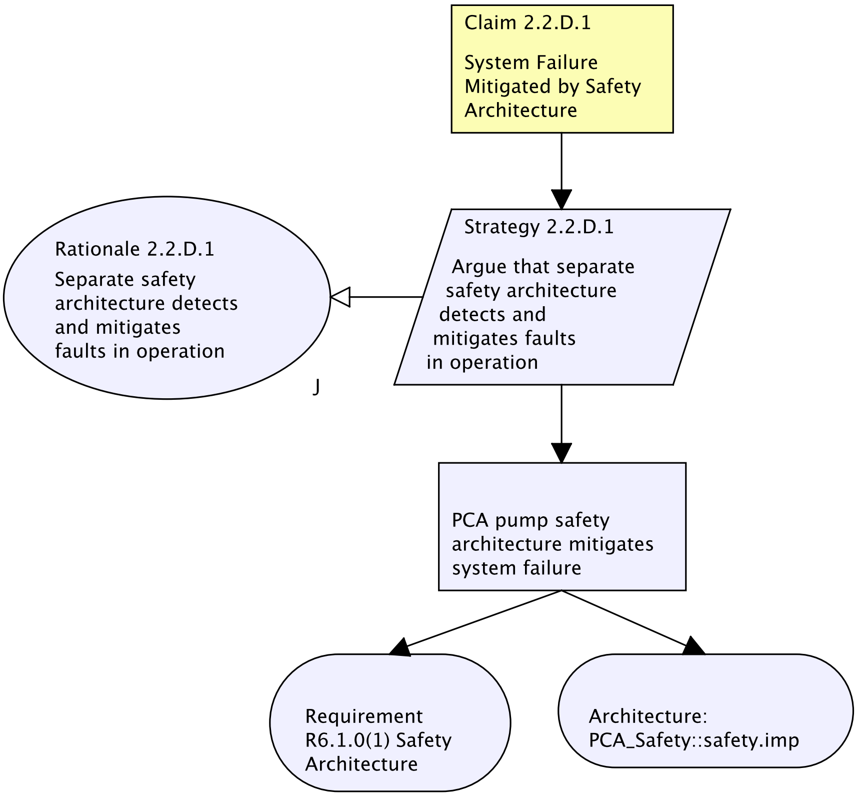
Table 4 – Hardware Hazard Examples

Table 4 – Hardware Hazard Examples

Evidence: IPGenera Guidance.pdf#page=17

Repository: NOR-STA SVN PCAPAC - NOR-STA

66. Claim 2.2.D.1: System Failure Mitigated by Safety Architecture


Claim 2.2.D.1
System Failure Mitigated by Safety Architecture
Strategy 2.2.D.1
Argue that separate safety architecture detects and mitigates faults in operation
Rationale 2.2.D.1
Separate safety architecture detects and mitigates faults in operation
J
PCA pump safety architecture mitigates system failure
Requirement R6.1.0(1) Safety Architecture
Architecture: PCA_Safety::safety.imp

Claim 2.2.D.1: System Failure Mitigated by Safety Architecture

Underdose Delay in therapy Incorrect therapy

Malfunctioning component
Synchronization error between pump components Watchdog failure
Reliability specification not met

Strategy 2.2.D.1: Argue that separate safety architecture detects and mitigates faults in operation

Rationale 2.2.D.1: Separate safety architecture detects and mitigates faults in operation

PCA pump safety architecture mitigates system failure

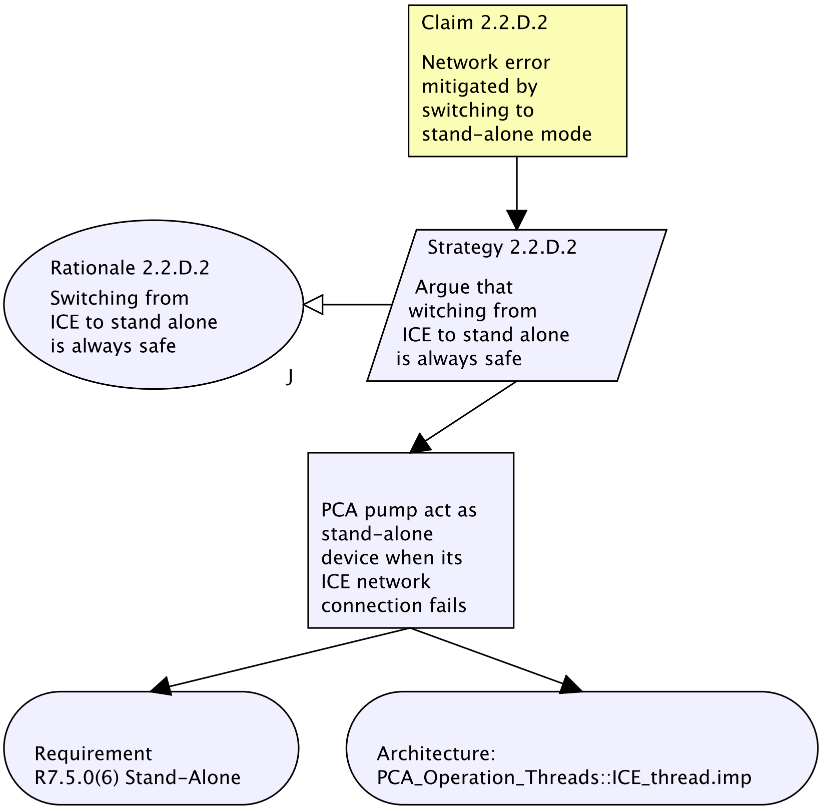
Requirement R6.1.0(1) Safety Architecture

Evidence:	ICE-PCArequirements.pdf#nameddest=safety architecture
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Safety::safety.imp

Evidence:	PCA_Safety.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

67. Claim 2.2.D.2: Network error mitigated by switching to stand-alone mode


Claim 2.2.D.2
Network error mitigated by switching to stand-alone mode
Strategy 2.2.D.2
Argue that witching from ICE to stand alone is always safe
Rationale 2.2.D.2
Switching from ICE to stand alone is always safe
J
PCA pump act as stand-alone device when its ICE network connection fails
Requirement R7.5.0(6) Stand-Alone
Architecture: PCA_Operation_Threads::ICE_thread.imp

Claim 2.2.D.2: Network error mitigated by switching to stand-alone mode

Strategy 2.2.D.2: Argue that witching from ICE to stand alone is always safe

Rationale 2.2.D.2: Switching from ICE to stand alone is always safe

PCA pump act as stand-alone device when its ICE network connection fails

Requirement R7.5.0(6) Stand-Alone

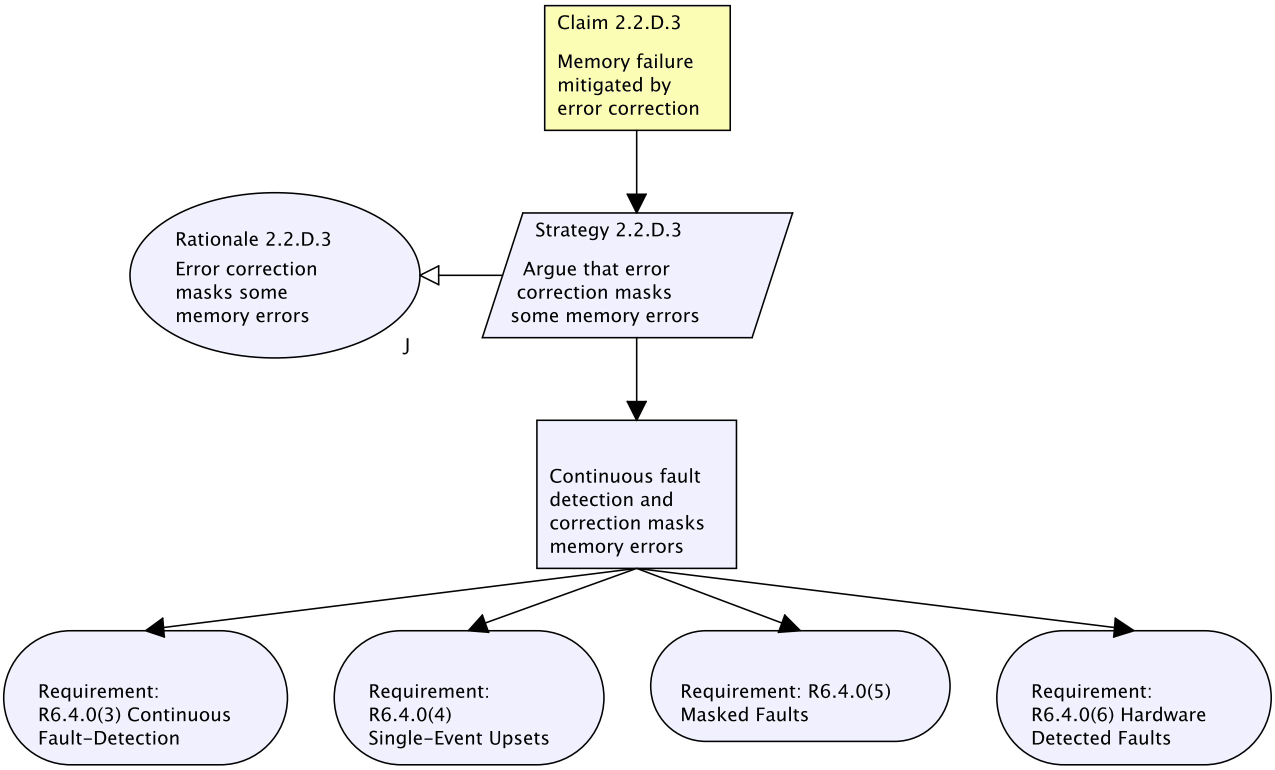
Evidence:	ICE-PCArequirements.pdf#nameddest=stand-alone
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Operation_Threads::ICE_thread.imp

Evidence: PCA_Operation_Threads.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

68. Claim 2.2.D.3: Memory failure mitigated by error correction


Claim 2.2.D.3
Memory failure mitigated by error correction
Rationale 2.2.D.3
Error correction masks some memory errors
J
Strategy 2.2.D.3
Argue that error correction masks some memory errors
Continuous fault detection and correction masks memory errors
Requirement: R6.4.0(3) Continuous Fault–Detection
Requirement: R6.4.0(4) Single–Event Upsets
Requirement: R6.4.0(5) Masked Faults
Requirement: R6.4.0(6) Hardware Detected Faults

Claim 2.2.D.3: Memory failure mitigated by error correction

Strategy 2.2.D.3: Argue that error correction masks some memory errors

Rationale 2.2.D.3: Error correction masks some memory errors

Continuous fault detection and correction masks memory errors

Requirement: R6.4.0(3) Continuous Fault-Detection

Evidence: ICE-PCArequirements.pdf#nameddest=continuous fault-detection

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R6.4.0(4) Single-Event Upsets

Evidence: ICE-PCArequirements.pdf#nameddest=single-event upsets

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R6.4.0(5) Masked Faults

Evidence: ICE-PCArequirements.pdf#nameddest=masked faults

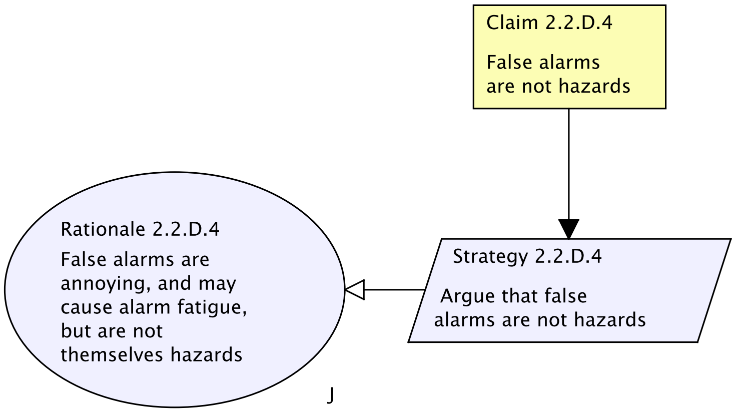
Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R6.4.0(6) Hardware Detected Faults

Evidence: ICE-PCArequirements.pdf#nameddest=hardware detected faults

Repository: NOR-STA SVN PCAPAC - NOR-STA

69. Claim 2.2.D.4: False alarms are not hazards

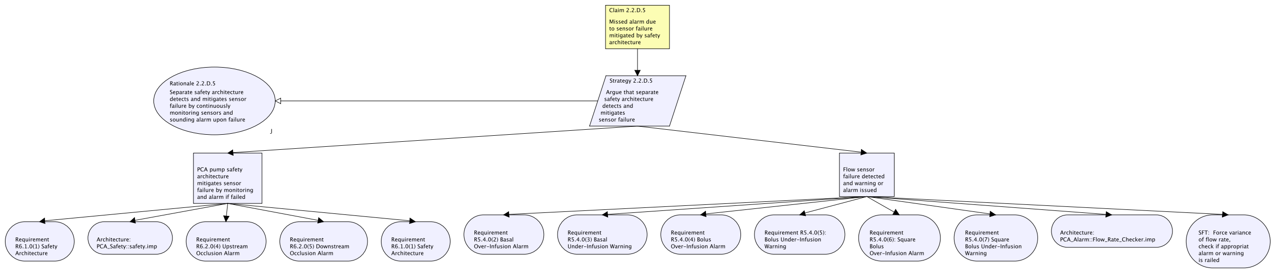

Claim 2.2.D.4
False alarms are not hazards
Strategy 2.2.D.4
Argue that false alarms are not hazards
Rationale 2.2.D.4
False alarms are annoying, and may cause alarm fatigue, but are not themselves hazards
J

Claim 2.2.D.4: False alarms are not hazards

Strategy 2.2.D.4: Argue that false alarms are not hazards

Rationale 2.2.D.4: False alarms are annoying, and may cause alarm fatigue, but are not themselves hazards

70. Claim 2.2.D.5: Missed alarm due to sensor failure mitigated by safety architecture


Claim 2.2.D.5
Missed alarm due to sensor failure mitigated by safety architecture
Rationale 2.2.D.5
Separate safety architecture detects and mitigates sensor failure by continuously monitoring sensors and sounding alarm upon failure
J
Strategy 2.2.D.5
Argue that separate safety architecture detects and mitigates sensor failure
PCA pump safety architecture mitigates sensor failure by monitoring and alarm if failed
Flow sensor failure detected and warning or alarm issued
Requirement R6.1.0(1) Safety Architecture
Architecture: PCA_Safety::safety.imp
Requirement R6.2.0(4) Upstream Occlusion Alarm
Requirement R6.2.0(5) Downstream Occlusion Alarm
Requirement R6.1.0(1) Safety Architecture
Requirement R5.4.0(2) Basal Over-Infusion Alarm
Requirement R5.4.0(3) Basal Under-Infusion Warning
Requirement R5.4.0(4) Bolus Over-Infusion Alarm
Requirement R5.4.0(5): Bolus Under-Infusion Warning
Requirement R5.4.0(6): Square Bolus Over-Infusion Alarm
Requirement R5.4.0(7) Square Bolus Under-Infusion Warning
Architecture: PCA_Alarm::Flow_Rate_Checker.imp
SFT: Force variance of flow rate, check if appropriat alarm or warning is railed

Claim 2.2.D.5: Missed alarm due to sensor failure mitigated by safety architecture

Strategy 2.2.D.5: Argue that separate safety architecture detects and mitigates sensor failure

Rationale 2.2.D.5: Separate safety architecture detects and mitigates sensor failure by continuously monitoring sensors and sounding alarm upon failure

PCA pump safety architecture mitigates sensor failure by monitoring and alarm if failed

Requirement R6.1.0(1) Safety Architecture

Evidence: ICE-PCArequirements.pdf#nameddest=safety architecture

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Safety::safety.imp

Evidence: PCA_Safety.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R6.2.0(4) Upstream Occlusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=upstream occlusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R6.2.0(5) Downstream Occlusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=downstream occlusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R6.1.0(1) Safety Architecture

Evidence: ICE-PCArequirements.pdf#nameddest=safety architecture

Repository: NOR-STA SVN PCAPAC - NOR-STA

Flow sensor failure detected and warning or alarm issued

Requirement R5.4.0(2) Basal Over-Infusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=basal over-infusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(3) Basal Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=basal under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(4) Bolus Over-Infusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=bolus over-infusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(5): Bolus Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=bolus under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(6): Square Bolus Over-Infusion Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=square bolus over-infusion alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(7) Square Bolus Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=square bolus under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Alarm::Flow_Rate_Checker.imp

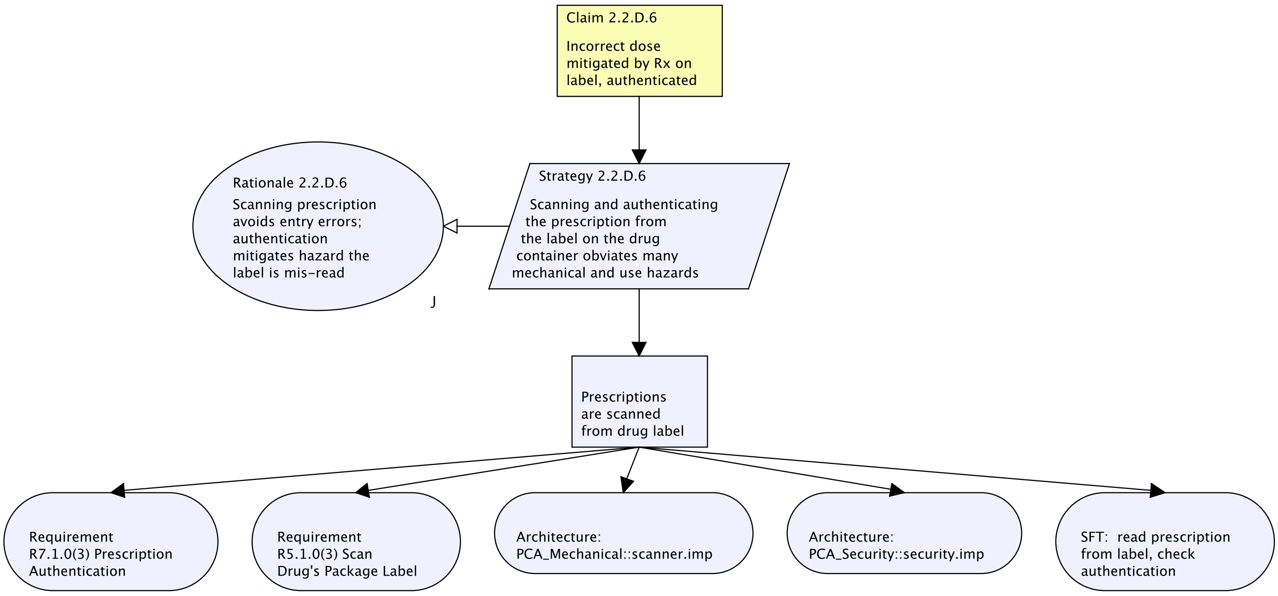
Evidence: PCA_Alarm.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Force variance of flow rate, check if appropriat alarm or warning is railed

Repository: NOR-STA SVN PCAPAC - NOR-STA

71. Claim 2.2.D.6: Incorrect dose mitigated by Rx on label, authenticated


Claim 2.2.D.6
Incorrect dose mitigated by Rx on label, authenticated
Rationale 2.2.D.6
Scanning prescription avoids entry errors; authentication mitigates hazard the label is mis-read
J
Strategy 2.2.D.6
Scanning and authenticating the prescription from the label on the drug container obviates many mechanical and use hazards
Prescriptions are scanned from drug label
Requirement R7.1.0(3) Prescription Authentication
Requirement R5.1.0(3) Scan Drug's Package Label
Architecture: PCA_Mechanical::scanner.imp
Architecture: PCA_Security::security.imp
SFT: read prescription from label, check authentication

Claim 2.2.D.6: Incorrect dose mitigated by Rx on label, authenticated

Strategy 2.2.D.6: Scanning and authenticating the prescription from the label on the drug container obviates many mechanical and use hazards

Rationale 2.2.D.6: Scanning prescription avoids entry errors; authentication mitigates hazard the label is mis-read

Prescriptions are scanned from drug label

Requirement R7.1.0(3) Prescription Authentication

Evidence:	ICE-PCArequirements.pdf#nameddest=prescription authentication
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.1.0(3) Scan Drug's Package Label

Evidence:	ICE-PCArequirements.pdf#nameddest=drug's package label
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Mechanical::scanner.imp

Evidence:	PCA_Mechanical.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

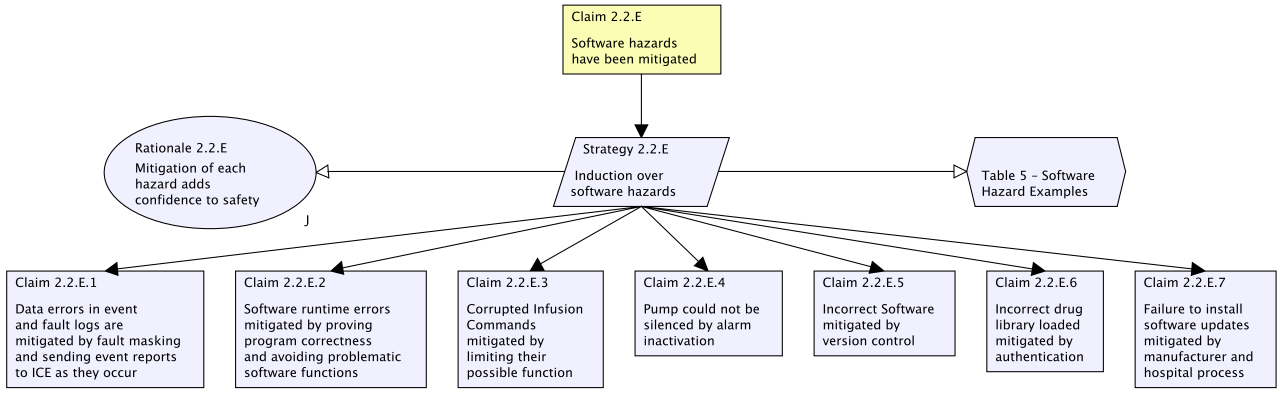
Architecture: PCA_Security::security.imp

Evidence:	PCA_Security.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

SFT: read prescription from label, check authentication

Repository:	NOR-STA SVN PCAPAC - NOR-STA

72. Claim 2.2.E: Software hazards have been mitigated


Claim 2.2.E
Software hazards have been mitigated
Rationale 2.2.E
Mitigation of each hazard adds confidence to safety
J
Strategy 2.2.E
Induction over software hazards
Table 5 – Software Hazard Examples
Claim 2.2.E.1
Data errors in event and fault logs are mitigated by fault masking and sending event reports to ICE as they occur
Claim 2.2.E.2
Software runtime errors mitigated by proving program correctness and avoiding problematic software functions
Claim 2.2.E.3
Corrupted Infusion Commands mitigated by limiting their possible function
Claim 2.2.E.4
Pump could not be silenced by alarm inactivation
Claim 2.2.E.5
Incorrect Software mitigated by version control
Claim 2.2.E.6
Incorrect drug library loaded mitigated by authentication
Claim 2.2.E.7
Failure to install software updates mitigated by manufacturer and hospital process

Claim 2.2.E: Software hazards have been mitigated

following Table E in guidance

Strategy 2.2.E: Induction over software hazards

Rationale 2.2.E: Mitigation of each hazard adds confidence to safety

Table 5 – Software Hazard Examples

See details in section 73

Claim 2.2.E.1: Data errors in event and fault logs are mitigated by fault masking and sending event reports to ICE as they occur

See details in section 74

Claim 2.2.E.2: Software runtime errors mitigated by proving program correctness and avoiding problematic software functions

See details in section 75

Claim 2.2.E.3: Corrupted Infusion Commands mitigated by limiting their possible function

See details in section 76

Claim 2.2.E.4: Pump could not be silenced by alarm inactivation

See details in section 77

Claim 2.2.E.5: Incorrect Software mitigated by version control

See details in section 78

Claim 2.2.E.6: Incorrect drug library loaded mitigated by authentication

See details in section 79

Claim 2.2.E.7: Failure to install software updates mitigated by manufacturer and hospital process

See details in section 80

73. Table 5 – Software Hazard Examples

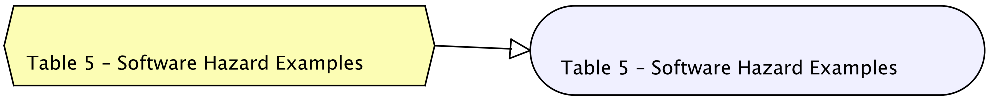


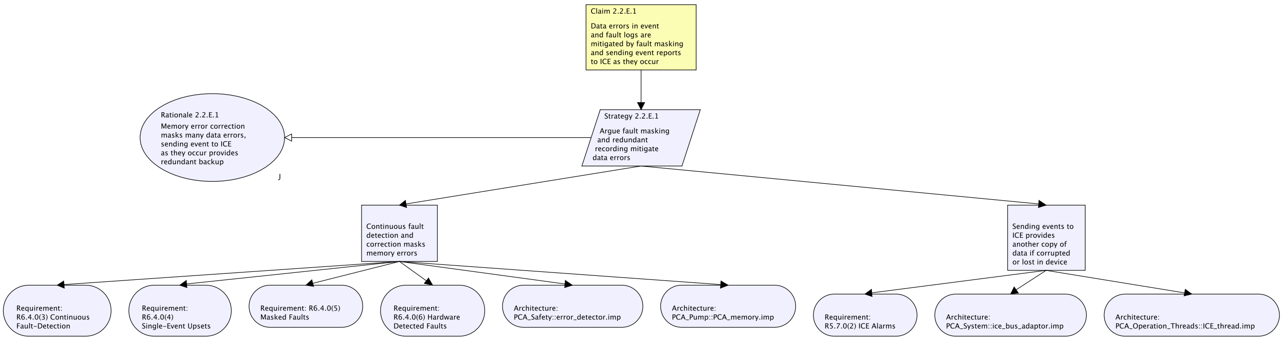
Table 5 – Software Hazard Examples
Table 5 – Software Hazard Examples

ℹ Table 5 – Software Hazard Examples

Table 5 – Software Hazard Examples

Evidence:	IPGenera Guidance.pdf#page=18
Repository:	NOR-STA SVN PCAPAC - NOR-STA

74. Claim 2.2.E.1: Data errors in event and fault logs are mitigated by fault masking and sending event reports to ICE as they occur


Claim 2.2.E.1
Data errors in event and fault logs are mitigated by fault masking and sending event reports to ICE as they occur
Rationale 2.2.E.1
Memory error correction masks many data errors, sending event to ICE as they occur provides redundant backup
J
Strategy 2.2.E.1
Argue fault masking and redundant recording mitigate data errors
Continuous fault detection and correction masks memory errors
Sending events to ICE provides another copy of data if corrupted or lost in device
Requirement: R6.4.0(3) Continuous Fault-Detection
Requirement: R6.4.0(4) Single-Event Upsets
Requirement: R6.4.0(5) Masked Faults
Requirement: R6.4.0(6) Hardware Detected Faults
Architecture: PCA_Safety::error_detector.imp
Architecture: PCA_Pump::PCA_memory.imp
Requirement: R5.7.0(2) ICE Alarms
Architecture: PCA_System::ice_bus_adaptor.imp
Architecture: PCA_Operation_Threads::ICE_thread.imp

Claim 2.2.E.1: Data errors in event and fault logs are mitigated by fault masking and sending event reports to ICE as they occur

Strategy 2.2.E.1: Argue fault masking and redundant recording mitigate data errors

Rationale 2.2.E.1: Memory error correction masks many data errors, sending event to ICE as they occur provides redundant backup

Continuous fault detection and correction masks memory errors

Requirement: R6.4.0(3) Continuous Fault-Detection

Evidence: ICE-PCArequirements.pdf#nameddest=continuous fault-detection

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R6.4.0(4) Single-Event Upsets

Evidence: ICE-PCArequirements.pdf#nameddest=single-event upsets

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R6.4.0(5) Masked Faults

Evidence: ICE-PCArequirements.pdf#nameddest=masked faults

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R6.4.0(6) Hardware Detected Faults

Evidence: ICE-PCArequirements.pdf#nameddest=hardware detected faults

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Safety::error_detector.imp

Evidence: PCA_Safety.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Pump::PCA_memory.imp

Evidence: PCA_Pump.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Sending events to ICE provides another copy of data if corrupted or lost in device

Requirement: R5.7.0(2) ICE Alarms

Evidence: ICE-PCArequirements.pdf#nameddest=ICE alarms

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_System::ice_bus_adaptor.imp

Evidence: PCA_System.aadl

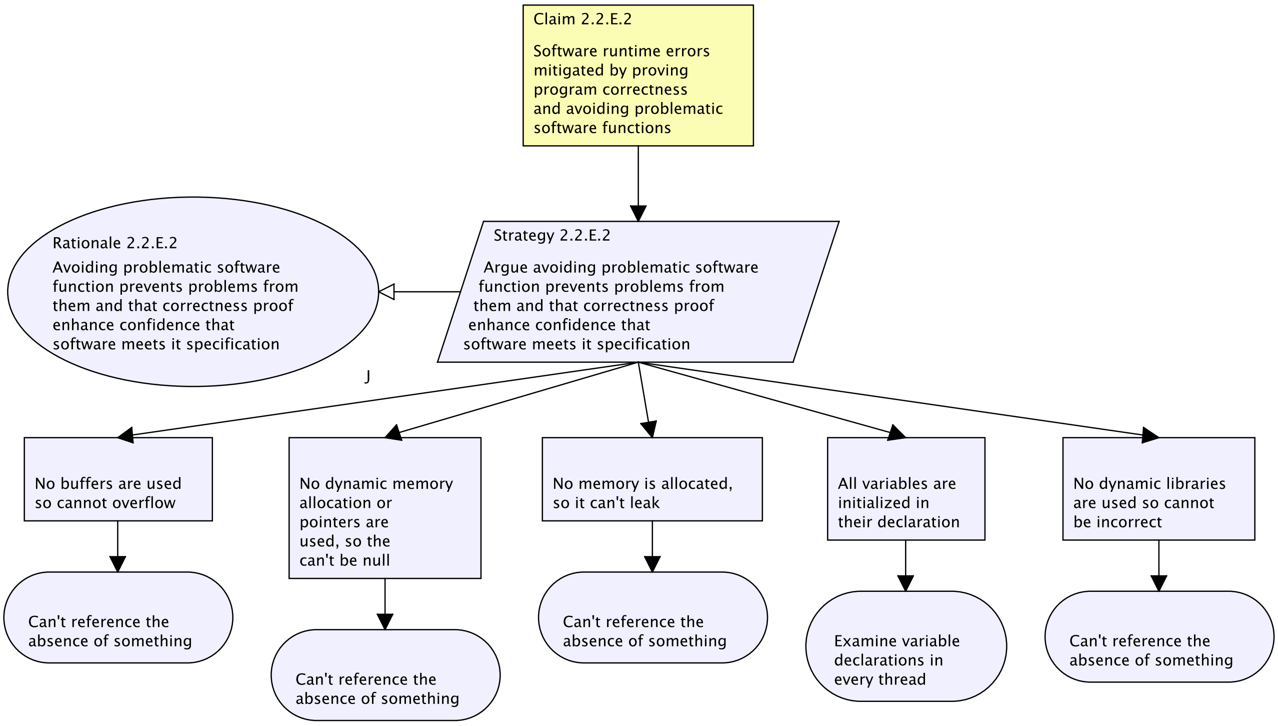
Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Operation_Threads::ICE_thread.imp

Evidence: PCA_Operation_Threads.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

75. Claim 2.2.E.2: Software runtime errors mitigated by proving program correctness and avoiding problematic software functions



Claim 2.2.E.2
Software runtime errors mitigated by proving program correctness and avoiding problematic software functions
Strategy 2.2.E.2
Argue avoiding problematic software function prevents problems from them and that correctness proof enhance confidence that software meets it specification
Rationale 2.2.E.2
Avoiding problematic software function prevents problems from them and that correctness proof enhance confidence that software meets it specification
J
No buffers are used so cannot overflow
No dynamic memory allocation or pointers are used, so the can't be null
No memory is allocated, so it can't leak
All variables are initialized in their declaration
No dynamic libraries are used so cannot be incorrect
Can't reference the absence of something
Can't reference the absence of something
Can't reference the absence of something
Examine variable declarations in every thread
Can't reference the absence of something

Claim 2.2.E.2: Software runtime errors mitigated by proving program correctness and avoiding problematic software functions

Strategy 2.2.E.2: Argue avoiding problematic software function prevents problems from them and that correctness proof enhance confidence that software meets it specification

Rationale 2.2.E.2: Avoiding problematic software function prevents problems from them and that correctness proof enhance confidence that software meets it specification

No buffers are used so cannot overflow

Can't reference the absence of something

Repository: NOR-STA SVN PCAPAC - NOR-STA

No dynamic memory allocation or pointers are used, so the can't be null

Can't reference the absence of something

Repository: NOR-STA SVN PCAPAC - NOR-STA

No memory is allocated, so it can't leak

Can't reference the absence of something

Repository: NOR-STA SVN PCAPAC - NOR-STA

All variables are initialized in their declaration

Examine variable declarations in every thread

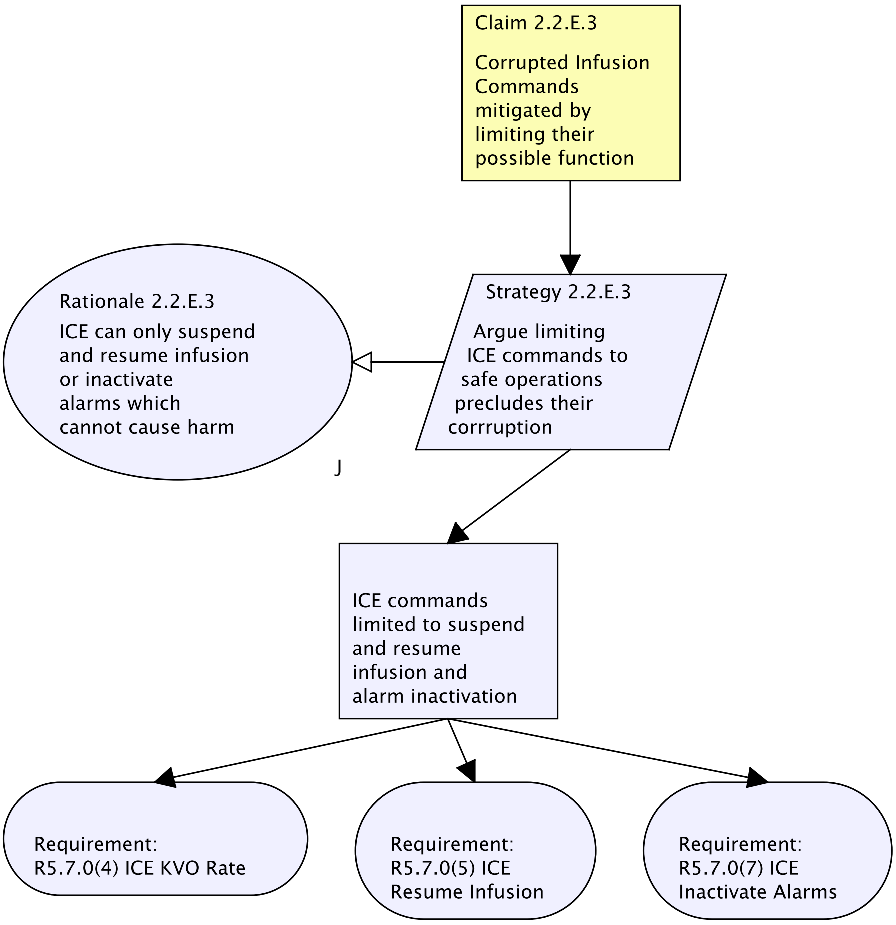
Repository: NOR-STA SVN PCAPAC - NOR-STA

No dynamic libraries are used so cannot be incorrect

Can't reference the absence of something

Repository: NOR-STA SVN PCAPAC - NOR-STA

76. Claim 2.2.E.3: Corrupted Infusion Commands mitigated by limiting their possible function


Claim 2.2.E.3
Corrupted Infusion Commands mitigated by limiting their possible function
Strategy 2.2.E.3
Argue limiting ICE commands to safe operations precludes their corrruption
Rationale 2.2.E.3
ICE can only suspend and resume infusion or inactivate alarms which cannot cause harm
J
ICE commands limited to suspend and resume infusion and alarm inactivation
Requirement: R5.7.0(4) ICE KVO Rate
Requirement: R5.7.0(5) ICE Resume Infusion
Requirement: R5.7.0(7) ICE Inactivate Alarms

Claim 2.2.E.3: Corrupted Infusion Commands mitigated by limiting their possible function

Strategy 2.2.E.3: Argue limiting ICE commands to safe operations precludes their corrruption

Rationale 2.2.E.3: ICE can only suspend and resume infusion or inactivate alarms which cannot cause harm

ICE commands limited to suspend and resume infusion and alarm inactivation

Requirement: R5.7.0(4) ICE KVO Rate

Evidence: ICE-PCArequirements.pdf#nameddest=cICE KVO rate

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R5.7.0(5) ICE Resume Infusion

Evidence: ICE-PCArequirements.pdf#nameddest=ICE resume infusion

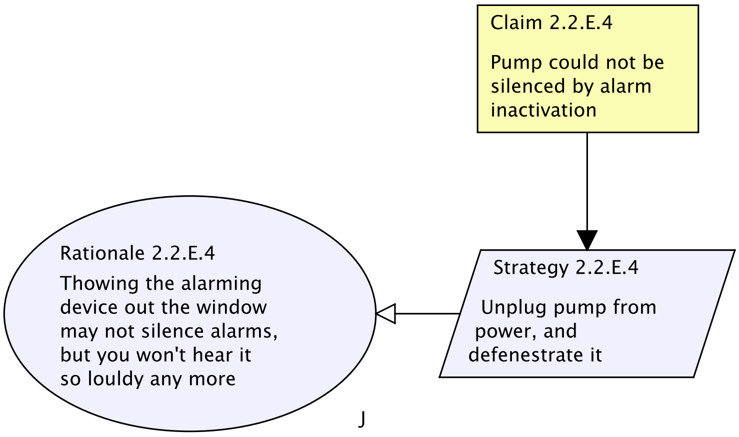
Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement: R5.7.0(7) ICE Inactivate Alarms

Evidence: ICE-PCArequirements.pdf#nameddest=ICE inactivate alarms

Repository: NOR-STA SVN PCAPAC - NOR-STA

77. Claim 2.2.E.4: Pump could not be silenced by alarm inactivation

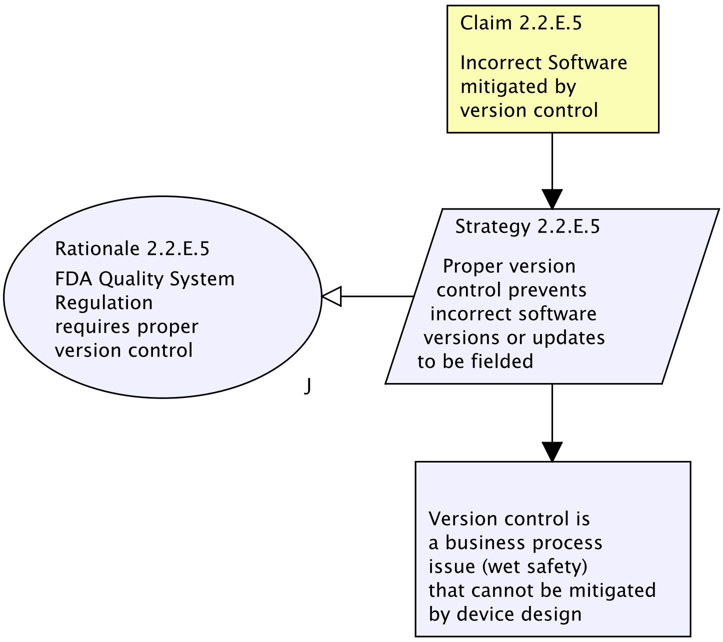

Claim 2.2.E.4
Pump could not be silenced by alarm inactivation
Strategy 2.2.E.4
Unplug pump from power, and defenestrate it
Rationale 2.2.E.4
Thowing the alarming device out the window may not silence alarms, but you won't hear it so louldy any more
J

Claim 2.2.E.4: Pump could not be silenced by alarm inactivation

Strategy 2.2.E.4: Unplug pump from power, and defenestrate it

Rationale 2.2.E.4: Thowing the alarming device out the window may not silence alarms, but you won't hear it so louldy any more

78. Claim 2.2.E.5: Incorrect Software mitigated by version control


Claim 2.2.E.5
Incorrect Software mitigated by version control
Strategy 2.2.E.5
Proper version control prevents incorrect software versions or updates to be fielded
Rationale 2.2.E.5
FDA Quality System Regulation requires proper version control
J
Version control is a business process issue (wet safety) that cannot be mitigated by device design

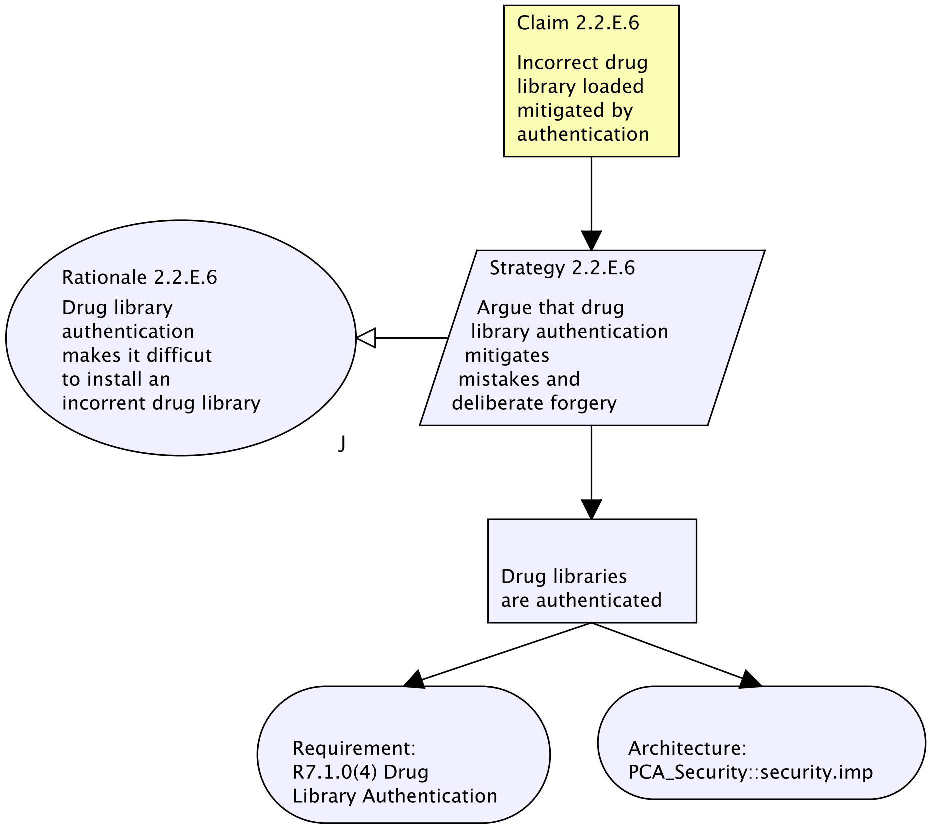
- **Claim 2.2.E.5: Incorrect Software mitigated by version control**

- **Strategy 2.2.E.5: Proper version control prevents incorrect software versions or updates to be fielded**

- **Rationale 2.2.E.5: FDA Quality System Regulation requires proper version control**

- **Version control is a business process issue (wet safety) that cannot be mitigated by device design**

79. Claim 2.2.E.6: Incorrect drug library loaded mitigated by authentication


Claim 2.2.E.6
Incorrect drug library loaded mitigated by authentication
Strategy 2.2.E.6
Argue that drug library authentication mitigates mistakes and deliberate forgery
Rationale 2.2.E.6
Drug library authentication makes it difficult to install an incorrent drug library
J
Drug libraries are authenticated
Requirement: R7.1.0(4) Drug Library Authentication
Architecture: PCA_Security::security.imp

Claim 2.2.E.6: Incorrect drug library loaded mitigated by authentication

Strategy 2.2.E.6: Argue that drug library authentication mitigates mistakes and deliberate forgery

Rationale 2.2.E.6: Drug library authentication makes it difficut to install an incorrent drug library

Drug libraries are authenticated

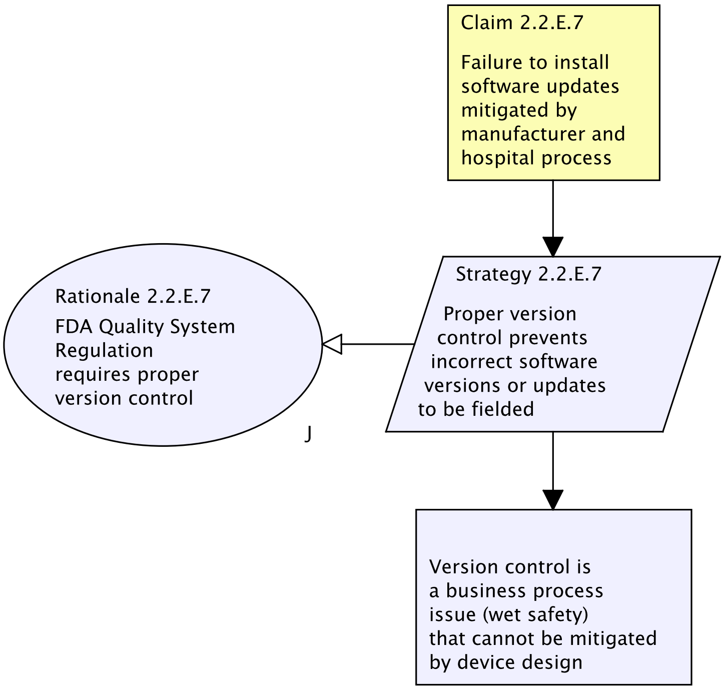
Requirement: R7.1.0(4) Drug Library Authentication

Evidence:	ICE-PCArequirements.pdf#nameddest=drug library authentication
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Security::security.imp

Evidence:	PCA_Security.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

80. Claim 2.2.E.7: Failure to install software updates mitigated by manufacturer and hospital process


Claim 2.2.E.7
Failure to install software updates mitigated by manufacturer and hospital process
Strategy 2.2.E.7
Proper version control prevents incorrect software versions or updates to be fielded
Rationale 2.2.E.7
FDA Quality System Regulation requires proper version control
J
Version control is a business process issue (wet safety) that cannot be mitigated by device design

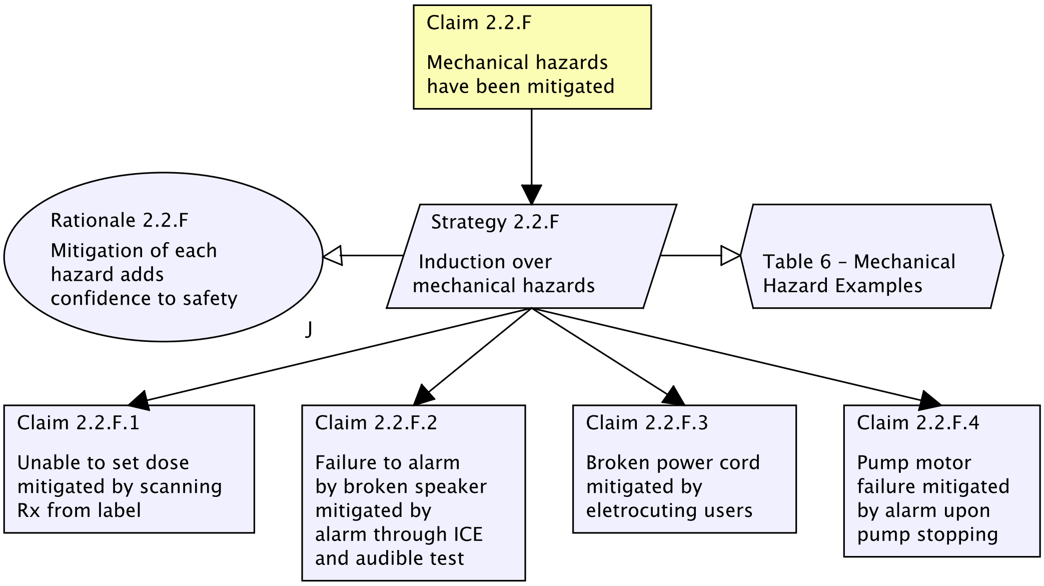
Claim 2.2.E.7: Failure to install software updates mitigated by manufacturer and hospital process

Strategy 2.2.E.7: Proper version control prevents incorrect software versions or updates to be fielded

Rationale 2.2.E.7: FDA Quality System Regulation requires proper version control

Version control is a business process issue (wet safety) that cannot be mitigated by device design

81. Claim 2.2.F: Mechanical hazards have been mitigated


Claim 2.2.F
Mechanical hazards have been mitigated
Rationale 2.2.F
Mitigation of each hazard adds confidence to safety
J
Strategy 2.2.F
Induction over mechanical hazards
Table 6 – Mechanical Hazard Examples
Claim 2.2.F.1
Unable to set dose mitigated by scanning Rx from label
Claim 2.2.F.2
Failure to alarm by broken speaker mitigated by alarm through ICE and audible test
Claim 2.2.F.3
Broken power cord mitigated by eletrocuting users
Claim 2.2.F.4
Pump motor failure mitigated by alarm upon pump stopping

Claim 2.2.F: Mechanical hazards have been mitigated

following Table F in guidance

Strategy 2.2.F: Induction over mechanical hazards

Rationale 2.2.F: Mitigation of each hazard adds confidence to safety

Table 6 – Mechanical Hazard Examples

See details in section 82

Claim 2.2.F.1: Unable to set dose mitigated by scanning Rx from label

See details in section 83

Claim 2.2.F.2: Failure to alarm by broken speaker mitigated by alarm through ICE and audible test

See details in section 84

Claim 2.2.F.3: Broken power cord mitigated by eletrocuting users

See details in section 85

Claim 2.2.F.4: Pump motor failure mitigated by alarm upon pump stopping

See details in section 86

82. Table 6 – Mechanical Hazard Examples

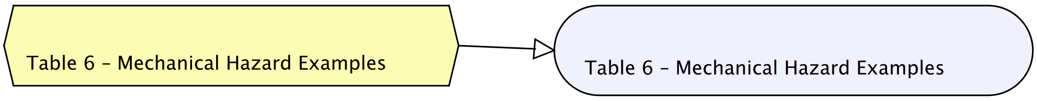


Table 6 – Mechanical Hazard Examples
Table 6 – Mechanical Hazard Examples

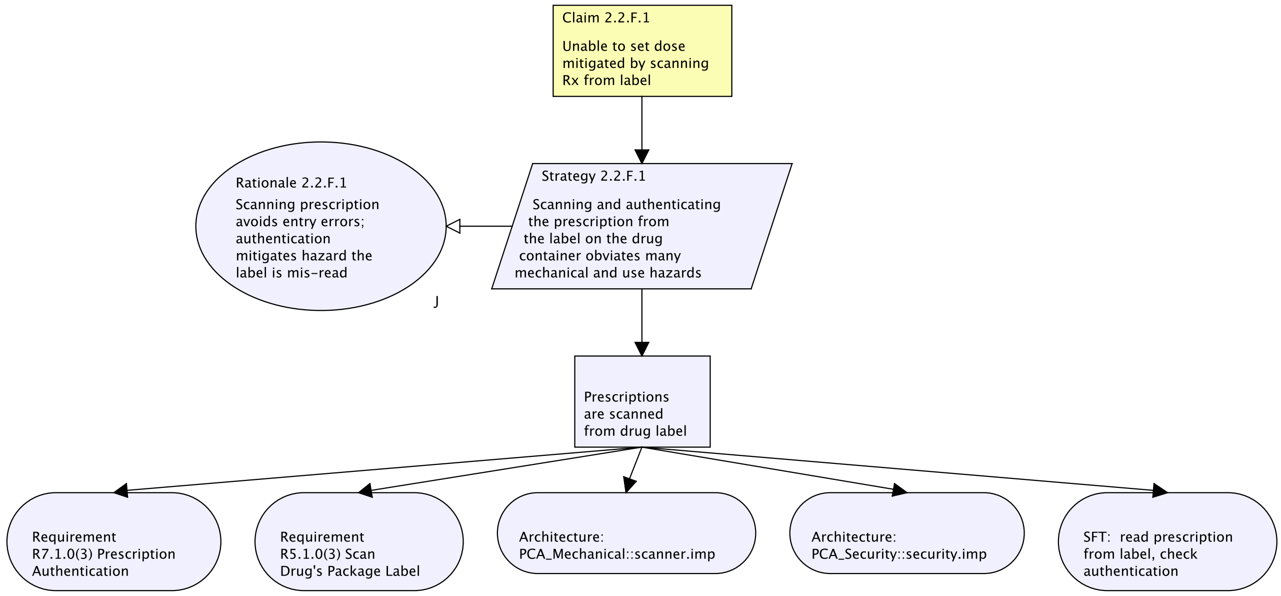
Table 6 – Mechanical Hazard Examples

Table 6 – Mechanical Hazard Examples

Evidence: IPGenera Guidance.pdf#page=12

Repository: NOR-STA SVN PCAPAC - NOR-STA

83. Claim 2.2.F.1: Unable to set dose mitigated by scanning Rx from label


Claim 2.2.F.1
Unable to set dose mitigated by scanning Rx from label
Rationale 2.2.F.1
Scanning prescription avoids entry errors; authentication mitigates hazard the label is mis-read
J
Strategy 2.2.F.1
Scanning and authenticating the prescription from the label on the drug container obviates many mechanical and use hazards
Prescriptions are scanned from drug label
Requirement R7.1.0(3) Prescription Authentication
Requirement R5.1.0(3) Scan Drug's Package Label
Architecture: PCA_Mechanical::scanner.imp
Architecture: PCA_Security::security.imp
SFT: read prescription from label, check authentication

Claim 2.2.F.1: Unable to set dose mitigated by scanning Rx from label

Strategy 2.2.F.1: Scanning and authenticating the prescription from the label on the drug container obviates many mechanical and use hazards

Rationale 2.2.F.1: Scanning prescription avoids entry errors; authentication mitigates hazard the label is mis-read

Prescriptions are scanned from drug label

Requirement R7.1.0(3) Prescription Authentication

Evidence: ICE-PCArequirements.pdf#nameddest=prescription authentication

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.1.0(3) Scan Drug's Package Label

Evidence: ICE-PCArequirements.pdf#nameddest=drug's package label

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Mechanical::scanner.imp

Evidence: PCA_Mechanical.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Security::security.imp

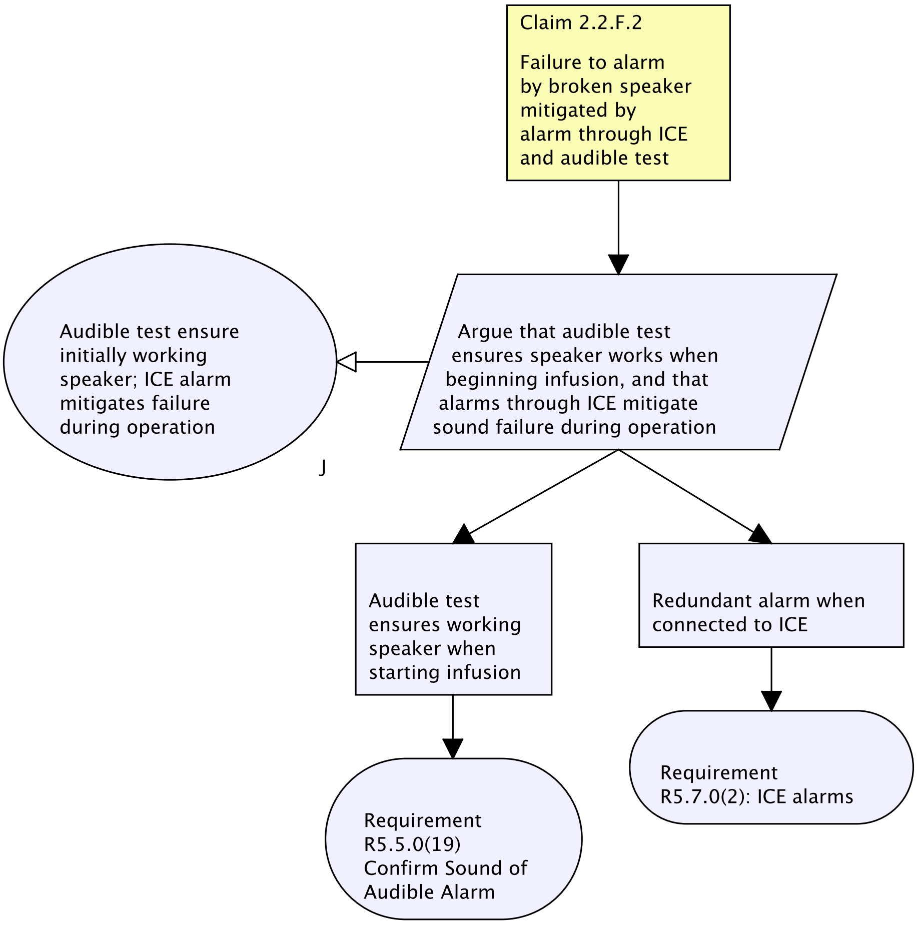
Evidence: PCA_Security.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: read prescription from label, check authentication

Repository: NOR-STA SVN PCAPAC - NOR-STA

84. Claim 2.2.F.2: Failure to alarm by broken speaker mitigated by alarm through ICE and audible test


Claim 2.2.F.2
Failure to alarm by broken speaker mitigated by alarm through ICE and audible test
Audible test ensure initially working speaker; ICE alarm mitigates failure during operation
J
Argue that audible test ensures speaker works when beginning infusion, and that alarms through ICE mitigate sound failure during operation
Audible test ensures working speaker when starting infusion
Redundant alarm when connected to ICE
Requirement R5.5.0(19) Confirm Sound of Audible Alarm
Requirement R5.7.0(2): ICE alarms

Claim 2.2.F.2: Failure to alarm by broken speaker mitigated by alarm through ICE and audible test

Argue that audible test ensures speaker works when beginning infusion, and that alarms through ICE mitigate sound failure during operation

Audible test ensure initially working speaker; ICE alarm mitigates failure during operation

Audible test ensures working speaker when starting infusion

Requirement R5.5.0(19) Confirm Sound of Audible Alarm

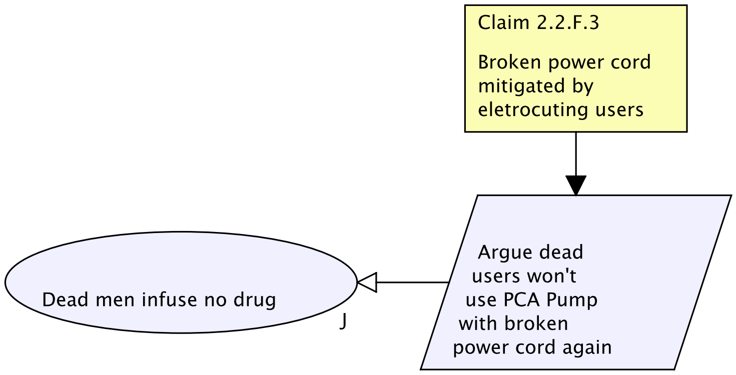
Evidence:	ICE-PCArequirements.pdf#nameddest=sound of audible alarm
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Redundant alarm when connected to ICE

Requirement R5.7.0(2): ICE alarms

Evidence:	ICE-PCArequirements.pdf#nameddest=ICE alarms
Repository:	NOR-STA SVN PCAPAC - NOR-STA

85. Claim 2.2.F.3: Broken power cord mitigated by eletrocuting users


Claim 2.2.F.3
Broken power cord mitigated by eletrocuting users
Argue dead users won't use PCA Pump with broken power cord again
Dead men infuse no drug
J

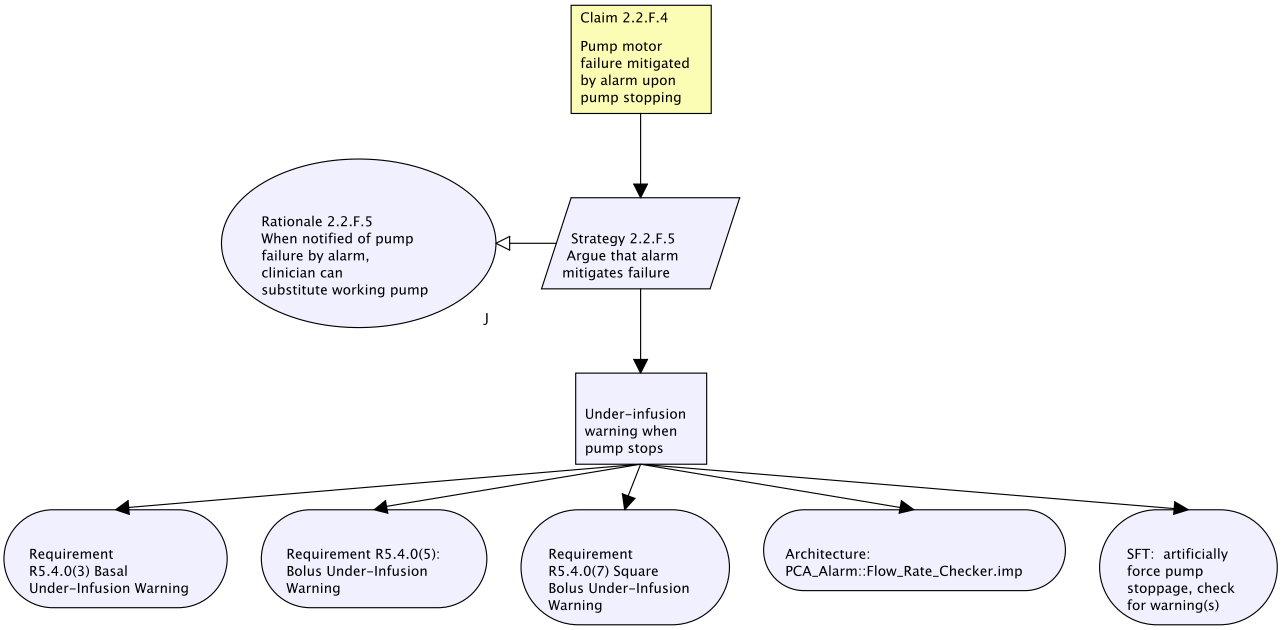
Claim 2.2.F.3: Broken power cord mitigated by eletrocuting users

Argue dead users won't use PCA Pump with broken power cord again

Yes, this is a joke.

Dead men infuse no drug

86. Claim 2.2.F.4: Pump motor failure mitigated by alarm upon pump stopping



Claim 2.2.F.4
Pump motor failure mitigated by alarm upon pump stopping
Rationale 2.2.F.5 When notified of pump failure by alarm, clinician can substitute working pump
J
Strategy 2.2.F.5 Argue that alarm mitigates failure
Under-infusion warning when pump stops
Requirement R5.4.0(3) Basal Under-Infusion Warning
Requirement R5.4.0(5): Bolus Under-Infusion Warning
Requirement R5.4.0(7) Square Bolus Under-Infusion Warning
Architecture: PCA_Alarm::Flow_Rate_Checker.imp
SFT: artificially force pump stoppage, check for warning(s)

Claim 2.2.F.4: Pump motor failure mitigated by alarm upon pump stopping

Strategy 2.2.F.5 Argue that alarm mitigates failure

Rationale 2.2.F.5 When notified of pump failure by alarm, clinician can substitute working pump

Under-infusion warning when pump stops

Requirement R5.4.0(3) Basal Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=basal under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(5): Bolus Under-Infusion Warning

Evidence: ICE-PCArequirements.pdf#nameddest=bolus under-infusion warning

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.0(7) Square Bolus Under-Infusion Warning

Evidence:	ICE-PCArequirements.pdf#nameddest=square bolus under-infusion warning
Repository:	NOR-STA SVN PCAPAC - NOR-STA

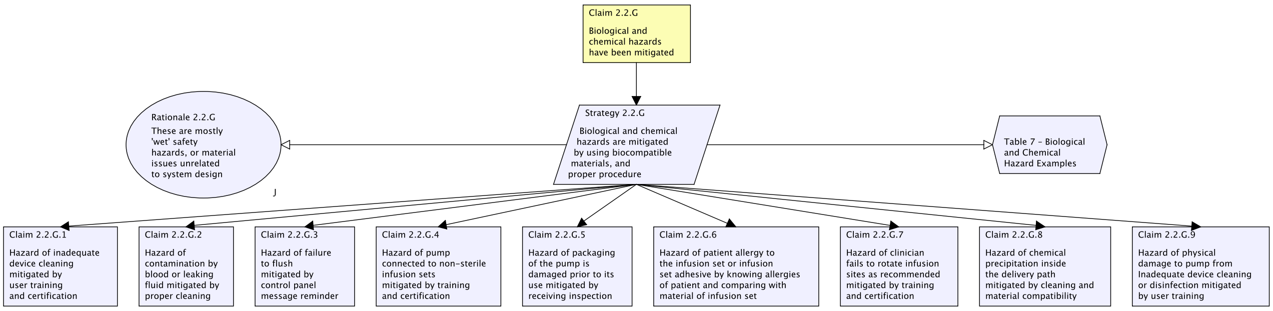
Architecture: PCA_Alarm::Flow_Rate_Checker.imp

Evidence:	PCA_Alarm.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

SFT: artificially force pump stoppage, check for warning(s)

Repository:	NOR-STA SVN PCAPAC - NOR-STA

87. Claim 2.2.G: Biological and chemical hazards have been mitigated


Claim 2.2.G
Biological and chemical hazards have been mitigated
Rationale 2.2.G
These are mostly 'wet' safety hazards, or material issues unrelated to system design
J
Strategy 2.2.G
Biological and chemical hazards are mitigated by using biocompatible materials, and proper procedure
Table 7 – Biological and Chemical Hazard Examples
Claim 2.2.G.1
Hazard of inadequate device cleaning mitigated by user training and certification
Claim 2.2.G.2
Hazard of contamination by blood or leaking fluid mitigated by proper cleaning
Claim 2.2.G.3
Hazard of failure to flush mitigated by control panel message reminder
Claim 2.2.G.4
Hazard of pump connected to non-sterile infusion sets mitigated by training and certification
Claim 2.2.G.5
Hazard of packaging of the pump is damaged prior to its use mitigated by receiving inspection
Claim 2.2.G.6
Hazard of patient allergy to the infusion set or infusion set adhesive by knowing allergies of patient and comparing with material of infusion set
Claim 2.2.G.7
Hazard of clinician fails to rotate infusion sites as recommended mitigated by training and certification
Claim 2.2.G.8
Hazard of chemical precipitation inside the delivery path mitigated by cleaning and material compatibility
Claim 2.2.G.9
Hazard of physical damage to pump from Inadequate device cleaning or disinfection mitigated by user training

Claim 2.2.G: Biological and chemical hazards have been mitigated

following Table G in guidance

Strategy 2.2.G: Biological and chemical hazards are mitigated by using biocompatible materials, and proper procedure

Rationale 2.2.G: These are mostly 'wet' safety hazards, or material issues unrelated to system design

Wet safety hazards arise from human misuse of the product, few of which can be mitigated by dry safety features. Therefore, mitigation of many misuse hazards can only be procedural, addressed by clinician training and restriction to authenticated users.

The exception is reminding to flush, and adapt priming functionality to do something similar with cleaning fluid after use.

Table 7 – Biological and Chemical Hazard Examples

See details in section 88

Claim 2.2.G.1: Hazard of inadequate device cleaning mitigated by user training and certification

Claim 2.2.G.2: Hazard of contamination by blood or leaking fluid mitigated by proper cleaning

Claim 2.2.G.3: Hazard of failure to flush mitigated by control panel message reminder

Claim 2.2.G.4: Hazard of pump connected to non-sterile infusion sets mitigated by training and certification

Claim 2.2.G.5: Hazard of packaging of the pump is damaged prior to its use mitigated by receiving inspection

Claim 2.2.G.6: Hazard of patient allergy to the infusion set or infusion set adhesive by knowing allergies of patient and comparing with material of infusion set

Claim 2.2.G.7: Hazard of clinician fails to rotate infusion sites as recommended mitigated by training and certification

Claim 2.2.G.8: Hazard of chemical precipitation inside the delivery path mitigated by cleaning and material compatibility

Claim 2.2.G.9: Hazard of physical damage to pump from Inadequate device cleaning or disinfection mitigated by user training

88. Table 7 – Biological and Chemical Hazard Examples

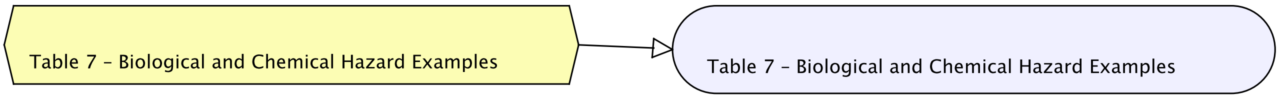


Table 7 – Biological and Chemical Hazard Examples
Table 7 – Biological and Chemical Hazard Examples

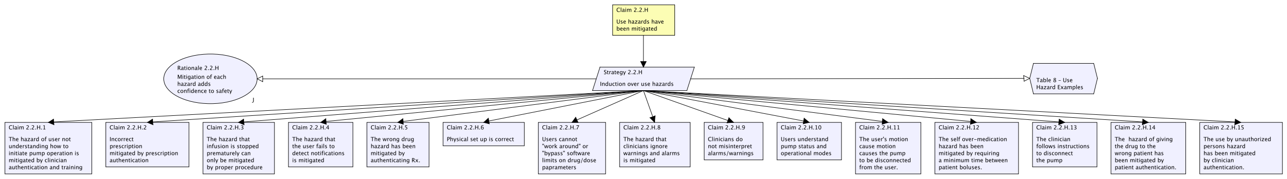
Table 7 – Biological and Chemical Hazard Examples

Table 7 – Biological and Chemical Hazard Examples

Evidence: IPGenera Guidance.pdf#page=20

Repository: NOR-STA SVN PCAPAC - NOR-STA

89. Claim 2.2.H: Use hazards have been mitigated


Claim 2.2.H
Use hazards have been mitigated
Strategy 2.2.H
Induction over use hazards
Rationale 2.2.H
Mitigation of each hazard adds confidence to safety
J
Table 8 – Use Hazard Examples
Claim 2.2.H.1
The hazard of user not understanding how to initiate pump operation is mitigated by clinician authentication and training
Claim 2.2.H.2
Incorrect prescription mitigated by prescription authentication
Claim 2.2.H.3
The hazard that infusion is stopped prematurely can only be mitigated by proper procedure
Claim 2.2.H.4
The hazard that the user fails to detect notifications is mitigated
Claim 2.2.H.5
The wrong drug hazard has been mitigated by authenticating Rx.
Claim 2.2.H.6
Physical set up is correct
Claim 2.2.H.7
Users cannot "work around" or "bypass" software limits on drug/dose papremeters
Claim 2.2.H.8
The hazard that clinicians ignore warnings and alarms is mitigated
Claim 2.2.H.9
Clinicians do not misinterpret alarms/warnings
Claim 2.2.H.10
Users understand pump status and operational modes
Claim 2.2.H.11
The user's motion cause motion causes the pump to be disconnected from the user.
Claim 2.2.H.12
The self over-medication hazard has been mitigated by requiring a minimum time between patient boluses.
Claim 2.2.H.13
The clinician follows instructions to disconnect the pump
Claim 2.2.H.14
The hazard of giving the drug to the wrong patient has been mitigated by patient authentication.
Claim 2.2.H.15
The use by unauthorized persons hazard has been mitigated by clinician authentication.

Claim 2.2.H: Use hazards have been mitigated

following Table H in FDA guidance

Strategy 2.2.H: Induction over use hazards

Rationale 2.2.H: Mitigation of each hazard adds confidence to safety

Table 8 – Use Hazard Examples

See details in section 90

Claim 2.2.H.1: The hazard of user not understanding how to initiate pump operation is mitigated by clinician authentication and training

See details in section 91

Claim 2.2.H.2: Incorrect prescription mitigated by prescription authentication

See details in section 92

Claim 2.2.H.3: The hazard that infusion is stopped prematurely can only be mitigated by proper procedure

See details in section 93

Claim 2.2.H.4: The hazard that the user fails to detect notifications is mitigated

See details in section 94

Claim 2.2.H.5: The wrong drug hazard has been mitigated by authenticating Rx.

See details in section 97

Claim 2.2.H.6: Physical set up is correct

See details in section 98

Claim 2.2.H.7: Users cannot "work around" or "bypass" software limits on drug/dose paprameters

See details in section 99

Claim 2.2.H.8: The hazard that clinicians ignore warnings and alarms is mitigated

See details in section 100

Claim 2.2.H.9: Clinicians do not misinterpret alarms/warnings

See details in section 102

Claim 2.2.H.10: Users understand pump status and operational modes

See details in section 105

Claim 2.2.H.11: The user's motion cause motion causes the pump to be disconnected from the user.

This is a 'wet' safety hazard that pump design can do nothing about

Claim 2.2.H.12: The self over-medication hazard has been mitigated by requiring a minimum time between patient boluses.

See details in section 106

Claim 2.2.H.13: The clinician follows instructions to disconnect the pump

See details in section 107

Claim 2.2.H.14: The hazard of giving the drug to the wrong patient has been mitigated by patient authentication.

See details in section 108

💬 Claim 2.2.H.15: The use by unauthorized persons hazard has been mitigated by clinician authentication.

See details in section 109

90. Table 8 – Use Hazard Examples

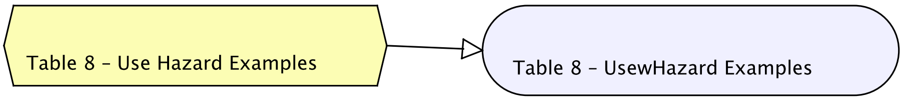


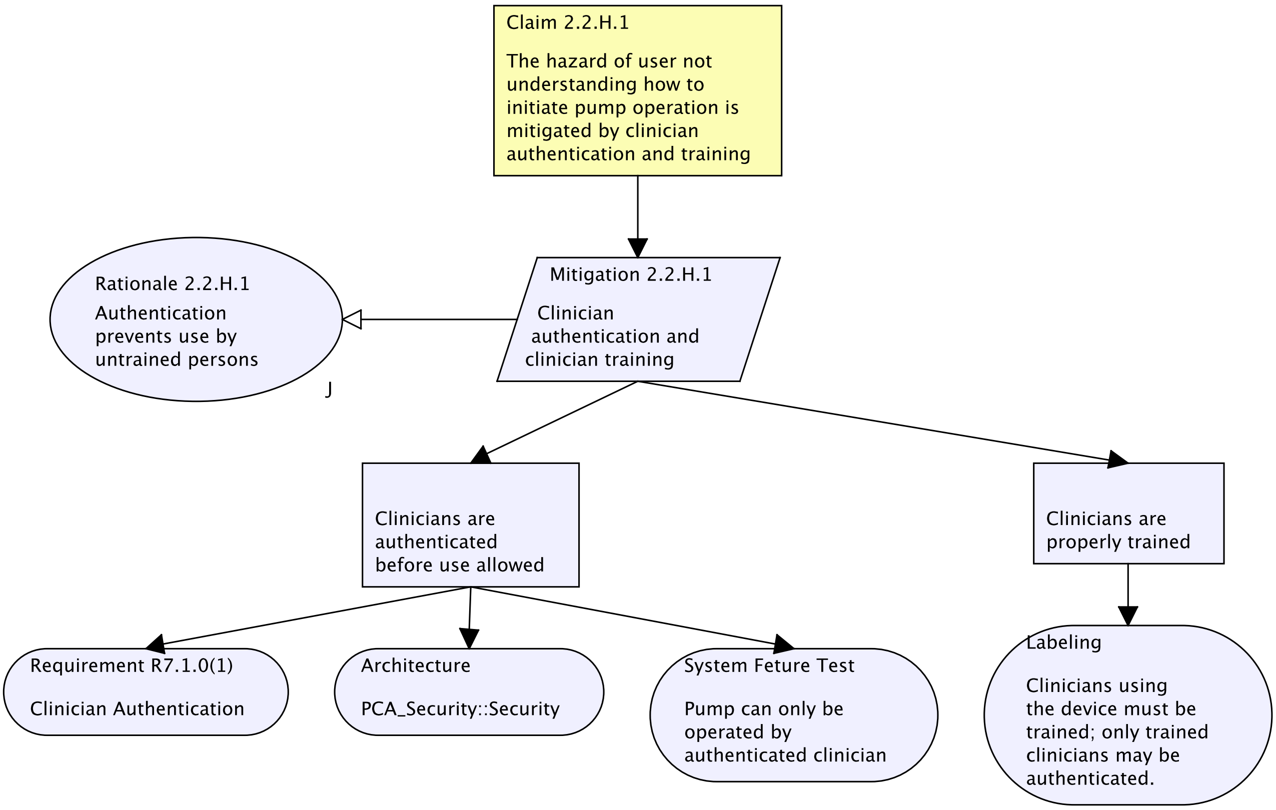
Table 8 – Use Hazard Examples

Table 8 – UsewHazard Examples

Evidence: IPGenera Guidance.pdf#page=22

Repository: NOR-STA SVN PCAPAC - NOR-STA

91. Claim 2.2.H.1: The hazard of user not understanding how to initiate pump operation is mitigated by clinician authentication and training



Claim 2.2.H.1
The hazard of user not understanding how to initiate pump operation is mitigated by clinician authentication and training
Rationale 2.2.H.1
Authentication prevents use by untrained persons
J
Mitigation 2.2.H.1
Clinician authentication and clinician training
Clinicians are authenticated before use allowed
Clinicians are properly trained
Requirement R7.1.0(1)
Clinician Authentication
Architecture
PCA_Security::Security
System Feture Test
Pump can only be operated by authenticated clinician
Labeling
Clinicians using the device must be trained; only trained clinicians may be authenticated.

Claim 2.2.H.1: The hazard of user not understanding how to initiate pump operation is mitigated by clinician authentication and training

Mitigation 2.2.H.1: Clinician authentication and clinician training

Rationale 2.2.H.1: Authentication prevents use by untrained persons

Clinicians are authenticated before use allowed

Requirement R7.1.0(1): Clinician Authentication

Evidence:	ICE-PCArequirements.pdf#nameddest=clinician authentication
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Security::Security

Evidence: PCA_Security.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

System Feture Test: Pump can only be operated by authenticated clinician

Repository: NOR-STA SVN PCAPAC - NOR-STA

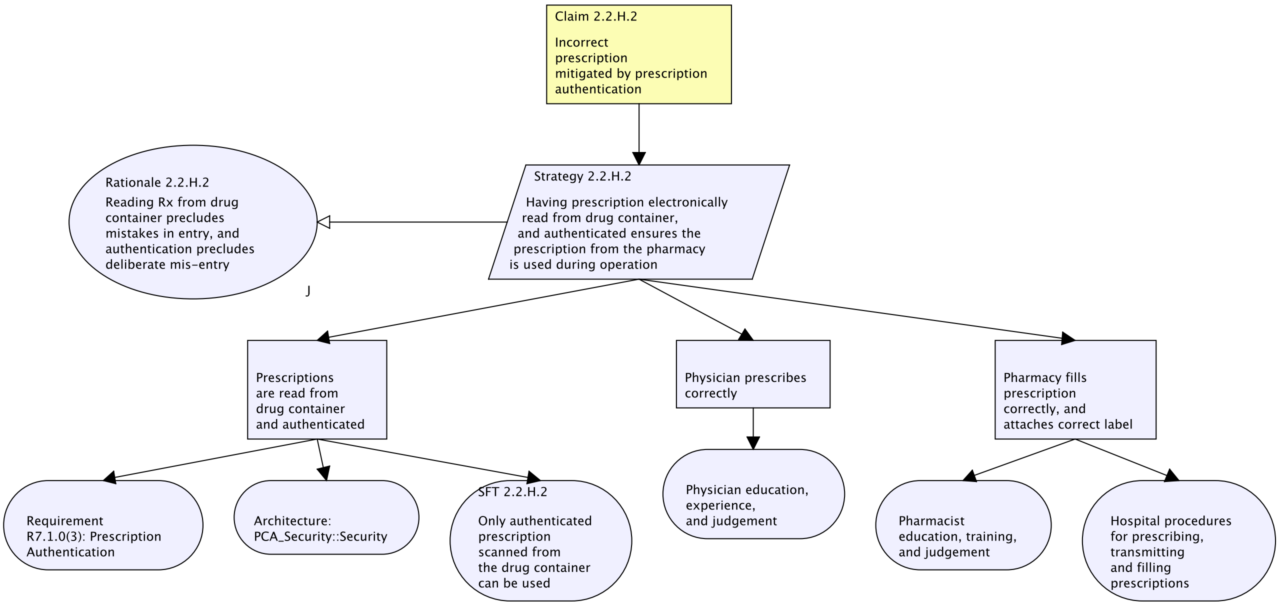
Clinicians are properly trained

Labeling: Clinicians using the device must be trained; only trained clinicians may be authenticated.

Evidence: ICE-PCArequirements.pdf#nameddest=labeling

Repository: NOR-STA SVN PCAPAC - NOR-STA

92. Claim 2.2.H.2: Incorrect prescription mitigated by prescription authentication


Claim 2.2.H.2
Incorrect prescription mitigated by prescription authentication
Rationale 2.2.H.2
Reading Rx from drug container precludes mistakes in entry, and authentication precludes deliberate mis-entry
J
Strategy 2.2.H.2
Having prescription electronically read from drug container, and authenticated ensures the prescription from the pharmacy is used during operation
Prescriptions are read from drug container and authenticated
Physician prescribes correctly
Pharmacy fills prescription correctly, and attaches correct label
Requirement R7.1.0(3): Prescription Authentication
Architecture: PCA_Security::Security
SFT 2.2.H.2
Only authenticated prescription scanned from the drug container can be used
Physician education, experience, and judgement
Pharmacist education, training, and judgement
Hospital procedures for prescribing, transmitting and filling prescriptions

Claim 2.2.H.2: Incorrect prescription mitigated by prescription authentication

Strategy 2.2.H.2: Having prescription electronically read from drug container, and authenticated ensures the prescription from the pharmacy is used during operation

Rationale 2.2.H.2: Reading Rx from drug container precludes mistakes in entry, and authentication precludes deliberate mis-entry

Prescriptions are read from drug container and authenticated

Requirement R7.1.0(3): Prescription Authentication

Evidence: ICE-PCArequirements.pdf#nameddest=prescription authentication

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Security::Security

Evidence: PCA_Security.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT 2.2.H.2: Only authenticated prescription scanned from the drug container can be used

Repository: NOR-STA SVN PCAPAC - NOR-STA

Physician prescribes correctly

Physician education, experience, and judgement

Repository: NOR-STA SVN PCAPAC - NOR-STA

Pharmacy fills prescription correctly, and attaches correct label

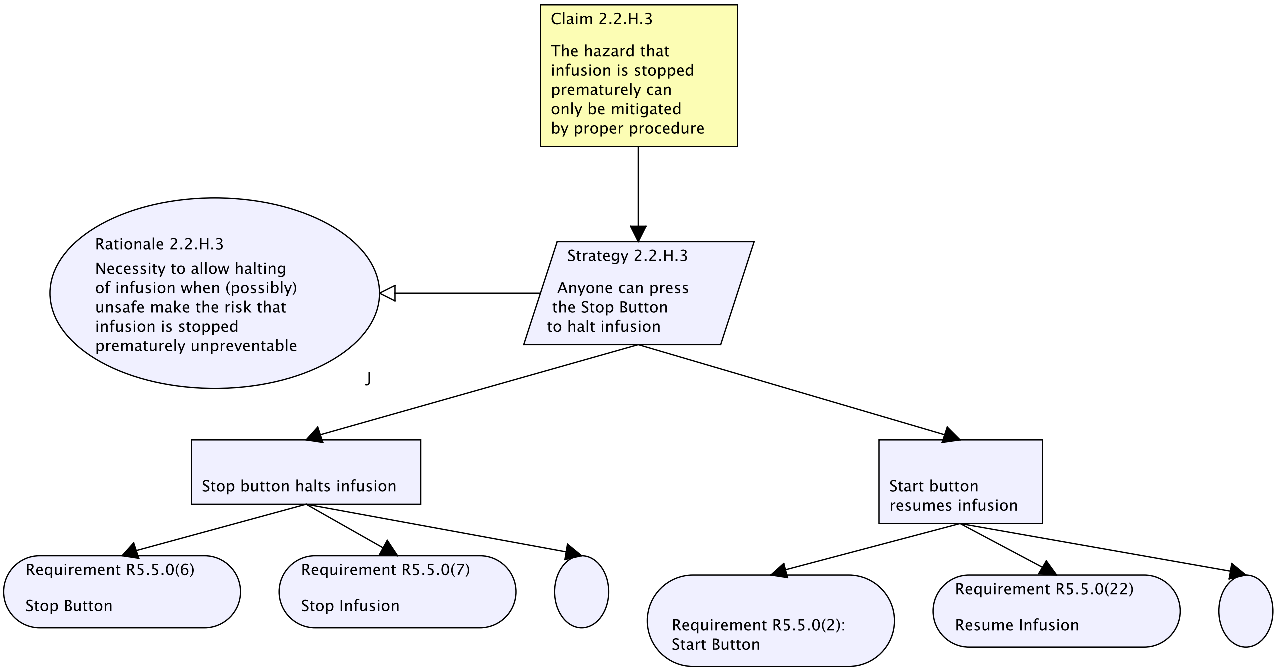
Pharmacist education, training, and judgement

Repository: NOR-STA SVN PCAPAC - NOR-STA

Hospital procedures for prescribing, transmitting and filling prescriptions

Repository: NOR-STA SVN PCAPAC - NOR-STA

93. Claim 2.2.H.3: The hazard that infusion is stopped prematurely can only be mitigated by proper procedure


Claim 2.2.H.3
The hazard that infusion is stopped prematurely can only be mitigated by proper procedure
Rationale 2.2.H.3
Necessity to allow halting of infusion when (possibly) unsafe make the risk that infusion is stopped prematurely unpreventable
J
Strategy 2.2.H.3
Anyone can press the Stop Button to halt infusion
Stop button halts infusion
Start button resumes infusion
Requirement R5.5.0(6)
Stop Button
Requirement R5.5.0(7)
Stop Infusion
Requirement R5.5.0(2): Start Button
Requirement R5.5.0(22)
Resume Infusion

Claim 2.2.H.3: The hazard that infusion is stopped prematurely can only be mitigated by proper procedure

Strategy 2.2.H.3: Anyone can press the Stop Button to halt infusion

Rationale 2.2.H.3: Necessity to allow halting of infusion when (possibly) unsafe make the risk that infusion is stopped prematurely unpreventable

Stop button halts infusion

Requirement R5.5.0(6): Stop Button

Evidence: ICE-PCArequirements.pdf#nameddest=stop button

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.5.0(7): Stop Infusion

Evidence: ICE-PCArequirements.pdf#nameddest=stop infusion

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Control_Panel::ui_thread

Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Start button resumes infusion

Requirement R5.5.0(2): Start Button

Evidence: ICE-PCArequirements.pdf#nameddest=start button

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.5.0(22): Resume Infusion

Evidence: ICE-PCArequirements.pdf#nameddest=resume infusion

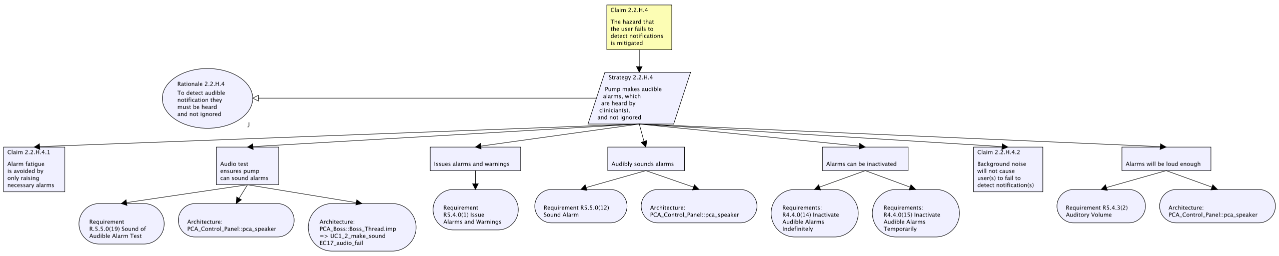
Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Control_Panel::ui_thread

Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

94. Claim 2.2.H.4: The hazard that the user fails to detect notifications is mitigated



Claim 2.2.H.4
The hazard that the user fails to detect notifications is mitigated
Strategy 2.2.H.4
Pump makes audible alarms, which are heard by clinician(s), and not ignored
Rationale 2.2.H.4
To detect audible notification they must be heard and not ignored
J
Claim 2.2.H.4.1
Alarm fatigue is avoided by only raising necessary alarms
Audio test ensures pump can sound alarms
Requirement R.5.5.0(19) Sound of Audible Alarm Test
Architecture: PCA_Control_Panel::pca_speaker
Architecture: PCA_Boss::Boss_Thread.imp => UC1_2_make_sound EC17_audio_fail
Issues alarms and warnings
Requirement R5.4.0(1) Issue Alarms and Warnings
Audibly sounds alarms
Requirement R5.5.0(12) Sound Alarm
Architecture: PCA_Control_Panel::pca_speaker
Alarms can be inactivated
Requirements: R4.4.0(14) Inactivate Audible Alarms Indefinitely
Requirements: R4.4.0(15) Inactivate Audible Alarms Temporarily
Claim 2.2.H.4.2
Background noise will not cause user(s) to fail to detect notification(s)
Alarms will be loud enough
Requirement R5.4.3(2) Auditory Volume
Architecture: PCA_Control_Panel::pca_speaker

Claim 2.2.H.4: The hazard that the user fails to detect notifications is mitigated

Strategy 2.2.H.4: Pump makes audible alarms, which are heard by clinician(s), and not ignored

Rationale 2.2.H.4: To detect audible notification they must be heard and not ignored

Claim 2.2.H.4.1: Alarm fatigue is avoided by only raising necessary alarms

See details in section 95

Audio test ensures pump can sound alarms

Requirement R.5.5.0(19) Sound of Audible Alarm Test

Evidence: ICE-PCArequirements.pdf#nameddest=sound of audible alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Control_Panel::pca_speaker

Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Boss::Boss_Thread.imp => UC1_2_make_sound EC17_audio_fail

Evidence: PCA_Boss.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Issues alarms and warnings

Requirement R5.4.0(1) Issue Alarms and Warnings

Evidence: ICE-PCArequirements.pdf#nameddest=issue alarms and warnings

Repository: NOR-STA SVN PCAPAC - NOR-STA

Audibly sounds alarms

Requirement R5.5.0(12) Sound Alarm

Evidence: ICE-PCArequirements.pdf#nameddest=sound alarm

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Control_Panel::pca_speaker

Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Alarms can be inactivated

Because alarms can be inactivated, they may not be heard.

Requirements: R4.4.0(14) Inactivate Audible Alarms Indefinitely

Evidence: ICE-PCArequirements.pdf#nameddest=inactivate audible alarms indefinitely

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirements: R4.4.0(15) Inactivate Audible Alarms Temporarily

Evidence: ICE-PCArequirements.pdf#nameddest=inactivate audible alarms temporarily

Repository: NOR-STA SVN PCAPAC - NOR-STA

Claim 2.2.H.4.2: Background noise will not cause user(s) to fail to detect notification(s)

See details in section 96

Alarms will be loud enough

Requirement R5.4.3(2) Auditory Volume

Evidence: ICE-PCArequirements.pdf#nameddest=auditory volume

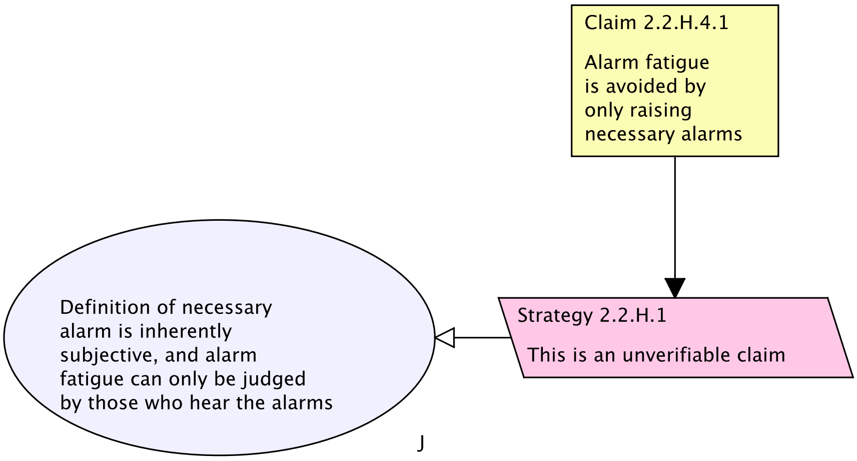
Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Control_Panel::pca_speaker

Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

95. Claim 2.2.H.4.1: Alarm fatigue is avoided by only raising necessary alarms

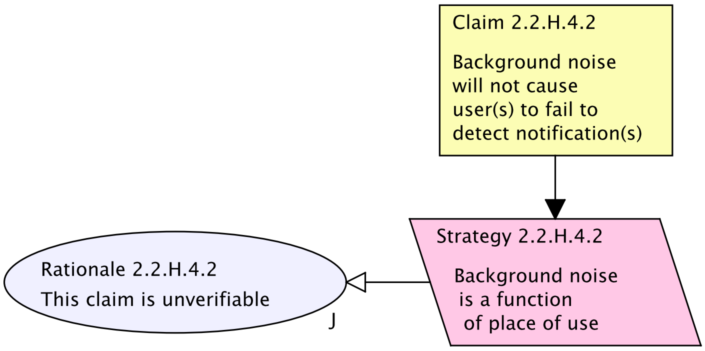

Claim 2.2.H.4.1
Alarm fatigue is avoided by only raising necessary alarms
Strategy 2.2.H.1
This is an unverifiable claim
Definition of necessary alarm is inherently subjective, and alarm fatigue can only be judged by those who hear the alarms
J

Claim 2.2.H.4.1: Alarm fatigue is avoided by only raising necessary alarms

Strategy 2.2.H.1: This is an unverifiable claim

Definition of necessary alarm is inherently subjective, and alarm fatigue can only be judged by those who hear the alarms

96. Claim 2.2.H.4.2: Background noise will not cause user(s) to fail to detect notification(s)

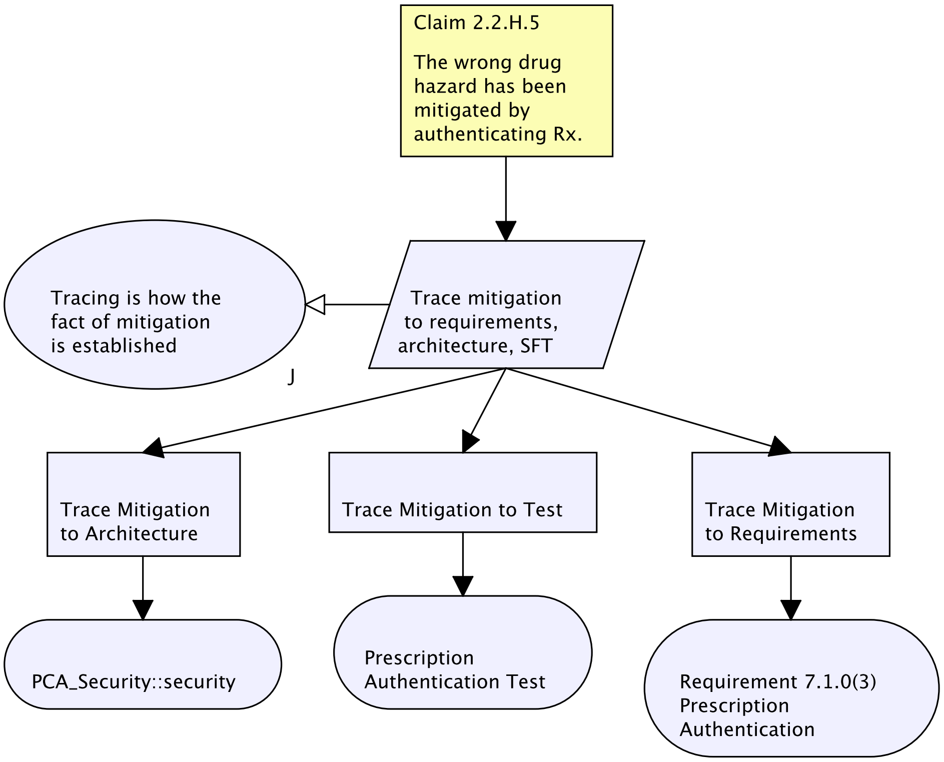

Claim 2.2.H.4.2
Background noise will not cause user(s) to fail to detect notification(s)
Strategy 2.2.H.4.2
Background noise is a function of place of use
Rationale 2.2.H.4.2
This claim is unverifiable
J

Claim 2.2.H.4.2: Background noise will not cause user(s) to fail to detect notification(s)

Strategy 2.2.H.4.2: Background noise is a function of place of use

Rationale 2.2.H.4.2: This claim is unverifiable

97. Claim 2.2.H.5: The wrong drug hazard has been mitigated by authenticating Rx.


Claim 2.2.H.5
The wrong drug hazard has been mitigated by authenticating Rx.
Tracing is how the fact of mitigation is established
J
Trace mitigation to requirements, architecture, SFT
Trace Mitigation to Architecture
Trace Mitigation to Test
Trace Mitigation to Requirements
PCA_Security::security
Prescription Authentication Test
Requirement 7.1.0(3) Prescription Authentication

Claim 2.2.H.5: The wrong drug hazard has been mitigated by authenticating Rx.

Trace mitigation to requirements, architecture, SFT

Tracing is how the fact of mitigation is established

Trace Mitigation to Architecture

PCA_Security::security

Evidence: PCA_Security.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace Mitigation to Test

Prescription Authentication Test

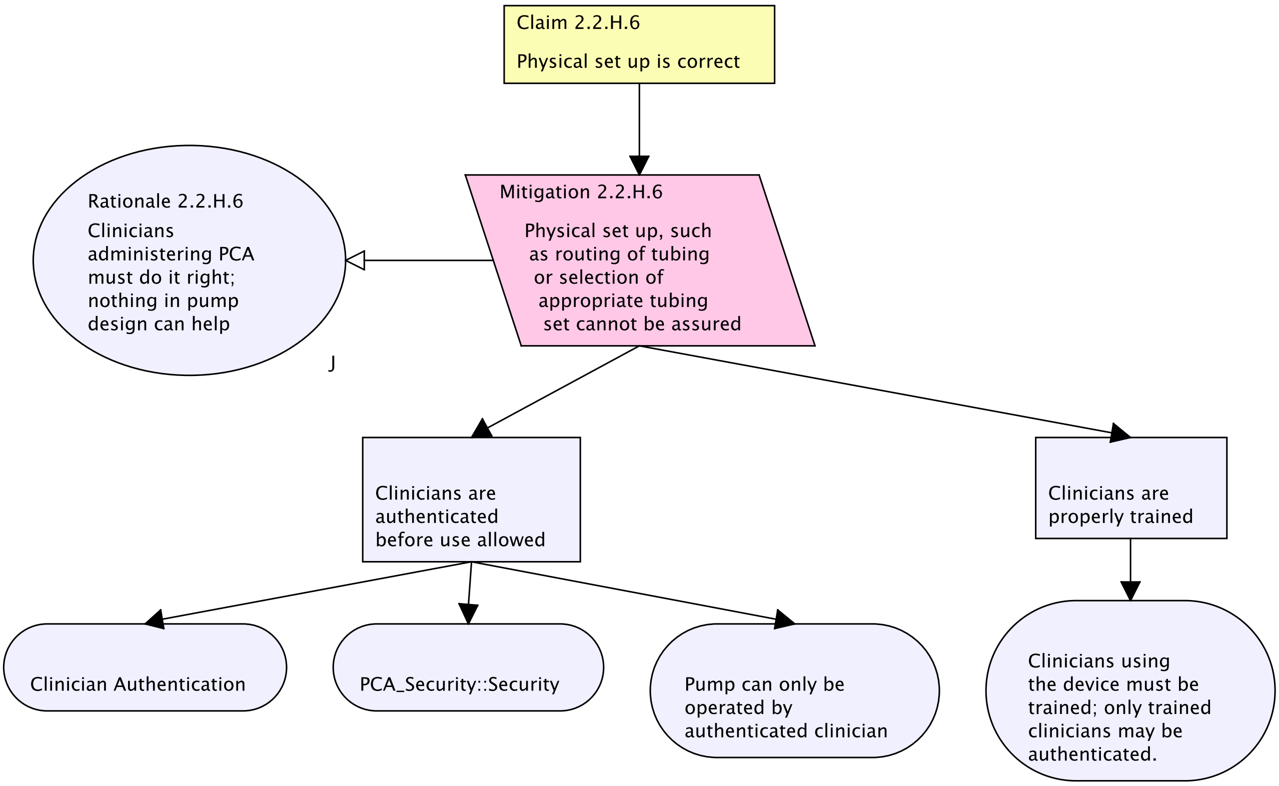
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Trace Mitigation to Requirements

Requirement 7.1.0(3) Prescription Authentication

Evidence:	ICE-PCArequirements.pdf#nameddest=prescription authentication
Repository:	NOR-STA SVN PCAPAC - NOR-STA

98. Claim 2.2.H.6: Physical set up is correct


Claim 2.2.H.6
Physical set up is correct
Mitigation 2.2.H.6
Physical set up, such as routing of tubing or selection of appropriate tubing set cannot be assured
Rationale 2.2.H.6
Clinicians administering PCA must do it right; nothing in pump design can help
J
Clinicians are authenticated before use allowed
Clinicians are properly trained
Clinician Authentication
PCA_Security::Security
Pump can only be operated by authenticated clinician
Clinicians using the device must be trained; only trained clinicians may be authenticated.

Claim 2.2.H.6: Physical set up is correct

Mitigation 2.2.H.6: Physical set up, such as routing of tubing or selection of appropriate tubing set cannot be assured

Rationale 2.2.H.6: Clinicians administering PCA must do it right; nothing in pump design can help

Clinicians are authenticated before use allowed

Clinician Authentication

Evidence: ICE-PCArequirements.pdf#nameddest=clinician authentication

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Security::Security

Evidence:	PCA_Security.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Pump can only be operated by authenticated clinician

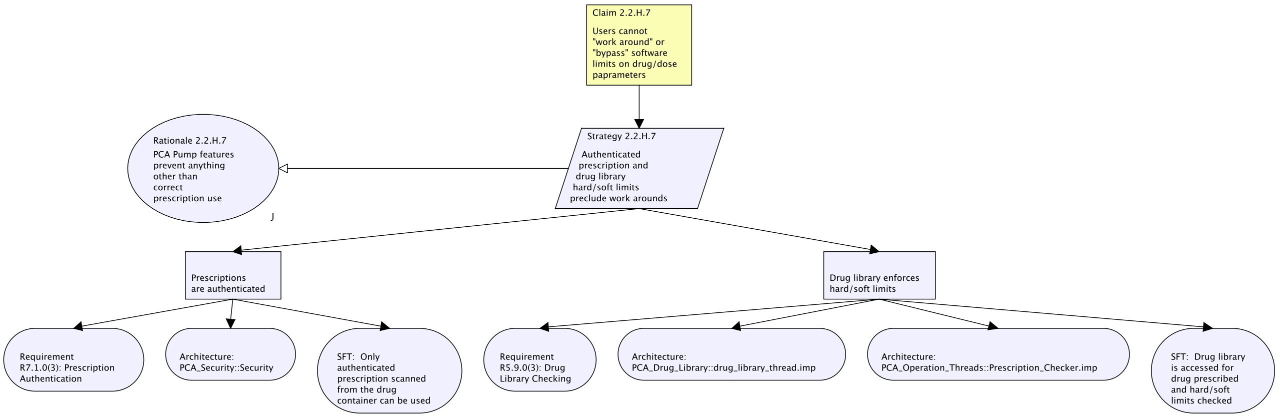
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Clinicians are properly trained

Clinicians using the device must be trained; only trained clinicians may be authenticated.

Evidence:	ICE-PCArequirements.pdf#nameddest=labeling
Repository:	NOR-STA SVN PCAPAC - NOR-STA

99. Claim 2.2.H.7: Users cannot "work around" or "bypass" software limits on drug/dose paprameters


Claim 2.2.H.7
Users cannot "work around" or "bypass" software limits on drug/dose paprameters
Rationale 2.2.H.7
PCA Pump features prevent anything other than correct prescription use
J
Strategy 2.2.H.7
Authenticated prescription and drug library hard/soft limits preclude work arounds
Prescriptions are authenticated
Drug library enforces hard/soft limits
Requirement R7.1.0(3): Prescription Authentication
Architecture: PCA_Security::Security
SFT: Only authenticated prescription scanned from the drug container can be used
Requirement R5.9.0(3): Drug Library Checking
Architecture: PCA_Drug_Library::drug_library_thread.imp
Architecture: PCA_Operation_Threads::Prescription_Checker.imp
SFT: Drug library is accessed for drug prescribed and hard/soft limits checked

Claim 2.2.H.7: Users cannot "work around" or "bypass" software limits on drug/dose paprameters

Strategy 2.2.H.7: Authenticated prescription and drug library hard/soft limits preclude work arounds

Rationale 2.2.H.7: PCA Pump features prevent anything other than correct prescription use

Prescriptions are authenticated

Requirement R7.1.0(3): Prescription Authentication

Evidence: ICE-PCArequirements.pdf#nameddest=prescription authentication

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Security::Security

Evidence: PCA_Security.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Only authenticated prescription scanned from the drug container can be used

Repository: NOR-STA SVN PCAPAC - NOR-STA

Drug library enforces hard/soft limits

Requirement R5.9.0(3): Drug Library Checking

Evidence: ICE-PCArequirements.pdf#nameddest=drug library checking

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Drug_Library::drug_library_thread.imp

Evidence: PCA_Drug_Library.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Operation_Threads::Prescription_Checker.imp

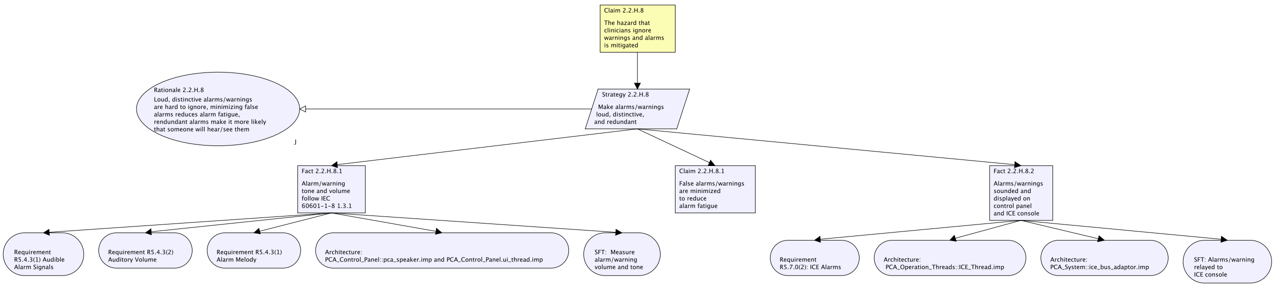
Evidence: PCA_Operation_Threads.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Drug library is accessed for drug prescribed and hard/soft limits checked

Repository: NOR-STA SVN PCAPAC - NOR-STA

100. Claim 2.2.H.8: The hazard that clinicians ignore warnings and alarms is mitigated


Claim 2.2.H.8
The hazard that clinicians ignore warnings and alarms is mitigated
Rationale 2.2.H.8
Loud, distinctive alarms/warnings are hard to ignore, minimizing false alarms reduces alarm fatigue, rendundant alarms make it more likely that someone will hear/see them
J
Strategy 2.2.H.8
Make alarms/warnings loud, distinctive, and redundant
Fact 2.2.H.8.1
Alarm/warning tone and volume follow IEC 60601-1-8 1.3.1
Claim 2.2.H.8.1
False alarms/warnings are minimized to reduce alarm fatigue
Fact 2.2.H.8.2
Alarms/warnings sounded and displayed on control panel and ICE console
Requirement R5.4.3(1) Audible Alarm Signals
Requirement R5.4.3(2) Auditory Volume
Requirement R5.4.3(1) Alarm Melody
Architecture: PCA_Control_Panel::pca_speaker.imp and PCA_Control_Panel.ui_thread.imp
SFT: Measure alarm/warning volume and tone
Requirement R5.7.0(2): ICE Alarms
Architecture: PCA_Operation_Threads::ICE_Thread.imp
Architecture: PCA_System::ice_bus_adaptor.imp
SFT: Alarms/warning relayed to ICE console

Claim 2.2.H.8: The hazard that clinicians ignore warnings and alarms is mitigated

Strategy 2.2.H.8: Make alarms/warnings loud, distinctive, and redundant

Rationale 2.2.H.8: Loud, distinctive alarms/warnings are hard to ignore, minimizing false alarms reduces alarm fatigue, rendundant alarms make it more likely that someone will hear/see them

Fact 2.2.H.8.1: Alarm/warning tone and volume follow IEC 60601-1-8 1.3.1

Requirement R5.4.3(1) Audible Alarm Signals

Evidence: ICE-PCArequirements.pdf#nameddest=audible alarms signals

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.3(2) Auditory Volume

Evidence: ICE-PCArequirements.pdf#nameddest=auditory volume

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.3(1) Alarm Melody

Evidence: ICE-PCArequirements.pdf#nameddest=alarm melody

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Control_Panel::pca_speaker.imp and PCA_Control_Panel.ui_thread.imp

Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Measure alarm/warning volume and tone

Repository: NOR-STA SVN PCAPAC - NOR-STA

Claim 2.2.H.8.1: False alarms/warnings are minimized to reduce alarm fatigue

See details in section 101

Fact 2.2.H.8.2: Alarms/warnings sounded and displayed on control panel and ICE console

Requirement R5.7.0(2): ICE Alarms

Evidence: ICE-PCArequirements.pdf#nameddest=ICE alarms

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Operation_Threads::ICE_Thread.imp

Evidence: PCA_Operation_Threads.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_System::ice_bus_adaptor.imp

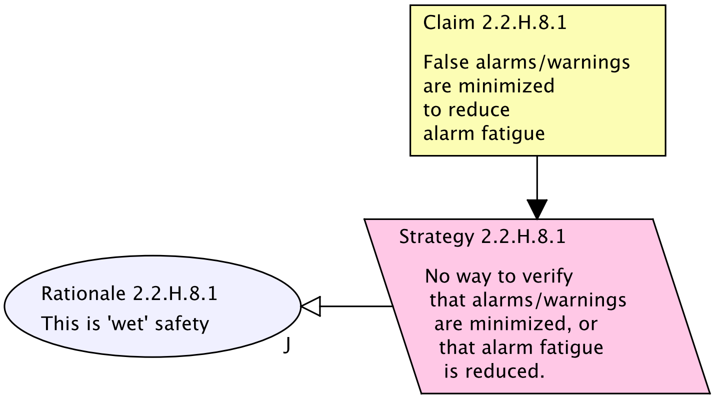
Evidence: PCA_System.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Alarms/warning relayed to ICE console

Repository: NOR-STA SVN PCAPAC - NOR-STA

101. Claim 2.2.H.8.1: False alarms/warnings are minimized to reduce alarm fatigue

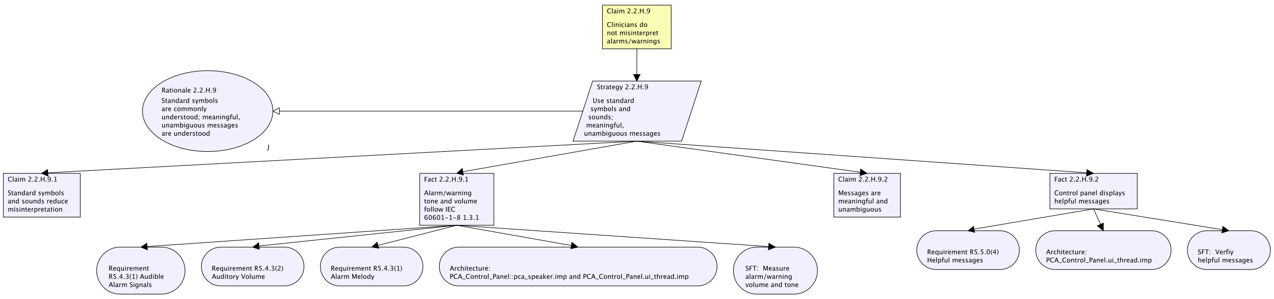

Claim 2.2.H.8.1
False alarms/warnings are minimized to reduce alarm fatigue
Strategy 2.2.H.8.1
No way to verify that alarms/warnings are minimized, or that alarm fatigue is reduced.
Rationale 2.2.H.8.1
This is 'wet' safety
J

Claim 2.2.H.8.1: False alarms/warnings are minimized to reduce alarm fatigue

Strategy 2.2.H.8.1: No way to verify that alarms/warnings are minimized, or that alarm fatigue is reduced.

Rationale 2.2.H.8.1: This is 'wet' safety

102. Claim 2.2.H.9: Clinicians do not misinterpret alarms/warnings


Claim 2.2.H.9
Clinicians do not misinterpret alarms/warnings
Strategy 2.2.H.9
Use standard symbols and sounds; meaningful, unambiguous messages
Rationale 2.2.H.9
Standard symbols are commonly understood; meaningful, unambiguous messages are understood
J
Claim 2.2.H.9.1
Standard symbols and sounds reduce misinterpretation
Fact 2.2.H.9.1
Alarm/warning tone and volume follow IEC 60601-1-8 1.3.1
Claim 2.2.H.9.2
Messages are meaningful and unambiguous
Fact 2.2.H.9.2
Control panel displays helpful messages
Requirement R5.4.3(1) Audible Alarm Signals
Requirement R5.4.3(2) Auditory Volume
Requirement R5.4.3(1) Alarm Melody
Architecture: PCA_Control_Panel::pca_speaker.imp and PCA_Control_Panel.ui_thread.imp
SFT: Measure alarm/warning volume and tone
Requirement R5.5.0(4) Helpful messages
Architecture: PCA_Control_Panel.ui_thread.imp
SFT: Verfiy helpful messages

Claim 2.2.H.9: Clinicians do not misinterpret alarms/warnings

Strategy 2.2.H.9: Use standard symbols and sounds; meaningful, unambiguous messages

Rationale 2.2.H.9: Standard symbols are commonly understood; meaningful, unambiguous messages are understood

Claim 2.2.H.9.1: Standard symbols and sounds reduce misinterpretation

See details in section 103

Fact 2.2.H.9.1: Alarm/warning tone and volume follow IEC 60601-1-8 1.3.1

Requirement R5.4.3(1) Audible Alarm Signals

Evidence: ICE-PCArequirements.pdf#nameddest=audible alarms signals

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.3(2) Auditory Volume

Evidence: ICE-PCArequirements.pdf#nameddest=auditory volume

Repository: NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.4.3(1) Alarm Melody

Evidence: ICE-PCArequirements.pdf#nameddest=alarm melody

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Control_Panel::pca_speaker.imp and PCA_Control_Panel.ui_thread.imp

Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Measure alarm/warning volume and tone

Repository: NOR-STA SVN PCAPAC - NOR-STA

Claim 2.2.H.9.2: Messages are meaningful and unambiguous

See details in section 104

Fact 2.2.H.9.2: Control panel displays helpful messages

Requirement R5.5.0(4) Helpful messages

Evidence: ICE-PCArequirements.pdf#nameddest=helpful messages

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Control_Panel.ui_thread.imp

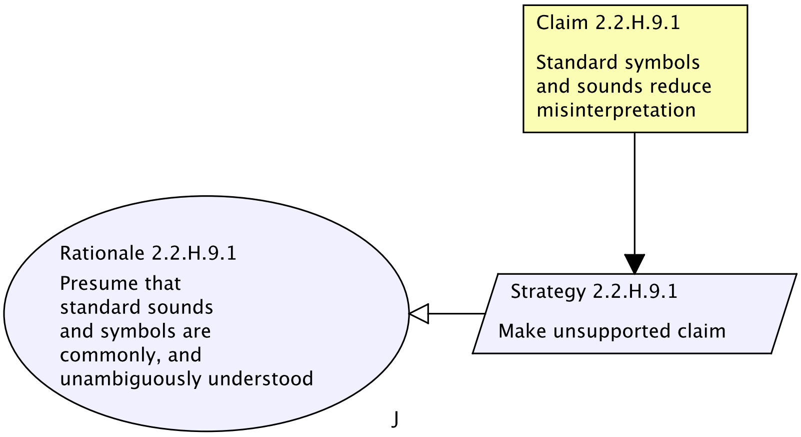
Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

SFT: Verfiy helpful messages

Repository: NOR-STA SVN PCAPAC - NOR-STA

103. Claim 2.2.H.9.1: Standard symbols and sounds reduce misinterpretation

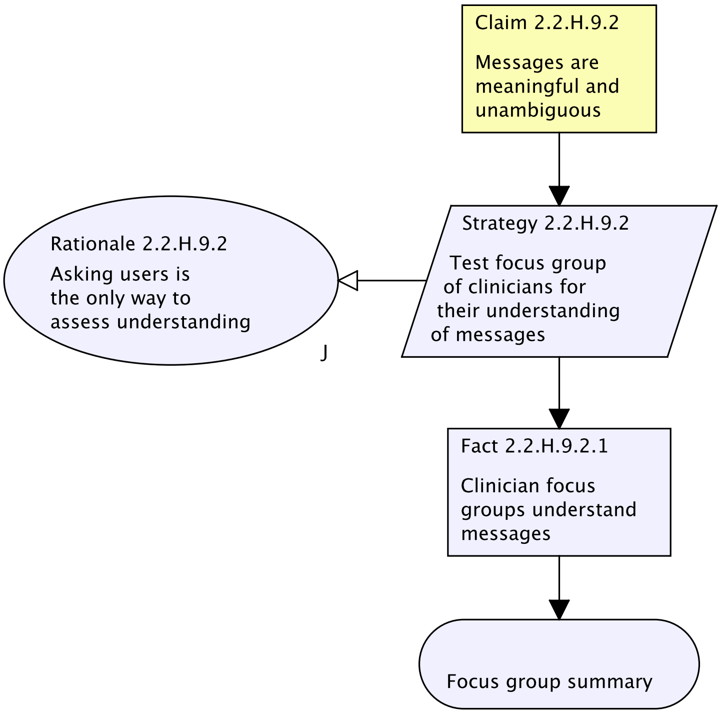

Claim 2.2.H.9.1
Standard symbols and sounds reduce misinterpretation
Strategy 2.2.H.9.1
Make unsupported claim
Rationale 2.2.H.9.1
Presume that standard sounds and symbols are commonly, and unambiguously understood
J

Claim 2.2.H.9.1: Standard symbols and sounds reduce misinterpretation

Strategy 2.2.H.9.1: Make unsupported claim

Rationale 2.2.H.9.1: Presume that standard sounds and symbols are commonly, and unambiguously understood

104. Claim 2.2.H.9.2: Messages are meaningful and unambiguous


Claim 2.2.H.9.2
Messages are meaningful and unambiguous
Strategy 2.2.H.9.2
Test focus group of clinicians for their understanding of messages
Rationale 2.2.H.9.2
Asking users is the only way to assess understanding
J
Fact 2.2.H.9.2.1
Clinician focus groups understand messages
Focus group summary

Claim 2.2.H.9.2: Messages are meaningful and unambiguous

Strategy 2.2.H.9.2: Test focus group of clinicians for their understanding of messages

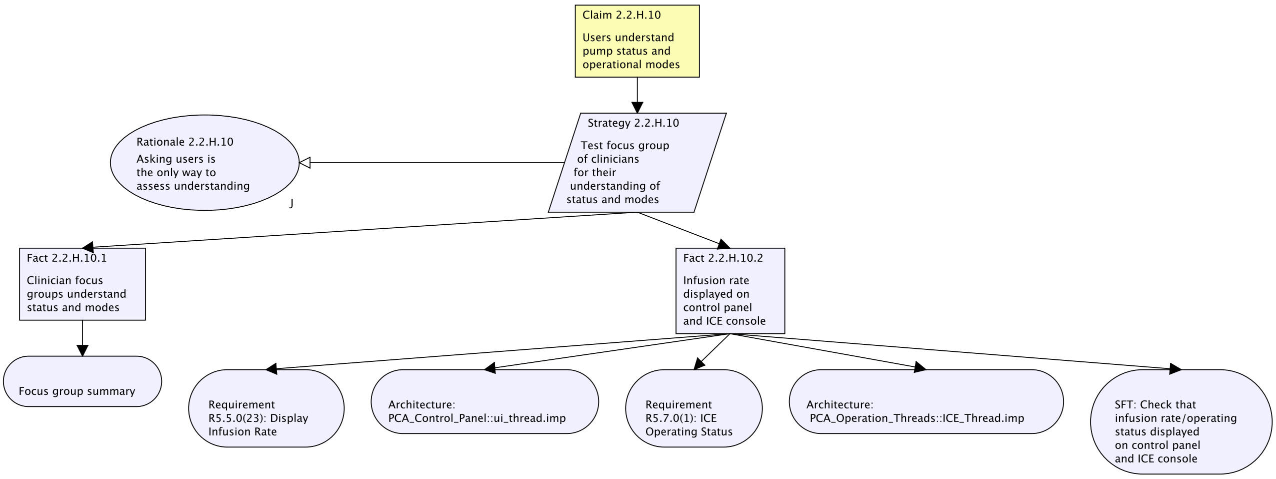
Rationale 2.2.H.9.2: Asking users is the only way to assess understanding

Fact 2.2.H.9.2.1: Clinician focus groups understand messages

Focus group summary

Repository: NOR-STA SVN PCAPAC - NOR-STA

105. Claim 2.2.H.10: Users understand pump status and operational modes


Claim 2.2.H.10
Users understand pump status and operational modes
Strategy 2.2.H.10
Test focus group of clinicians for their understanding of status and modes
Rationale 2.2.H.10
Asking users is the only way to assess understanding
J
Fact 2.2.H.10.1
Clinician focus groups understand status and modes
Fact 2.2.H.10.2
Infusion rate displayed on control panel and ICE console
Focus group summary
Requirement R5.5.0(23): Display Infusion Rate
Architecture: PCA_Control_Panel::ui_thread.imp
Requirement R5.7.0(1): ICE Operating Status
Architecture: PCA_Operation_Threads::ICE_Thread.imp
SFT: Check that infusion rate/operating status displayed on control panel and ICE console

Claim 2.2.H.10: Users understand pump status and operational modes

Strategy 2.2.H.10: Test focus group of clinicians for their understanding of status and modes

Rationale 2.2.H.10: Asking users is the only way to assess understanding

Fact 2.2.H.10.1: Clinician focus groups understand status and modes

Focus group summary

Repository: NOR-STA SVN PCAPAC - NOR-STA

Fact 2.2.H.10.2: Infusion rate displayed on control panel and ICE console

Requirement R5.5.0(23): Display Infusion Rate

Evidence: ICE-PCArequirements.pdf#nameddest=display infusion rate

Repository: NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Control_Panel::ui_thread.imp

Evidence:	PCA_Control_Panel.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Requirement R5.7.0(1): ICE Operating Status

Evidence:	CE-PCArequirements.pdf#nameddest=ICE operating status
Repository:	NOR-STA SVN PCAPAC - NOR-STA

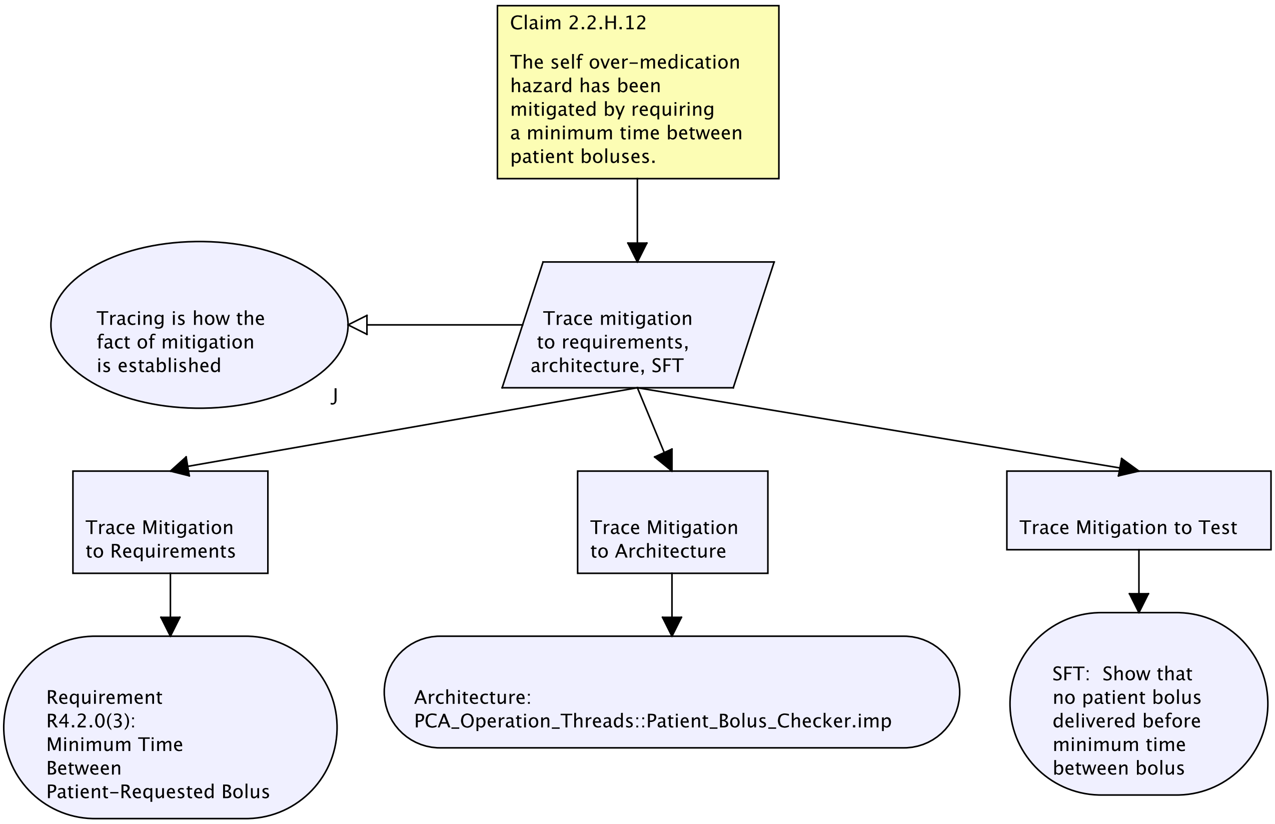
Architecture: PCA_Operation_Threads::ICE_Thread.imp

Evidence:	PCA_Operation_Threads.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

SFT: Check that infusion rate/operating status displayed on control panel and ICE console

Repository:	NOR-STA SVN PCAPAC - NOR-STA

106. Claim 2.2.H.12: The self over-medication hazard has been mitigated by requiring a minimum time between patient boluses.


Claim 2.2.H.12
The self over–medication hazard has been mitigated by requiring a minimum time between patient boluses.
Tracing is how the fact of mitigation is established
J
Trace mitigation to requirements, architecture, SFT
Trace Mitigation to Requirements
Trace Mitigation to Architecture
Trace Mitigation to Test
Requirement R4.2.0(3): Minimum Time Between Patient–Requested Bolus
Architecture: PCA_Operation_Threads::Patient_Bolus_Checker.imp
SFT: Show that no patient bolus delivered before minimum time between bolus

Claim 2.2.H.12: The self over-medication hazard has been mitigated by requiring a minimum time between patient boluses.

Trace mitigation to requirements, architecture, SFT

Tracing is how the fact of mitigation is established

Trace Mitigation to Requirements

Requirement R4.2.0(3): Minimum Time Between Patient-Requested Bolus

Evidence: ICE-PCArequirements.pdf#nameddest=minimum time between patient-requested bolus

Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace Mitigation to Architecture

Architecture: PCA_Operation_Threads::Patient_Bolus_Checker.imp

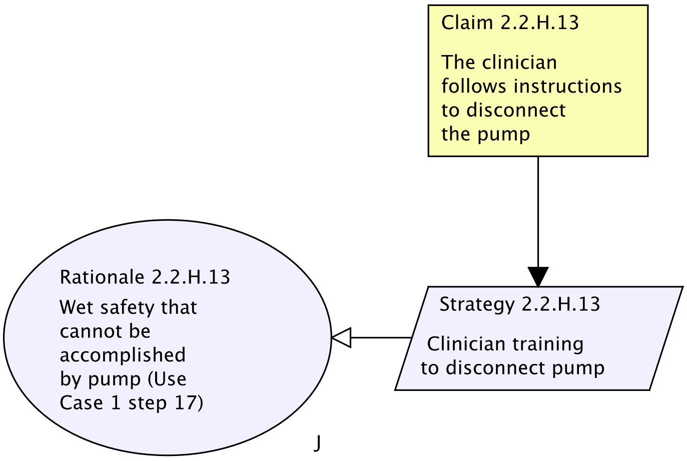
Evidence:	PCA_Operation_Threads.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Trace Mitigation to Test

SFT: Show that no patient bolus delivered before minimum time between bolus

Repository:	NOR-STA SVN PCAPAC - NOR-STA

107. Claim 2.2.H.13: The clinician follows instructions to disconnect the pump

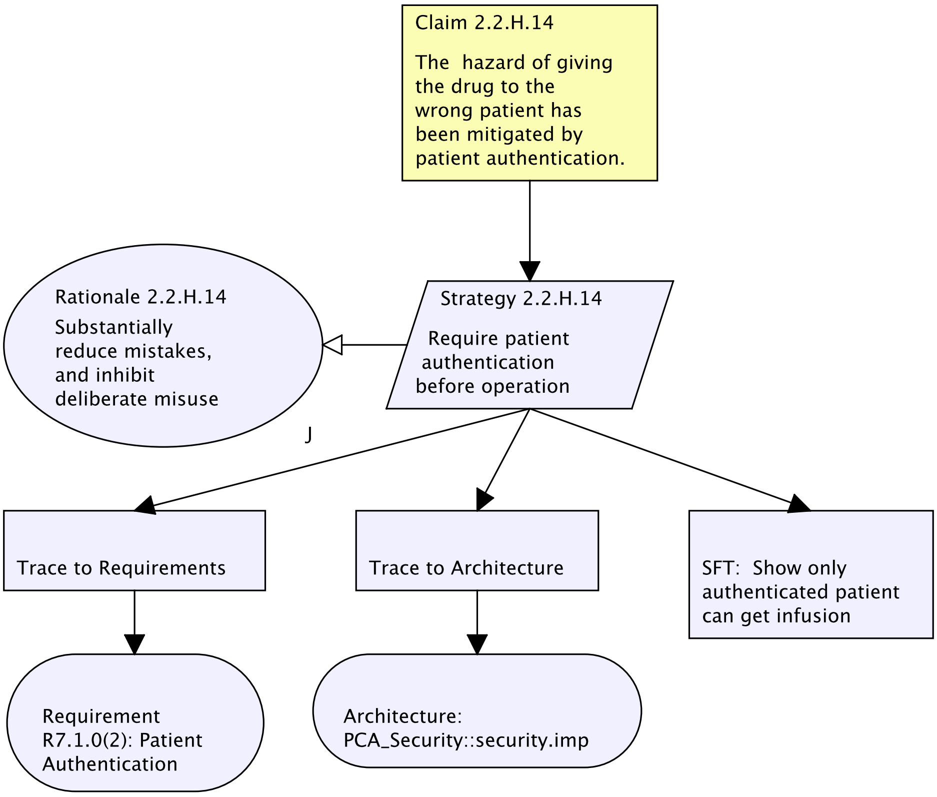

Claim 2.2.H.13
The clinician follows instructions to disconnect the pump
Strategy 2.2.H.13
Clinician training to disconnect pump
Rationale 2.2.H.13
Wet safety that cannot be accomplished by pump (Use Case 1 step 17)
J

Claim 2.2.H.13: The clinician follows instructions to disconnect the pump

Strategy 2.2.H.13: Clinician training to disconnect pump

Rationale 2.2.H.13: Wet safety that cannot be accomplished by pump (Use Case 1 step 17)

108. Claim 2.2.H.14: The hazard of giving the drug to the wrong patient has been mitigated by patient authentication.


Claim 2.2.H.14
The hazard of giving the drug to the wrong patient has been mitigated by patient authentication.
Rationale 2.2.H.14
Substantially reduce mistakes, and inhibit deliberate misuse
J
Strategy 2.2.H.14
Require patient authentication before operation
Trace to Requirements
Trace to Architecture
SFT: Show only authenticated patient can get infusion
Requirement R7.1.0(2): Patient Authentication
Architecture: PCA_Security::security.imp

Claim 2.2.H.14: The hazard of giving the drug to the wrong patient has been mitigated by patient authentication.

Strategy 2.2.H.14: Require patient authentication before operation

Rationale 2.2.H.14: Substantially reduce mistakes, and inhibit deliberate misuse

Trace to Requirements

Requirement R7.1.0(2): Patient Authentication

Evidence:	ICE-PCArequirements.pdf#nameddest=patient authentication
Repository:	NOR-STA SVN PCAPAC - NOR-STA

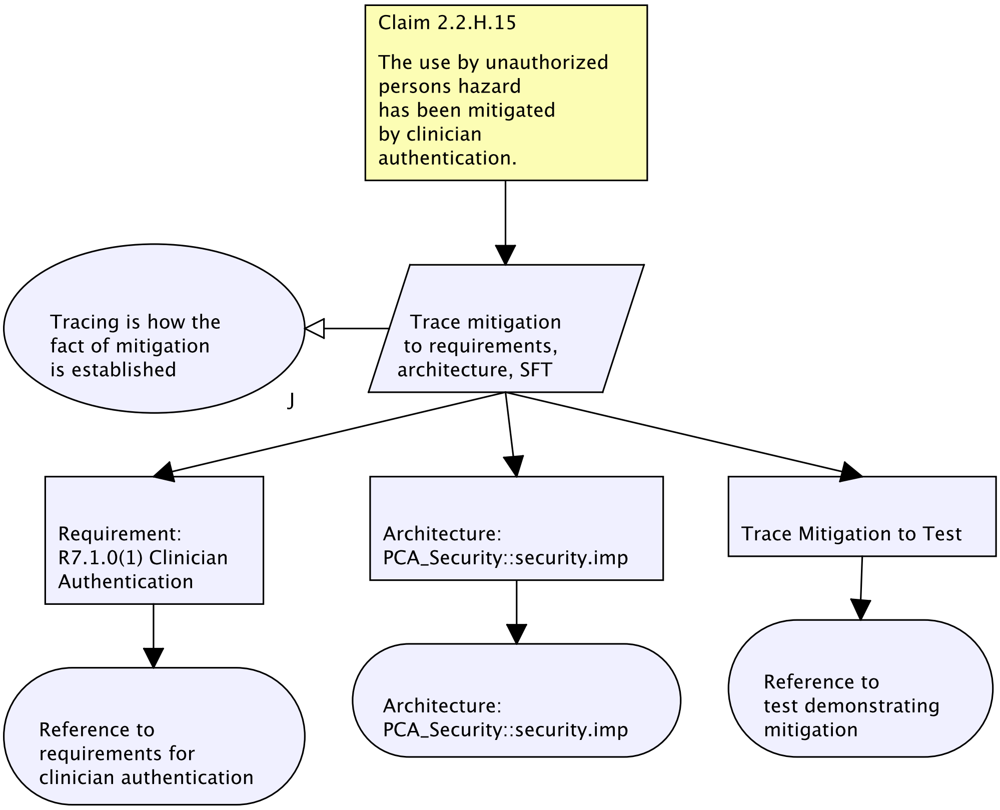
Trace to Architecture

Architecture: PCA_Security::security.imp

Evidence:	PCA_Security.aadl
Repository:	NOR-STA SVN PCAPAC - NOR-STA

SFT: Show only authenticated patient can get infusion

109. Claim 2.2.H.15: The use by unauthorized persons hazard has been mitigated by clinician authentication.


Claim 2.2.H.15
The use by unauthorized persons hazard has been mitigated by clinician authentication.
Tracing is how the fact of mitigation is established
J
Trace mitigation to requirements, architecture, SFT
Requirement: R7.1.0(1) Clinician Authentication
Architecture: PCA_Security::security.imp
Trace Mitigation to Test
Reference to requirements for clinician authentication
Architecture: PCA_Security::security.imp
Reference to test demonstrating mitigation

Claim 2.2.H.15: The use by unauthorized persons hazard has been mitigated by clinician authentication.

Trace mitigation to requirements, architecture, SFT

Tracing is how the fact of mitigation is established

Requirement: R7.1.0(1) Clinician Authentication

Reference to requirements for clinician authentication

Evidence:	ICE-PCArequirements.pdf#nameddest=clinician authentication
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Architecture: PCA_Security::security.imp

Architecture: PCA_Security::security.imp

Evidence: PCA_Security.aadl

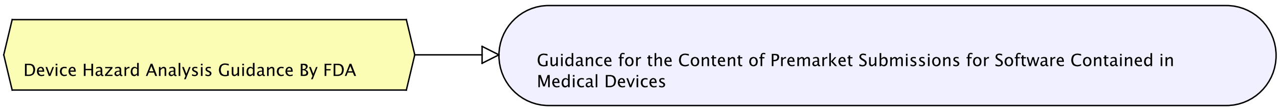
Repository: NOR-STA SVN PCAPAC - NOR-STA

Trace Mitigation to Test

Reference to test demonstrating mitigation

Repository: NOR-STA SVN PCAPAC - NOR-STA

110. Device Hazard Analysis Guidance By FDA

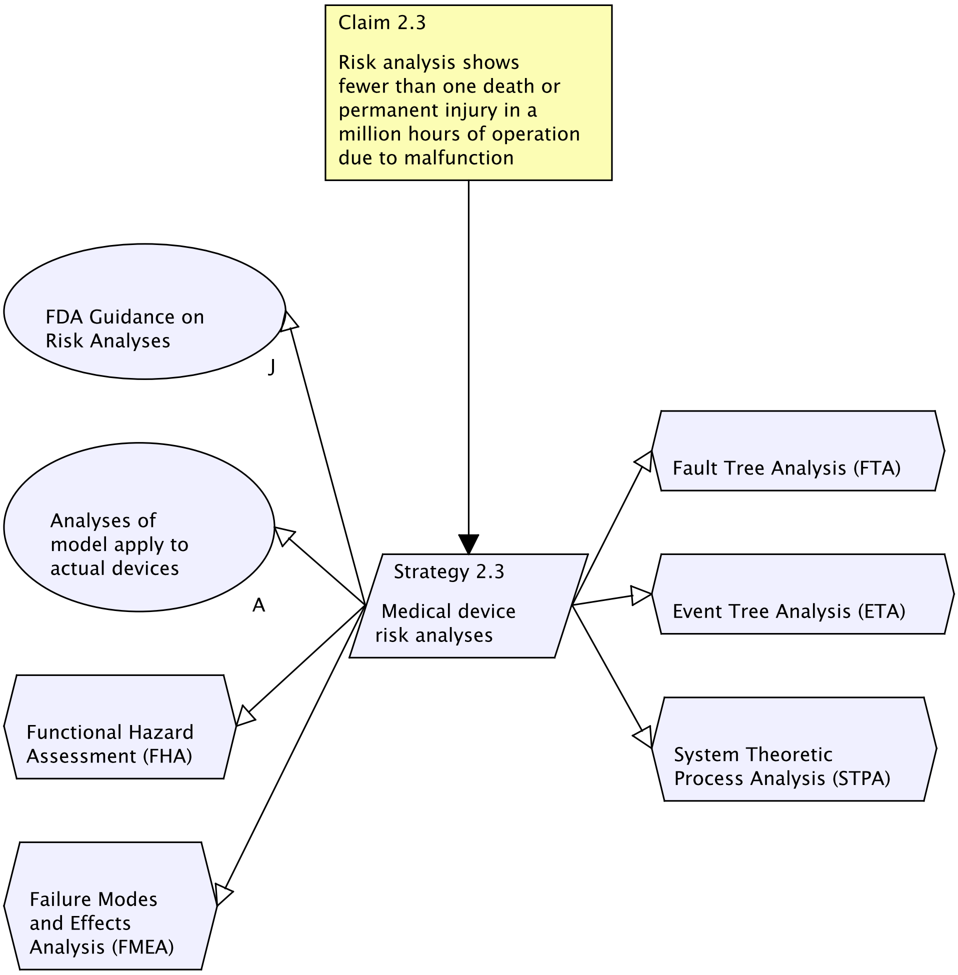

Device Hazard Analysis Guidance By FDA
Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Device Hazard Analysis Guidance By FDA

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Evidence:	FDAHazardAnalysis.pdf
Repository:	NOR-STA SVN PCAPAC - NOR-STA

111. Claim 2.3: Risk analysis shows fewer than one death or permanent injury in a million hours of operation due to malfunction


Claim 2.3
Risk analysis shows fewer than one death or permanent injury in a million hours of operation due to malfunction
FDA Guidance on Risk Analyses
J
Analyses of model apply to actual devices
A
Strategy 2.3
Medical device risk analyses
Functional Hazard Assessment (FHA)
Failure Modes and Effects Analysis (FMEA)
Fault Tree Analysis (FTA)
Event Tree Analysis (ETA)
System Theoretic Process Analysis (STPA)

Claim 2.3: Risk analysis shows fewer than one death or permanent injury in a million hours of operation due to malfunction

This claim concerns physical malfunction, including electronics and radiation effects, but not software

Strategy 2.3: Medical device risk analyses

FDA Guidance on Risk Analyses

FDA currently has no published guidance for risk analyses of medical devices.

The following are standard risk analyses performed by other safety-critical industries:
FHA - Functional Hazard Assessment
FMEA - Failure Modes and Effects Analysis
FTA - Fault Tree Analysis

Analyses of model apply to actual devices

Necessarily, only models can be *analyzed*.

Consequently, the question of how accurately the model abstracts error behavior arises.

Functional Hazard Assessment (FHA)

Placeholder for actual analysis.

Failure Modes and Effects Analysis (FMEA)

Placeholder for actual analysis.

Fault Tree Analysis (FTA)

Placeholder for actual analysis.

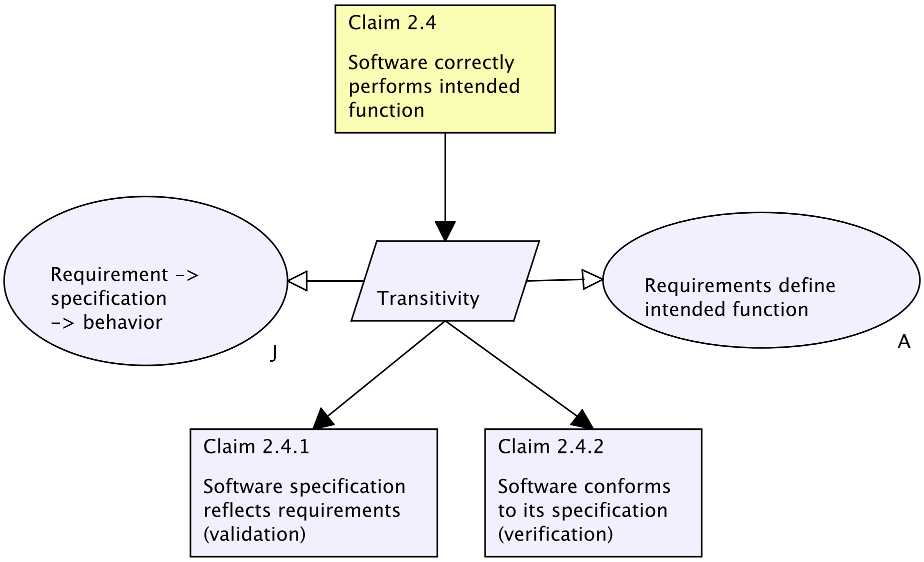
Event Tree Analysis (ETA)

Placeholder for actual analysis.

System Theoretic Process Analysis (STPA)

Placeholder for actual analysis.

112. Claim 2.4: Software correctly performs intended function


Claim 2.4
Software correctly performs intended function
Requirement -> specification -> behavior
J
Transitivity
Requirements define intended function
A
Claim 2.4.1
Software specification reflects requirements (validation)
Claim 2.4.2
Software conforms to its specification (verification)

Claim 2.4: Software correctly performs intended function

Transitivity

Requirement -> specification -> behavior

Requirements define intended function

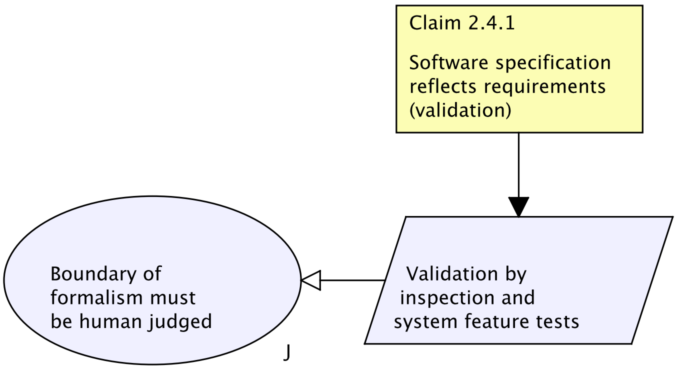
Claim 2.4.1: Software specification reflects requirements (validation)

See details in section 113

Claim 2.4.2: Software conforms to its specification (verification)

See details in section 114

113. Claim 2.4.1: Software specification reflects requirements (validation)


Claim 2.4.1
Software specification reflects requirements (validation)
Validation by inspection and system feature tests
Boundary of formalism must be human judged
J

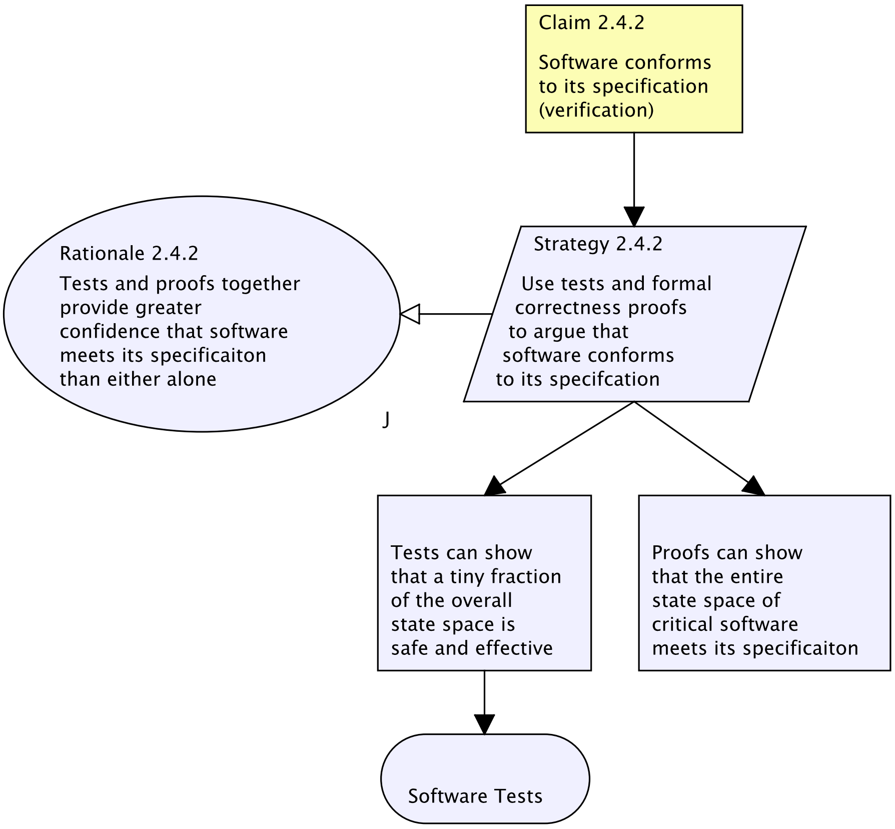
Claim 2.4.1: Software specification reflects requirements (validation)

Validation by inspection and system feature tests

Boundary of formalism must be human judged

Software *requirements* are written in natural language of domain experts.

114. Claim 2.4.2: Software conforms to its specification (verification)


Claim 2.4.2
Software conforms to its specification (verification)
Strategy 2.4.2
Use tests and formal correctness proofs to argue that software conforms to its specifcation
Rationale 2.4.2
Tests and proofs together provide greater confidence that software meets its specificaiton than either alone
J
Tests can show that a tiny fraction of the overall state space is safe and effective
Proofs can show that the entire state space of critical software meets its specificaiton
Software Tests

Claim 2.4.2: Software conforms to its specification (verification)

Strategy 2.4.2: Use tests and formal correctness proofs to argue that software conforms to its specifcation

Rationale 2.4.2: Tests and proofs together provide greater confidence that software meets its specificaiton than either alone

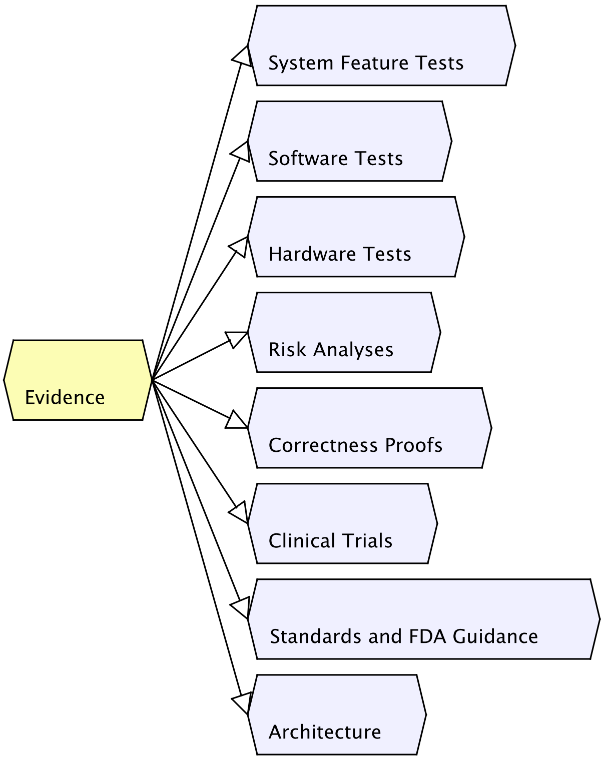
Tests can show that a tiny fraction of the overall state space is safe and effective

Software Tests

Repository: NOR-STA SVN PCAPAC - NOR-STA

□ **Proofs can show that the entire state space of critical software meets its specificaiton**

115. Evidence



Evidence

All evidence linked to this node

System Feature Tests

See details in section 116

Software Tests

Hardware Tests

Risk Analyses

FMEA, FTA, residual risk, etc.

Correctness Proofs

See details in section 117

Clinical Trials

See details in section 118

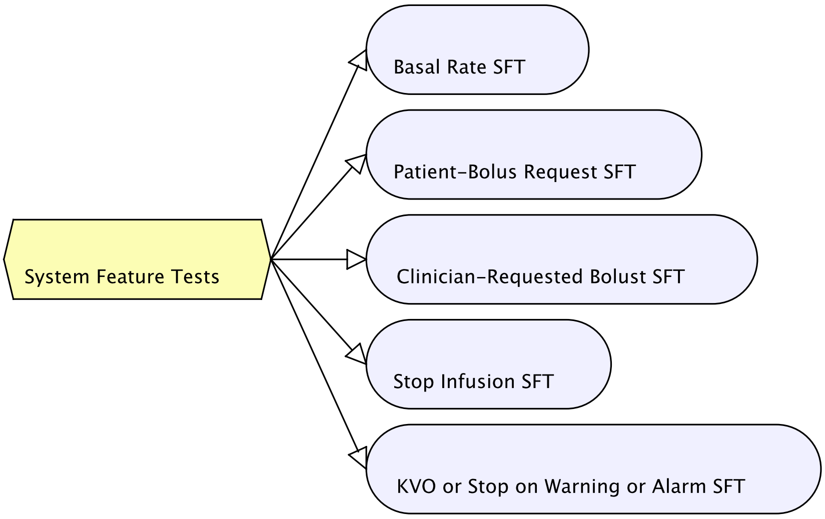
Standards and FDA Guidance

See details in section 119

Architecture

See details in section 120

116. System Feature Tests


System Feature Tests
Basal Rate SFT
Patient-Bolus Request SFT
Clinician-Requested Bolust SFT
Stop Infusion SFT
KVO or Stop on Warning or Alarm SFT

System Feature Tests

Basal Rate SFT

System feature test of basal rate infusion

Evidence: Basal Rate SFT.txt

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 12. Claim 1.1.2: PCA Pump infuses at basal rate

Patient-Bolus Request SFT

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 13. Claim 1.1.3: Upon pressing of Patient Button, a VTBI will be infused quickly, returning to basal rate

Clinician-Requested Bolust SFT

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 14. Claim 1.1.4: Clinician may command VTBI to be infused over a specified period of time

Stop Infusion SFT

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 15. Claim 1.1.5: Pressing Stop Button stops pumping

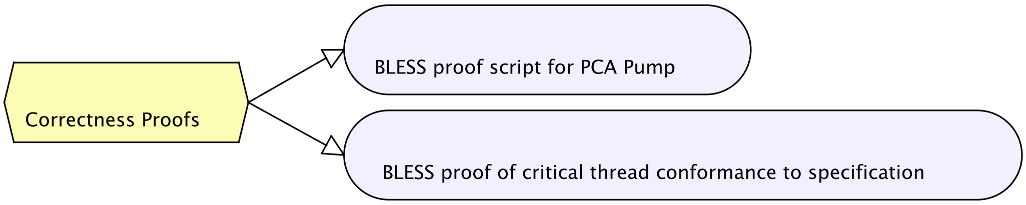
KVO or Stop on Warning or Alarm SFT

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 16. Claim 1.1.6: Upon detection of minor hazards, pump at KVO rate

117. Correctness Proofs


Correctness Proofs
BLESS proof script for PCA Pump
BLESS proof of critical thread conformance to specification

Correctness Proofs

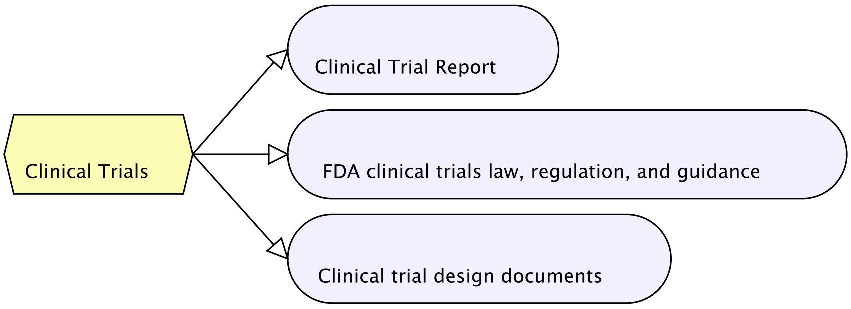
BLESS proof script for PCA Pump

Repository: NOR-STA SVN PCAPAC - NOR-STA

BLESS proof of critical thread conformance to specification

Repository: NOR-STA SVN PCAPAC - NOR-STA

118. Clinical Trials


Clinical Trials
Clinical Trial Report
FDA clinical trials law, regulation, and guidance
Clinical trial design documents

Clinical Trials

Clinical trials of the intended function on patients to gauge safety and effectiveness.

Clinical Trial Report

reference is to faux evidence that would be replaced by a real clinical trial report for a real medical device

Evidence: Clinical Trial Report.txt

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 18. Claim 1.2: Effectiveness of intended function demonstrated in clinical trials

Section 18. Claim 1.2: Effectiveness of intended function demonstrated in clinical trials

Section 18. Claim 1.2: Effectiveness of intended function demonstrated in clinical trials

FDA clinical trials law, regulation, and guidance

perhaps someone who knows these can add references

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 18. Claim 1.2: Effectiveness of intended function demonstrated in clinical trials

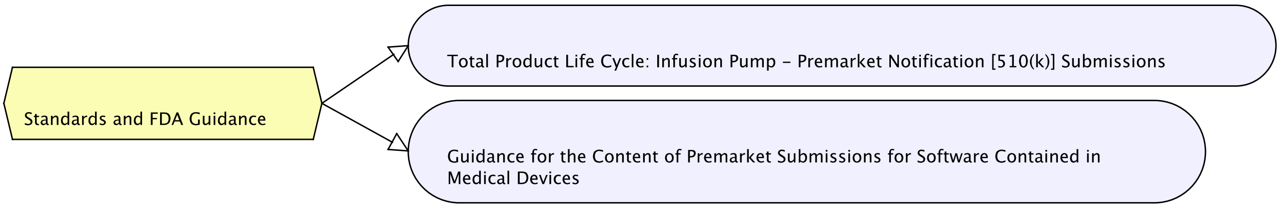
Clinical trial design documents

Repository: NOR-STA SVN PCAPAC - NOR-STA

Link(s) to this node in section(s):

Section 18. Claim 1.2: Effectiveness of intended function demonstrated in clinical trials

119. Standards and FDA Guidance


Standards and FDA Guidance
Total Product Life Cycle: Infusion Pump – Premarket Notification [510(k)] Submissions
Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Standards and FDA Guidance

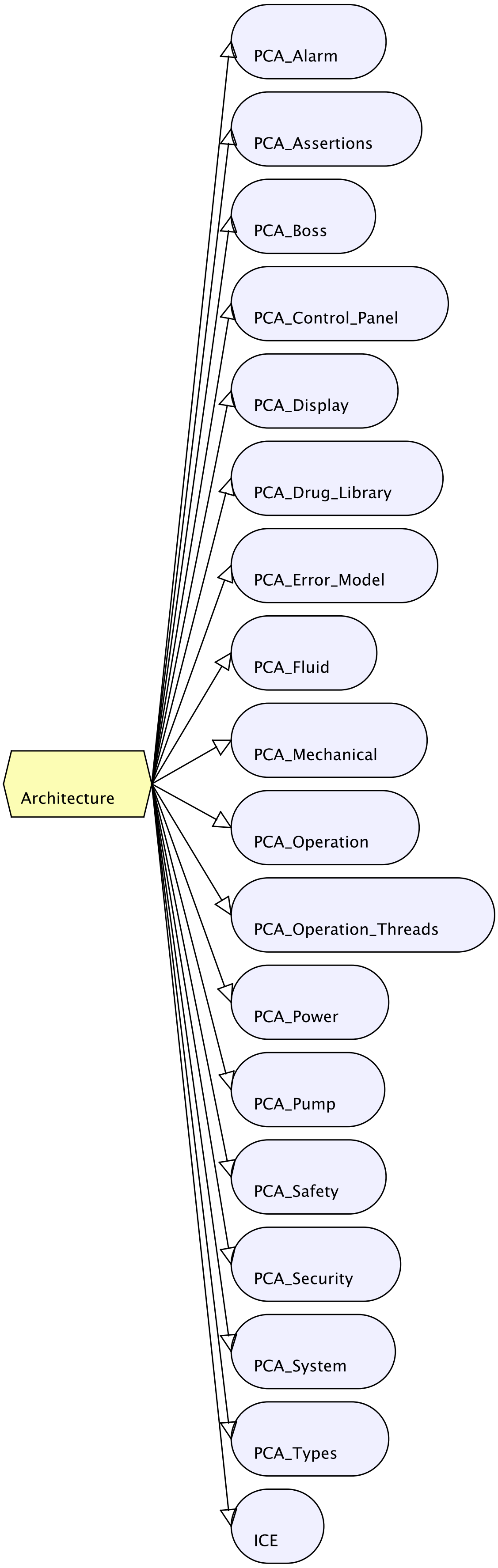
Total Product Life Cycle: Infusion Pump - Premarket Notification [510(k)] Submissions

Evidence:	IPGenera Guidance.pdf
Repository:	NOR-STA SVN PCAPAC - NOR-STA

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Evidence:	FDAHazardAnalysis.pdf
Repository:	NOR-STA SVN PCAPAC - NOR-STA

120. Architecture


Architecture
PCA_Alarm
PCA_Assertions
PCA_Boss
PCA_Control_Panel
PCA_Display
PCA_Drug_Library
PCA_Error_Model
PCA_Fluid
PCA_Mechanical
PCA_Operation
PCA_Operation_Threads
PCA_Power
PCA_Pump
PCA_Safety
PCA_Security
PCA_System
PCA_Types
ICE

Architecture

PCA_Alarm

Evidence: PCA_Alarm.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Assertions

Evidence: PCA_Assertions.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Boss

Evidence: PCA_Boss.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Control_Panel

Evidence: PCA_Control_Panel.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Display

Evidence: PCA_Display.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Drug_Library

Evidence: PCA_Drug_Library.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Error_Model

Evidence: PCA_Error_Model.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Fluid

Evidence: PCA_Fluid.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Mechanical

Evidence: PCA_Mechanical.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Operation

Evidence: PCA_Operation.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Operation_Threads

Evidence: PCA_Operation_Threads.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Power

Evidence: PCA_Power.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Pump

Evidence: PCA_Pump.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Safety

Evidence: PCA_Safety.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Security

Evidence: PCA_Security.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_System

Evidence: PCA_System.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

PCA_Types

Evidence: PCA_Types.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

ICE

Evidence: ICE.aadl

Repository: NOR-STA SVN PCAPAC - NOR-STA

Index of assurance case components

Architecture: PCA_Operation_Threads::ICE_thread.imp - section 67

Architecture: PCA_Operation_Threads::ICE_thread.imp - section 74

Architecture: PCA_Operation_Threads::ICE_Thread.imp - section 105

Architecture: PCA_Operation_Threads::ICE_Thread.imp - section 100

Architecture: PCA_Operation_Threads::Patient_Bolus_Checker.imp - section 38

Architecture: PCA_Operation_Threads::Patient_Bolus_Checker.imp - section 106

Architecture: PCA_Operation_Threads::Prescription_Checker.imp - section 99

Architecture: PCA_Power::power_control.imp - section 57

Architecture: PCA_Power::power_control.imp - section 58

Architecture: PCA_Power::power_control.imp - section 59

Architecture: PCA_Power::power_control.imp - section 60

Architecture: PCA_Power::power_control.imp - section 62

Architecture: PCA_Pump::PCA_memory.imp - section 74

Architecture: PCA_Safety::error_detector.imp - section 74

Architecture: PCA_Safety::safety.imp - section 70

Architecture: PCA_Safety::safety.imp - section 66

Architecture: PCA_Security::Security - section 47

Architecture: PCA_Security::Security - section 91

Architecture: PCA_Security::Security - section 99

Architecture: PCA_Security::Security - section 92

Architecture: PCA_Security::security.imp - section 83

Architecture: PCA_Security::security.imp - section 108

Architecture: PCA_Security::security.imp - section 109

Architecture: PCA_Security::security.imp - section 109

Architecture: PCA_Security::security.imp - section 79

Architecture: PCA_Security::security.imp - section 71

Architecture: PCA_System::ice_bus_adaptor.imp - section 100

Architecture: PCA_System::ice_bus_adaptor.imp - section 74

Claim 2.2.B.2: Pump Exposed to Pathogens, Allergens, Hazardous Substances Mitigated - section 45

Claim 2.2.B.3.1: Unauthorized tampering of pump settings mitigated - section 47

Claim 2.2.B.3.2: Panel lock broken mitigated by having strong lock and case - section 48

Claim 2.2.B.3.3: Panel/door opened during insfusion mitigated by strong lock and case - section 49

Claim 2.2.B.3.4: Infusion cannot be started with open door - section 50

Claim 2.2.B.3: Tampering mitigated - section 46

Claim 2.2.B.4.1: Electromagnetic Interference Mitigated by Shielding of Case - section 52

Claim 2.2.B.4.2: Electrostatic discharge mitigated by touch-screen and case design - section 53

Claim 2.2.B.4.3: Interference from power mitigated by ferrite filter - section 54

Claim 2.2.B.4: Non-human Interference mitigated - section 51

Claim 2.2.B: Environmental hazards have been mitigated - section 42

Claim 2.2.C.1: Power supply overheating mitigated by shutting down if temperature gets too high - section 57

Claim 2.2.C.2: Backup Battery Charge Fault Mitigated by Detection and Reporting - section 58

Claim 2.2.C.3: Supply voltage error mitiagetd by monitoring and reporting - section 59

Claim 2.2.C.4: Battery failure mitigated by detection and reporting - section 60

Claim 2.2.C.5: Leakage current mitigated by isolating mains power - section 61

Claim 2.2.C.6: Power supply circuit failure mitigated by detection and shut off - section 62

Claim 2.2.C.7: EMI from pump mitiageted by design - section 63

Claim 2.2.C: Electrical hazards have been mitigated - section 55

Claim 2.2.D.1: System Failure Mitigated by Safety Architecture - section 66

Claim 2.2.D.2: Network error mitigated by switching to stand-alone mode - section 67

Claim 2.2.D.3: Memory failure mitigated by error correction - section 68

Claim 2.2.D.4: False alarms are not hazards - section 69

Claim 2.2.D.5: Missed alarm due to sensor failure mitigated by safety architecture - section 70

Claim 2.2.D.6: Incorrect dose mitigated by Rx on label, authenticated - section 71

Claim 2.2.D: Hardware hazards have been mitigated - section 64

Claim 2.2.E.1: Data errors in event and fault logs are mitigated by fault masking and sending event reports to ICE as they occur - section 74

Claim 2.2.E.2: Software runtime errors mitigated by proving program correctness and avoiding problematic software functions - section 75

Claim 2.2.E.3: Corrupted Infusion Commands mitigated by limiting their possible function - section 76

Claim 2.2.E.4: Pump could not be silenced by alarm inactivation - section 77

Claim 2.2.E.5: Incorrect Software mitigated by version control - section 78

Claim 2.2.E.6: Incorrect drug library loaded mitigated by authentication - section 79

Claim 2.2.E.7: Failure to install software updates mitigated by manufacturer and hospital process - section 80

Claim 2.2.E: Software hazards have been mitigated - section 72

Claim 2.2.F.1: Unable to set dose mitigated by scanning Rx from label - section 83

Claim 2.2.F.2: Failure to alarm by broken speaker mitigated by alarm through ICE and audible test - section 84

Claim 2.2.F.3: Broken power cord mitigated by eletrocuting users - section 85

Claim 2.2.F.4: Pump motor failure mitigated by alarm upon pump stopping - section 86

Claim 2.2.F: Mechanical hazards have been mitigated - section 81

Claim 2.2.G.1: Hazard of inadequate device cleaning mitigated by user training and certification - section 87

Claim 2.2.G.2: Hazard of contamination by blood or leaking fluid mitigated by proper cleaning - section 87

Claim 2.2.G.3: Hazard of failure to flush mitigated by control panel message reminder - section 87

Claim 2.2.G.4: Hazard of pump connected to non-sterile infusion sets mitigated by training and certification - section 87

Claim 2.2.G.5: Hazard of packaging of the pump is damaged prior to its use mitigated by receiving inspection - section 87

Claim 2.2.G.6: Hazard of patient allergy to the infusion set or infusion set adhesive by knowing allergies of patient and comparing with material of infusion set - section 87

Claim 2.2.G.7: Hazard of clinician fails to rotate infusion sites as recommended mitigated by training and certification - section 87

Claim 2.2.G.8: Hazard of chemical precipitation inside the delivery path mitigated by cleaning and material compatibility - section 87

Claim 2.2.G.9: Hazard of physical damage to pump from Inadequate device cleaning or disinfection mitigated by user training - section 87

Claim 2.2.G: Biological and chemical hazards have been mitigated - section 87

Claim 2.2.H.10: Users understand pump status and operational modes - section 105

Claim 2.2.H.11: The user's motion cause motion causes the pump to be disconnected from the user. - section 89

Claim 2.2.H.12: The self over-medication hazard has been mitigated by requiring a minimum time between patient boluses. - section 106

Claim 2.2.H.13: The clinician follows instructions to disconnect the pump - section 107

Claim 2.2.H.14: The hazard of giving the drug to the wrong patient has been mitigated by patient authentication. - section 108

Claim 2.2.H.15: The use by unauthorized persons hazard has been mitigated by clinician authentication. - section 109

Claim 2.2.H.1: The hazard of user not understanding how to initiate pump operation is mitigated by clinician authentication and training - section 91

Claim 2.2.H.2: Incorrect prescription mitigated by prescription authentication - section 92

Claim 2.2.H.3: The hazard that infusion is stopped prematurely can only be mitigated by proper procedure - section 93

Claim 2.2.H.4.1: Alarm fatigue is avoided by only raising necessary alarms - section 95

Claim 2.2.H.4.2: Background noise will not cause user(s) to fail to detect notification(s) - section 96

Claim 2.2.H.4: The hazard that the user fails to detect notifications is mitigated - section 94

Claim 2.2.H.5: The wrong drug hazard has been mitigated by authenticating Rx. - section 97

Claim 2.2.H.6: Physical set up is correct - section 98

Claim 2.2.H.7: Users cannot "work around" or "bypass" software limits on drug/dose paprameters - section 99

Claim 2.2.H.8.1: False alarms/warnings are minimized to reduce alarm fatigue - section 101

Claim 2.2.H.8: The hazard that clinicians ignore warnings and alarms is mitigated - section 100

Claim 2.2.H.9.1: Standard symbols and sounds reduce misinterpretation - section 103

Claim 2.2.H.9.2: Messages are meaningful and unambiguous - section 104

Claim 2.2.H.9: Clinicians do not misinterpret alarms/warnings - section 102

Claim 2.2.H: Use hazards have been mitigated - section 89

Claim 2.3: Risk analysis shows fewer than one death or permanent injury in a million hours of operation due to malfunction - section 111

Rationale 2.2.D.5: Separate safety architecture detects and mitigates sensor failure by continuously monitoring sensors and sounding alarm upon failure - section 70

Rationale 2.2.D.6: Scanning prescription avoids entry errors; authentication mitigates hazard the label is mis-read - section 71

Rationale 2.2.D: Mitigation of each hazard adds confidence to safety - section 64

Rationale 2.2.E.1: Memory error correction masks many data errors, sending event to ICE as they occur provides redundant backup - section 74

Rationale 2.2.E.2: Avoiding problematic software function prevents problems from them and that correctness proof enhance confidence that software meets it specification - section 75

Rationale 2.2.E.3: ICE can only suspend and resume infusion or inactivate alarms which cannot cause harm - section 76

Rationale 2.2.E.4: Thowing the alarming device out the window may not silence alarms, but you won't hear it so louldy any more - section 77

Rationale 2.2.E.5: FDA Quality System Regulation requires proper version control - section 78

Rationale 2.2.E.6: Drug library authentication makes it difficut to install an incorrent drug library - section 79

Rationale 2.2.E.7: FDA Quality System Regulation requires proper version control - section 80

Rationale 2.2.E: Mitigation of each hazard adds confidence to safety - section 72

Rationale 2.2.F.1: Scanning prescription avoids entry errors; authentication mitigates hazard the label is mis-read - section 83

Rationale 2.2.F.5 When notified of pump failure by alarm, clinician can substitute working pump - section 86

Rationale 2.2.F: Mitigation of each hazard adds confidence to safety - section 81

Rationale 2.2.G: These are mostly 'wet' safety hazards, or material issues unrelated to system design - section 87

Rationale 2.2.H.10: Asking users is the only way to assess understanding - section 105

Rationale 2.2.H.13: Wet safety that cannot be accomplished by pump (Use Case 1 step 17) - section 107

Rationale 2.2.H.14: Substantially reduce mistakes, and inhibit deliberate misuse - section 108

Rationale 2.2.H.1: Authentication prevents use by untrained persons - section 91

Rationale 2.2.H.2: Reading Rx from drug container precludes mistakes in entry, and authentication precludes deliberate mis-entry - section 92

Rationale 2.2.H.3: Necessity to allow halting of infusion when (possibly) unsafe make the risk that infusion is stopped prematurely unpreventable - section 93

Rationale 2.2.H.4.2: This claim is unverifiable - section 96