Computer Science Department
Laboratory for Specification, Analysis, and Transformation of Software (SAnToS)

SAnToS TR 2019-1-1

SAnToS Lab Technical Report

Open Patient-Controlled Analgesia Infusion Pump System Requirements 1.0.0

Kansas State University

Contents

List of Figures

List of Tables

Preface

This document presents requirements for the Open Patient Control Analgesia (PCA) Pump. These requirements simulate the result of domain experts working with systems engineers to define function that will be safe for patients, and effective for some medical need. For PCA, the medical need is to provide narcotics to dull excruciating pain. Delivering medication as prescribed is what makes a PCA pump effective. Avoiding overdose, and all other harms to patients, is what makes a PCA pump safe.

These simulated requirements are provided as a public-domain example to facilitate research and standards development for people that do not have domain knowledge related to PCA or that need a non-propriety context in which to carry out their work. Real requirements documents are highly-confidential to medical device manufacturers, and thus detailed domain knowledge is exceedingly difficult to come by. However, since showing safety and effectiveness can be legal necessities for regulatory approval, and since university curricula and other training for engineers needs to address relevant topics in settings that are as realistic as possible, these simulated requirements were created to fill the vacuum.

0.1 Context, Goals, and Emphases

The first draft of this document was written by Brian R Larson, Research Associate, as part of an academic research project in the Laboratory for Specification, Analysis, and Transformation of Software (SAnToS) research group at Kansas State University (KSU) funded by funded by the National Science Foundation US Food and Drug Administration Scholar-in-Residence (NSF FDA SIR) program. Thus, the emphases and content of the document are driven by broader mission goals of the NSF FDA SIR program and SAnToS – specifically, the goal of providing resources primarily to the academic community (but also to industry and government agencies) that will facilitate research in safety critical systems, requirements engineering, hazard analysis and risk management, rigorous model-based development, formal specification and verification, and interoperable medical systems. Academic research groups and class instructors often do not have the resources to provide domain knowledge and artifacts that illustrate realistic challenges in medical system development.

This ongoing project attempts to gather relevant domain knowledge and supporting artifacts that will provide a more realistic context for research and pedagogical projects. Many persons have or will contribute including students, faculty, researchers and perhaps, *you*.

The primary goals of this document are as follows:

- *Illustrate best practices in systems engineering and requirements management.* This document follows the methodology and content suggestions presented in the Federal Aviation Administration (FAA) Requirements Engineering Management Handbook (REMH) (DOT/FAA/AR-08/32). We have found the FAA REMH to be especially well-aligned with our goals because, in contrast to other well-known requirements guidelines such as IEEE Std 830-1998, the FAA REMH brings a systems engineering perspective and emphasizes aspects relevant to embedded safety-critical systems.

- *Provide a pathway to formal architecture definitions and other associated formal development artifacts.* Although some argue that any notion of architectural specification falls in the domain of design rather than requirements, the FAA REMH emphasizes the initial high-level specification of a system architecture to enable allocation of requirements to subsystems as part of the requirements engineering process. This document amplifies that view by including formal architecture descriptions written in the SAE standard Architecture and Analysis Definition Language (AADL). This sets the stage for other activities that support our broader goals of illustrating formal/rigorous development artifacts – in particular, detailed architectural specifications in AADL with traceability links to requirements, formal annotations in the AADL Error Modeling Annex that support partial automation of hazard analyses and other risk management activities, formal interface and component behavioral specifications in the Behavioral Language for Embedded Software and Systems (BLESS).

- *Enable demonstrations of formal verification of system behavior and system assurance activities.* The mission of the KSU SAnToS research group and the focus of our NSF FDA SIR activities includes developing formal methods tools that can be applied to realistic systems. We aim to facilitate the same type of research within other groups in the academic community. Thus, this document focuses on requirements that will drive verification of behavioral properties. While other classes of requirements for useability, physical housing, electrical and other hardware aspects are important in real-world products, they are not as well-developed in this document due to our limited domain knowledge, resources, and the need to focus on requirements associated with functional and real-time behavior, risk management, and interoperability.

This document is part of a broader set of artifacts meant to illustrate best practices in engineering safety-critical medical devices. Other open source artifacts being developed by KSU SAnToS for the PCA pump include detailed hardware/software architectural descriptions specified in AADL, use cases and requirements modeling with automated tracability to the AADL architecture, formal behavioral specifications in BLESS, and an assurance case for the PCA pump.

Lecture materials with slides and lecture videos for the FAA REMH, hazard analyses and risk management, AADL, and BLESS are also available from the research group.

0.2 Licensing

0.3 Providing Feedback

The authors welcome feedback and suggestions for improving this document. To provide feedback send email to `openpcapump` ‘at’ `ksu.edu`.

0.4 Acknowlegements

This document builds off of the Generic Infusion Pump (GIP) and Generic PCA (GPCA) Pump work jointly developed by the University of Pennsylvania (U Penn) and FDA engineers Paul Jones and Raoul Jetly. Dave Arney, previously from U Penn and now from the CIMIT Medical Device Plug-and-Play (MDPnP) interoperability group, played a significant role in the GIP and GPCA efforts and provided several important forms of source material for this requirements document. FDA engineers Paul Jones and Sandy Weininger who shepherd the NSF FDA Scholars-in-Residence provided valuable feedback on earlier drafts of this document. Dr. Julian Goldman, head of the CIMIT MDPnP program also provided feedback, resources, and encouragement.

Funds for KSU SAnToS's broader work on medical device interoperability were provided by the National Science Foundation under grants #0932289,1065887,1238431,1239543 and by a subcontract from the CIMIT MDPnP group funded via an NIH/NIBIB Quantum grant.

Disclaimer

No physicians have reviewed these requirements to determine that they are actually safe and effective for real patients. DO NOT USE THESE REQUIREMENTS TO BUILD DEVICES USED ON PEOPLE. No warranty, expressed or implied, is made for these requirements by anyone.

1 Introduction

This document defines requirements for patient-controlled analgesia (PCA) infusion pumps. These requirements are based upon the Generic Patient-Controlled Analgesia (GPCA) infusion pump work done at the University of Pennsylvania, sponsored by the U.S. Food and Drug Administration, and FDA's guidance document on infusion pumps.[1]

1.1 PCA Pump Purpose

A patient-controlled analgesia (PCA) infusion pump infuses narcotic, liquid pain-killer at a prescribed basal rate plus any bolus doses that the patient may request to alleviate their pain, or be commanded by an attending clinician, most often, a registered clinician (Figure 1). Pain medication is prescribed by a licensed physician, which is dispensed by the hospital's pharmacy. The drug is placed into a vial labeled with the name of the drug, its concentration, the prescription, and the intended patient. A clinician loads the drug into the pump, and attaches it to the patient. The pump infuses a prescribed basal flow rate which may be augmented by a patient-requested bolus or a clinician-requested bolus. This allows additional pain medication in response to patient need within safe limits.

An interoperable PCA pump uses a network to communicate with other medical devices or hospital pharmacy (Figure 2).

1.2 Requirements from Use and Exception Cases

Part II defines the requirements–one per paragraph. Where applicable, the use or exception case(s) the requirement derives from, are listed and hyperlinked.

Each requirement is assigned a unique identifier, beginning with 'R', corresponding to their location in the document. In addition, the requirement identifier and title are listed in a footnote, and included in the index.

Each requirement is then allocated to a component[2] in the functional architecture in Part III. Each requirement entry in the index is thus linked to both the statement of the requirement, and the functional architecture component to which it was allocated.

1.3 References

Normative references are mandatory; informative references provide background.

1.3.1 Normative References

The following referenced documents are indispensable for the application of this document.

ASTM International F2761-09 *Medical Devices and Medical Systems–Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE)–Part 1 General requirements and conceptual model*

[1] PCA pumps are FDA product code "MEA."

[2] Some requirements require the cooperation of two or more functional components.

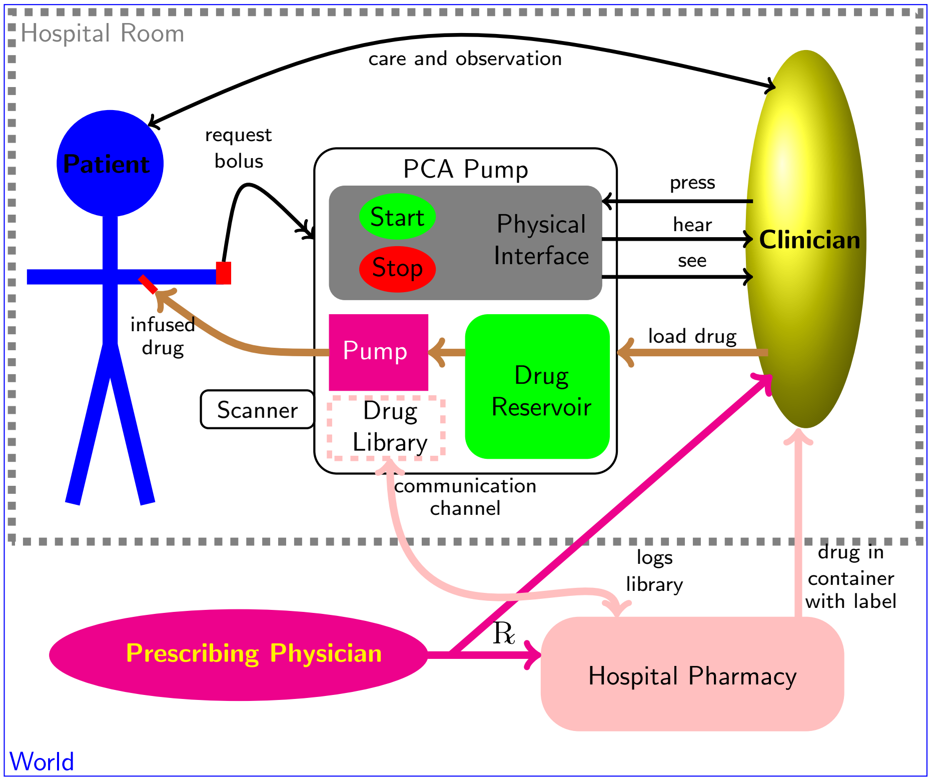


Figure 1: Independent PCA Pump Use

fig:non-ice-pca

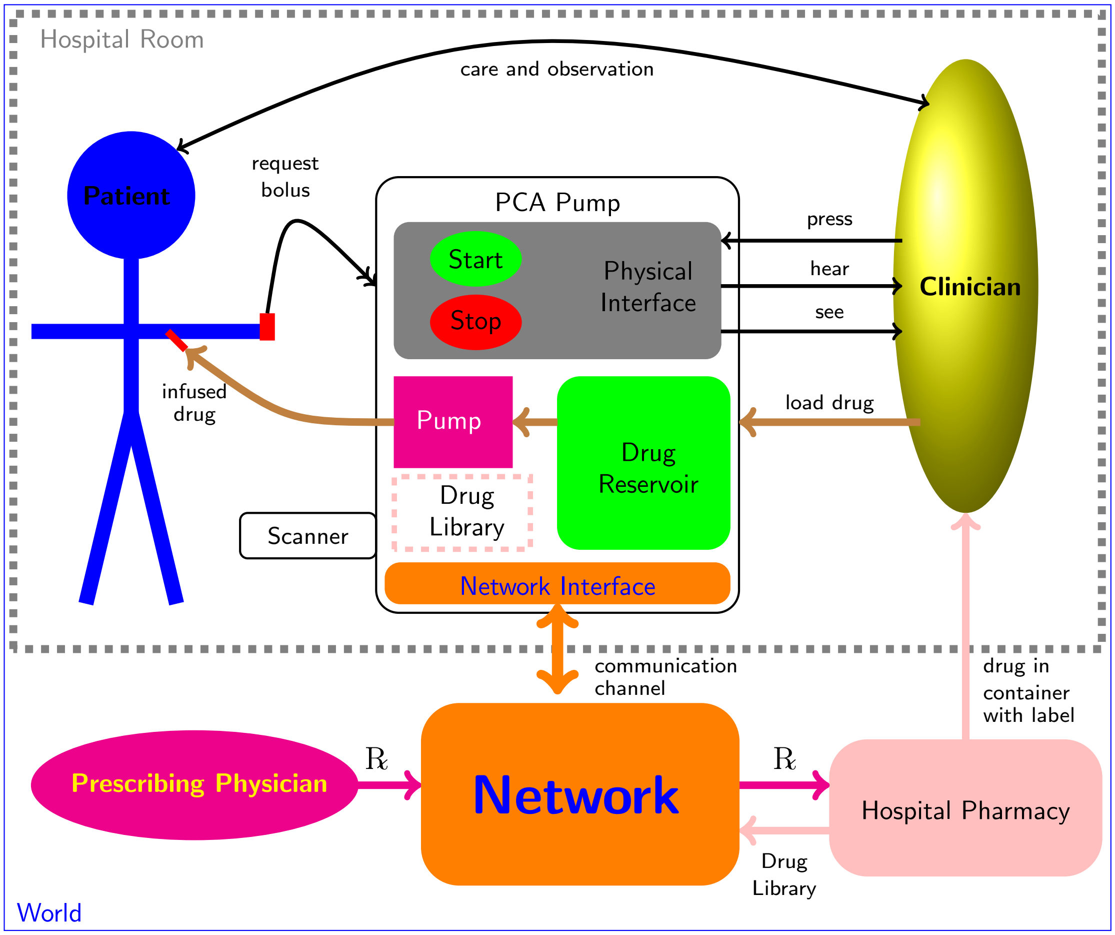


Figure 2: Networked PCA Pump Use

fig:ice-pca

IEC 60601-1-8 *Medical electrical equipment Part 1-8: General requirements for basic safety and essential performance Collateral Standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems* iec8

IEC 60601-1 (1988) *Medical electrical equipment Part 1: General requirements for safety, including Amendment 1 (1991) and Amendment 2 (1995) for Type B equipment*

IEC 60601-1 *Collateral Standard: Safety requirements for medical electrical systems*

IEC 60601-1-2 (2001) *Medical Electrical Equipment, Part 1: General Requirements for Safety, 2. Collateral Standard: Electromagnetic Compatibility - Requirements and Tests* IEC 60601-1-2

SAE International AS5506B *Architecture Analysis & Design Language (AADL)*

IEC 60601-2-24 *Particular Requirements for safety of infusion pumps and controllers* IEC 60601-2-24

1.3.2 Informative References

The following references provided a starting point from which these requirements were embellished and extended.

“Safety Requirements for the Generic Patient Controlled Analgesia Pump”[3]

“The Generic Patient Controlled Analgesia Pump Model,” Oleg Sokolsky, University of Pennsylvania.[4]

“gpca_spec_dlg.aadl,” Oleg Sokolsky, University of Pennsylvania

“Total Product Life Cycle: Infusion Pump - Premarket Notification [510(k)] Submissions,” U.S. Food and Drug Administration, April 23 2010.[5]

1.4 Terms and Acronyms

app application, a program that coordinates physical medical devices that is regulated as a medical device itself

ASTM International, formerly known as the American Society for Testing and Materials

basal base rate of drug infusion

bolus single dose of a drug or other medicinal preparation given all at once

btty battery

ccb clinician-requested bolus

C Celsius

CT Computerized Tomography

[3] Author unspecified, believed to be a collaboration between the FDA and the University of Pennsylvania.

[4] Similarities between these requirements and the GPCA pump developed at the University of Pennsylvania are deliberate. GPCA documents can be found at `http://rtg.cis.upenn.edu/gpca-aadl/wiki/`.

[5] `http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm206153.htm`

DEA U.S. Drug Enforcement Agency

FDA U.S. Food and Drug Administration

GPCA Generic Patient-Controlled Analgesia (pump)

Hg mercury

hr hour

IEC International Electrotechnical Commission

ISO International Organization for Standardization

KVO keep vein open

lba low battery alarm

LED light-emitting diode

lra low reservoir alarm

max maximum

min minimum

ml milliliter

NSF U.S. National Science Foundation

PCA Patient-Controlled Analgesia (pump)

POST power-on self test

psi pounds per square inch

RF radio frequency

RFID radio frequency identification

SAE International, formerly known as the Society of Automotive Engineers

TPM Trusted Platform Module

VTBI volume to be infused

Part I

Environment and Use

part:env

2 System Overview

Patient-controlled analgesia (PCA) is a means for the patient to self-administer analgesics (pain medications) intravenously by using a computerized pump, which introduces specific doses into an intravenous line.

2.1 Clinical Background

The purpose of PCA is pain reductioj. The patient receives immediate delivery of pain medication without the need for a clinician to administer it. The patient controls when the medication is given. More importantly, PCA uses more frequent but smaller doses of medication, and thus provides more even levels of medication within the patient's body. Syringe-injected pain management by a clinician requires larger doses of medication given less frequently. Larger doses peak shortly after administration, often causing undesirable side effects such as nausea and difficulty in breathing. Their pain-suppressing effects also often wear off before the next dose is scheduled.

2.2 Clinical Need

sec_clinicalneed

PCA uses a computer-controlled pump, which is controlled by the patient through a hand-held button that is connected to the machine. The pump usually delivers medications in small regular doses, and it can be programmed to issue a large initial dose and then a steady, even flow. The PCA pump can deliver medicine into a vein (intravenously, the most common method), under the skin (subcutaneously), or between the dura mater and the skull (epidurally).

When the patient feels the need for medication, the patient presses a button similar to a clinician call button. The pump delivers the medication through an intravenous line, a plastic tube connected to a needle inserted into a vein. Glucose and other medications can also be administered through intravenous lines, along with analgesics.

The medications most commonly used in PCA pumps are synthetic, opium-like pain-relievers (opioids), usually morphine and meperidine (Demerol).

The pump may be set to deliver a larger patient-requested dose of the prescribed drug. The health-care provider sets the pump to deliver a specified dose (a.k.a. bolus), determined by the prescribing physician, on demand, subject to a minimum time between deliveries. For example, 1 mg of medicine on demand, but not more frequently than one patient-requested dose every six minutes. If the patient presses the button before six minutes have elapsed, the pump will not dispense the medication. The pump also generates a record that the health personnel can access.

A continuous, even dose (a.k.a. basal rate) may also be set. The practitioner sets a total limit of medicine for an hour (or any other period) that takes into account the initial dose, the demand doses, and the around-the-clock doses. The pump's internal computer calculates all these amounts, makes a record of the requests it received and those it refused, and also keeps inventory of the medication being administered, which warns the staff when the supply is getting low.

2.3 System Synopsis

A patient-controlled analgesia (PCA) pump infuses pain killing medication into patients allowing patients to regulate (within bounds) the amount of medication they receive, and is depicted in Figure

1. A networked PCA pump augments the function of a stand-alone PCA pump with communication and control through a network which allows clinician's to remotely monitor the operation of the pump, and control applications to coordinate its operation with other medical devices, and is depicted in Figure 2.

2.3.1 Bolus Request Button

sec_bolusrequestbutton

Patients press a button to request a drug bolus in addition to a constant basal rate. The bolus request button is connected by a cable to the PCA pump, and may have a clip to attach to patient's bedding.

2.3.2 Delivery Tube and Needle

The drug is conveyed from the pump to a needle to to be infused into the patient. The needle is placed into a vein, usually in an arm or hand.

2.3.3 Physical Pump

A physical pump forces the drug into the delivery tube at specified rates. It also measures pressure and flow, and detects occlusion and air-in-line embolism (bubbles).

2.3.4 Drug Reservoir

A drug reservoir holds the prescribed drug in a vial for extraction by the physical pump. Because the drugs administered are narcotic and may be abused, the drug reservoir must be tamper resistant. The drug reservoir also has an electronic means, such as optical code, to read the prescription from the vial labeled by the hospital's pharmacy.

2.3.5 Control Panel

A Control Panel allows the pump to be started and stopped. It allows a clinician to command delivery of a bolus. It also allows a clinician to specify the duration a prescribed volume-to-be-infused is delivered. Pump status and alarms are displayed or sounded by the physical interface.

2.3.6 Drug Library

A drug library containing information about drugs that may be used by the pump is stored in non-volatile memory. The drug library is determined by the hospital pharmacy.

2.3.7 Scanner

A scanner allows the entry of patient, clinician, and prescription information automatically reducing both the work needed to operate the pump and possible harm to the patient through manual entry errors. The scanner may be optical or radio-frequency identification (RFID).

2.3.8 Network Interface

A network interface uses a communication channel to connect to clinician console, other medical devices, or hospital IT.

2.3.9 Safety Architecture

The system uses a safety architecture that separates normal operation from error and anomaly detection and response.

2.3.10 Security

Authentication of prescriptions, patients, and clinicians reduces risk of malicious or accidental harm.

2.4 System Context and External Interactions

The *environment* of the PCA pump is the patient, the clinician, the prescribing physician, the hospital room, and the hospital pharmacy.

By intent, the *patient* is part of the control loop determining the amount/rate of narcotic pain-killer infused into their blood through a tube leading to a needle in a patient's vein. Safety and efficacy properties of PCA relate to the patient.

The *clinician* connects the PCA pump to the patient, loads the liquid pain-killer received from the hospital pharmacy, and enters a physician's prescription for the particular patient connected to the pump.

The PCA pump will operate in a *hospital room* or similar clinical setting: controlled ambient temperature, assured power, [6] lighting, infection-control procedures and equipment, normal electromagnetic fields and particles,[7]

The *hospital pharmacy* dispenses the drug loaded into the PCA pump according to the physician's prescription. The hospital pharmacy also determines the drug library programed into the pump, regularly updated from the pharmacy's central repository.

The PCA pump may communicate with, and be controlled over, a *network*. Figure 3 depicts the PCA pump connected to a network along with other medical devices serving the same patient. A *network supervisor* may be attached to the network providing processing, memory, mass storage, connection to hospital IT network, and/or connection to a *clinician console*. In particular, a network supervisor may execute *control applications* which receive data from, and send commands to, networked medical devices. A network supervisor can display patient information, warnings and alarms on the clinician console. Generally, a clinician console may inactivate (silence) warnings and alarms.

2.5 Environmental Constraints

(1) The PCA pump must be able to operate within a *temperature range*[8] R2.5.0(1) of T_{lo} = 10C to T_{hi} = 50C.[9]

[6] source of power is an implementation choice, defaulting to 60 Hz 120V

[7] No MRI magnetic fields, CT scanner X-ray, radiation therapy, RF transmitters, etc.; just 50 or 60 cycle hum and unavoidable cosmic ray-induced neutrons and pions.

[8] requirement R2.5.0(1): *temperature range*

[9] These environmental requirements pertain to the use of the PCA pump, not its design or function.

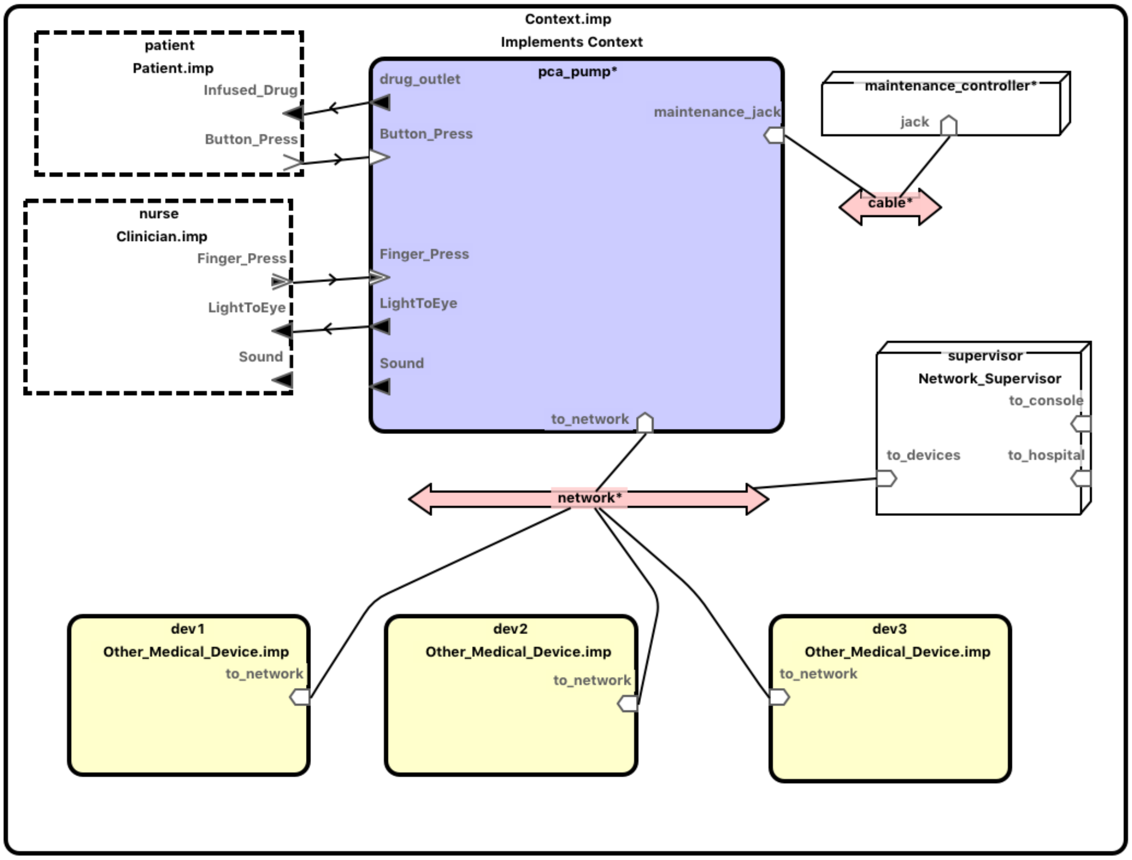


Figure 3: PCA Pump with Network and Supervisor

fig:context

(2) The pump must be able to withstand and operate under *atmospheric pressure*[10] R2.5.0(2) ranging from $P_{min} = 20\text{"Hg}$ to $P_{max} = 35\text{"Hg}$.

(3) The (external) pump must be able to operate at *relative humidity*[11] R2.5.0(3) ranging from $H_{min} = 0\%$ to $H_{max} = 100\%$ (non-condensing).

(4) The PCA pump shall withstand *splashing*[12] R2.5.0(4) (but not immersion) with water or bodily fluids.

2.6 Direct PCA Pump Interactions

A PCA pump interacts directly with the patient through the bolus request button and the delivery tube/needle. It interacts directly with an attending clinician who connects it to the patient, sets bolus delivery duration, commands bolus delivery, and responds to alarms.

2.7 Indirect PCA Pump Interactions

A PCA pump interacts indirectly through a network which may include a clinician console to monitor and control the pump, or control applications that may stop infusion if abnormal conditions are detected by other devices such as slow heart rate or low blood oxygenation.

2.8 System Goals

subsec_systemgoals

The high-level goals (G) of the PCA pump are:

G0 The pump will safely infuse drugs intravenously for pain relief.

G1 The patient should receive enough drug to reduce his pain.

G2 The patient should not receive so much drug that makes him unaware, or is harmful.

G3 Clinician(s) should be notified upon occurrence of hazardous conditions, unless alarms have been inactivated.

G4 The PCA pump should detect the smallest-possible air-in-line embolism (bubble) and halt the infusion drug.

G5 The PCA pump should infuse safely when failures occur or hazards are detected[13]

G6 Patients should receive the drug as prescribed by their physician, administered by appropriate clinicians.

G7 Patient's health information should be available to those caring for the patient, and only those.

G8 PCA pump operational status should be visible.

[10] requirement R2.5.0(2): *atmospheric pressure*

[11] requirement R2.5.0(3): *relative humidity*

[12] requirement R2.5.0(4): *splashing*

[13] Some failures/hazards halt pumping; others switch to keep-vein-open (KVO) rate; or continue current basal or bolus rate

3 System Operational Concepts

The PCA pump infuses a prescribed basal flow rate augmented with a bolus dose upon patient or clinician request. When infusion is suspended, the pump shall maintain a minimal keep-vein-open (KVO) rate of infusion. The pump shall halt infusion upon pump failures.

3.1 Use Cases

The following use cases describe normal operation of the PCA pump. Exception cases are described in Section 3.2. A summary of uses cases is provided in Table 1.

Table 1: Summary of PCA Use Cases

ID	Actor	Title	Description
UC1	Clinician	Normal Operation	initialization, attachement, basal infusion, detatchment
UC2	Patient	Patient-Requested Bolus	extra dose upon patient-determined need
UC3	Clinician	Clinician-Requested Bolus	extra dose upon clinician-determined need
UC4	Control Application	Externally-Detected Hazard	switch to KVO infusion rate upon control application-determined need
UC5	Clinician	Resume Operation After Externally-Detected Hazard	resume prescribed infusion after clinician determines it is safe
UC6	Clinician	Console-Initiated Audible Alarm Inactivation	suspend audible alarm from clinician console
UC7	Clinician	Resume Infusion	continue infusion after Stop
UC8	Clinician	Flush Pump	cleanse pump after use
UC9	Clinician	Prime Pump	expel air from tube and needle

tab:use-case

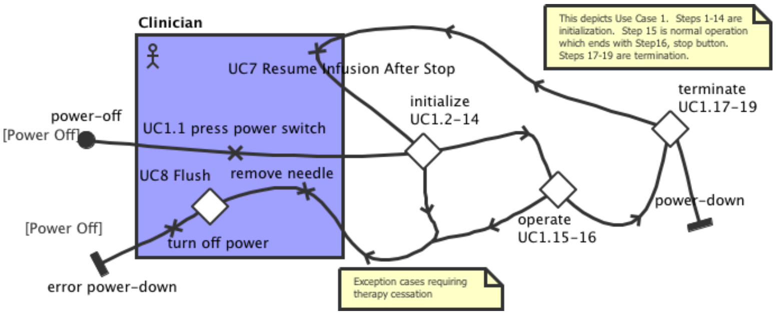
Use case maps *use case map* graphically depict use and exception cases as a flow of actions. Use cases begin at a filled circle and end at a perpendicular bars. An X represents an action or responsibility. A diamond represents a stub to a subordinate use case. A colored box represents some entity in the use case. Location of an X designates the entity that performs an action. A *scenario* is a particular sequence of actions. In each of the use case maps, the sequence of actions corresponding the use or exception case are colored blue.[14]

[14] These use case maps are part of an architectural model of a device that implements the requirements in this document. This model is defined in the Architecture Analysis and Design Language (AADL) using the Open-Source AADL Tool Environment (OSATE). OSATE is a plug-in to Eclipse which itself supports plugins. The plug-in used to create the use case maps is jUCMNav.

3.1.1 Use Case: Normal Operation of PCA Pump (UC1)

subsubsec_uc1

This use case describes normal operation of the PCA Pump. Steps 1 through 14 define the actions required to begin infusing. Steps 17 through 19 define the steps actions to cease infusing. Step 15 is infusion, defined in other use cases, terminated by step 16, pressing the stop button.



This depicts Use Case 1. Steps 1-14 are initialization. Step 15 is normal operation which ends with Step16, stop button. Steps 17-19 are termination.

Exception cases requiring therapy cessation

Figure 4: Use Case 1, Normal Operation

UC1

Related System Goals G1 and G2

Primary Actor Clinician

Precondition

- Patient is ready for infusion
- Physician has prescribed drug
- Pharmacy has filled prescription
- Pharmacy has installed drug library into PCA pump
- Drug has been delivered to clinician
- PCA pump is off

Postcondition

- PCA pump is turned off
- Infusion needle removed from patient

Main Success Scenario

1. Clinician turns on PCA pump (Exception Case: Power-On Self Test Failure)
2. Clinician presses button when hearing audible alarm sound (Exception Case: Sound Failure)
3. Clinician scans own badge
4. Clinician is authenticated to operate PCA pump (Exception Case: Clinician Authentication Failure)
5. Clinician scans patient information (wristband)
6. Patient is authenticated to receive medical care (Exception Case: Patient Authentication Failure)

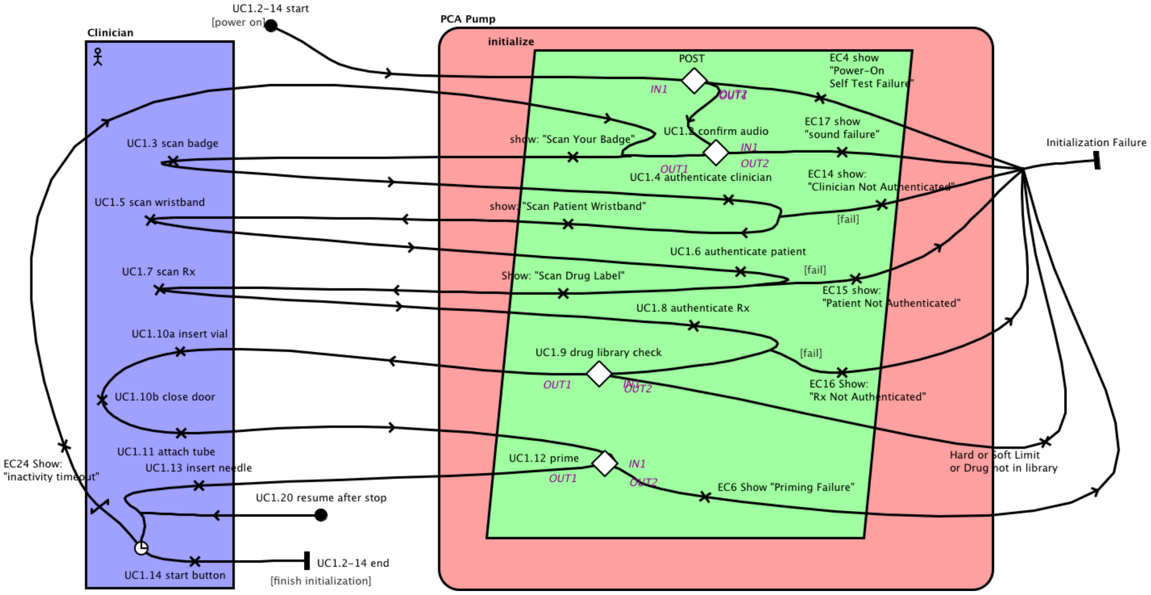


Figure 6: Use Case 1 Steps 2 to 14

default

7. Clinician scans drug information and patient's prescription from drug container (vial)
8. Prescription is authenticated for the patient (Exception Case: Prescription Authentication Failure)
9. PCA pump compares prescription with its drug library (Exception Cases: Drug Library Soft Limit and Drug Library Hard Limit)
10. Clinician puts drug vial into the reservoir and closes and locks the door
11. Clinician attaches infusion tube and needle to pump
12. Clinician primes pump (Exception Case: Pump Priming Failure)
13. Clinician inserts infusion needle into patient's vein
14. Clinician presses Start button to begin basal-rate infusion
15. Bolus dose infused upon request; see Use Case: Bolus Infusion
16. Clinician presses Stop button to halt infusion
17. Clinician removes infusion needle from patient's vein, and infusion tube from pump
18. Clinician removes drug vial, returning remaining drug to pharmacy
19. Clinician turns off PCA pump power.

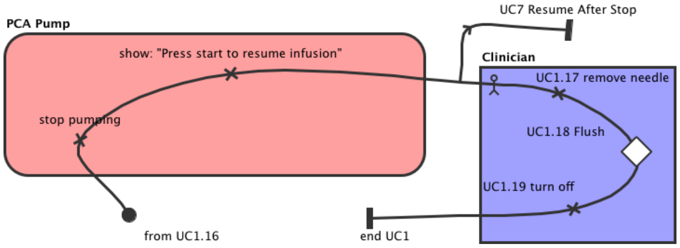


Figure 5: Use Case 1, Normal Operation, Steps 17 to 19 UC1-17-19

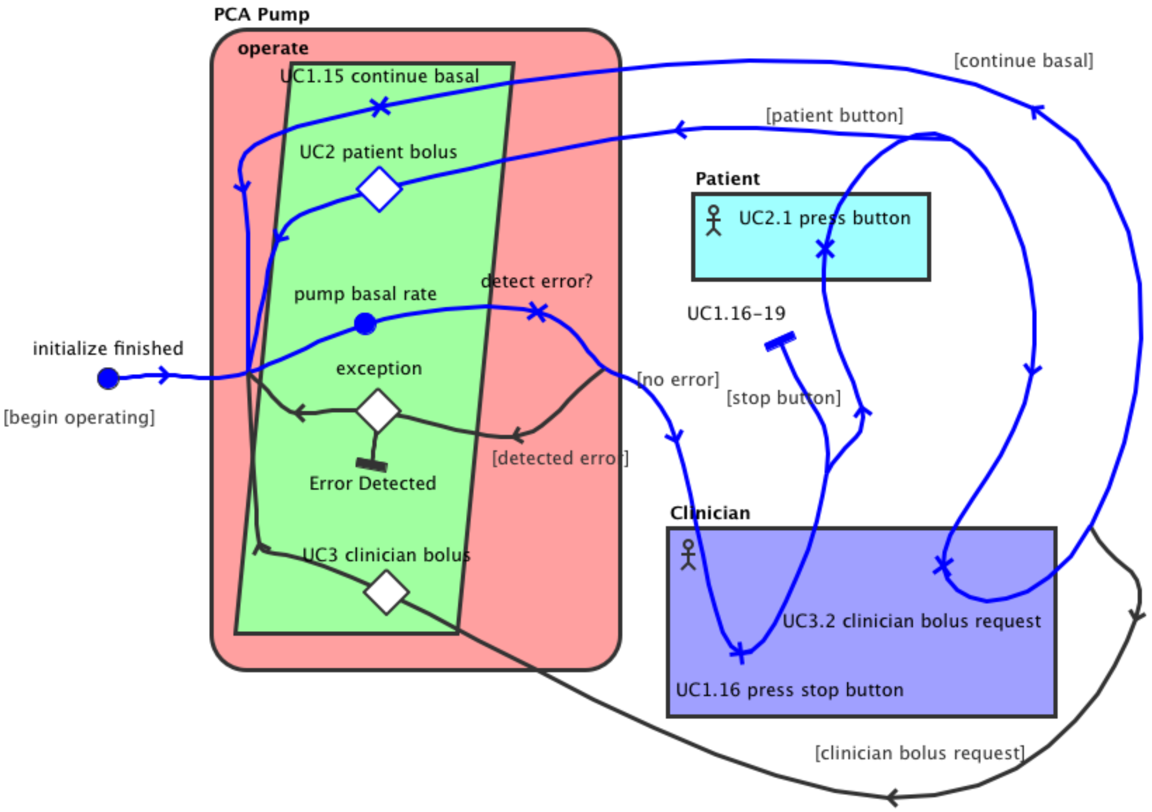


Figure 7: Use Case 2, Step 1 Patient Button UC2_1

3.1.2 Use Case: Patient-Requested Bolus (UC2) subsubsec_uc2

This use case describes operation when the patient requests an extra dose of drug.

Related System Goals G1 and G2

Primary Actor Patient

Precondition

- Steps 1 to 14 of Normal Operation Use Case completed
- Basal rate being infused
- Prescribed minimum time between boluses has elapsed

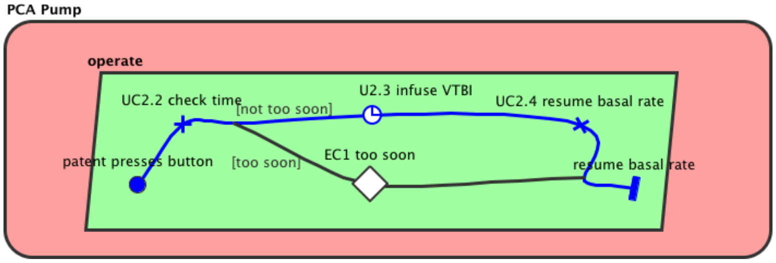


Figure 8: Use Case 2, Steps 2 to 4 Patient Bolus UC2_2

Postcondition

- Resume basal rate infusion

Main Success Scenario

1. Patient presses bolus request button
2. Time since last bolus compared with prescribed minimum time between boluses (Exception Case: Bolus Request Too Soon)
3. If not too soon, begin infusing VTBI (Exception Case: Maximum Safe Dose)
4. After prescribed volume-to-be-infused (VTBI) has been infused, resume basal rate infusion

3.1.3 Use Case: Clinician-Requested Bolus (UC3)

subsubsec_uc3

This use case describes operation when the clinician requests an extra dose of drug.

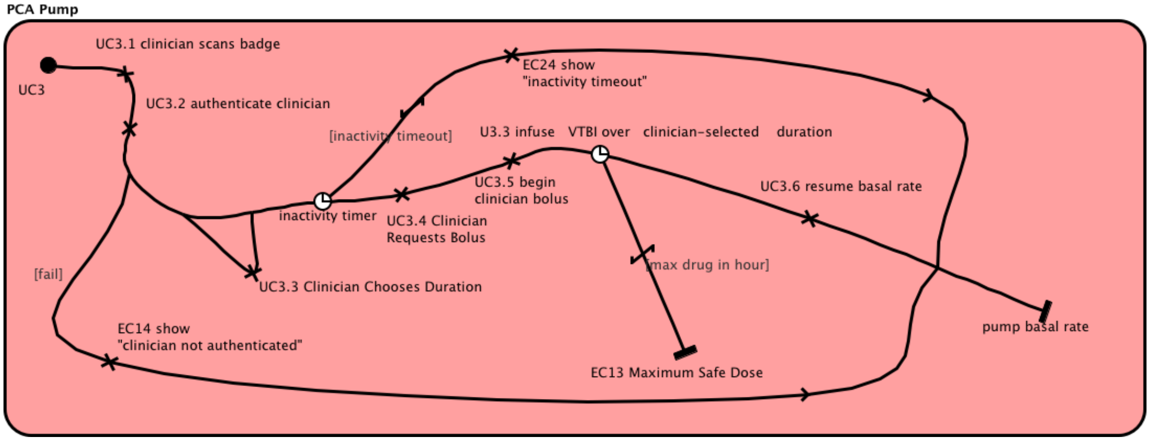

PCA Pump
UC3.1 clinician scans badge
UC3
UC3.2 authenticate clinician
EC24 show "inactivity timeout"
[inactivity timeout]
U3.3 infuse VTBI over clinician-selected duration
UC3.5 begin clinician bolus
inactivity timer
UC3.4 Clinician Requests Bolus
UC3.6 resume basal rate
[fail]
UC3.3 Clinician Chooses Duration
[max drug in hour]
EC14 show "clinician not authenticated"
pump basal rate
EC13 Maximum Safe Dose

Figure 9: Use Case 3, Clinician-Requested Bolus

UC3_2

Related System Goals G1 and G2

Primary Actor Clinician

Precondition

- Steps 1 to 14 of Normal Operation Use Case completed
- Basal rate being infused

Postcondition

- Resume basal rate infusion

Main Success Scenario

1. Clinician scans own badge
2. Clinician is authenticated to operate PCA pump (Exception Case: Clinician Authentication Failure)
3. Clinician (optionally) sets duration of bolus infusion on Control Panel
4. Clinician requests bolus infusion on Control Panel, by pressing the Start Button (Exception Case: Inactivity Timeout)
5. Begin infusing bolus at rate so that prescribed VTBI is infused over the duration selected by the clinician, interrupted by a patient-requested bolus, and resumed afterward. (Exception Case: Maximum Safe Dose)
6. When the duration ends, resume basal rate infusion

3.1.4 Use Case: Externally-Detected Hazard (UC4)

subsubsec_uc4

This use case describes operation when a control application, executed by a network supervisor, determines a hazard may exist by monitoring other networked devices such as pulse oximeters, respiration monitors, or electrocardiograms.

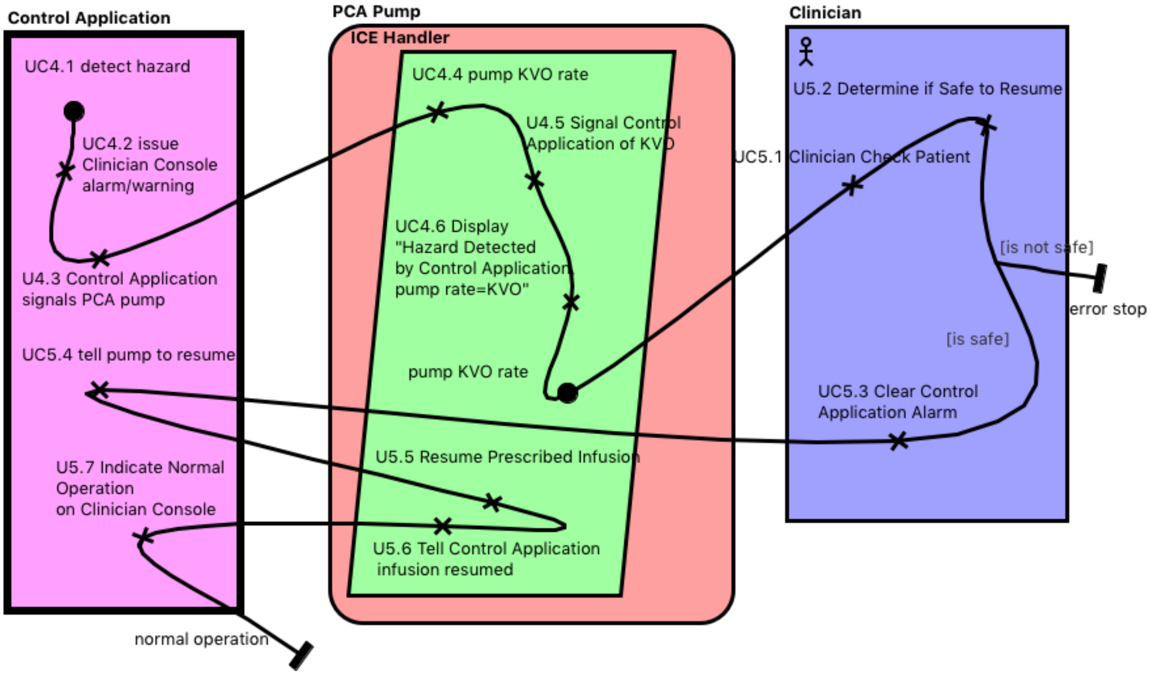

Control Application
UC4.1 detect hazard
UC4.2 issue Clinician Console alarm/warning
U4.3 Control Application signals PCA pump
UC5.4 tell pump to resume
U5.7 Indicate Normal Operation on Clinician Console
normal operation
PCA Pump
ICE Handler
UC4.4 pump KVO rate
U4.5 Signal Control Application of KVO
UC4.6 Display "Hazard Detected by Control Application pump rate=KVO"
pump KVO rate
U5.5 Resume Prescribed Infusion
U5.6 Tell Control Application infusion resumed
Clinician
U5.2 Determine if Safe to Resume
UC5.1 Clinician Check Patient
[is not safe]
error stop
[is safe]
UC5.3 Clear Control Application Alarm

Figure 10: Use Cases 4 and 5, Control Application-Detected Hazard

UC4-5

Related System Goals G2 and G3

Primary Actor Control Application (on Network Supervisor)

Precondition

- Steps 1 to 14 of Normal Operation Use Case completed
- Basal rate or bolus rate being infused
- PCA pump communicating with Control Application over network
- Monitoring device(s) communicating with Control Application over network
- Control Application app initialized and registered to PCA pump and monitoring devices

Postcondition

- KVO rate infusion

Main Success Scenario

1. Control Application determines that a patient-hazard may be occurring
2. Control Application issues alarm which displays and sounds on the Clinician Console
3. Control Application signals PCA pump to switch to KVO infusion rate
4. PCA pump switches to KVO infusion rate
5. PCA pump signals Control Application that it has switched to KVO rate infusion
6. Display “Hazard Detected by Control Application, pump rate=KVO” on Control Panel and Clinician Console

3.1.5 Use Case: Resume Operation After Externally-Detected Hazard (UC5)

subsubsec_uc5

This use case describes operation when the infusion rate had been switched to KVO because a Control Application determined a hazard may exist, and the clinician has determined it is safe to return to normal operation.

Related System Goals G1

Primary Actor Clinician

Precondition

- Control Application determined a hazard may exist
- Clinician notified of hazard by alarm on Clinician Console
- PCA pump switched to KVO infusion rate

Postcondition

- Normal operation resumed

Main Success Scenario

1. Clinician checks patient vital signs
2. Clinician determines it is safe to resume prescribed infusion, or stops pump
3. Clinician clears Control Application-generated alarm on Clinician Console
4. Control Application signals PCA pump to resume prescribed infusion
5. PCA pump resumes prescribed infusion
6. PCA pump signals Control Application and Control Panel of resumption
7. Control Application indicates normal operation has resumed on Clinician Console

3.1.6 Use Case: Audible Alarm Inactivation (UC6)

subsubsec_uc6

The Clinician using the Control Panel, or the Clinician Console, may inactive audible alarm indication either temporarily or indefinitely.

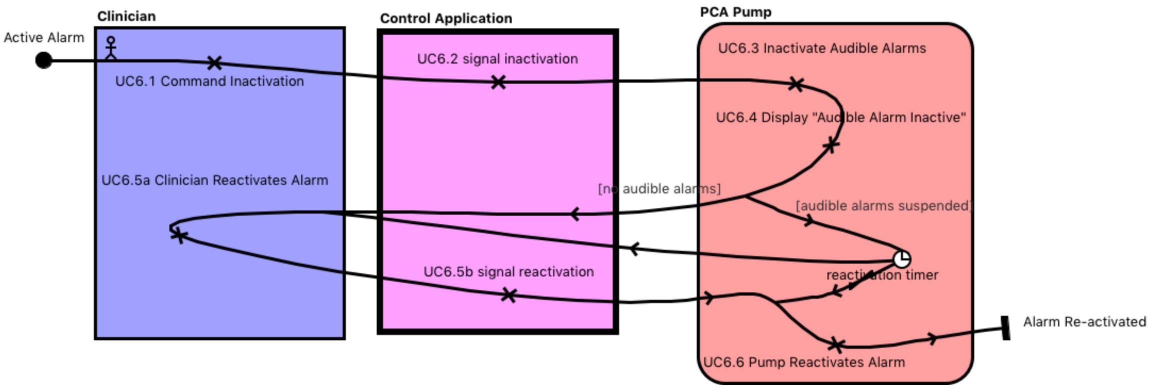

Active Alarm
Clinician
UC6.1 Command Inactivation
UC6.5a Clinician Reactivates Alarm
Control Application
UC6.2 signal inactivation
UC6.5b signal reactivation
PCA Pump
UC6.3 Inactivate Audible Alarms
UC6.4 Display "Audible Alarm Inactive"
[no audible alarms]
[audible alarms suspended]
reactivation timer
UC6.6 Pump Reactivates Alarm
Alarm Re-activated

Figure 11: Use Case 6, Audible Alarm Inactivation

fig_uc6

Related System Goals G3

Primary Actor Clinician

Precondition Normal operation

Postcondition

- Audible alarm on PCA pump inactivated;
- Visual indication of audible alarm inactivation

Main Success Scenario

1. Clinician using the Control Panel, or the Clinician Console, tells device to inactivate audible alarms either temporarily or indefinitely
2. PCA pump inactivates audible alarms
3. PCA pump indicates audible alarm inactivation to both the Control Panel and the Clinician Console
4. If temporary, alarm reactivates after alarm pause duration $\Delta_{ap} = 10$ minutes
5. Clinician may reactivate audible alarm from either the Control Panel, or the Clinician Console

Alternate Success Scenario

All alarms and warnings are cancelled upon pressing the stop button.

3.1.7 Use Case: Resume Infusion After Stop (UC7)

subsubsec_uc7

Resume infusion after stop. (See Figures 4 and 5)

Related System Goals

Primary Actor Clinician

Precondition Infusion Halted by Stop Button

Postcondition Resume previous normal operation

Main Success Scenario

1. Clinician presses Start Button
2. Previous normal operation resumes

3.1.8 Use Case: Flush (UC8)

subsubsec_uc8

Flush drug from pump after removal of needle before turning off.

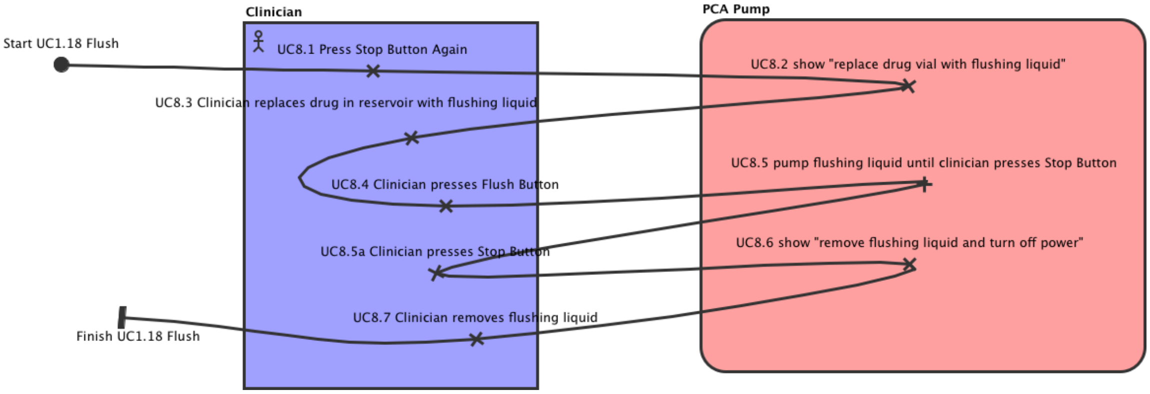

Clinician
PCA Pump
Start UC1.18 Flush
UC8.1 Press Stop Button Again
UC8.2 show "replace drug vial with flushing liquid"
UC8.3 Clinician replaces drug in reservoir with flushing liquid
UC8.4 Clinician presses Flush Button
UC8.5 pump flushing liquid until clinician presses Stop Button
UC8.5a Clinician presses Stop Button
UC8.6 show "remove flushing liquid and turn off power"
UC8.7 Clinician removes flushing liquid
Finish UC1.18 Flush

Figure 12: Use Case 8: Flush Pump

fig_uc8

Related System Goals

Primary Actor Clinician

Precondition

- Infusion Halted by Stop Button
- Needle Removed From Patient
- Infusion Tube Removed From Pump

Postcondition Drug Flushed from Pump

Main Success Scenario

1. Clinician presses Stop Button again
2. Message displayed to replace drug vial with flushing liquid
3. Clinician removes current drug in reservoir
4. Clinician scans drug to be used for flush and checks that it is correct
5. Clinician places flush liquid into the reservoir
6. Clinician presses Flush Button
7. Pump flushing liquid until Clinician presses Stop Button
8. Message displayed to remove flushing liquid, then turn off power
9. Clinician removes flushing liquid

3.1.9 Use Case: Prime Pump (UC9)

subsubsec_uc9

Pump drug through tube and needle to expel any residual air after loading drug into reservoir.

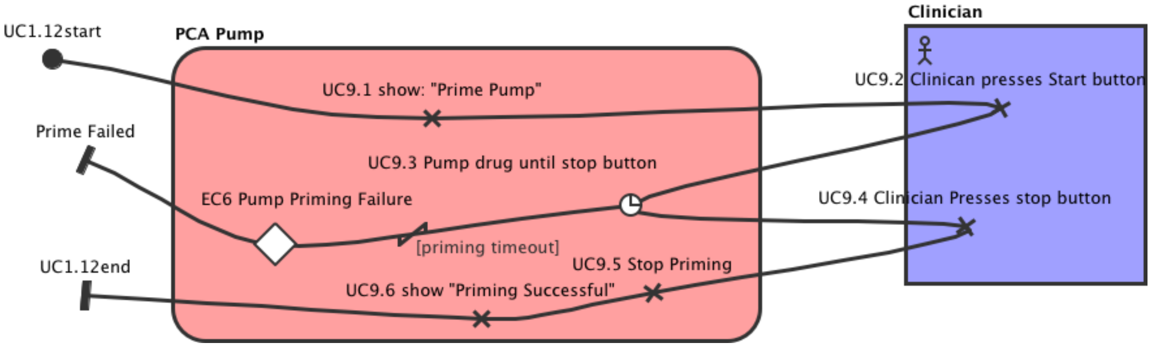

UC1.12start
PCA Pump
Clinician
UC9.1 show: "Prime Pump"
UC9.2 Clinican presses Start button
Prime Failed
UC9.3 Pump drug until stop button
EC6 Pump Priming Failure
UC9.4 Clinician Presses stop button
[priming timeout]
UC9.5 Stop Priming
UC1.12end
UC9.6 show "Priming Successful"

Figure 13: Use Case 9: Prime Pump

fig_uc9

Related System Goals

Primary Actor Clinician

Precondition

- Infusion Halted by Stop Button
- Needle Removed From Patient
- Infusion Tube Removed From Pump

Postcondition Drug Flushed from Pump

Main Success Scenario

1. Message displayed to start priming
2. Clinician presses Start Button
3. Pump drug until Clinician presses Stop Button (time-out Exception Case: Pump Priming Failure)
4. Clinician presses Stop Button before priming time-out
5. Stop pumping
6. Message displayed that priming was successful

3.2 Exception Cases

subsec_exceptioncases

The following exception cases describe unusual situations and the PCA pump's behavior for them. A summary of exception cases is provided in Table 2.

Table 2: Summary of PCA Exception Cases

ID	Actor	Title	Description
EC1	Patient or Clinician	Bolus Request Too Soon	bolus request denied because minimum time between boluses had not elapsed
EC2	Clinician	Drug Library Soft Limit	basal rate or bolus VTBI exceeded soft limit
EC3	Clinician	Drug Library Hard Limit	basal rate or bolus VTBI exceeded hard limit
EC4		Power-On Self Test Failure	power-on self test fails
EC5		Internal Electronic Failure	PCA pump detects its own failure
EC6	Clinician	Pump Priming Failure	pump fails to prime after loading drug reservoir
EC7		Over-Flow Rate Alarm	measured flow rate exceeds setting
EC8		Under-Flow Rate Alarm	measured flow rate below setting
EC9		Pump Overheating	pump temperature exceeds 55 C
EC10		Downstream Occlusion	blockage between pump and patient
EC11		Upstream Occlusion	blockage between reservoir and pump
EC12		Air-in-line Embolism	bubble detection
EC13		Maximum Safe Dose	dose reaches maximum allowed by drug library
EC14	Clinician	Clinician Authentication Failure	clinician not authorized to operate pump
EC15	Clinician	Patient Authentication Failure	patient not admitted to hospital
EC16	Clinician	Prescription Authentication Failure	drug or prescription not intended for this patient
EC17	Clinician	Sound Failure	no audible alarm
EC18		Network Failure	indication clinician console alarms disabled
EC19		Drug Library Not Present or Corrupted	the drug library fails authenticity or integrity check
EC20		Reservoir Low	little drug remaining
EC21		Reservoir Empty	no drug remaining
EC22		Diagnostic Detected Hazards	battery or power supply reservoir door open, self tests continuous fault detection fault masking, failure LED
EC23	Clinician	Alert-Stop-Sequence	repeated warning or alarm
EC24	Clinician	Inactivity Timeout	long pause after authentication

excase

3.2.1 Exception Case: Bolus Request Too Soon (EC1)

ec_bolusrequesttoosoon

A bolus is requested prior to prescribed minimum time elapsing between boluses.

Related System Goals G2 and G3

Primary Actor Patient or Clinician

Precondition Patient received recent bolus

Postcondition No bolus infused

Exception Success Scenario

1. Check of minimum time between boluses fails (Use Cases: Patient-Requested Bolus or Clinician-Requested Bolus)
2. Control Panel and Clinician Console (if connected) issue audible warning and display visual warning
3. Warning recorded in Fault Log

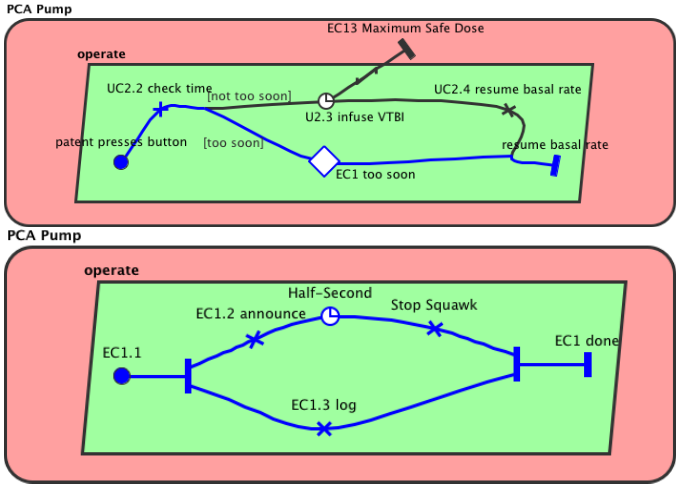


Figure 14: Exception Case 1, Bolus Request Too Soon EC1

3.2.2 Exception Case: Drug Library Soft Limit (EC2)

ec_druglibrarysoftlimit

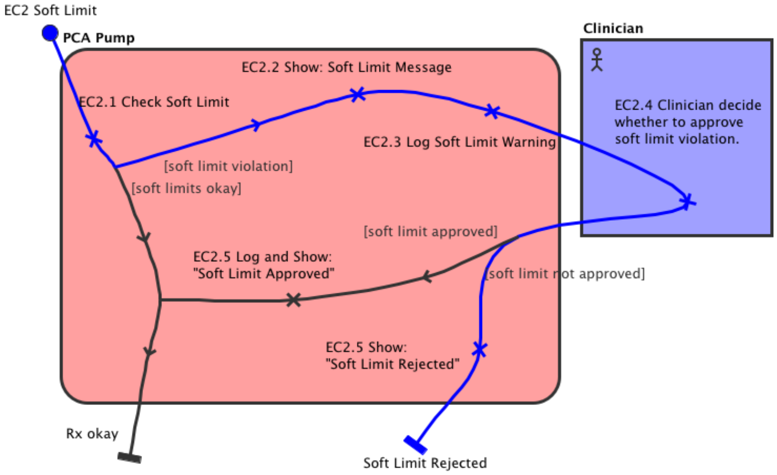

EC2 Soft Limit
PCA Pump
EC2.2 Show: Soft Limit Message
EC2.1 Check Soft Limit
EC2.3 Log Soft Limit Warning
[soft limit violation]
[soft limits okay]
Clinician
EC2.4 Clinician decide whether to approve soft limit violation.
[soft limit approved]
EC2.5 Log and Show: "Soft Limit Approved"
[soft limit not approved]
EC2.5 Show: "Soft Limit Rejected"
Rx okay
Soft Limit Rejected

Figure 15: Exception Case 2, Drug Library Soft Limit

EC2

Programmed or prescribed basal rate or bolus VTBI exceeds Drug Library soft limits.

Related System Goals G2 and G3

Primary Actor Clinician

Precondition Drug library loaded into PCA pump by pharmacy

Postcondition Either

- Clinician sets infusion rate within soft limits, or
- Clinician explicitly authorizes infusion rate exceeding soft limits

Exception Success Scenario

1. Detection that entered infusion rate exceeded soft limit of drug library by
   - less volume than VTBI Lower Soft limit
   - more volume than VTBI Upper Soft limit
   - smaller infusion rate than Basal Rate Lower Soft limit
   - greater infusion rate than Basal Rate Upper Soft limit
2. Warning sound and message on Control Panel and Clinician Console
3. Attempt to exceed soft limit recorded in Event Log
4. Clinician confirms or rejects VTBI or basal rate
   - If confirmed, programmed or prescribed rate used for infusion
   - if rejected, typical VTBI or basal rate from Drug Library used for infusion
5. Clinician confirmation or rejection recorded in Event Log

3.2.3 Exception Case: Drug Library Hard Limit (EC3)

ec_druglibraryhardlimit

Programmed or prescribed basal rate or VTBI exceeds Drug Library hard limits.

Related System Goals G2, G3 and G5

Primary Actor Clinician

Precondition Drug library loaded into PCA pump by pharmacy

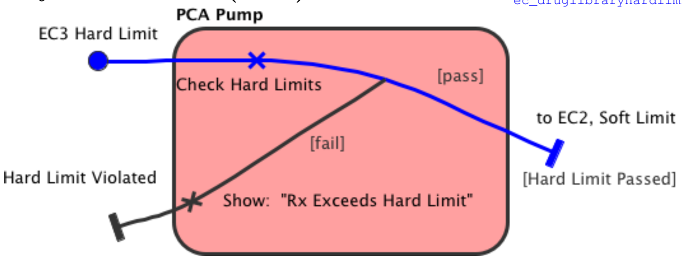


Figure 16: Exception Case 3, Drug Library Hard Limit

EC3

Postcondition Either

- Typical VTBI or basal rate from Drug Library used for infusion, or
- Clinician sets infusion rate within hard limits

Exception Success Scenario

1. Detection that entered infusion rate exceeded hard limit of drug library by
   - less volume than VTBI Lower Hard limit
   - more volume than VTBI Upper Hard limit
   - smaller infusion rate than Basal Rate Lower Hard limit
   - greater infusion rate than Basal Rate Upper Hard limit
2. Warning sound and message on Control Panel and Clinician Console
3. Typical VTBI or basal rate from Drug Library used for infusion
4. Attempt to exceed hard limit recorded in Fault Log
5. Clinician may try to program rate not exceeding hard limit

3.2.4 Exception Case: Power-On Self Test Failure (EC4)

ec_postfailure

Power-on self test (POST) fails.

Related System Goals G5

Primary Actor none

Precondition

- PCA pump connected to mains power
- PCA pump turned on

Postcondition

- Alarm sounded and displayed
- Infusion inhibited

Exception Success Scenario

1. POST fails
2. Alarm sounded and displayed by Control Panel and Clinician Console
3. Failure recorded in Fault Log
4. All infusion inhibited.

3.2.5 Exception Case: Internal Electronic Failure (EC5)

ec_electroinicfailure

Memory fails, processor fails, thread monitor fails, power supply fails, or battery fails during operation.

Related System Goals G5

Primary Actor none

Precondition normal operation

Postcondition

- Alarm sounded and displayed
- Infusion rate switched to KVO or halted

Exception Success Scenario

1. Electronic fault detected
   (a) Random-access memory fault, issue *RAM failure alarm*
   (b) Read-only memory fault, issue *ROM failure alarm*
   (c) Microprocessor fault, issue *CPU failure alarm*
   (d) Thread monitor fault, issue *thread monitor alarm*
   (e) Battery failure, issue *battery failure alarm*
   (f) Power supply voltage our of range, issue *voltage out-of-range alarm*
2. Alarm sounded and displayed by Control Panel and Clinician Console
3. Failure recorded in Fault Log
4. Infusion halted or switched to infusion rate in Table 4 PCA Pump Alarm Priority and Alarm Pump Rate.

3.2.6 Exception Case: Pump Priming Failure (EC6)

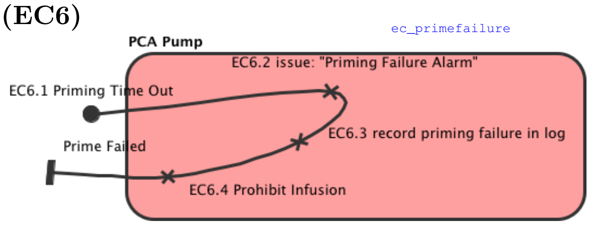


Figure 17: Exception Case 6, Priming Failure EC6

Pump fails to prime indicated by time-out while priming.

Related System Goals G5

Primary Actor Clinician

Precondition

- Drug loaded into reservoir
- Door Closed
- Tube attached

Postcondition

- Alarm sounded and displayed
- Infusion inhibited

Exception Success Scenario

1. Pump priming failure detected by time-out
2. *priming failure alarm* sounded and displayed by Control Panel and Clinician Console
3. Failure recorded in Fault Log
4. No infusion allowed

3.2.7 Exception Case: Over-Flow Rate Alarm (EC7)

ec_overflow

Measured drug flow rate exceeds programmed value by more than allowed tolerance.

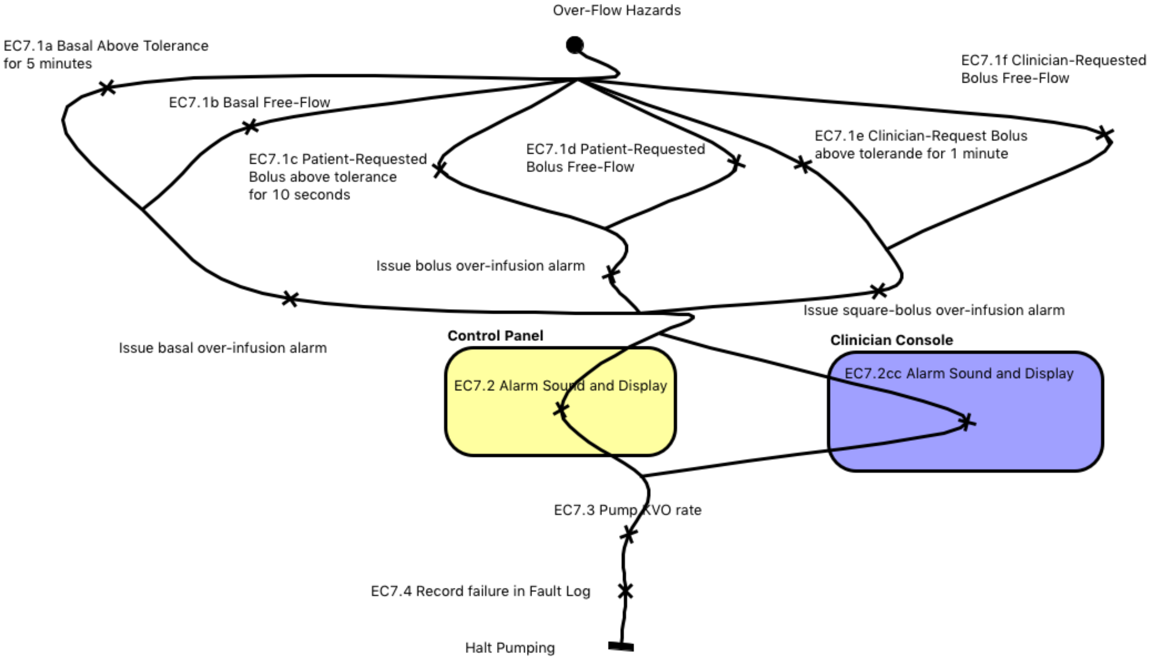

Over-Flow Hazards
EC7.1a Basal Above Tolerance for 5 minutes
EC7.1b Basal Free-Flow
EC7.1c Patient-Requested Bolus above tolerance for 10 seconds
EC7.1d Patient-Requested Bolus Free-Flow
EC7.1e Clinician-Request Bolus above tolerande for 1 minute
EC7.1f Clinician-Requested Bolus Free-Flow
Issue bolus over-infusion alarm
Issue square-bolus over-infusion alarm
Issue basal over-infusion alarm
Control Panel
EC7.2 Alarm Sound and Display
Clinician Console
EC7.2cc Alarm Sound and Display
EC7.3 Pump KVO rate
EC7.4 Record failure in Fault Log
Halt Pumping

Figure 18: Exception Case 7, Over-Flow Rate Alarm

EC7

Related System Goals G5

Primary Actor none

Precondition normal operation

Postcondition

- Alarm sounded and displayed
- Infusion halted

Exception Success Scenario

1. Measured drug flow rate checked
   (a) basal flow rate exceeds prescribed basal flow rate by more than its allowed tolerance over a period of more than 5 minutes, issue *basal over-infusion alarm*
   (b) basal flow rate goes into free flow, issue *basal over-infusion alarm* immediately
   (c) patient-requested bolus flow rate exceeds the prescribed patient-requested bolus rate setting by more than its allowed tolerance over a period of more than 10 seconds the pump shall issue a *bolus over-infusion alarm*

   (d) patient-requested bolus flow rate goes into free flow, issue a *bolus over-infusion alarm* immediately

   (e) clinician-requested bolus flow rate exceeds the prescribed patient-requested bolus rate setting by more than its allowed tolerance over a period of more than 1 minutes the pump shall issue a *square bolus over-infusion alarm*

   (f) clinician-requested bolus flow rate goes into free flow, issue a *square bolus over-infusion alarm* immediately

2. Alarm sounded and displayed by Control Panel and Clinician Console
3. Pump at KVO rate
4. Failure recorded in Fault Log

3.2.8 Exception Case: Under-Flow Rate Warning (EC8)

ec_underflow

Measured drug flow rate is less than programmed value by more than allowed tolerance.

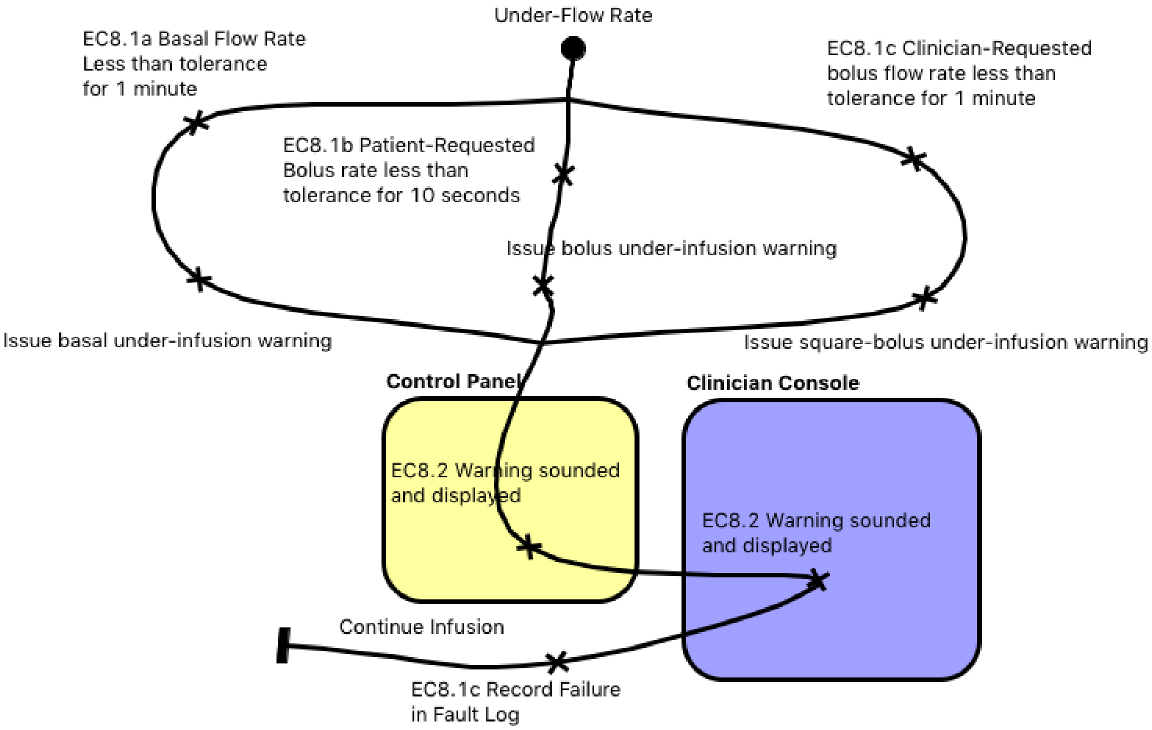

Under-Flow Rate
EC8.1a Basal Flow Rate Less than tolerance for 1 minute
EC8.1c Clinician-Requested bolus flow rate less than tolerance for 1 minute
EC8.1b Patient-Requested Bolus rate less than tolerance for 10 seconds
Issue bolus under-infusion warning
Issue basal under-infusion warning
Issue square-bolus under-infusion warning
Control Panel
Clinician Console
EC8.2 Warning sounded and displayed
EC8.2 Warning sounded and displayed
Continue Infusion
EC8.1c Record Failure in Fault Log

Figure 19: Exception Case 8, Under-Flow Rate Warning

EC8

Related System Goals G5

Primary Actor none

Precondition normal operation

Postcondition Alarm sounded and displayed

Exception Success Scenario

1. Measured drug flow rate
   (a) basal flow rate is less than prescribed basal flow rate by more than its allowed tolerance over a period of more than 5 minutes, issue *basal under-infusion warning*
   (b) patient-requested bolus flow rate is less than the prescribed patient-requested bolus rate by more than its allowed tolerance over a period of more than 10 seconds the pump shall issue a *bolus under-infusion warning*
   (c) clinician-requested bolus flow rate is less than the prescribed patient-requested bolus rate setting by more than its allowed tolerance over a period of more than 1 minutes

the pump issues a *square bolus under-infusion warning*

2. Warning sounded and displayed by Control Panel and Clinician Console
3. Failure recorded in Fault Log

3.2.9 Exception Case: Pump Overheating (EC9)

ec_pumphot

Pump temperature exceeds limit.

Related System Goals G5

Primary Actor none

Precondition normal operation

Postcondition

- Alarm sounded and displayed
- Infusion halted

Exception Success Scenario

1. Pump temperature exceeds 55 C, issue *pump overheated alarm*
2. Alarm sounded and displayed by Control Panel and Clinician Console
3. Pumping halted
4. Failure recorded in Fault Log

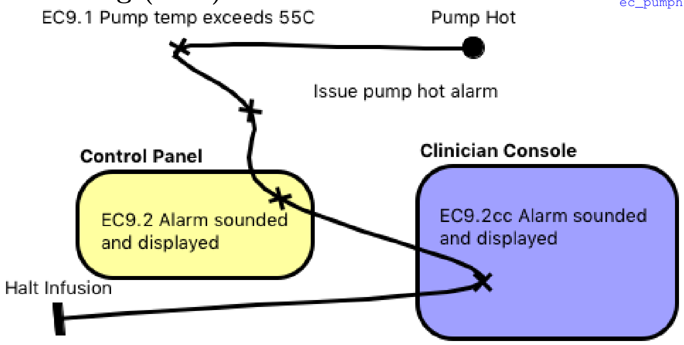

EC9.1 Pump temp exceeds 55C
Pump Hot
Issue pump hot alarm
Control Panel
Clinician Console
EC9.2 Alarm sounded and displayed
EC9.2cc Alarm sounded and displayed
Halt Infusion

Figure 20: Exception Case 9, Pump Overheating

EC9

3.2.10 Exception Case: Downstream Occlusion (EC10)

ec_dsocclusion

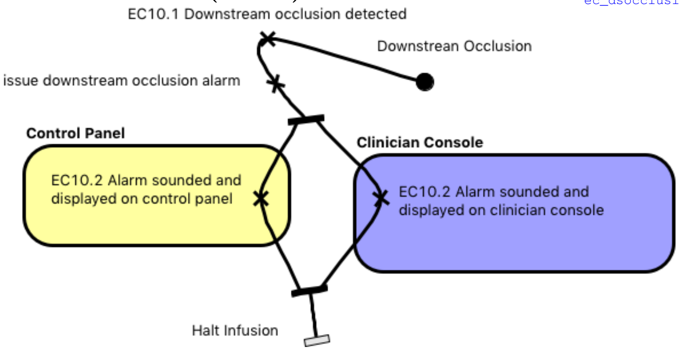

EC10.1 Downstream occlusion detected
Downstrean Occlusion
issue downstream occlusion alarm
Control Panel
Clinician Console
EC10.2 Alarm sounded and displayed on control panel
EC10.2 Alarm sounded and displayed on clinician console
Halt Infusion

Figure 21: Exception Case 10, Downstream Occlusion

EC10

Blockage detected between pump and patient.

Related System Goals G5

Primary Actor none

Precondition normal operation

Postcondition

- Alarm sounded and displayed
- Infusion halted

Exception Success Scenario

1. Downstream occlusion detected, issue *downstream occlusion alarm*
2. Alarm sounded and displayed by Control Panel and Clinician Console
3. Pumping halted
4. Failure recorded in Fault Log

3.2.11 Exception Case: Upstream Occlusion (EC11)

ec_usocclusion

Blockage detected between pump and patient.

Related System Goals G5

Primary Actor none

Precondition normal operation

Postcondition

- Alarm sounded and displayed
- Infusion halted

Exception Success Scenario

1. Upstream occlusion detected, issue *upstream occlusion alarm*
2. Alarm sounded and displayed by Control Panel and Clinician Console
3. Pumping halted
4. Failure recorded in Fault Log

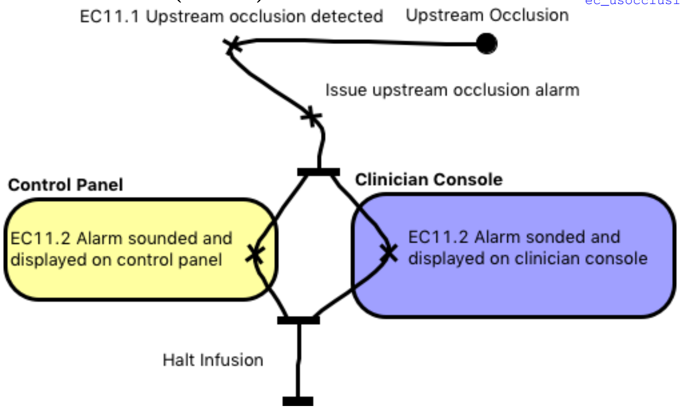

EC11.1 Upstream occlusion detected
Upstream Occlusion
Issue upstream occlusion alarm
Control Panel
Clinician Console
EC11.2 Alarm sounded and displayed on control panel
EC11.2 Alarm sonded and displayed on clinician console
Halt Infusion

Figure 22: Exception Case 11, Upstream Occlusion

EC11

3.2.12 Exception Case: Air-in-line Embolism (EC12)

ec_bubble

Air-in-line embolism (bubble) detected between pump and patient.

Related System Goals G4

Primary Actor none

Precondition normal operation

Postcondition

- Alarm sounded and displayed
- Infusion halted

Exception Success Scenario

1. Air-in-line embolism detected, issue *air-in-line embolism alarm*
2. Alarm sounded and displayed by Control Panel and Clinician Console
3. Pumping halted
4. Failure recorded in Fault Log

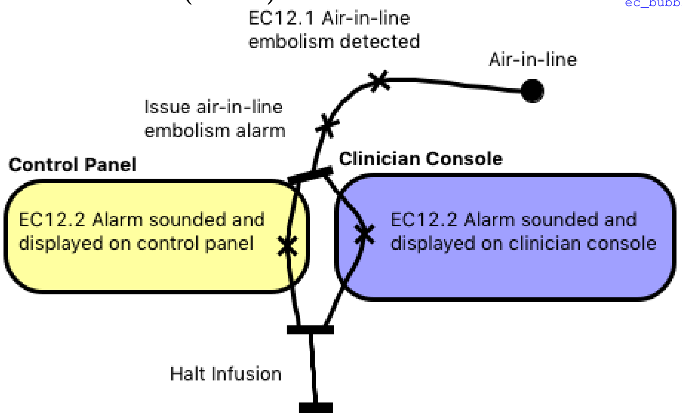

EC12.1 Air-in-line embolism detected
Air-in-line
Issue air-in-line embolism alarm
Control Panel
Clinician Console
EC12.2 Alarm sounded and displayed on control panel
EC12.2 Alarm sounded and displayed on clinician console
Halt Infusion

Figure 23: Exception Case 12, Air-in-line Embolism

EC12

3.2.13 Exception Case: Maximum Safe Dose (EC13)

ec_maxdose

Maximum dose of drug over period of time allowed by Drug Library reached.

Related System Goals G2

Primary Actor none

Precondition normal operation

Postcondition

- Alarm sounded and displayed
- Infusion switched to KVO rate

Exception Success Scenario

1. Total drug dose for period of time in Drug Library exceeded, issue *max dose warning*
2. Warning sounded and displayed by Control Panel and Clinician Console
3. Infusion switched to KVO rate
4. Event recorded in Fault Log and Event Log

3.2.14 Exception Case: Clinician Authentication Failure (EC14) ec_clinicianauthenticationfailure

Related System Goals G6

Primary Actor Clinician

Precondition

- Clinician badge scanned
- Information from badge fails authentication

Postcondition

- Display clinician authentication failure on Control Panel and Clinician Console
- Record clinician authentication failure in Event Log
- Inhibit pump operation

Exception Success Scenario

1. Pump cannot be operated by unauthorized person

3.2.15 Exception Case: Patient Authentication Failure (EC15)

ec_patientauthenticationfailure

Related System Goals G6

Primary Actor Clinician

Precondition

- Patient wristband scanned
- Information from wristband fails authentication

Postcondition

- Display patient authentication failure on Control Panel and Clinician Console
- Record patient authentication failure in Event Log
- Inhibit pump operation

Exception Success Scenario

1. Pump can only be used on admitted patients

Special Case

- In the event that the PCA Pump is unable to identify the patient (due to an issue with the patient's wristband, etc.), it may be necessary to allow authorization of a temporarily "Unidentified Patient" record to continue healthcare, and require clinicians to reconcile the discrepancy later.

3.2.16 Exception Case: Prescription Authentication Failure (EC16) ec_prescriptionauthenticationfailure

Related System Goals G6

Primary Actor Clinician

Precondition

- Drug container label scanned
- Information from label fails authentication

Postcondition

- Display prescription authentication failure on Control Panel and Clinician Console
- Record prescription authentication failure in Event Log
- Inhibit pump operation

Exception Success Scenario

1. Pump may only administer drug to the patient for which it was prescribed

3.2.17 Exception Case: Sound Failure (EC17)

ec_soundfailure

Related System Goals G5

Primary Actor Clinician

Precondition

- PCA pump plugged-in and turned-on
- Clinician (normal hearing) in room, nearby

Postcondition

- Display sound failure on Control Panel and Clinician Console
- Record sound failure in Event Log
- Inhibit pump operation

Exception Success Scenario

1. Pump may only administer drug to the patient when audible alarms can alert clinician(s) to a possibly-hazardous condition.

3.2.18 Exception Case: Network Failure (EC18)

ec_icefailure

The control panel will visually indicate when the PCA pump is not connected to an operational network. When the network fails, all alarms are reactivated, and is indicated visually on the control panel.

Related System Goals G3

Primary Actor PCA pump

Precondition PCA pump plugged-in and turned-on

Postcondition

- Lack of network connection indicated on control panel
- All alarms enabled

3.2.19 Exception Case: Drug Library Not Present or Corrupted (EC19) ec_libraryauthfail

The Drug Library is absent, corrupted, or incorrectly authenticated.

Related System Goals G2, G3 and G5

Primary Actor none

Precondition normal operation

Postcondition

- Alarm sounded and displayed
- Infusion halted

Exception Success Scenario

1. Alarm sounded and displayed by Control Panel and Clinician Console
2. Pumping halted
3. Failure recorded in Fault Log

3.2.20 Exception Case: Reservoir Low (EC20)

ec_reservoirlow

Remaining drug falls below reservoir low limit.

Related System Goals G1

Primary Actor none

Precondition normal operation

Postcondition Warning sounded and displayed; pump rate limited to basal rate

Exception Success Scenario

1. Remaining volume of drug falls below a reservoir low limit, either measured or determined
2. Warning sounded and displayed by Control Panel and Clinician Console
3. Pump rate limited to basal rate
4. Occurrence recorded in Fault Log

3.2.21 Exception Case: Reservoir Empty (EC21)

ec_reservoirempty

Remaining drug falls below reservoir empty limit.

Related System Goals G1

Primary Actor none

Precondition low drug (EC20)

Postcondition Alarm sounded and displayed; pumping halted

Exception Success Scenario

1. Remaining volume of drug falls below a reservoir empty limit, either measured or determined
2. Alarm sounded and displayed by Control Panel and Clinician Console
3. Pumping halted
4. Occurrence recorded in Fault Log

3.2.22 Exception Case: Diagnostic Detected Hazards (EC22)

ec_diagnostic

Internal diagnostics detect a hazard.

Related System Goals G1

Primary Actor none

Precondition normal operation

Postcondition depends on hazard

Exception Success Scenarios

a) **power supply** Because with either working battery or power supply can operate the pump, if the battery failure alarm and either the voltage out-of-range or the power supply failure alarms, then the pump rate will be off, otherwise the pump rate will continue at its previous value.

b) **reservoir door** An open door alarm is triggered when the reservoir door is opened while the pump is not stopped.

c) **self tests** Perform periodic self-tests to assure system integrity during long periods of use. Failure of a self-test shall raise a self-test alarm, stop pump, record it in the Fault Log, and display the reason for failure on the user interface.

d) **continuous fault detection** Continuously monitor faults.

e) **masked faults** Faults may be masked, but must be recorded.

f) **failure LED** Faults that cannot be displayed on the Control Panel will illuminate a LED indicating failure.

In all cases log the fault, raise alarm and change pump rate if warranted.

3.2.23 Exception Case: Alert-Stop-Start Sequence (EC23)

ec_alertstopstart

Repeated alert (alarm or warning) followed by attempt to resume infusion indicate a serious problem such as downstream occlusion. Therefore alert-stop-start sequences are limited.

Related System Goals G1

Primary Actor clinician

Precondition normal operation

Postcondition pumping halted

Exception Success Scenario

If the same alert-stop-start sequence occurs 3 or more times in ten minutes, infusion will be stopped, and an audible alarm sounded.

3.2.24 Exception Case: Inactivity Timeout (EC24)

ec_alertstopstart

Inactivity following clinician authentication indicates that the clinician may have been called away, thus requiring re-authentication.

Related System Goals

Primary Actor clinician

Precondition clinician authenticated and action expected

Postcondition require new clinician authentication

Exception Success Scenario

During initialization, following clinician authentication (UC1.4 §3.1.1) and before start of infusion (UC1.14), inactivity of $T_{to} = 3$ minutes will restart initialization at clinician authentication. Display ”inactivity timeout” for $T_{dt} = 3$ seconds.

Similarly, following clinician authentication for clinician requested bolus (UC3.2 §3.1.3) and before its commencement, (UC3.5) inactivity of $T_{to} = 3$ minutes will require new clinician authentication.

Part II

Requirements

part:requirements

4 PCA Pump Function

sec_function

The PCA pump infuses at prescribed basal, bolus, or KVO rates.

4.1 Basal Flow Rate

subsec_basalflow

(1) The *basal flow rate*[15] R4.1.0(1), F_{basal}, is prescribed by a physician, and entered into the PCA pump by scanning the prescription from the drug container label as it is loaded into the reservoir. (UC1.7 §3.1.1)

(2) The pump shall be able to deliver basal infusion at flows throughout the *basal infusion flow range*[16] R4.1.0(2) of $F_{basal\ min} = 1$ to $F_{basal\ max} = 10$ ml/hr. (UC1 §3.1.1)

(3) The pump shall deliver basal infusion at the prescribed basal rate within a *basal infusion flow tolerance*[17] R4.1.0(3) of $F_{basal\ tol} = 0.5$ ml/hr of the prescribed basal rate. par:basal_flow_rate_tolerance (UC1.12 §3.1.1)

(4) Any *alarm stops basal rate*[18] R4.1.0(4) delivery either halting pump or switching to KVO rate as defined in Table 4. (many EC)

(5) The pump shall maintain a *minimum KVO flow rate*[19] R4.1.0(5) of $F_{KVO} = 1$ ml/hr at all times during infusion, even during alarms, unless the alarm also stops flow, or the stop button is pressed. Table 4 defines which alarms also stop drug flow completely. (EC7.4 §3.2.7)

4.2 Patient-Requested Bolus

subsec_prbolus

(1) Upon patient's press of the PCA pump's patient-button, a prescribed bolus volume-to-be-infused, $VTBI$, of the drug loaded in the pump shall be delivered to the patient.[20] (UC2 §3.1.2)

(2) A *patient-requested bolus*[21] R4.2.0(2) shall be delivered at its prescribed rate, F_{bolus}, in addition to the prescribed basal flow rate, F_{basal}, but no more than the maximum flow rate for the pump, F_{max}. (UC2.3 §3.1.2)

(3) Patient-requested bolus shall not be delivered more often than a prescribed *minimum time between patient-requested bolus*[22] R4.2.0(3), Δ_{prb}. (UC2.2 §3.1.2)

(4) Prescribed $VTBI$ and rate shall not exceed the *maximum* $VTBI$[23] R4.2.0(4) limit set by the drug library from the hospital pharmacy for the drug loaded in the PCA pump. (EC3 §3.2.3)

(5) Patient-requested bolus shall *not* be delivered if infusing prescribed $VTBI$ will exceed hard limits retrieved from the drug library for the volume of drug infused over a period of time. Pump rate shall be reduced to KVO and a *max dose warning*[24] R4.2.0(5) be issued. (EC13 §3.2.13)

[15] requirement R4.1.0(1): *basal flow rate*

[16] requirement R4.1.0(2): *basal infusion flow range*

[17] requirement R4.1.0(3): *basal infusion flow tolerance*

[18] requirement R4.1.0(4): *alarm stops basal rate*

[19] requirement R4.1.0(5): *minimum KVO flow rate*

[20] Subject to safety constraints.

[21] requirement R4.2.0(2): *patient-requested bolus*

[22] requirement R4.2.0(3): *minimum time between patient-requested bolus*

[23] requirement R4.2.0(4): *maximum VTBI*

[24] requirement R4.2.0(5): *max dose warning*

(6) Any *alarm stops patient-requested bolus*[25] R4.2.0(6) delivery either halting pump or switching to KVO rate as defined in Table 4. (many EC)

4.3 Clinician-Requested Bolus

subsec_crbolus

(1) A clinician observing the discomfort of the patient may command the PCA pump to deliver a *square bolus* of the same volume-to-be-infused, $VTBI$, as patient-requested bolus over a period of time chosen by the clinician.[26] (UC3 §3.1.3)

(2) A *clinician-requested bolus*[27] R4.3.0(2) shall be delivered at the rate, F_{ccb}, of $VTBI$ divided by the duration chosen by the clinician, Δ_{ccb}, in addition to the prescribed basal flow rate, F_{basal}, but no more than the maximum flow rate for the pump, F_{max}. (UC3.3 §3.1.3)

$$F_{ccb} = min(VTBI/\Delta_{ccb} + F_{basal}, F_{max})$$

(3) A *patient-requested bolus takes precedence*[28] R4.3.0(3) over a clinician-requested bolus. The clinician-requested bolus shall be suspended while the patient-requested bolus dose is administered, and resumed afterward. (UC3.3 §3.1.3)

(4) Any *alarm halts clinician-requested bolus*[29] R4.3.0(4) delivery either halting pump or switching to KVO rate as defined in Table 4. (many EC)

(5) The *maximum clinician-chosen duration*[30] R4.3.0(5) for a clinician-requested bolus shall be $\Delta_{ccb\ max} = 6$ hours.

(6) The *minimum clinician-chosen duration*[31] R4.3.0(6) for a clinician-requested bolus shall be the prescribed minimum number of minutes between consecutive patient-requested bolus deliveries, Δ_{prb}.

(7) Clinician-commanded bolus shall be halted when continuing to infuse exceeds prescribed volume of drug infused over a period of time (ml/hr). Pump rate shall be reduced to KVO and a *max dose warning*[32] R4.3.0(7) be issued. (EC13 §3.2.13)

[25] requirement R4.2.0(6): *alarm stops patient-requested bolus*

[26] The prescription is determined by a physician. Duration for clinician-requested bolus is one of the few parameters chosen by the clinician.

[27] requirement R4.3.0(2): *clinician-requested bolus*

[28] requirement R4.3.0(3): *patient-requested bolus takes precedence*

[29] requirement R4.3.0(4): *alarm halts clinician-requested bolus*

[30] requirement R4.3.0(5): *maximum clinician-chosen duration*

[31] requirement R4.3.0(6): *minimum clinician-chosen duration*

[32] requirement R4.3.0(7): *max dose warning*

5 PCA Pump Interfaces

sec_interfaces

5.1 Sensors

subsec_sensors

(1) The PCA pump shall *measure drug flow*[33] R5.1.0(1) within a tolerance of $F_{mdf\ tol} = 0.1$ ml/hr. (many EC)

(2) The PCA pump shall *detect downstream occlusion*[34] R5.1.0(2). (EC10 §3.2.10)

(3) The PCA pump shall *detect upstream occlusion*[35] R5.1.0(3). (EC11 §3.2.11)

(4) The PCA pump shall *detect air-in-line embolism*[36] R5.1.0(4) (bubble). (EC12 §3.2.12)

5.2 Actuators

subsec_actuators

(1) The mechanical pump shall *pump drug*[37] R5.2.0(1) at prescribed flow rates for basal, bolus, and KVO infusion when commanded. (UC1 §3.1.1 UC2 §3.1.2 UC3 §3.1.3)

(2) The mechanical pump shall *halt pumping*[38] R5.2.0(2) when commanded, or caused in response to an alarm condition.(many EC)

(3) The mechanical pump shall not allow *reverse flow*[39] R5.2.0(3) from the patient into the pump. (Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff Table 3–Operational Sources, Retrograde Flow of Infusate)

5.3 Device Parameters

subsec_parameters

(1) The PCA pump shall use a physician's prescription as *device parameters*[40] R5.3.0(1). (UC1 §3.1.1 UC2 §3.1.2 UC3 §3.1.3)

5.4 Alarms

subsec_alarms

(1) The PCA pump shall *issue alarms and warnings*[41] R5.4.0(1) that require clinician attention. (many EC)

(2) If delivered basal flow rate exceeds the prescribed basal rate setting by more than its allowed tolerance over a period of more than 5 minutes, or immediately if the pump goes into free flow, the pump shall issue an *basal over-infusion alarm*[42] R5.4.0(2) (EC7 §3.2.7).

(3) If delivered basal flow rate is less than the prescribed basal rate setting by more than its allowed tolerance over a period of more than 5 minutes, or immediately if the flow stops, the pump shall issue an *basal under-infusion warning*[43] R5.4.0(3) (EC8 §3.2.8).

[33] requirement R5.1.0(1): *measure drug flow*
[34] requirement R5.1.0(2): *detect downstream occlusion*
[35] requirement R5.1.0(3): *detect upstream occlusion*
[36] requirement R5.1.0(4): *detect air-in-line embolism*
[37] requirement R5.2.0(1): *pump drug*
[38] requirement R5.2.0(2): *halt pumping*
[39] requirement R5.2.0(3): *reverse flow*
[40] requirement R5.3.0(1): *device parameters*
[41] requirement R5.4.0(1): *issue alarms and warnings*
[42] requirement R5.4.0(2): *basal over-infusion alarm*
[43] requirement R5.4.0(3): *basal under-infusion warning*

(4) If delivered patient-requested bolus flow rate exceeds the prescribed patient-requested bolus rate setting by more than its allowed tolerance over a period of more than 1 minutes, or immediately if the pump goes into free flow, the pump shall issue a *bolus over-infusion alarm*[44] R5.4.0(4) (EC7 §3.2.7).

(5) If delivered patient-requested bolus flow rate is less than the prescribed bolus rate setting by more than its allowed tolerance over a period of more than 1 minutes, or immediately if the flow stops, the pump shall issue a *bolus under-infusion warning*[45] R5.4.0(5) (EC8 §3.2.8).

(6) If delivered clinician-requested bolus flow rate exceeds the calculated square bolus rate by more than its allowed tolerance over a period of more than 5 minutes, or immediately if the pump goes into free flow, the pump shall issue a *square bolus over-infusion alarm*[46] R5.4.0(6) (EC7 §3.2.7).

(7) If delivered clinician-requested bolus flow rate is less than the calculated square bolus rate by more than its allowed tolerance over a period of more than 5 minutes, or immediately if the flow stops, the pump shall issue a *square bolus under-infusion warning*[47] R5.4.0(7) (EC8 §3.2.8).

(8) If the pump gets overheated to more than $T_{poh} = 55$ C, the pump shall issue an *pump overheated alarm*[48] R5.4.0(8) (EC9 §3.2.9).

Other alarm conditions are described in Section 6, Safety Requirements.

5.4.1 Alarm Priority

subsubsec_alarmpriority

(1) Alarm's and warning's *priority*[49] R5.4.1(1) shall be determined in accordance with standard IEC 60601-1-8 *Medical electrical equipment - Part 1-8: General requirements for safety - Collateral standard: Alarm systems - General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems.* Table 201 - Alarm Condition Priorities is reproduced as Table 3 for convenience. (IEC 60601-1-8 1.3.1)

Table 3: Alarm Condition Priorities

Potential result of failure to respond to the cause of Alarm Condition	Onset of potential harm		
	Immediate	Prompt	Delayed
Death or irreversible injury	HIGH	HIGH	MEDIUM
Reversible injury	HIGH	MEDIUM	LOW
Minor injury or discomfort	MEDIUM	LOW	LOW or no ALARM SIGNAL

acp

(2) Priority for alarms and warnings is shown in Table 4; warnings are low-priority alarms. The last column show the *alarm pump rate*[50] R5.4.1(2) to be used while the alarm is in effect. For "special" flow rates for power malfunctions see Section 6.3.

[44] requirement R5.4.0(4): *bolus over-infusion alarm*
[45] requirement R5.4.0(5): *bolus under-infusion warning*
[46] requirement R5.4.0(6): *square bolus over-infusion alarm*
[47] requirement R5.4.0(7): *square bolus under-infusion warning*
[48] requirement R5.4.0(8): *pump overheated alarm*
[49] requirement R5.4.1(1): *priority*
[50] requirement R5.4.1(2): *alarm pump rate*

Table 4: PCA Pump Alarm Priority and Alarm Pump Rate

Alarm	Potential Harm	Harm Onset	Priority	Pump Rate
basal over-infusion alarm	death	immediate	HIGH	KVO
bolus over-infusion alarm	death	immediate	HIGH	KVO
square bolus over-infusion alarm	death	immediate	HIGH	KVO
alert-stop-start sequence	discomfort	immediate	MEDIUM	KVO
air-in-line alarm	minor injury	immediate	MEDIUM	off
empty-reservoir alarm	discomfort	immediate	MEDIUM	off
pump overheated alarm	discomfort	immediate	MEDIUM	off
downstream occlusion alarm	discomfort	immediate	MEDIUM	off
upstream occlusion alarm	discomfort	immediate	MEDIUM	off
POST failure alarm	discomfort	delayed	LOW	off
RAM failure alarm	discomfort	delayed	LOW	off
ROM failure alarm	discomfort	delayed	LOW	off
CPU failure alarm	discomfort	delayed	LOW	off
thread monitor alarm	discomfort	delayed	LOW	off
battery failure alarm	discomfort	delayed	LOW	special
voltage out-of-range alarm	discomfort	delayed	LOW	special
power supply failure alarm	discomfort	delayed	LOW	special
max dose warning	discomfort	delayed	LOW	KVO
basal under-infusion warning	discomfort	delayed	LOW	basal
bolus under-infusion warning	discomfort	delayed	LOW	bolus
square bolus under-infusion warning	discomfort	delayed	LOW	bolus
battery-backup warning	discomfort	delayed	LOW	previous
low-battery warning	discomfort	delayed	LOW	KVO
low-reservoir warning	discomfort	delayed	LOW	KVO
long pause warning	discomfort	delayed	LOW	KVO

pap

(3) Because with either working battery or power supply can operate the pump, if the battery failure alarm and either the voltage out-of-range or the power supply failure alarms, then the pump rate will be off, otherwise the pump rate will continue at its previous value.[51] (EC22 §3.2.22)

5.4.2 Alarm Visual

subsubsec_alarmvisual

Requirements for alarm visibility are derived from standard IEC 60601-1-8 section 201.3.2.2 *Characteristics of visual ALARM SIGNALS*

(1) If a visual indicator is necessary for the clinician to identify the equipment or part of the equipment that requires clinician response or awareness, at least one *visual alarm signal*[52] shall be provided that:

1. indicates the priority of the highest priority alarm condition; and
2. can be perceived correctly at a distance of 4 m from the PCA pump.

(IEC 60601-1-8 1.3.1)

(2) The *alarm indicator appearance*[53] shall comply with color, flashing frequency, and duty cycle given in Table 5. (IEC 60601-1-8 1.3.1)

Table 5: Alarm Indicator Appearance

Alarm Category	Indicator Color	Flashing Frequency	Duty Cycle
HIGH	Red	1.4 Hz to 2.8 Hz	20% to 80% on
MEDIUM	Yellow	0.4 Hz to 0.8 Hz	20% to 60% on
LOW	Cyan	Constant (on)	100%

aia

(3) At least one visual alarm signal shall be provided that identifies the specific alarm condition and its priority. This signal shall be perceived correctly (be legible) at a distance of 1 m from the equipment or part of the equipment or from the clinician's position.[54] (IEC 60601-1-8 1.3.1)

(4) Visual alarms shall display *alarm symbols*[55] from Table D.201 *Graphical symbols for ALARM SYSTEMS* of standard IEC 60601-1-8. (IEC 60601-1-8 1.3.1)

5.4.3 Alarm Audible

subsubsec_alarmaudible

(1) Alarms shall cause *audible alarms signals*[56] that meet the requirements of Tables 203 and 204 of standard IEC 60601-1-8 for alarm pulses, bursts, and harmonics. (IEC 60601-1-8 1.3.1)

(2) The *auditory volume*[57] of audible alarms signals shall conform to Section 201.3.3.2 *Volume of auditory ALARM SIGNALS and INFORMATION SIGNALS* of standard IEC 60601-1-8. (IEC 60601-1-8 1.3.1)

[51] requirement R5.4.1(3): *power and battery failure*
[52] requirement R5.4.2(1): *visual alarm signal*
[53] requirement R5.4.2(2): *alarm indicator appearance*
[54] requirement R5.4.2(3): *see alarm signal*
[55] requirement R5.4.2(4): *alarm symbols*
[56] requirement R5.4.3(1): *audible alarms signals*
[57] requirement R5.4.3(2): *auditory volume*

(3) The *alarm melody*[58] R5.4.3(3) of audible alarms signals shall conform to Table AAA.1 of standard IEC 60601-1-8 for drug or fluid delivery. “C d g” shall be used for medium priority alarms; “C d g - C d” shall be used for high priority alarms; “e c” shall be used for warnings and low priority alarms.[59] (IEC 60601-1-8 1.3.1)

(4) Each tone in the alarm melody shall be composed of a minimum of 4 *harmonic components*[60] R5.4.3(4) in the range 300 Hz to 4000 Hz comprising an inverted 9th jazz chord. (IEC 60601-1-8 1.3.1)

The Control Panel panel, Section 5.5, and the network interface 5.7 allows audible alarm inactivation. (UC6 3.1.6)

(5) Temporarily paused alarms shall reactivate alarm pause duration $\Delta_{ap} = 10$ minutes after inactivation. (UC6.5 3.1.6)

5.4.4 Alarms Networked

subsubsec_alarmsnetworked

(1) Alarms shall be issued in order of occurrence.

(2) If alarms are inactivated or paused through the network interface, they shall be reactivated upon loss of connection to the network. (EC18 3.2.18)

5.5 Control Panel

subsec_controlpanel

(1) The *control panel*[61] R5.5.0(1) must display currently-programmed patient data, physician’s prescription, and current infusion rate. (G8)

(2) The PCA pump shall have a *start button*[62] R5.5.0(2). (UC1.14 §3.1.1 UC7.1 §3.1.7)

(3) Upon the clinician’s pressing of the start button, *start infusion*[63] R5.5.0(3) prescribed. (UC1.14 §3.1.1 UC7.1 §3.1.7)

(4) The control panel shall display *helpful messages*[64] R5.5.0(4). (G8)

(5) The PCA pump shall have a *stop button*[65] R5.5.0(5). (UC1.16 §3.1.1)

(6) Upon the clinician’s pressing of the stop button, *stop infusion*[66] R5.5.0(6). (UC1.16 §3.1.1)

(7) The control panel shall allow *clinician bolus request*[67] R5.5.0(7) and choice of duration. (UC3.1 §3.1.3)

(8) (removed)

(9) Prescriptions that violate the soft limits of the drug in the drug library shall issue a visible and audible warning requiring a *soft limit confirmation*[68] R5.5.0(9) by the clinician. (EC2 §3.2.2)

[58] requirement R5.4.3(3): *alarm melody*

[59] The characters c, d, e, g, C refer to relative musical pitches and C is one octave above c.

[60] requirement R5.4.3(4): *harmonic components*

[61] requirement R5.5.0(1): *control panel*

[62] requirement R5.5.0(2): *start button*

[63] requirement R5.5.0(3): *start infusion*

[64] requirement R5.5.0(4): *helpful messages*

[65] requirement R5.5.0(5): *stop button*

[66] requirement R5.5.0(6): *stop infusion*

[67] requirement R5.5.0(7): *clinician bolus request*

[68] requirement R5.5.0(9): *soft limit confirmation*

(10) Prescriptions that violate a *hard limit*[69] of the drug in the drug library shall be rejected with visible and audible indication when confirmation is attempted by the clinician. (EC3 §3.2.3)

(11) The Control Panel shall *show alarm*[70] condition as described in Section 5.4.2.[71] (IEC 60601-1-8 1.3.1)

(12) The Control Panel shall audibly *sound alarm*[72] condition as described in Section 5.4.3.[73] (IEC 60601-1-8 1.3.1)

(13) Pressing the *stop button silences all alarms* and terminates any alarm signal inactivation.[74] (UC6 §3.1.6)

(14) The Control Panel shall provide means to *inactivate audible alarms indefinitely*[75]. (UC6 §3.1.6)

(15) The Control Panel shall provide means to *inactivate audible alarms temporarily*[76] for a predefined period of time. (UC6.5 §3.1.6)

(16) The Control Panel shall provide means to *cancel alarm signal inactivation*[77]. (UC6.5 §3.1.6)

(17) When auditory alarms are inactive the control panel shall display an *inactive auditory alarm symbol*[78] from Table D.201 *Graphical symbols for ALARM SYSTEMS* of standard IEC 60601-1-8. (IEC 60601-1-8 1.3.1)

(18) If the same *alert-stop-start sequence*[79] occurs 3 or more times in ten minutes, infusion will be stopped, and an audible alarm sounded. (EC23 §**??**)

The Control Panel confirms operation after power-on self-test of

(19) *sound of audible alarm*[80], (UC1.2 §3.1.1 EC17 §3.2.17)

(20) *display of visual information*[81], and (UC1.2 §3.1.1)

(21) *tactile response*[82] (button press). (UC1.2 §3.1.1 EC17 §3.2.17)

(22) The PCA pump shall resume prescribed infusion when the Start button is pressed.[83] (UC7 §3.1.7)

(23) The PCA pump shall *display infusion rate*[84] currently pumping. (UC1.15 §3.1.1)

[69] requirement R5.5.0(10): *hard limit*
[70] requirement R5.5.0(11): *show alarm*
[71] requirement R5.5.0(11): *show alarm*
[72] requirement R5.5.0(12): *sound alarm*
[73] requirement R5.5.0(12): *sound alarm*
[74] requirement R5.5.0(13): *stop silences alarms*
[75] requirement R5.5.0(14): *inactivate audible alarms indefinitely*
[76] requirement R5.5.0(15): *inactivate audible alarms temporarily*
[77] requirement R5.5.0(16): *cancel alarm signal inactivation*
[78] requirement R5.5.0(17): *inactive auditory alarm symbol*
[79] requirement R5.5.0(18): *alert-stop-start sequence*
[80] requirement R5.5.0(19): *sound of audible alarm*
[81] requirement R5.5.0(20): *display of visual information*
[82] requirement R5.5.0(21): *tactile response*
[83] requirement R5.5.0(22): *resume infusion*
[84] requirement R5.5.0(23): *display infusion rate*

5.6 Logging

(1) The PCA pump shall maintain an electronic *event log*[85] R5.6.0(1) to record each action taken by the pump and each event sensed of its environment. (no UC or EC specific to logging)

(2) The PCA pump shall maintain an electronic *fault log*[86] R5.6.0(2) to record each fault condition, and the associated alarm and/or alert issued.

(3) Each log entry shall have a *time stamp*[87] R5.6.0(3) with its time of occurrence.

(4) The patient's prescription shall be retained[88] R5.6.0(4) for at least.$\Delta_{data} = 96$ hours after the PCA pump is turned-off and unplugged.

(5) Information in event and Fault Logs shall be retained[89] R5.6.0(5) for at least $\Delta_{log} = 1000$ hours after the PCA pump is turned-off and unplugged.

(6) The event log shall record 30 days of typical events before overwriting oldest event records first.[90] R5.6.0(6)

(7) The fault log shall record at least 1000 faults before overwriting oldest fault records first.[91] R5.6.0(7)

(8) A *real-time clock*[92] R5.6.0(8) must produce timestamps accurate to 10 ms.

5.7 Network Interface

subsec_iceinterface

The Network Interface allows the PCA pump to be monitored and controlled remotely, either by a clinician using a clinician console, through a network. These transactions may also be recorded in a patient's electronic health record (EHR). However, both clinician console and EHR are external to the PCA pump, with information sent or received on a *network*, not further defined by these requirements.

(1) The Network Interface shall transmit current operating status and infusion rate.[93] R5.7.0(1)

(2) The Network Interface shall transmit events, alarms, and warnings to the network.[94] R5.7.0(2)

(3) The Network Interface shall allow a clinician to set the duration of clinician-requested boluses through a clinician console.[95] R5.7.0(3) (UC3.1 §3.1.3)

(4) The PCA pump shall switch to KVO infusion rate when commanded through its Network Interface.[96] R5.7.0(4) (UC4.4 §3.1.4)

(5) The PCA pump shall resume prescribed infusion when commanded through its Network Interface.[97] R5.7.0(5) (UC5.5 §3.1.5)

[85] requirement R5.6.0(1): *event log*
[86] requirement R5.6.0(2): *fault log*
[87] requirement R5.6.0(3): *time stamp*
[88] requirement R5.6.0(4): *prescription retention*
[89] requirement R5.6.0(5): *log retention*
[90] requirement R5.6.0(6): *event log size*
[91] requirement R5.6.0(7): *fault log size*
[92] requirement R5.6.0(8): *real-time clock*
[93] requirement R5.7.0(1): *network operating status*
[94] requirement R5.7.0(2): *network alarms*
[95] requirement R5.7.0(3): *network bolus duration*
[96] requirement R5.7.0(4): *network KVO rate*
[97] requirement R5.7.0(5): *network resume infusion*

(6) When the PCA pump is not connected to a network, or the network connection fails, the PCA pump shall operate as a singular, *stand-alone*[98] device.

(7) The Network Interface may inactivate alarms.[99] (UC6 3.1.6)

5.8 Drug Reservoir

subsec_drugreservoir

(1) The *drug reservoir*[100] holds liquid pain-killer supplied by the hospital pharmacy and loaded into the PCA pump by the clinician. (UC1.10 §3.1.1)

(2) The drug reservoir shall measure its contents.[101] (EC20 §3.2.20 EC21 §3.2.21)

(3) The measured drug volume shall be within $V_{rt} = 1$ ml of the actual drug volume.[102]

(4) All filled prescriptions (liquid, narcotic pain-killer dispensed by the hospital pharmacy) must be labeled at least visibly with[103]

a. Patient name

b. Drug code

c. Name of drug

d. Concentration

e. Initial volume of drug

f. Basal flow rate

g. VTBI

h. Minimum time between bolus

i. Date prescription filled

j. Prescribing physician's name

k. Pharmacist name

Labels may show additional information. Labels should be difficult to counterfeit or modify without detection, only created and attached to filled prescriptions by a pharmacist in the hospital pharmacy. (UC1.7 §3.1.1)

(5) Prior to, or coincident with, loading the drug reservoir must also *enter prescription*[104] on the drug container's label using the scanner. (UC1.7 §3.1.1)

(6) A clinician must personally confirm the prescription[105] is for the patient to be infused. The routine procedures by which clinicians load the drug reservoir must ensure that the prescription filled by

[98] requirement R5.7.0(6): *stand-alone*
[99] requirement R5.7.0(7): *network inactivate alarms*
[100] requirement R5.8.0(1): *drug reservoir*
[101] requirement R5.8.0(2): *reservoir contents*
[102] requirement R5.8.0(3): *reservoir tolerance*
[103] requirement R5.8.0(4): *drug label*
[104] requirement R5.8.0(5): *enter prescription*
[105] requirement R5.8.0(6): *prescription confirmation*

the hospital pharmacy is meant for the patient (to be) connected to the PCA pump.[106] (UC1.7 §3.1.1)

(7) –removed

(8) The drug loaded into the reservoir must also be found in the PCA pump's *drug in library*[107]. The drug code of the prescription must match the drug code of a drug library entry. (UC1.9 §3.1.1)

(9) If the drug volume in the reservoir measures less than $V_{lra} = 1$ ml, and an infusion is in progress, a *low-reservoir warning*[108] shall be issued. (EC2 §3.2.2)

(10) If the drug volume in the reservoir measures less than V_{ers} =0.5 ml, and an infusion is in progress, an *empty-reservoir alarm*[109] shall be issued stopping the pump. (EC3 §3.2.3)

5.9 Drug Library

(1) The *drug library*[110] can be thought of as a lookup table that, given a drug name and a location, provides typical and safe limits of different infusion parameters. The drug library shall be determined by the hospital pharmacist, and loaded into the PCA pump via its communication port.

(2) For each drug that may be infused with a PCA pump, the *drug library entry*[111] for that drug shall have data elements listed in Table 6.[112]

(3) Before commencing infusion, the values of $VTBI$ and F_{basal} are checked against the drug library entry of the drug to be infused.[113] (UC1.9 §3.1.1)

(4) If the drug loaded into the drug reservoir is not present in the drug library, that the drug is unknown is indicated by the user interface, and recorded in the Fault Log. Pump remains stopped.[114] (UC1.9 §3.1.1)

5.10 Scanner

The *scanner* reads information from patient wristbands, clinician badges, and drug labels. It may read the information optically or by RFID.

(1) The scanner shall read and authenticate information from the *patient's wristband*[115]. (UC1.5 UC1.6 §3.1.1)

[106] This involves clinicians checking wristbands with names attached to filled prescriptions by the hospital pharmacy. This is a requirement placed by the PCA pump on its environment so that the pump may safely perform the prescription determined by the physician.

[107] requirement R5.8.0(8): *drug in library*

[108] requirement R5.8.0(9): *low-reservoir warning*

[109] requirement R5.8.0(10): *empty-reservoir alarm*

[110] requirement R5.9.0(1): *drug library*

[111] requirement R5.9.0(2): *drug library entry*

[112] This table of elements of drug library entries removes hard and soft limits upon drug concentration from the drug library entries in "PCA Pump Model.doc"; each different concentration of the same drug dispensed by the hospital pharmacy must have its own entry in the drug library.

[113] requirement R5.9.0(3): *drug library checking*

[114] requirement R5.9.0(4): *unknown drug*

[115] requirement R5.10.0(1): *patient's wristband*

Table 6: Data Elements of a Drug Library Entry

Element Name	**Explanation**
Drug Code	Unique identifier of the drug and its concentration
Drug Name	Name of the drug
Location	Context of drug application
Dose Rate Unit	The unit of drug dose (for example milliliters/hour)
VTBI Unit	The unit of VTBI (for example milliliter)
Amount	The weight of the drug dissolved in the diluent
Concentration	Drug concentration; as prescribed
VTBI Lower Soft	Lower soft limit of drug volume to be infused
VTBI Lower Hard	Lower hard limit of drug volume to be infused
VTBI Typical	Typical drug volume to be infused
VTBI Upper Soft	Upper soft limit of drug volume to be infused
VTBI Upper Hard	Upper hard limit of drug volume to be infused
Basal Rate Lower Soft	Lower soft limit of basal drug dose rate
Basal Rate Lower Hard	Lower hard limit of basal drug dose rate
Basal Rate Typical	Typical basal drug dose rate
Basal Rate Upper Soft	Upper soft limit of basal drug dose rate
Basal Rate Upper Hard	Upper hard limit of basal drug dose rate
Bolus Typical	Typical Value of Bolus Volume
Bolus Time Typical	Typical duration of clinician commanded bolus

tab:druglibraryentry

(2) The scanner shall read and authenticate information from the *clinician's badge*R5.10.0(2)[116]. (UC1.3 UC1.4 §3.1.1)

(3) The scanner shall read and authenticate information from the *drug's package label*R5.10.0(3)[117]. (UC1.7 UC1.8 §3.1.1)

[116] requirement R5.10.0(2): *clinician's badge*

[117] requirement R5.10.0(3): *drug's package label*

6 Safety Requirements

sec_safetyrequirements

Because PCA pumps can harm or kill patients, safety is paramount. Although the only safe medical devices are those that are never used, adequate safety can be achieved by a combination of proper use, proper operation, and device features that detect faults and anomalies, changing behavior accordingly.

6.1 Safety Architecture

(1) The PCA pump shall implement a *safety architecture*[118] R6.1.0(1) that separates normal operation from fault detection and response. (reference to Safety Architecture paper)

6.2 Anomaly Detection and Response

sec_anomalydetectionandresponse

(1) When the stop button is pressed, the current pump stroke shall be completed prior to stopping the pump.[119] R6.2.0(1) (applicable to *metering pumps*, `https://en.wikipedia.org/wiki/Metering_pump`)

(2) During normal use and/or single fault condition of the equipment, *continuous reverse delivery*[120] R6.2.0(2) shall not be possible. (IEC 60601-2-24 1.3.1)

(3) An *air-in-line alarm*[121] R6.2.0(3) shall be triggered by the pump if detectable air bubbles are infused into the patient.[122] (EC12 §3.2.12)

(4) An *upstream occlusion alarm*[123] R6.2.0(4) shall be triggered when the pump senses an upstream (drug reservoir side) occlusion exceeding $P_{uo} = 1$ psi. (EC11 §3.2.11)

(5) A *downstream occlusion alarm*[124] R6.2.0(5) shall be triggered if the pump senses a downstream (patient side) occlusion exceeding $P_{do} = 10$ psi. (EC10 §3.2.10)

(6) When an *occlusion alarm*[125] R6.2.0(6) occurs, the pump shall be stopped immediately without completing
the current pump stroke.[126] (EC10 §3.2.10 EC11 §3.2.11) ? (7) When an *empty-reservoir*
alarm[127] R6.2.0(7) occurs, the current pump stroke shall be completed prior to stopping the pump.[128] (EC21
§3.2.21)

(8) An *open door alarm*[129] R6.2.0(8) shall be triggered when the reservoir door is opened while the pump is not stopped. (EC23b §3.2.22)

[118] requirement R6.1.0(1): *safety architecture*

[119] requirement R6.2.0(1): *complete pump stroke*

[120] requirement R6.2.0(2): *continuous reverse delivery*

[121] requirement R6.2.0(3): *air-in-line alarm*

[122] Detecting the smallest-possible air bubble is a goal, not a requirement.

[123] requirement R6.2.0(4): *upstream occlusion alarm*

[124] requirement R6.2.0(5): *downstream occlusion alarm*

[125] requirement R6.2.0(6): *occlusion alarm*

[126] If the mechanical pump chosen has a pump stroke.

[127] requirement R6.2.0(7): *empty-reservoir alarm*

[128] If the mechanical pump chosen has a pump stroke.

[129] requirement R6.2.0(8): *open door alarm*

6.3 Power Supply

sec_powersupply

Many crucial medical devices continue to operate on battery backup when mains electricity supply fails.

(1) The PCA pump shall continue to infuse for 10 minutes during interruption of mains electricity supply using *battery backup*[130] R6.3.0(1), either continuously or spread over an hour. (Five minutes to recharge per minute using battery.)

(2) The user interface must show that the PCA pump is working on battery backup, and an estimate of the number of minutes of battery-powered infusion remain.[131] R6.3.0(2)

(3) The estimate of remaining battery energy must be accurate to within $X_{btty} = 25\%$.[132] R6.3.0(3)

(4) If the estimated battery life remaining is less than $\Delta_{lba} = 3$ minutes, the pump shall issue a *low-battery warning*[133] R6.3.0(4).

(5) The PCA pump shall detect battery failure and issue a *battery failure alarm*[134] R6.3.0(5).

(6) The PCA pump shall detect power supply voltage out-of-range, issue a *voltage out-of-range warning*[135] R6.3.0(6), and switch to battery backup when out-of-range.

(7) The PCA pump must not leak current greater than 150 µA.[136] R6.3.0(7) (UL 60601-1 for Class II device in patient-care area)

(8) Component failure must not harm patient (beyond stopping function).[137] R6.3.0(8)

(9) The PCA pump must be *electromagnetically compatible*[138] R6.3.0(9) according to IEC 60601-1-2 (2001) *Medical Electrical Equipment, Part 1: General Requirements for Safety, 2. Collateral Standard: Electromagnetic Compatibility - Requirements and Tests.* (IEC 60601-1-2 1.3.1)

(10) The PCA pump must withstand *electrostatic discharge*[139] R6.3.0(10).

(11) The PCA pump must *filter power interference*[140] R6.3.0(11) from mains.

6.4 Diagnostics and Fail-Stop

Correct operation depends on system (hardware) integrity. Typically this is assured by power-on-self-tests, periodic self-tests, and continuous fault-detection and masking. These requirements demand *assurance*; how that assurance is achieved is left up to the designer.

(1) The PCA pump shall perform a *power-on self-test*[141] R6.4.0(1) (POST) to assure system integrity after being turned on, yet before any infusion begins. Failure of POST shall raise a *POST alarm*, stop

[130] requirement R6.3.0(1): *battery backup*
[131] requirement R6.3.0(2): *remaining battery minutes*
[132] requirement R6.3.0(3): *remaining battery accuracy*
[133] requirement R6.3.0(4): *low-battery warning*
[134] requirement R6.3.0(5): *battery failure alarm*
[135] requirement R6.3.0(6): *voltage out-of-range warning*
[136] requirement R6.3.0(7): *leakage current*
[137] requirement R6.3.0(8): *component failure*
[138] requirement R6.3.0(9): *electromagnetically compatible*
[139] requirement R6.3.0(10): *electrostatic discharge*
[140] requirement R6.3.0(11): *filter power interference*
[141] requirement R6.4.0(1): *power-on self-test*

pump, record it in the Fault Log, and display the reason for failure on the user interface. (EC4 §3.2.4)

(2) The PCA pump shall perform *periodic self-tests*[142] to assure system integrity during long periods of use. Failure of a self-test shall raise a *self-test alarm*, stop pump, record it in the Fault Log, and display the reason for failure on the user interface. (EC22c §3.2.22)

(3) The PCA pump shall have *continuous fault-detection*[143] and masking. Hardware monitors of thread heartbeat, memory error correction codes are examples. (EC22d §3.2.22)

(4) Occurrence of unavoidable *single-event upsets*[144] caused by cosmic-ray-induced high- and thermal-energy neutrons must be either masked, or detected to fail-stop. (EC22d §3.2.22)

(5) Successfully *masked faults*[145] shall be recorded in the Fault Log, but not raise an alarm. (EC22e §3.2.22)

(6) All unmasked *hardware detected faults*[146] shall raise a fault alarm, stop pump, record it in the Fault Log, and display the reason for fault on the user interface. (EC22 §3.2.22)

(7) Hardware faults that prevent operation of the Control Panel shall illuminate a *hardware fault indicator*[147] (light-emitting diode). (EC22f §3.2.22)

6.5 Tamper-Resistant Door

(1) Because the drugs used for analgesia are often narcotic, requiring Drug Enforcement Agency (DEA) tracking if used in the United States, the drug reservoir and means to change prescriptions during infusion must be inhibited with a locked, *tamper-resistant door*[148].

(2) Before infusion, the door must be closed and locked.[149] (UC1.10 §3.1.1)

(3) Hospital procedures must endow the attending clinician access to the *door key*[150], yet prevent other persons' access. Key-handling processes are beyond the scope of these requirements, but much depends on the attending clinician: it's the right drug, in the right patient, with the right prescription from a physician authorized to prescribe narcotics for those suffering great pain.

(4) The PCA *pump case*[151] must be at least difficult to breech as its tamper-resistant door. Breaking the case shall not be easier to access the drug reservoir than breeching the door.

6.6 Biocompatibility

(1) All materials that contact fluid shall be *biocompatible*[152].

[142] requirement R6.4.0(2): *periodic self-tests*
[143] requirement R6.4.0(3): *continuous fault-detection*
[144] requirement R6.4.0(4): *single-event upsets*
[145] requirement R6.4.0(5): *masked faults*
[146] requirement R6.4.0(6): *hardware detected faults*
[147] requirement R6.4.0(7): *hardware fault indicator*
[148] requirement R6.5.0(1): *tamper-resistant door*
[149] requirement R6.5.0(2): *door closed and locked*
[150] requirement R6.5.0(3): *door key*
[151] requirement R6.5.0(4): *pump case*
[152] requirement R6.6.0(1): *biocompatible*

(2) The PCA pump shall be *cleaned and disinfected*[153] after use.

6.7 Mechanical

(1) The PCA pump shall *minimize drug leakage*[154].

[153] requirement R6.6.0(2): *cleaned and disinfected*

[154] requirement R6.7.0(1): *minimize drug leakage*

7 Security

The PCA pump uses security processes, sparingly, to minimize erroneous usage and control access to patient information. These security processes include encryption (for confidentiality), hashing (for authentication), key generation, and key repository.

7.1 Authentication

(1) Clinicians authorization to operate the PCA pump must be authenticated.[155] R7.1.0(1) (UC1.4 §3.1.1)

(2) Patient's identity and admittance to the hospital must be authenticated.[156] R7.1.0(2) (UC1.6 §3.1.1)

(3) Drug container must have a valid prescription for the particular patient to be infused by the PCA pump.[157] R7.1.0(3) (UC1.8 §3.1.1)

(4) Drug library information shall be authenticated before it is accepted.[158] R7.1.0(4)

7.2 Confidentiality

(1) Patient information must be restricted to those providing care for the patient, and the patient.[159] R7.2.0(1)

7.3 Provisioning

(1) Provisioning of initial security keys which form a root of trust must require physical connection to a jack distinct from normal operation.[160] R7.3.0(1)

(2) The provisioning jack must be physically inaccessible, except to authorized technical personnel.[161] R7.3.0(2) Jacks for test equipment must be similarly inaccessible.

(3) Provisioning (or re-provisioning) shall not be possible through a network.[162] R7.3.0(3)

(4) Provisioning shall be a single, unitary block-transfer.[163] R7.3.0(4)

Each of the requirements in preceding sections, must be allocated to an architectural component in section 9 or labeling in section 8, following.

[155] requirement R7.1.0(1): *clinician authentication*
[156] requirement R7.1.0(2): *patient authentication*
[157] requirement R7.1.0(3): *prescription authentication*
[158] requirement R7.1.0(4): *drug library authentication*
[159] requirement R7.2.0(1): *confidentiality*
[160] requirement R7.3.0(1): *provisioning jack*
[161] requirement R7.3.0(2): *protected jack*
[162] requirement R7.3.0(3): *provisioning channel disjointness*
[163] requirement R7.3.0(4): *provisioning unitarily*

Part III

Labeling and Architecture

part:architecture

8 Labeling of Nonfunctional Requirements

sec_labeling

Some system requirements (environmental or nonfunctional) are properly allocated to medical device *labeling*.[164]

Requirements for temperature range, atmospheric pressure, humidity, and splashing must be met by the user as listed in device labeling. Drug containers must be labeled with patient name, drug code, name of drug, concentration, initial volume in container, prescribed basal flow rate, VTBI, minimum time between bolus, date of filling, prescribing physician, and pharmacist's name.

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

Allocated Requirements
R2.4.0(1) temperature range
R2.4.0(2) atmospheric pressure
R2.4.0(3) relative humidity
R2.4.0(4) splashing
R5.8.0(4) drug label
R6.6.0(2) cleaned and disinfected

Non-functional electrical requirements that must be upheld by the design.

Allocated Requirements
R6.3.0(7) leakage current
R6.3.0(8) component failure
R6.3.0(9) electromagnetically compatible
R6.3.0(10) electrostatic discharge
R6.3.0(11) filter power interference

[164] Labeling is a term-of-art for FDA encompassing not just what written on the product itself, but its packaging, user manuals, and even advertisements and presentations made by sales staff. Fobbing-off requirements onto labeling should be shunned.

9 Functional Architecture

sec_functionalarchitecture

The context for using the PCA pump is depicted in Figure 3. A *patient* receives infused drug, and requests more by pushing the patient button. A *nurse* (a.k.a. clinician) sees, hears, and touches the control panel on the PCA pump. The PCA pump is connected to a network, along with other medical devices. The PCA pump interacts with software (a.k.a. app) running on the network supervisor processor that controls the network. The app may coordinate the operation of the PCA pumps with other medical devices. The app also displays information and on a console at a nurses station, and transmits commands from the console to the PCA pump. A technician may connect a cable to a protected maintenance jack, through which logs can be queried, drug library may be installed, and security can be provisioned.

The PCA Pump *functional architecture* partitions system operation into smaller, simpler pieces, recursively. The PCA Pump's top-level functional architecture is shown in Figure 24. The behaviors of each component are summarized in Table 7.

Table 7: Functional Components

Component	**Behavior**	§
operation	controls pump operation	9.1
safety	checks for hazard occurrence; inhibits possibly harmful infusion; signals alarms and warnings	9.2
power	coordinates battery and power supply; detects power anomalies	9.5
fluid	devices that perform medical function	**??**
communication	networking to patient health record; nurse's station console; other medical devices	9.5
security	authentication, signing, encryption, decryption	9.7
gui	graphical user interface; touchscreen, controller, software	9.8

tabl:fc

9.1 Operation Subsystem

subsec_operation

The *operation subsystem*, depicted in Figure 25, controls the medical function of the PCA pump. The operation software is contained in the Operation Process which proves a protected address space. An abstract component models the function of a scanner (optical or RFID) which get bound to an actual device.

9.1.1 Operation Process

The *operation process* contains threads for drug library and event logging, and a thread group holding threads that work closely together as depicted in Figure 26.

9.1.2 Drug Library Thread

The *drug library thread* stores the drug library provided by the hospital pharmacy, and retrieves the drug record corresponding to the drug loaded into the reservoir.

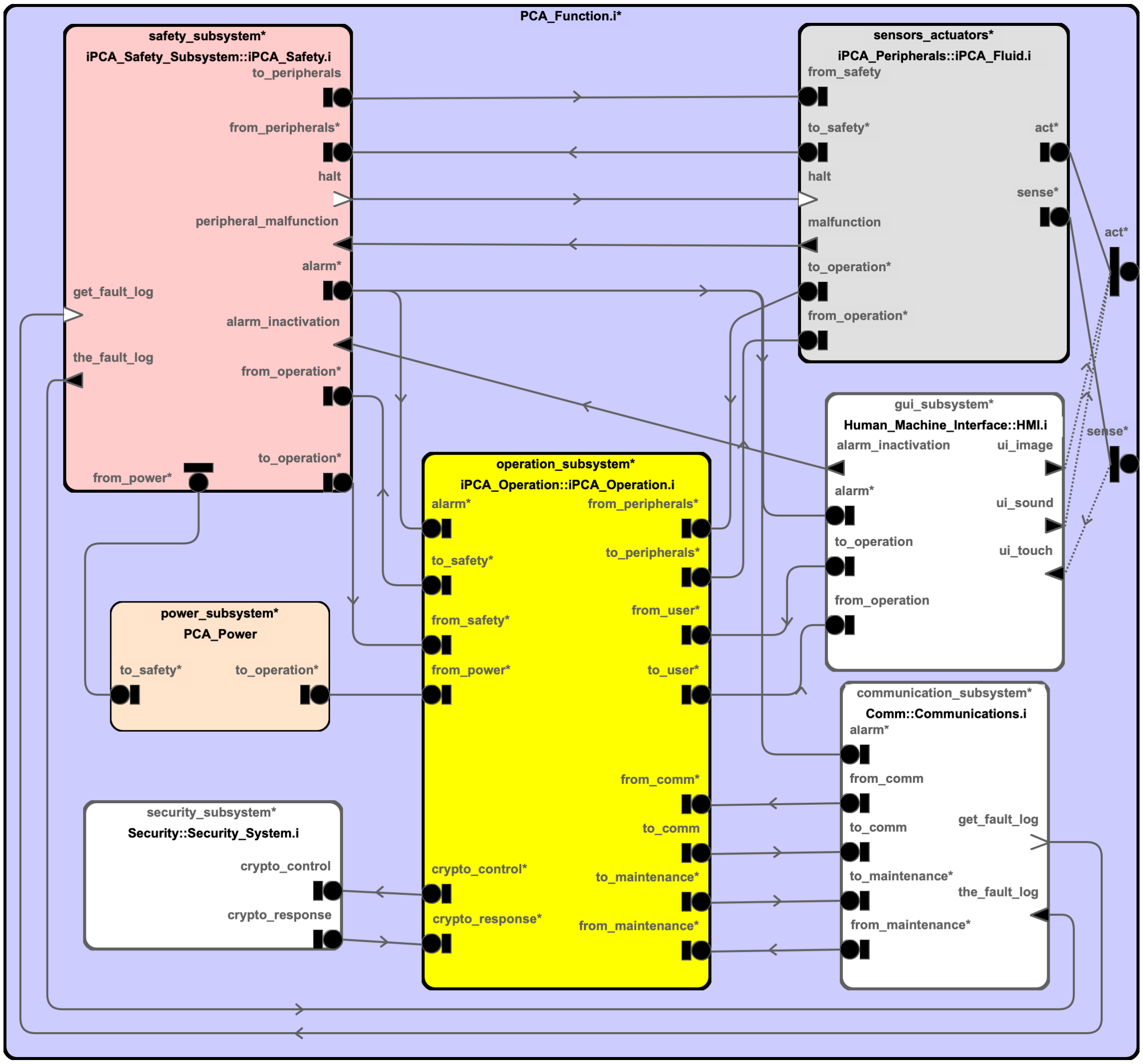


Figure 24: PCA Pump Functional Architecture (Top-Level)

fig_fa

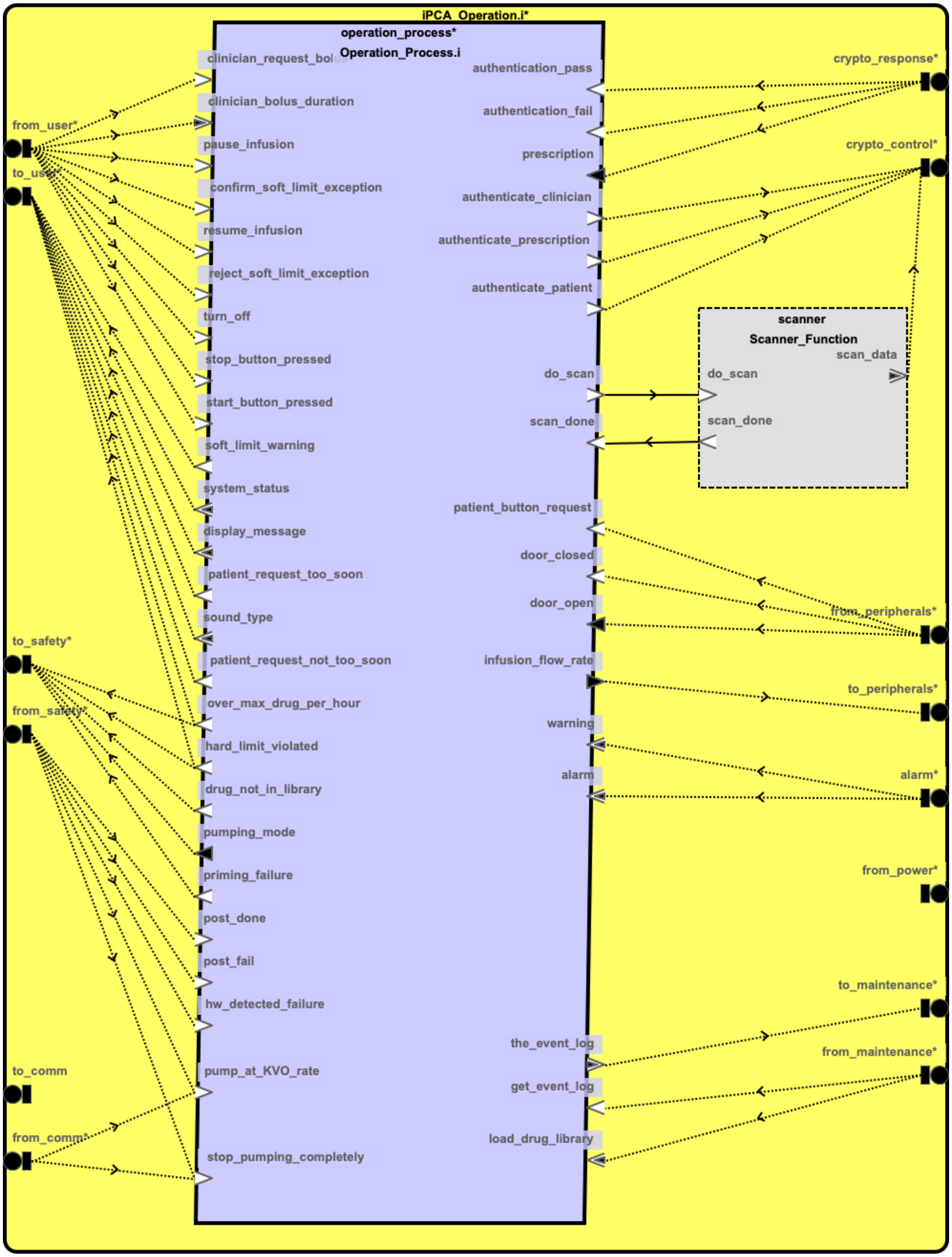


Figure 25: Operation Subsystem

fig_op

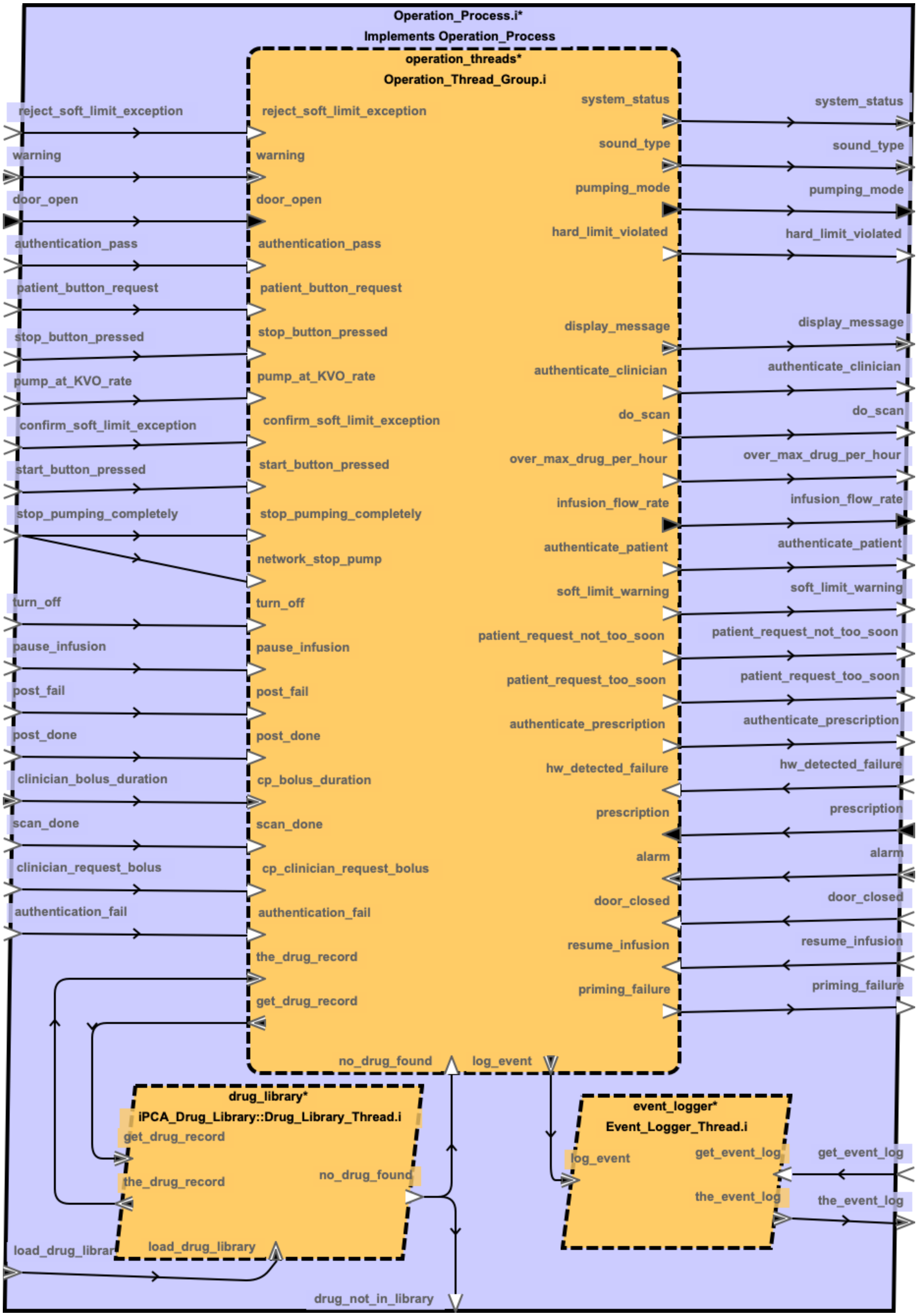


Figure 26: Operation Process

fig_cat

Allocated Requirements
R5.8.0(8) drug in library
R5.9.0(1) drug library
R5.9.0(2) drug library entry
R5.9.0(3) drug library checking
R5.9.0(4) unknown drug

9.1.3 Event Logger Thread

The *event logger thread* records all actions or events for later review or audit.

Allocated Requirements
R5.6.0(1) event log
R5.6.0(3) time stamp
R5.6.0(5) log retention
R5.6.0(6) event log size

9.1.4 Operation Thread Group

The *operation thread group* (Figure 27) combines operation threads that work together in a single component.

9.1.5 Boss Thread

The *boss thread* coordinates and controls the other threads.

9.1.6 Rate Controller Thread

subsec_ratecontrollerthread

The *rate controller thread* determines the pump rate.

Allocated Requirements
R4.1.0(1) basal flow rate
R4.1.0(5) minimum KVO flow rate
R4.2.0(2) patient-requested bolus
R4.1.0(4) alarm stops basal rate
R4.2.0(6) alarm stops patient-requested bolus
R4.3.0(2) clinician-requested bolus
R4.3.0(3) patient-requested bolus takes precedence
R4.3.0(4) alarm halts clinician-requested bolus
R4.3.0(7) max dose warning
R5.2.0(2) halt pumping
R5.5.0(3) start infusion
R5.5.0(6) stop infusion
R6.5.0(2) door closed and locked

9.1.7 Prescription Checker Thread

The *prescription checker thread* checks hard and soft limits.

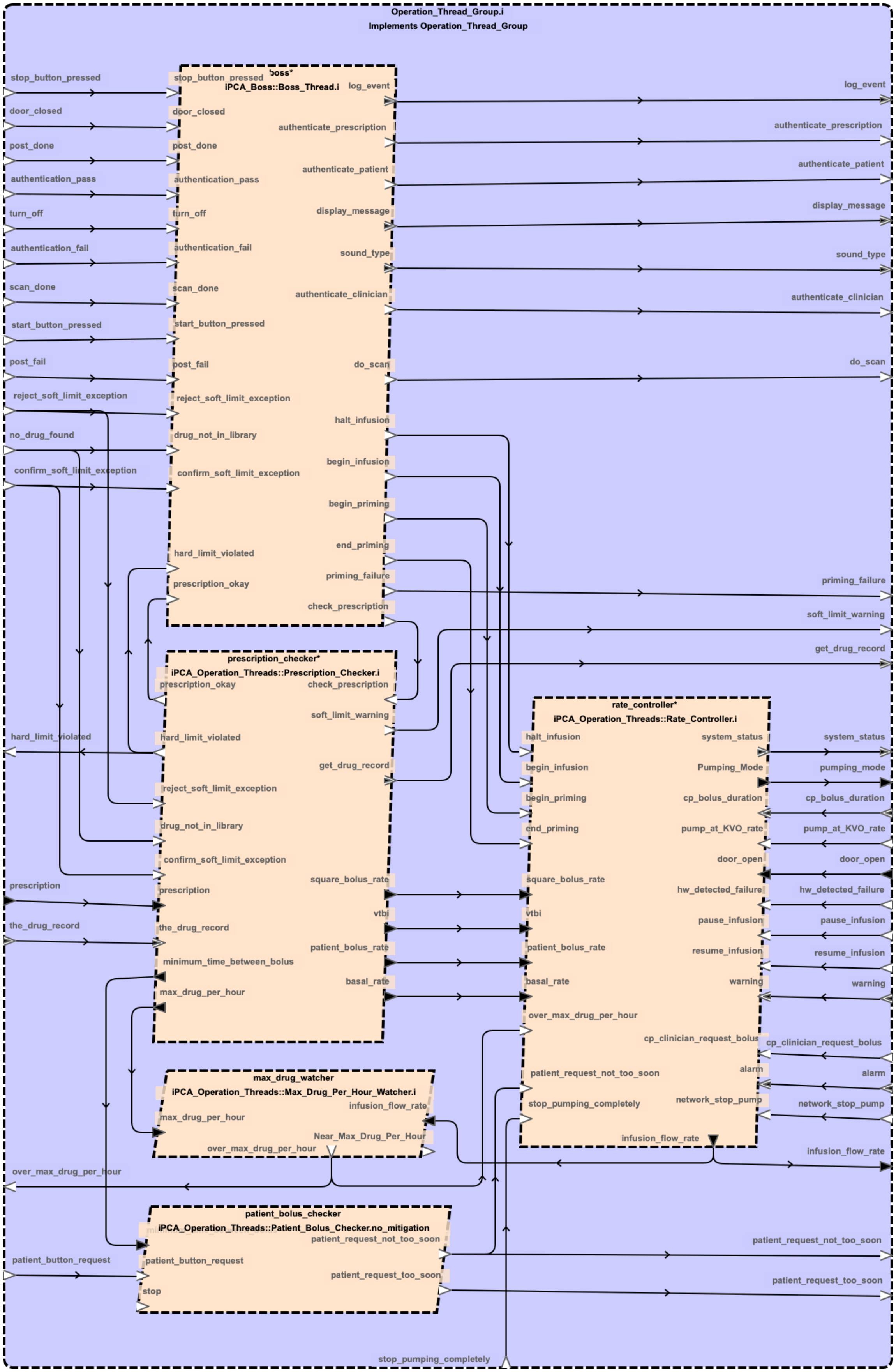


Figure 27: Operation Thread Group

fig_otg

Allocated Requirements
R4.2.0(4) maximum VTBI
R4.3.0(5) maximum clinician-chosen duration
R4.3.0(6) minimum clinician-chosen duration
R5.3.0(1) device parameters
R5.5.0(10) hard limit
R5.5.0(8) prescription confirmation
R5.5.0(9) soft limit confirmation
R5.6.0(4) prescription retention
R5.8.0(6) prescription confirmation
R5.9.0(5) hard limit
R5.9.0(6) soft limit

9.1.8 Max Drug Per Hour Thread

The *max dug per hour thread* keeps track of how much drug has been infused within the previous hour.

Allocated Requirements
R4.2.0(5) max dose warning

9.1.9 Patient Bolus Checker

The *patient bolus checker* thread prevents patient-requests bolus delivery sooner than the minimum time between patient-requested bolus.

Allocated Requirements
R4.2.0(3) minimum time between patient-requested bolus

9.1.10 Scanner

The *scanner* reads an optical or RFID code on the patient, clinician, and the drug container that is loaded into the reservoir.

Allocated Requirements
R4.1.0(1) basal flow rate
R5.3.0(1) device parameters
R5.8.0(5) enter prescription
R5.10.0(1) patient's wristband
R5.10.0(2) clinician's badge
R5.10.0(3) drug's package label

9.2 Safety Subsystem

subsec_safety

The *safety subsystem* works with, but is distinct from, the operation subsystem. The safety subsystem detects faults that may harm the patient, signals an alarm or warning, and stop infusion or reduces infusion to a keep vein open rate depending on the fault(s) detected. The components in the safety system are listed in Table 8, and depicted in Figure 28.

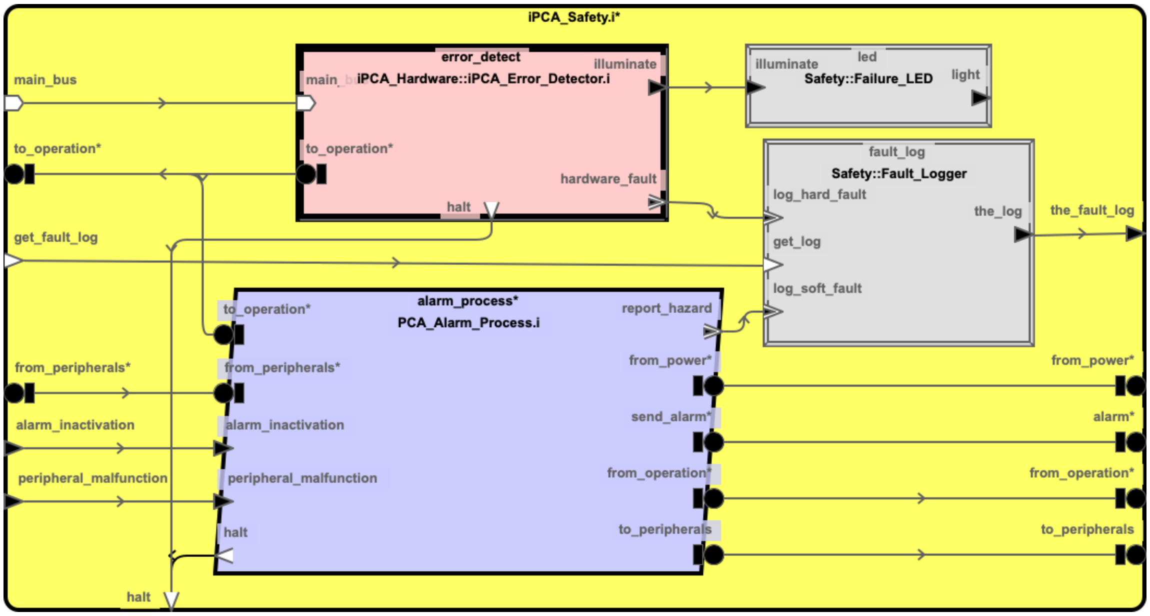


Figure 28: Safety Subsystem fig_safety

Table 8: Safety Components

Component	**Behavior**
pump_fault_manager	handles pump fault signals
alarm_process	holds thread which controls alarms
fault_logger	record faults
error_detector	handle hardware-detected faults
failure_led	indicates hardware failure

tabl:safety

Allocated Requirements
R6.1.0(1) safety architecture

9.2.1 Failure LED

Hardware faults that prevent execution of thread cause the *failure LED* to illuminate.

Allocated Requirements
R6.4.0(7) hardware fault indicator

9.2.2 Error Detector

The *error detector* detects conditions that prevent threads from operating thus could not be detected by the alarm thread.

Allocated Requirements
R6.4.0(1) power-on self-test
R6.4.0(2) periodic self-tests
R6.4.0(3) continuous fault-detection
R6.4.0(4) single-event upsets

9.2.3 Fault Logger

The *fault logger* records all errors that are detected. As such it is pure hardware that does not depend on thread execution. It also maintains a hardware *real-time clock* used for timestamps by both event and fault logs, and by network messaging.

Allocated Requirements
R5.6.0(2) fault log
R5.6.0(3) time stamp
R5.6.0(5) log retention
R6.4.0(5) masked faults
R6.4.0(6) hardware detected faults
R5.6.0(7) fault log size
R5.6.0(8) real-time clock

9.2.4 Alarm Process

The *alarm process* (Figure 29) holds two threads, one of which checks flow rate, and the other controls what alarm gets raised.

9.2.5 Alarm Thread

The *alarm thread* evaluates fault signals to determine whether the infusion rate should be changed, issues alarm and warning signals to be sounded and displayed by the control panel, and creates fault entries to be stored in the fault log.

Allocated Requirements
R5.4.0(1) issue alarms and warnings
R5.4.0(2) basal over-infusion alarm

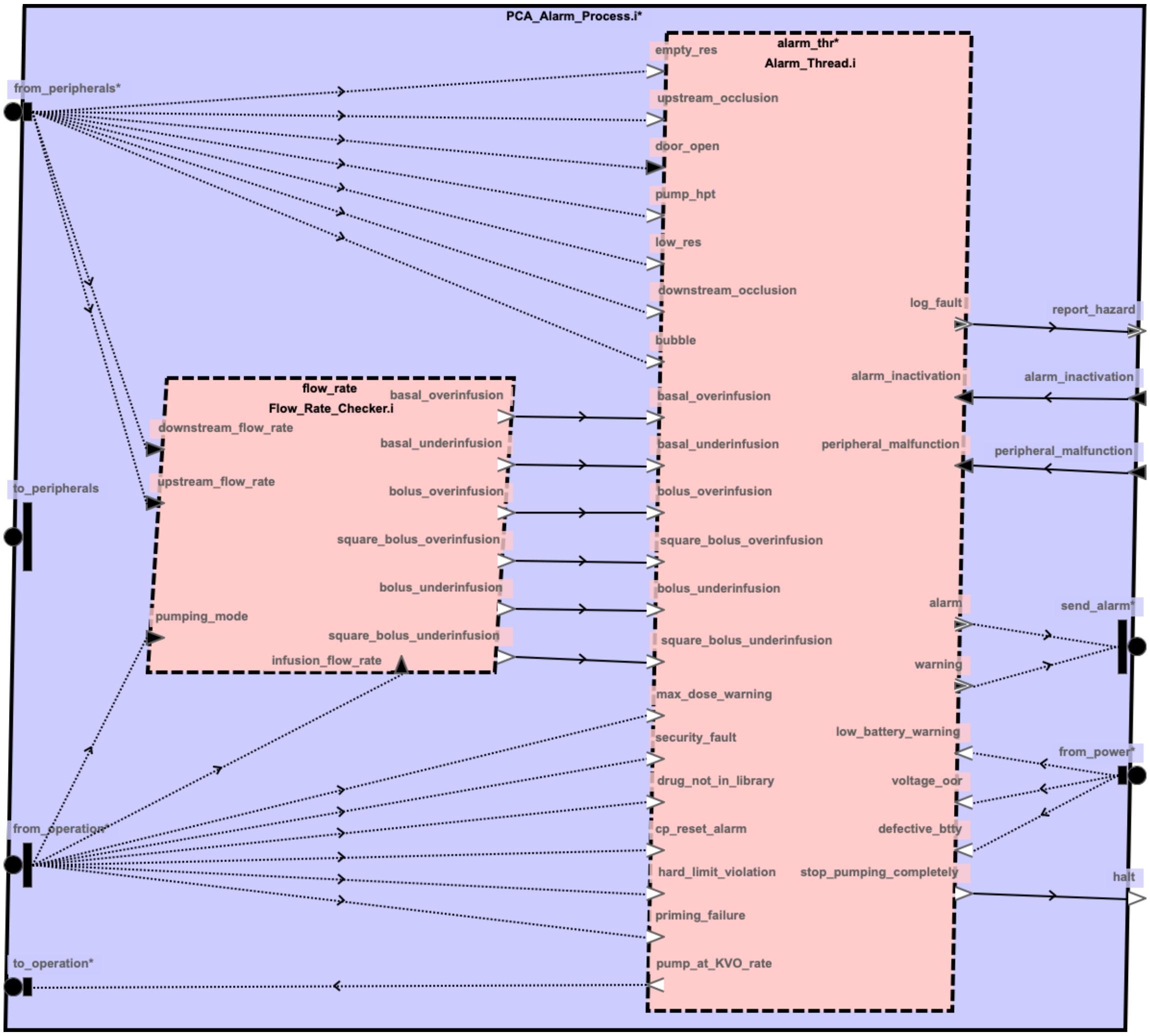


Figure 29: Alarm Process

fig_ap

R5.4.0(3) basal under-infusion warning
R5.4.0(4) bolus over-infusion alarm
R5.4.0(5) bolus under-infusion warning
R5.4.0(6) square bolus over-infusion alarm
R5.4.0(7) square bolus under-infusion warning
R5.4.0(8) pump overheated alarm
R5.4.1(1) priority
R5.4.1(2) alarm pump rate
R5.9.0(5) hard limit
R5.9.0(6) soft limit
R6.2.0(3) air-in-line alarm
R6.2.0(4) upstream occlusion alarm
R6.2.0(5) downstream occlusion alarm
R6.2.0(6) occlusion alarm
R6.2.0(7) empty-reservoir alarm

9.2.6 Flow Rate Checker

The *pump fault manager* determines if the measured upstream and downstream flow rates are within tolerance of the specified rate, and aggregates other pump fault indications into a combined pump fault indication.

Allocated Requirements
R5.4.0(2) basal over-infusion alarm
R5.4.0(3) basal under-infusion warning
R5.4.0(4) bolus over-infusion alarm
R5.4.0(5) bolus under-infusion warning
R5.4.0(6) square bolus over-infusion alarm
R5.4.0(7) square bolus under-infusion warning

9.3 Power Subsystem

The *power subsystem* consists of a battery, power control, and an implicit power supply as depicted in Figure 30.

9.3.1 Power Supply

The *power supply* converts alternating current energy into direct current that powers the electronic components.

Allocated Requirements
R6.3.0(6) voltage out-of-range warning

9.3.2 Battery

The *battery* provides reserve energy to operate the PCA pump when mains power fails.

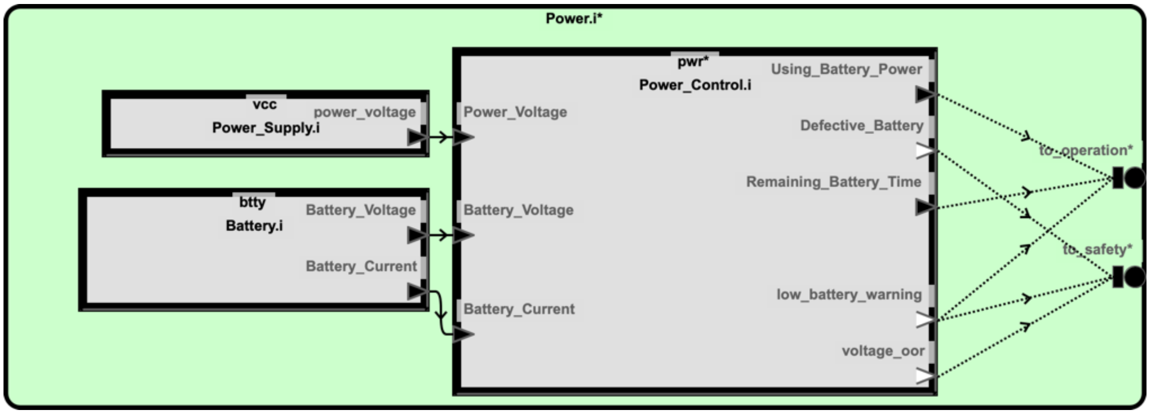


Figure 30: Power Subsystem

fig_ps

Allocated Requirements
R6.3.0(1) battery backup

9.3.3 Power Control

The *power control* switches between battery-backup and mains supply, and detects anomalies like voltage out-of-range.

Allocated Requirements
R5.4.1(3) power and battery failure
R6.3.0(2) remaining battery minutes
R6.3.0(3) remaining battery accuracy
R6.3.0(4) low-battery warning
R6.3.0(5) battery failure alarm
R6.3.0(6) voltage out-of-range warning

9.4 Fluid Subsystem

sec_fluid_subsystem

The *fluid subsystem* moves drug from the reservoir to the line to the patient and is depicted in Figure 31. The drug flows from the reservoir, through the upstream monitor to the pump, then through the downstream monitor to the tube to the patient.

Allocated Requirements
R6.6.0(1) biocompatible

9.4.1 Patient Button

The *patient button* allows the patient to request an extra bolus of drug on demand. It may be connected by wire or RF to the PCA pump so that it is conveniently located for the patient.

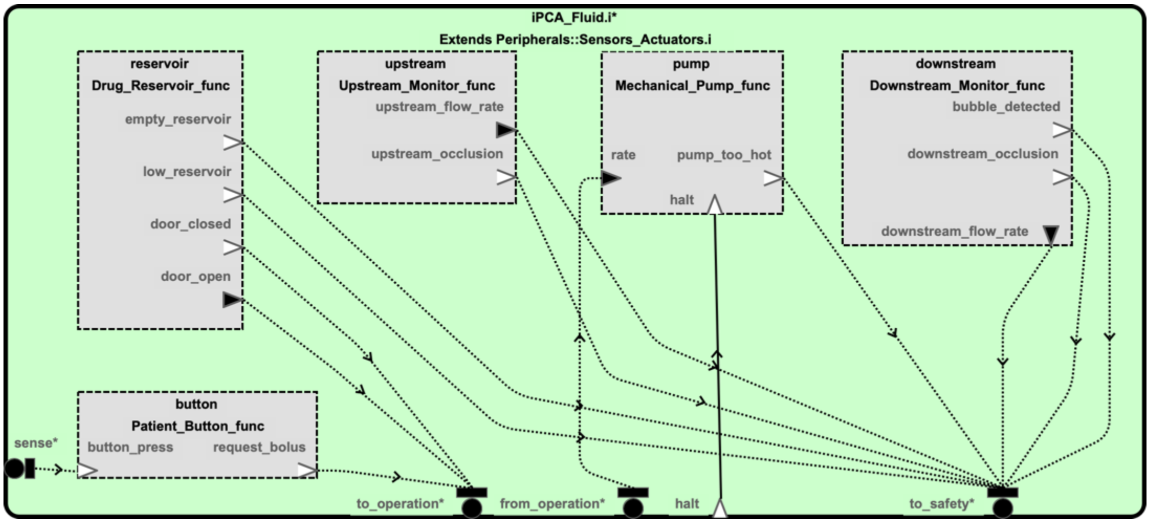


Figure 31: Fluid Subsystem

fig_mps

Allocated Requirements
R4.2.0(2) patient-requested bolus

9.4.2 Pump

The *pump* moves fluid at specified rate, primes itself, announces if priming fails, indicates when it's too hot, and halts pumping when commanded.

Allocated Requirements
R4.1.0(2) basal infusion flow range
R4.1.0(3) basal infusion flow tolerance
R5.2.0(1) pump drug
R5.2.0(2) halt pumping
R5.4.0(8) pump overheated alarm
R6.2.0(1) complete pump stroke
R6.2.0(2) continuous reverse delivery
R6.2.0(6) occlusion alarm
R5.2.0(3) reverse flow

9.4.3 Upstream Monitor

The *upstream monitor* measures drug flow into the pump and detects upstream occlusion.

Allocated Requirements
R5.1.0(1) measure drug flow
R5.1.0(3) detect upstream occlusion

9.4.4 Downstream Monitor

sec_downstreammonitor

The *downstream monitor* measures drug flow out of the pump and detects downstream occlusion, and air-in-line embolism.

Allocated Requirements
R5.1.0(1) measure drug flow
R5.1.0(2) detect downstream occlusion
R5.1.0(4) detect air-in-line embolism

9.4.5 Drug Reservoir

The *drug reservoir* holds liquid drug until infused.

Allocated Requirements
R5.8.0(1) drug reservoir
R5.8.0(2) reservoir contents
R5.8.0(3) reservoir tolerance
R5.8.0(9) low-reservoir warning
R5.8.0(10) empty-reservoir alarm
R6.5.0(1) tamper-resistant door
R6.5.0(3) door key
R6.5.0(4) pump case
R6.2.0(8) open door alarm

9.5 Communication Subsystem

subsec_communication

The *communication subsystem* (Figure 32) provides a flexible way for network devices to communicate with the network system which may include network apps in addition to a supervisor user interface which allows a clinician, usually a nurse, to monitor and control all network devices used in a unit.

9.5.1 Network Thread

The *network thread* sends and receives signals through the ice bus adaptor.

Allocated Requirements
R5.7.0(1) network operating status
R5.7.0(2) network alarms
R5.7.0(3) network bolus duration
R5.7.0(4) network KVO rate
R5.7.0(5) network resume infusion
R5.7.0(6) stand-alone
R5.7.0(7) network inactivate alarms

The *network Bus Adaptor* converts data and events on an network interface, into transactions on an network bus.

Allocated Requirements
R5.4.0(1) issue alarms and warnings

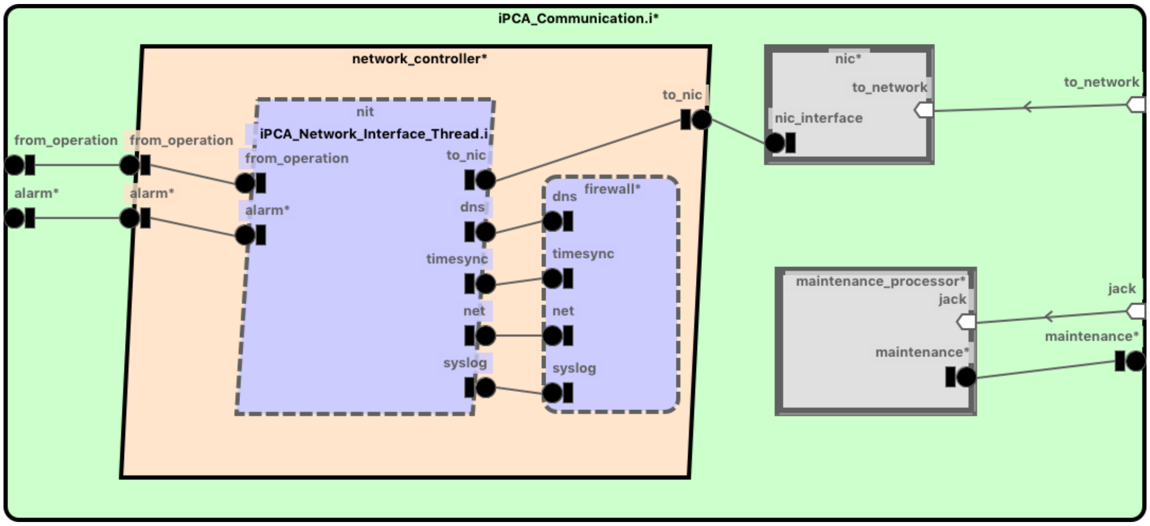


Figure 32: Communication Subsystem fig_comm

R5.7.0(1) network operating status
R5.7.0(2) network alarms
R5.7.0(3) network bolus duration
R5.7.0(4) network KVO rate
R5.7.0(5) network resume infusion
R7.3.0(3) provisioning channel disjointness

9.6 Maintenance Processor

subsec_maintenanceprocessor

The *maintenance processor* provides a test interface and security provisioning channel.

Allocated Requirements
R7.3.0(1) provisioning jack R7.3.0(2) protected jack

9.7 Security Subsystem

subsec_security

The *security subsystem*, depicted in Figure 33 performs authentication calculations of patient wrist bands, clinician badges, prescription labels, drug libraries, and messages with network. It will also encrypt patient data to be sent to an electronic health record system. Within the security subsystem, a crypto process holds a crypto thread which controls a trusted platform module (TPM). A personal presence button must be pressed by a person for certain TPM initializations.[165]

Allocated Requirements
R7.1.0(1) clinician authentication
R7.1.0(2) patient authentication
R7.1.0(3) prescription authentication

[165] Provisioning?

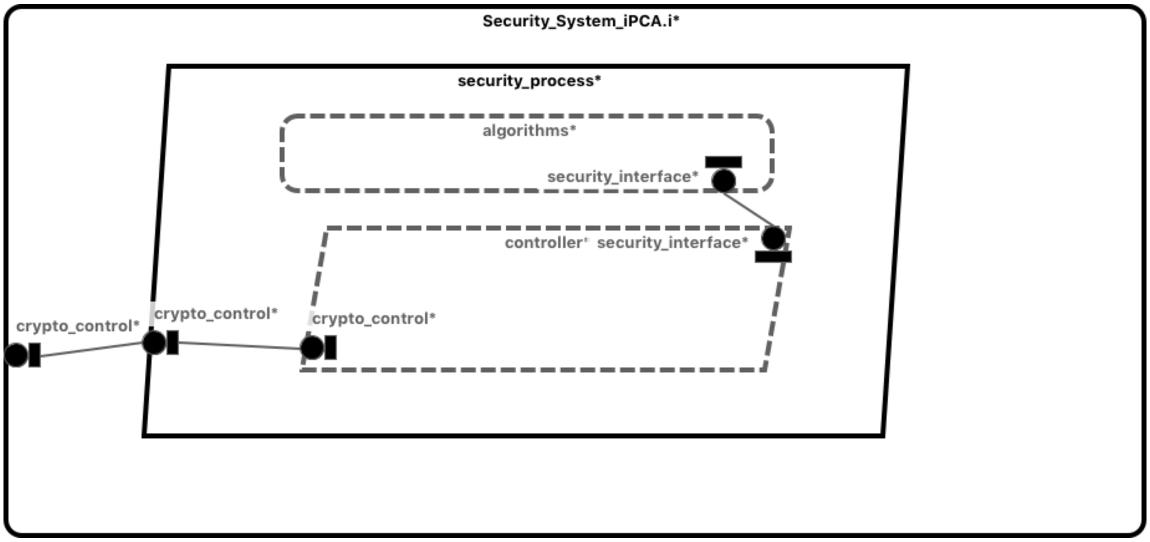


Figure 33: Security Subsystem

fig_ss

R7.1.0(4) drug library authentication
R7.2.0(1) confidentiality
R7.3.0(3) provisioning channel disjointness
R7.3.0(4) provisioning unitarily

9.7.1 Security Thread

The *security thread* authenticates.

Allocated Requirements
R7.1.0(1) clinician authentication
R7.1.0(2) patient authentication
R7.1.0(3) prescription authentication
R7.1.0(4) drug library authentication

9.8 Graphical User Interface

subsec_gui

9.8.1 Control Panel

The *control panel* combines a touch panel with a speaker by which a clinician can enter and confirm configuration and see and hear alarms and warnings.

It

- is used by the clinician to start and stop infusion.[166]

[166] Is a separate priming operation needed before the needle is inserted and infusion is started?

- displays the prescription read from the drug container by the scanner for confirmation or rejection.
- displays the PCA pump's status.
- allows request of a bolus by a clinician.
- allows entry of the clinician requested bolus duration.
- displays alarm and warning indications
- sounds alerts for alarm and warning indications
- allows alarm inactivation
- displays if and how alarms are currently inactivated

Allocated Requirements
R5.4.0(1) issue alarms and warnings
R5.4.2(1) visual alarm signal
R5.4.2(2) alarm indicator appearance
R5.4.2(3) see alarm signal
R5.4.2(4) alarm symbols
R5.4.3(1) audible alarms signals
R5.4.3(2) auditory volume
R5.4.3(3) alarm melody
R5.4.3(4) harmonic components
R5.5.0(1) control panel
R5.5.0(2) start button
R5.5.0(5) stop button
R5.5.0(7) clinician bolus request
R5.5.0(8) prescription confirmation
R5.5.0(9) soft limit confirmation
R5.5.0(11) show alarm
R5.5.0(12) sound alarm
R5.5.0(13) stop silences alarms
R5.5.0(14) inactivate audible alarms indefinitely
R5.5.0(15) inactivate audible alarms temporarily
R5.5.0(16) cancel alarm signal inactivation
R5.5.0(17) inactive auditory alarm symbol
R5.5.0(18) alert-stop-start sequence
R5.5.0(19) sound of audible alarm
R5.5.0(20) display of visual information
R5.5.0(21) tactile response
R5.5.0(22) resume infusion
R5.5.0(23) display infusion rate
R5.8.0(6) prescription confirmation
R5.9.0(5) hard limit
R5.9.0(6) soft limit

Part IV

Index

Index