Brian R. Larson

SAnToS TR 2012-01-24

Integrated Clinical Environment Patient-Controlled Analgesia Infusion Pump System Requirements DRAFT 0.9.3

2012-01-25

Kansas State University

Contents

List of Figures

List of Tables

Integrated Clinical Environment
Patient-Controlled Analgesia Infusion Pump
System Requirements
DRAFT 0.9.3[×]

Brian R. Larson
Kansas State University
brl@k-state.edu

January 24, 2013

Abstract

This document contains system requirements for a patient-controlled analgesia (PCA) infusion pump for the Integrated Clinical Environment (ICE). These requirements define *what* a PCA pump must do to be ICE-compliant, not *how* any particular implementation works.

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 that 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, because real requirements are highly-confidential to medical device manufacturers, often using proprietary clinical data. Furthermore, showing safety and effectiveness can be legal necessities for regulatory approval. Therefore these simulated requirements were created to fill the vacuum. No physicians have reviewed these simulated requirements for a generic system 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.

[×] Work supported in part by the US National Science Foundation (NSF) (#0932289, #1239543), the NSF US Food and Drug Administration Scholar-in-Residence Program (#1065887, #1238431) the National Institutes of Health / NIBIB Quantum Program.

1 Introduction

This document defines requirements for patient-controlled analgesia (PCA) infusion pumps for use in an Integrated Clinical Environment (ICE). In particular, this device may communicate with, and be controlled by an ICE application or “app”.

As much as possible, these requirements define what an ICE PCA infusion pump must do, and how it interacts with ICE apps. Implementations may have other features not mentioned in these requirements; they are a minimum for ICE-compliance. As much as possible design and implementation of an ICE-compliant PCA infusion pump are left unspecified.

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 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).[2] 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 ICE PCA pump provides a standard ICE interface so it may be integrated with ICE apps and displays (Figure 2). The interface must provide prescription and patient information, current status to be displayed remotely on a supervisor user interface, and a means to stop infusing upon human command, or determination of an ICE app. Such an ICE app could monitor a patient’s blood oxygenation and pulse rate, stopping the pump if depressed respiratory function is indicated.

[1] PCA pumps are FDA product code “MEA”.

[2] Essentially, FDA’s GPCA pump without an ICE interface.

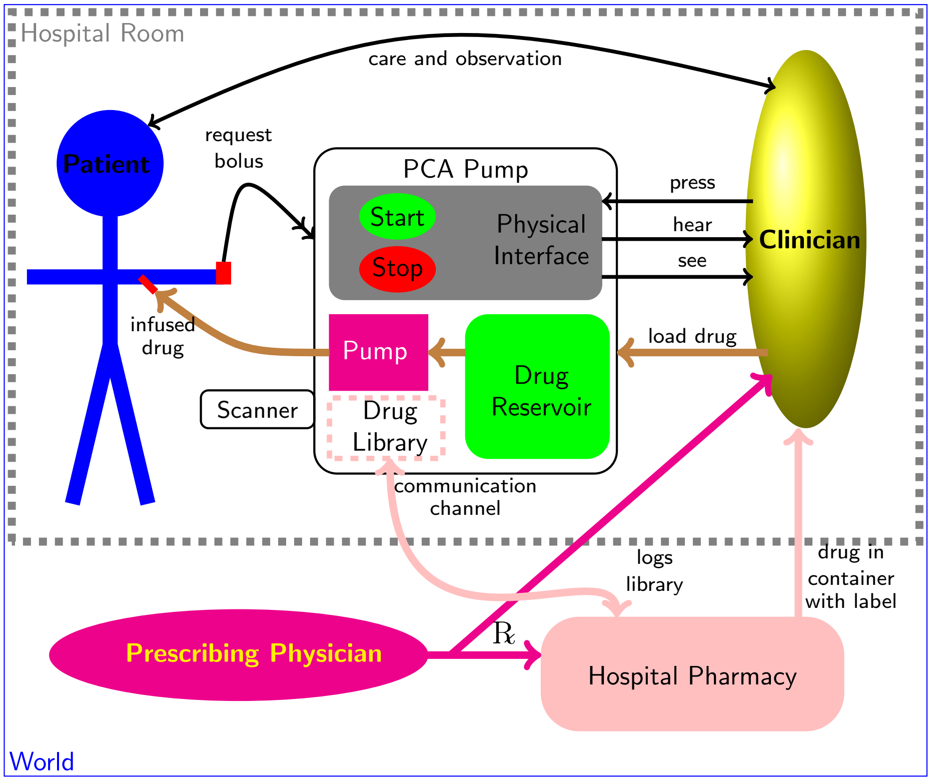

Figure 1: Independant PCA Pump Use

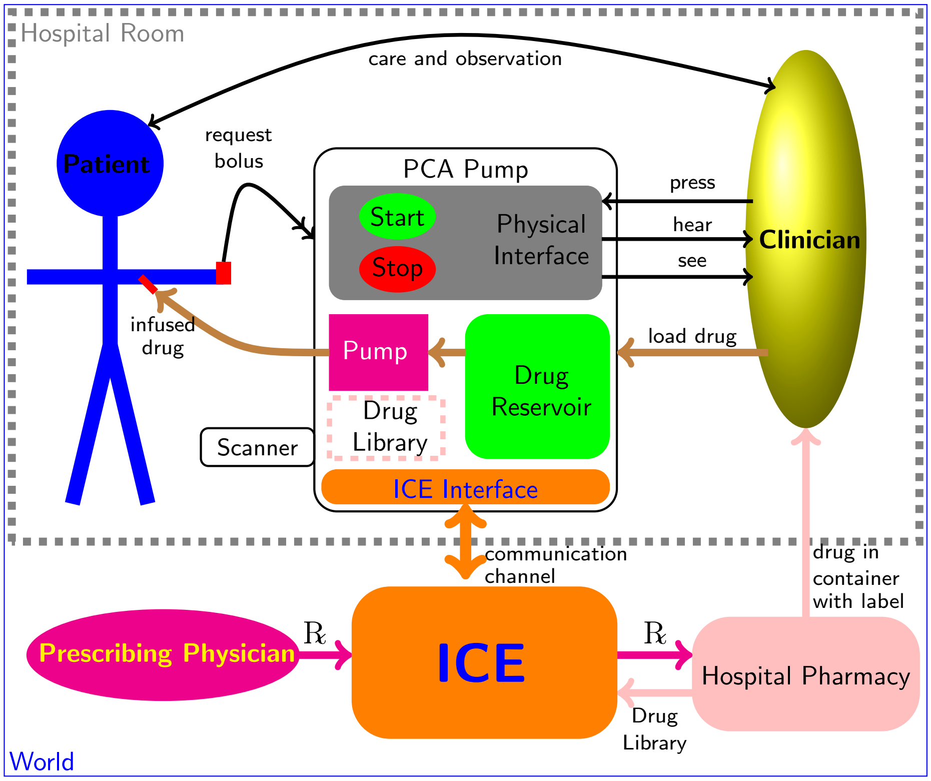

Figure 2: ICE PCA Pump Use

1.2 References

Normative references are mandatory; informative references provide background.

1.2.1 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*

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*

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*

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

1.2.2 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]

1.3 Terms and Acronyms

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

[3] author unspecified, believed to be collaboration between FDA and 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`

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

DEA U.S. Drug Enforcement Agency

FDA U.S. Food and Drug Administration

GPCA Generic Patient-Controlled Analgesia (pump)

Hg mercury

hr hour

ICE Integrated Clinical Environment

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

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 improved pain control. 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

PCA uses a computerized 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. When this button is pressed, some sound (usually a beep) is heard, indicating that the pump is working properly and that the button was pressed correctly. 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 initial dose of the prescribed drug. The health-care provider sets the pump to deliver a specified dose, determined by the physician, on demand with a lockout time (for example, 1 mg of morphine on demand, but not more frequently than one 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. An around-the-clock, even dose may also be set. The practitioner sets a total limit 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. An ICE PCA pump augments the function of a stand-alone PCA pump with communication and control by the ICE system which allows clinician's to remotely monitor the operation of the pump, and ICE apps to coordinate its operation with other ICE devices, and is depicted in Figure 2.

2.3.1 Bolus Request Button

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.[6] 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.

[6] Allow door opening only by authenticated clinician?

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 ICE Interface

An ICE interface uses a communication channel to connect to the ICE system.

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. Patient information may be stored in electronic health records, protected for confidentiality, authenticity, and accountability/provenance.

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, [7] lighting, infection-control procedures and equipment, normal electromagnetic fields and particles,[8]

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 by, an ICE app.

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

(2) The pump should be able to withstand and operate under *atmospheric pressure*[11] ranging from $P_{min} = 20$"Hg to $P_{max} = 35$"Hg.

(3) The (external) pump should be able to operate at *relative humidity*[12] ranging from $H_{min} = 0\%$ to $H_{max} = 100\%$ (non-condensing).

(4) The PCA pump shall withstand *splashing*[13] (but not immersion) with water or bodily fluids.

2.5 Direct PCA Pump Interactions

An ICE 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.

2.6 Indirect PCA Pump Interactions

An ICE PCA pump interacts indirectly, over an encrypted and authenticated channel, with the ICE system which may include a supervisor user interface to monitor and control the pump, or app(s) that may stop infusion if abnormal conditions are detected by other devices such as slow heart rate or low blood oxygenation.

2.7 System Goals

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

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

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

[8] 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.

[9] requirement R2.4.0(1): *temperature range*

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

[11] requirement R2.4.0(2): *atmospheric pressure*

[12] requirement R2.4.0(3): *relative humidity*

[13] requirement R2.4.0(4): *splashing*

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).

G5 The PCA pump shall infuse safely when failures occur or hazards are detected.[14]

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.

2.8 System Boundary and Monitored/Controlled Variables

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	Primary 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	ICE app	ICE-Detected Hazard	switch to KVO infusion rate upon ICE app-determined need
UC5	Clinician	Resume Operation After ICE-Detected Hazard	resume prescribed infusion after clinician determines it is safe
UC6	Clinician or App	ICE-Initiated Audible Alarm Inactivation	suspend audible alarm from ICE

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

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

This use case describes normal operation of the PCA Pump.

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 for $\Delta_{auth} = 5$ minutes (Exception Case: Clinician Authentication Failure)
5. Clinician enters scans patient information
6. Patient is authenticated to receive medical care for $\Delta_{auth} = 5$ minutes (Exception Case: Patient Authentication Failure)
7. Clinician scans drug information and patient's prescription from drug container (vial)
8. Prescription is authenticated as originating from an authorized pharmacist (Exception Case: Prescription Authentication Failure)
9. Prescription is authenticated for the patient for $\Delta_{auth} = 5$ minutes (Exception Case: Prescription Authentication Failure)
10. PCA pump compares prescription with its drug library (Exception Cases: Drug Library Soft Limit and Drug Library Hard Limit and Drug Library Not Present or Corrupted)
11. PCA pump unlocks and clinician opens the reservoir door
12. Clinician puts drug vial into the reservoir and closes the door

13. PCA pump locks reservoir door and terminates clinician authentication
14. Clinician attaches infusion tube and needle to pump
15. Clinician primes pump (Exception Case: Pump Priming Failure)
16. Clinician inserts infusion needle into patient's vein
17. Clinician presses Start button to begin basal-rate infusion
18. Bolus dose infused upon request; see Use Cases UC2 and UC3: Bolus Infusion
19. Clinician presses Stop button to halt infusion
20. Clinician removes infusion needle from patient's vein
21. Clinician scan own badge
22. Clinician is authenticated to operate PCA pump for $\Delta_{auth} = 5$ minutes (Exception Case: Clinician Authentication Failure)
23. PCA pump unlocks and clinician opens the reservoir door
24. Clinician removes drug vial, closes the door, returning remaining drug to pharmacy
25. PCA pump locks reservoir door and terminates clinician authentication
26. Clinician turns off PCA pump.

3.1.2 Use Case: Patient-Requested Bolus (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 10 of Normal Operation Use Case completed
- Basal rate being infused
- Prescribed minimum time between boluses has elapsed

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
3. If not Exception Case: Bolus Request Too Soon, begin infusing bolus

4. After prescribed volume-to-be-infused (VTBI) has been infused, resume basal rate infusion

3.1.3 Use Case: Clinician-Requested Bolus (UC3)

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

Related System Goals G1 and G2

Primary Actor Clinician

Precondition

- Steps 1 to 10 of Normal Operation Use Case completed
- Basal rate being infused
- Prescribed minimum time between boluses has elapsed

Postcondition

- Resume basal rate infusion

Main Success Scenario

1. Clinician (optionally) sets duration of bolus infusion on Control Panel or ICE supervisor user interface
2. Clinician requests bolus infusion on Control Panel or ICE supervisor user interface
3. Time since last bolus compared with prescribed minimum time between boluses
4. If not Exception Case: Bolus Request Too Soon, begin infusing bolus
5. After prescribed volume-to-be-infused (VTBI) has been infused, resume basal rate infusion

3.1.4 Use Case: ICE-Detected Hazard (UC4)

This use case describes operation when an ICE app determines a hazard may exist by monitoring other ICE devices such as pulse oximeters, respiration monitors, or electrocardiograms.

Related System Goals G2 and G3

Primary Actor ICE App

Precondition

- Steps 1 to 10 of Normal Operation Use Case completed
- Basal rate or bolus rate being infused
- PCA pump communicating with ICE system
- Monitoring device(s) communicating with ICE system

- ICE app initialized and registered to PCA pump and monitoring devices

Postcondition

- KVO rate infusion

Main Success Scenario

1. ICE app determines that a patient-hazard may be occurring
2. ICE app issues alarm which displays and sounds on the ICE supervisor user interface
3. ICE app sends authenticated signal to PCA pump to switch to KVO infusion rate
4. PCA pump verifies the authenticity of the command
5. PCA pump switches to KVO infusion rate if authentication checks pass
6. PCA pump signals ICE app that it has switched to KVO rate infusion

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

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

Related System Goals G1

Primary Actor Clinician

Precondition

- ICE app determined a hazard may exist
- Clinician notified of hazard by alarm on ICE supervisor user interface
- 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
3. Clinician authenticates (scans own badge if using device control panel)
4. Clinician is authenticated to operate PCA pump for $\Delta_{auth} = 5$ minutes (Exception Case: Clinician Authentication Failure)
5. Clinician clears ICE app-generated alarm on ICE supervisor user interface
6. ICE app sends authenticated signal instructing PCA pump to resume prescribed infusion
7. PCA pump verifies the authenticity of the command

8. PCA pump resumes prescribed infusion if authentication checks pass
9. PCA pump sends authenticated signal to the ICE app that it has resumed prescribed infusion
10. ICE app indicates normal operation has resumed on ICE supervisor user interface

3.1.6 Use Case: ICE-Initiated Audible Alarm Inactivation (UC6)

An app running on the ICE supervisor, or a clinician via the supervisor user interface, the may inactive audible alarm indication either temporarily or indefinitely.

Related System Goals G3

Primary Actor Clinician or App

Precondition Normal operation

Postcondition

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

Main Success Scenario

1. Authorized clinician on ICE supervisor user interface, or app on ICE supervisor, tells device to inactivate audible alarms either temporarily or indefinitely
2. ICE authenticated signal instructing PCA pump to inactivate audible alarm
3. PCA pump verifies the authenticity of the command
4. PCA pump inactivates audible alarms if authentication checks pass
5. PCA pump indicates audible alarm inactivation
6. If temporary, alarm reactivates after xxxxx minutes
7. Clinician may reactivate audible alarm from either supervisor user interface or control panel

3.2 Exception Cases

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.

3.2.1 Exception Case: Bolus Request Too Soon (EC1)

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

Related System Goals G2 and G3

Table 2: Summary of PCA Exception Cases

ID	Primary 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		ICE Failure	indication of no ICE alarms enabled
EC19		Drug Library Not Present or Corrupted	the drug library fails authenticity or integrity check

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 ICE supervisor user interface (if connected) issue audible warning and display visual warning
3. Warning recorded in Fault Log
4. Clinician resets warning on either control panel or ICE supervisor user interface, which resets audible warning on both.[15]
5. Identity of clinician resetting warning recorded in Event Log.

3.2.2 Exception Case: 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 ICE supervisor user interface
3. Attempt to exceed soft limit recorded in Event Log
4. Clinician confirms or rejects VTBI or basal rate

[15] Should the visual alarm on the control panel be reset by action on the SUI? Potential asymmetry between what's displayed on SUI and control panel

    - 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)

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

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 ICE supervisor user interface
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)

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 ICE supervisor user interface
3. Failure recorded in Fault Log
4. All infusion inhibited.

3.2.5 Exception Case: Internal Electronic Failure (EC5)

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
   - Random-access memory fault, issue *RAM failure alarm*
   - Read-only memory fault, issue *ROM failure alarm*
   - Microprocessor fault, issue *CPU failure alarm*
   - Thread monitor fault, issue *thread monitor alarm*
   - Battery failure, issue *battery failure alarm*
   - Power supply voltage our of range, issue *voltage out-of-range alarm*
2. Alarm sounded and displayed by Control Panel and ICE supervisor user interface
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)

Pump fails to prime when commanded to do so.

Related System Goals G5

Primary Actor Clinician

Precondition Drug loaded into reservoir

Postcondition

- Alarm sounded and displayed
- Infusion inhibited

Exception Success Scenario

1. Pump priming failure detected
2. *priming failure alarm* sounded and displayed by Control Panel and ICE supervisor user interface
3. Failure recorded in Fault Log
4. No infusion allowed

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

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

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
   - 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*
   - basal flow rate goes into free flow, issue *basal over-infusion alarm* immediately
   - 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 the pump shall issue a *bolus over-infusion alarm*

- patient-requested bolus flow rate goes into free flow, issue a *bolus over-infusion alarm* immediately
- 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*
- 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 ICE supervisor user interface
3. Pumping halted
4. Failure recorded in Fault Log

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

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

Related System Goals G5

Primary Actor none

Precondition normal operation

Postcondition Alarm sounded and displayed

Exception Success Scenario

1. Measured drug flow rate
   - 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*
   - patient-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 shall issue a *basal under-infusion warning*
   - 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 ICE supervisor user interface
3. Failure recorded in Fault Log

3.2.9 Exception Case: Pump Overheating (EC9)

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 ICE supervisor user interface
3. Pumping halted
4. Failure recorded in Fault Log

3.2.10 Exception Case: 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 ICE supervisor user interface
3. Pumping halted
4. Failure recorded in Fault Log

3.2.11 Exception Case: Upstream Occlusion (EC11)

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 ICE supervisor user interface
3. Pumping halted
4. Failure recorded in Fault Log

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

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 ICE supervisor user interface
3. Pumping halted
4. Failure recorded in Fault Log

3.2.13 Exception Case: Maximum Safe Dose (EC13)

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 ICE supervisor user interface
3. Infusion switched to KVO rate
4. Event recorded in Fault Log and Event Log

3.2.14 Exception Case: Clinician Authentication Failure (EC14)

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 ICE supervisor user interface
- 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)

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 ICE supervisor user interface
- Record patient authentication failure in Event Log
- Inhibit pump operation

Exception Success Scenario

1. Pump can only be used on admitted patients

3.2.16 Exception Case: Prescription Authentication Failure (EC16)

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 ICE supervisor user interface
- Record prescription authentication failure in Event Log
- Inhibit pump operation

Exception Success Scenario

1. Pump may only administer drug from authorized pharmacist
2. Pump may only administer drug to the patient for which it was prescribed

3.2.17 Exception Case: Sound Failure (EC17)

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 ICE supervisor user interface
- 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: ICE Failure (EC18)

The control panel will visually indicate when the PCA pump is not connected to an operational ICE. When the ICE network or manager 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 ICE connection indicated on control panel
- All alarms enabled

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

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 ICE supervisor user interface
2. Pumping halted
3. Failure recorded in Fault Log

4 PCA Pump Function

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

4.1 Basal Flow Rate

(1) The *basal flow rate*[16], 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.

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

(2) The pump shall be able to deliver basal infusion at flows throughout the *basal infusion flow range*[17] of $F_{basal\ min} = 1$ to $F_{basal\ max} = 10$ ml/hr.

(3) The pump shall deliver basal infusion at the prescribed basal rate within a *basal infusion flow tolerance*[18] of $F_{basal\ tol} = 0.5$ ml/hr of the prescribed basal rate.

(4) (requirement deleted because Rx is scanned from drug container, not entered by clinician)

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

4.2 Patient-Requested Bolus

(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 is delivered to the patient.[20]

(2) A *patient-requested bolus*[21] 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}.

(3) Patient-requested bolus shall not be delivered more often than a prescribed number of minutes, Δ_{prb}.

(4) Prescribed $VTBI$ and rate shall not exceed the hard limits set by the drug library from the hospital pharmacy for the drug loaded in the PCA pump.

(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*[22] be issued.

(6) Patient-requested bolus delivery shall be immediately halted when alarms sound.

4.3 Clinician-Requested Bolus

(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.[23]

(2) A *clinician-requested bolus*[24] 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}.

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

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

[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(5): *max dose warning*

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

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

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

(3) A patient-requested bolus shall take precedence over a clinician-requested bolus. The clinician-requested bolus shall be suspended while the patient-requested bolus dose is administered, and resumed afterward.

(4) Clinician-requested bolus delivery shall be immediately halted when alarms sound.

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

(6) The minimum clinician-chosen duration 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 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*[25] be issued.

5 PCA Pump Interfaces

5.1 Sensors

(1) The PCA pump shall *measure drug flow*[26] within a tolerance of $F_{mdf\ tol} = 0.1$ ml/hr.

(2) The PCA pump shall *detect downstream occlusion*[27].

(3) The PCA pump shall *detect upstream occlusion*[28].

(4) The PCA pump shall *detect air-in-line embolism*[29] (bubble).

5.2 Actuators

(1) The mechanical pump shall *pump drug*[30] at prescribed flow rates for basal, bolus, and KVO infusion when commanded.

(2) The mechanical pump shall *halt pumping*[31] when commanded, or caused in response to an alarm condition.[32]

(3) The mechanical pump shall not allow *reverse flow*[33] from the patient into the pump.

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

[26] requirement R5.1.0(1): *measure drug flow*

[27] requirement R5.1.0(2): *detect downstream occlusion*

[28] requirement R5.1.0(3): *detect upstream occlusion*

[29] requirement R5.1.0(4): *detect air-in-line embolism*

[30] requirement R5.2.0(1): *pump drug*

[31] requirement R5.2.0(2): *halt pumping*

[32] at end of pump stroke?

[33] requirement R5.2.0(3): *reverse flow*

5.3 Device Parameters

(1) The PCA pump shall use a physician's prescription as *device parameters*[34].

5.4 Alarms

(1) The PCA pump shall *issue alarms and warnings*[35] that require clinician attention.

(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*[36] (EC3.2.7).

(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*[37] (EC3.2.8).

(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*[38] (EC3.2.7).

(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*[39] (EC3.2.8).

(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*[40] (EC3.2.7).

(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*[41] (EC3.2.8).

(8) If the pump gets overheated to more than $T_{poh} = 55$ C, the pump shall issue an *pump overheated alarm*[42] (EC3.2.9).

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

[34] requirement R5.3.0(1): *device parameters*
[35] requirement R5.4.0(1): *issue alarms and warnings*
[36] requirement R5.4.0(2): *basal over-infusion alarm*
[37] requirement R5.4.0(3): *basal under-infusion warning*
[38] requirement R5.4.0(4): *bolus over-infusion alarm*
[39] requirement R5.4.0(5): *bolus under-infusion warning*
[40] requirement R5.4.0(6): *square bolus over-infusion alarm*
[41] requirement R5.4.0(7): *square bolus under-infusion warning*
[42] requirement R5.4.0(8): *pump overheated alarm*

5.4.1 Alarm Priority

(1) Alarm's and warning's *priority*[43] 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.

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

(2) Priority for alarms and warnings is shown in Table 4; warnings are low-priority alarms. The last column show the *alarm pump rate*[44] to be used while the alarm is in effect. For "special" flow rates for power malfunctions see Section 6.3.

(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.[45]

5.4.2 Alarm Visual

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*[46] 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.

(2) The *alarm indicator appearance*[47] shall comply with color, flashing frequency, and duty cycle given in Table 5.

[43] requirement R5.4.1(1): *priority*

[44] requirement R5.4.1(2): *alarm pump rate*

[45] requirement R5.4.1(3): *power and battery failure*

[46] requirement R5.4.2(1): *visual alarm signal*

[47] requirement R5.4.2(2): *alarm indicator appearance*

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

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%

(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.[48]

(4) Visual alarms shall display *alarm symbols*[49] from Table D.201 *Graphical symbols for ALARM SYSTEMS* of standard IEC 60601-1-8.

5.4.3 Alarm Audible

(1) Alarms shall cause *audible alarms signals*[50] that meet the requirements of Tables 203 and 204 of standard IEC 60601-1-8 for alarm pulses, bursts, and harmonics.

(2) The *auditory volume*[51] 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.

(3) The *alarm melody*[52] 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.[53]

(4) Each tone in the alarm melody shall be composed of a minimum of 4 *harmonic components*[54] in the range 300 Hz to 4000 Hz comprising an inverted 9th jazz chord.

The Control Panel panel, Section 5.5 allows audible alarm inactivation.

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

5.4.4 Alarms Networked

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

(2) All alarms not of high priority shall be encrypted and authenticated. High priority alarms may be encrypted and authenticated.

The ICE supervisor user interface, Section 5.7 allows audible alarm inactivation.

(3) If alarms are inactivated or paused through the ICE supervisor user interface, they shall be reactivated upon loss of connection to ICE (see Exception Case 18 3.2.18).

May need to ask (tell) devices to shut up.

[48] requirement R5.4.2(3): *see alarm signal*

[49] requirement R5.4.2(4): *alarm symbols*

[50] requirement R5.4.3(1): *audible alarms signals*

[51] requirement R5.4.3(2): *auditory volume*

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

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

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

5.5 Control Panel

(1) The *control panel*[55] must display currently-programmed patient data and physician's prescription.

(2) The PCA pump shall have a *start button*[56].

(3) Upon the clinician's pressing of the start button, prescribed infusion shall commence.[57]

(4) –requirement removed, Rx read from drug container by scanner

(5) The PCA pump shall have a *stop button*[58].

(6) Upon the clinician's pressing of the stop button, prescribed infusion shall halt.[59]

(7) The control panel shall allow authorized *clinician bolus request*[60] and choice of duration.

(8) Changing prescription during infusion shall require *prescription confirmation*[61], *clinician authentication*[62], *patient authentication*[63], *prescription authentication*[64] (patient-to-drug match) and *drug authentication*[65] (an authorized pharmacist filled the prescription).

(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*[66] by the clinician.

(10) Prescriptions that violate a *hard limit*[67] of the drug in the drug library shall be rejected with visible and audible indication when confirmation is attempted by the clinician.

(11) The Control Panel shall visually indicate the specific problem causing the alarm condition as described in Section 5.4.2.[68]

(12) The Control Panel shall audibly indicate the specific problem causing the alarm condition as described in Section 5.4.3.[69]

(13) Pressing the stop button confirms and silences all alarms and terminates any alarm signal inactivation.[70]

(14) The Control Panel shall provide means to *inactivate audible alarms indefinitely*[71].

[55] requirement R5.5.0(1): *control panel*
[56] requirement R5.5.0(2): *start button*
[57] requirement R5.5.0(3): *start infusion*
[58] requirement R5.5.0(5): *stop button*
[59] requirement R5.5.0(6): *stop infusion*
[60] requirement R5.5.0(7): *clinician bolus request*
[61] requirement R5.5.0(8): *prescription confirmation*
[62] requirement R5.5.0(8): *clinician authentication*
[63] requirement R5.5.0(8): *patient authentication*
[64] requirement R5.5.0(8): *prescription authentication*
[65] requirement R5.5.0(8): *drug authentication*
[66] requirement R5.5.0(9): *soft limit confirmation*
[67] requirement R5.5.0(10): *hard limit*
[68] requirement R5.5.0(11): *show alarm*
[69] requirement R5.5.0(12): *sound alarm*
[70] requirement R5.5.0(13): *stop silences alarms*
[71] requirement R5.5.0(14): *inactivate audible alarms indefinitely*

(15) The Control Panel shall provide means to *inactivate audible alarms temporarily*[72] for a predefined period of time.

(16) The Control Panel shall provide means to *cancel alarm signal inactivation*[73].

(17) When auditory alarms are inactive the control panel shall display an *inactive auditory alarm symbol*[74] from Table D.201 *Graphical symbols for ALARM SYSTEMS* of standard IEC 60601-1-8.

(18) If the same *alert-stop-start sequence*[75] occurs 3 or more times in ten minutes, infusion will be stopped, and an audible alarm sounded.

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

(19) *sound of audible alarm*[76],

(20) *display of visual information*[77], and

(21) *tactile response*[78] (button press).

5.6 Logging

(1) The PCA pump shall maintain an electronic *event log*[79] to record each action taken by the pump and each event sensed of its environment.

(2) The PCA pump shall maintain an electronic *fault log*[80] to record each fault condition, and the associated alarm and/or alert issued.

(3) Each log entry shall have a *time stamp*[81] with its time of occurrence.

(4) The patient's prescription shall be retained[82] 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[83] 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.[84]

(7) The fault log shall record at least 1000 faults before overwriting oldest fault records first.[85]

[72] requirement R5.5.0(15): *inactivate audible alarms temporarily*
[73] requirement R5.5.0(16): *cancel alarm signal inactivation*
[74] requirement R5.5.0(17): *inactive auditory alarm symbol*
[75] requirement R5.5.0(18): *alert-stop-start sequence*
[76] requirement R5.5.0(19): *sound of audible alarm*
[77] requirement R5.5.0(20): *display of visual information*
[78] requirement R5.5.0(21): *tactile response*
[79] requirement R5.6.0(1): *event log*
[80] requirement R5.6.0(2): *fault log*
[81] requirement R5.6.0(3): *time stamp*
[82] requirement R5.6.0(4): *prescription retention*
[83] requirement R5.6.0(5): *log retention*
[84] requirement R5.6.0(6): *event log size*
[85] requirement R5.6.0(7): *fault log size*

(8) A *real-time clock*[86] must produce timestamps accurate to 10 ms.

5.7 ICE Interface

The ICE interface allows the PCA pump to be monitored and controlled remotely, either by a clinician using an ICE supervisor user interface or an ICE app.

(1) The ICE Interface shall transmit encrypted and authenticated current operating status to the ICE system.[87]

(2) The ICE interface shall transmit encrypted and authenticated alarms and warnings to the ICE system.[88]

(3) The ICE interface shall allow an authorized clinician to set the duration of clinician-requested boluses through an ICE supervisor user interface.[89]

(4) The PCA pump shall switch to KVO infusion rate upon receiving an authenticated command through its ICE interface.[90]

(5) The PCA pump shall resume prescribed infusion upon receiving an authenticated command through its ICE interface.[91]

5.8 Drug Reservoir

(1) The *drug reservoir*[92] holds liquid pain-killer supplied by the hospital pharmacy and loaded into the PCA pump by the clinician.

(2) The drug reservoir shall measure its contents.[93]

(3) The measured drug volume shall be within $V_{rt} = 1$ ml of the actual drug volume.[94]

(4) All filled prescriptions (liquid, narcotic pain-killer dispensed by the hospital pharmacy) must be labeled at least visibly with[95]

a. Patient name

b. Drug code

c. Name of drug

d. Concentration

[86] requirement R5.6.0(8): *real-time clock*
[87] requirement R5.7.0(1): *ICE operating status*
[88] requirement R5.7.0(2): *ICE alarms*
[89] requirement R5.7.0(3): *ICE bolus duration*
[90] requirement R5.7.0(4): *ICE KVO rate*
[91] requirement R5.7.0(5): *ICE resume infusion*
[92] requirement R5.8.0(1): *drug reservoir*
[93] requirement R5.8.0(2): *reservoir contents*
[94] requirement R5.8.0(3): *reservoir tolerance*
[95] requirement R5.8.0(4): *drug label*

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.

(5) Prior to, or coincident with, loading the drug reservoir must also *enter prescription*[96] on the drug container's label using the scanner.

(6) An authorized clinician must personally confirm the prescription[97] is authentic and meant for the patient to be infused. The routine procedures by which clinicians load the drug reservoir must ensure that the prescription filled by an authorized pharmacist at the hospital pharmacy is meant for the patient (to be) connected to the PCA pump.[98]

(7) –removed all Rx entry via scanner

(8) The drug loaded into the reservoir must also be found in the PCA pump's *drug in library*[99]. The drug code of the prescription must match the drug code of a drug library entry. The drug library must pass authenticity and integrity checks.

(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*[100] shall be issued.

(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*[101] shall be issued stopping the pump.

5.9 Drug Library

(1) The *drug library*[102] 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 an authorized and authenticated hospital pharmacist, and loaded into the PCA pump via its communication port after verifying its authenticity and integrity.

[96] requirement R5.8.0(5): *enter prescription*

[97] requirement R5.8.0(6): *prescription confirmation*

[98] 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.

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

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

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

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

(2) For each drug that may be infused with a PCA pump, the *drug library entry*[103] for that drug shall have data elements listed in Table 6.[104]

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

(3) After the clinician presses the start button, but before commencing infusion, the values of $VTBI$ and F_{basal} are checked against the drug library entry of the drug to be infused.[105]

(4) If the drug loaded into the drug reservoir is not present in the drug library or the library does not pass authentication and integrity checks, that the drug is unknown or drug library error has occurred is indicated by the user interface, and recorded in the Fault Log. Pump remains stopped.[106]

(5) If a drug library's *hard limit*[107] is violated by the proposed settings, the limit violated is indicated by the user interface, and recorded in the Fault Log. Pump remains stopped.

(6) If a drug library's *soft limit*[108] is violated by the proposed settings, but not a hard limit, a warning is shown to the clinician by the user interface and a distinctive, irritating sound made and recorded in the Event Log. If the clinician again confirms proposed settings, then pump operation shall commence using them, otherwise typical values from the Drug Library.

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

[104] 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.

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

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

[107] requirement R5.9.0(5): *hard limit*

[108] requirement R5.9.0(6): *soft limit*

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*[109].

(2) The scanner shall read and authenticate information from the *clinician's badge*[110].

(3) The scanner shall read and authenticate information from the *drug's package label*[111].

6 Safety Requirements

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*[112] that separates normal operation from fault detection and response.[113]

6.2 Anomaly Detection and Response

(1) When the stop button is pressed, the current pump stroke shall be completed prior to stopping the pump.[114]

(2) During normal use and/or single fault condition of the equipment, *continuous reverse delivery*[115] shall not be possible (from IEC 601-2-24).

(3) An *air-in-line alarm*[116] shall be triggered by the pump if detectable air bubbles are infused into the patient.[117]

(4) An *upstream occlusion alarm*[118] shall be triggered when the pump senses an upstream (drug reservoir side) occlusion exceeding $P_{uo} = 1$ psi.

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

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

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

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

[113] Does the network interface remain active?

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

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

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

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

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

(5) A *downstream occlusion alarm*[119] shall be triggered if the pump senses a downstream (patient side) occlusion exceeding $P_{do} = 10$ psi.

(6) When an *occlusion alarm*[120] occurs, the pump shall be stopped immediately without completing the current pump stroke.

(7) When an *empty-reservoir alarm*[121] occurs, the current pump stroke shall be completed prior to stopping the pump.

(8) A *open door alarm*[122] shall be triggered when the reservoir door is opened while the pump is not stopped.

6.3 Power Supply

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*[123], 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.[124]

(3) The estimate of remaining battery energy must be accurate to within $X_{btty} = 25\%$.[125]

(4) If the estimated battery life remaining is less than $\Delta_{lba} = 3$ minutes, the pump shall issue a *low-battery warning*[126].

(5) The PCA pump shall detect battery failure and issue a *battery failure alarm*[127].

(6) The PCA pump shall detect power supply voltage out-of-range, issue a voltage out-of-range warning, and switch to battery backup when out-of-range.[128]

(7) The PCA pump must not leak current greater than 10 mA.

(8) Component failure must not harm patient (beyond stopping function).

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

[119] requirement R6.2.0(5): *downstream occlusion alarm*
[120] requirement R6.2.0(6): *occlusion alarm*
[121] requirement R6.2.0(7): *empty-reservoir alarm*
[122] requirement R6.2.0(8): *open door alarm*
[123] requirement R6.3.0(1): *battery backup*
[124] requirement R6.3.0(2): *remaining battery minutes*
[125] requirement R6.3.0(3): *remaining battery accuracy*
[126] requirement R6.3.0(4): *low-battery warning*
[127] requirement R6.3.0(5): *battery failure alarm*
[128] Power supply and battery voltage and allowed range is implementation dependant.

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 (POST) to assure system integrity after being turned on, yet before any infusion begins. Failure of POST shall raise a *POST alarm*, stop pump, record it in the Fault Log, and display the reason for failure on the user interface.

(2) The PCA pump shall 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.

(3) The PCA pump shall have *continuous fault-detection*[129] and masking. Hardware monitors of thread heartbeat, memory error correction codes are examples.

(4) Occurrence of unavoidable *single-event upsets*[130] caused by cosmic-ray-induced high- and thermal-energy neutrons must be either masked, or detected to fail-stop.

(5) Successfully *masked faults*[131] shall be recorded in the Fault Log, but raise an alarm.

(6) Hardware faults detected, but not masked,[132] shall raise a fault alarm, stop pump, record it in the Fault Log, and display the reason for fault on the user interface.

(7) Hardware faults that prevent operation of the Control Panel shall illuminate a *hardware fault indicator*[133] (light-emitting diode).

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*[134].

(2) –removed, must scan Rx from label of drug container

(3) Hospital procedures must endow the attending clinician access to the *door key*[135], 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. If the key is electronic, some of this information may be automatically verified and authenticated.

[129] requirement R6.4.0(3): *continuous fault-detection*
[130] requirement R6.4.0(4): *single-event upsets*
[131] requirement R6.4.0(5): *masked faults*
[132] requirement R6.4.0(6): *unmasked faults*
[133] requirement R6.4.0(7): *hardware fault indicator*
[134] requirement R6.5.0(1): *tamper-resistant door*
[135] requirement R6.5.0(3): *door key*

(4) The PCA *pump case*[136] 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.

(5) The PCA pump shall include *electronic tamper detection mechanisms*[137] and shall record detected tampering attempts in the Fault Log and Event Log as well as issuing an authenticated ICE message.

6.6 Biocompatibility

(1) All materials that contact fluid shall be *biocompatible*[138].

(2) The PCA pump shall be *cleaned and disinfected*[139] after use.

7 Security Requirements

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.[140]

(2) Patient's identity and admittance to the hospital must be authenticated.[141]

(3) Drug container must have a valid prescription, filled by an authorized pharmacist, for the particular patient to be infused by the PCA pump.[142]

(4) Drug library information shall be authenticated before it is accepted.[143]

7.2 Confidentiality

(1) Patient information must be restricted to those providing care for the patient, and the patient.[144]

[136] requirement R6.5.0(4): *pump case*
[137] requirement R6.5.0(5): *electronic tamper detection mechanisms*
[138] requirement R6.6.0(1): *biocompatible*
[139] requirement R6.6.0(2): *cleaned and disinfected*
[140] requirement R7.1.0(1): *clinician authentication*
[141] requirement R7.1.0(2): *patient authentication*
[142] requirement R7.1.0(3): *prescription authentication*
[143] requirement R7.1.0(4): *drug library authentication*
[144] requirement R7.2.0(1): *confidentiality*

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.[145]

(2) The provisioning jack must be physically inaccessible, except to authorized technical personnel.[146] Jacks for test equipment must be similarly inaccessible.

(3) Provisioning (or re-provisioning) shall not be possible through an ICE network.[147]

(4) Provisioning shall be a single, unitary block-transfer.[148]

8 Requirements Allocation

Each of the requirements in preceding sections, must be allocated to an architectural component in section 10 or labeling in section 9, following.

9 Labeling of Nonfunctional Requirements

Some system requirements (environmental or nonfunctional) are properly allocated to medical device *labeling*.[149]

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.

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

10 Functional Architecture

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 3. The behaviors

[145] requirement R7.3.0(1): *provisioning jack*
[146] requirement R7.3.0(2): *protected jack*
[147] requirement R7.3.0(3): *provisioning channel disjointness*
[148] requirement R7.3.0(4): *provisioning unitarily*
[149] 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.

of each component are summarized in Table 7.

The ICE Bus Adaptor translates the events and data from the five feature groups comprising the ICE Interface into transactions on the ICE Bus[150]. The function of the ICE Bus Adaptor is defined in section 10.8. The Maintenance Processor allows a technician to read the logs, or load the drug library through a connector behind the drug reservoir door. The function of the Maintenance Processor is defined in section 10.9.

The PCA function is partitioned into the functional components in Table 8, depicted in Figure 4.

Table 7: Top-Level Components

Component	**Behavior**
ICE Bus Adaptor	translates events and data into bus transactions
PCA	performs pump operation
Maintenance	technician access to logs, drug library

Table 8: Functional Components

Component	**Behavior**
fluid	holds and moves drug
operation	controls pump operation
safety	checks for faults; inhibits possibly hazardous infusion; signals alarms and warnings
power	coordinates battery and power supply; detects power anomalies

10.1 ICE Bus Adaptor

An *ICE interface* provides a standard[151] yet flexible way for ICE devices to communicate with the ICE system which may include ICE apps in addition to a supervisor user interface which allows a clinician, usually a nurse, to monitor and control all ICE devices used in a unit.

An ICE interface has five parts: commands, parameters, security status, and alarms. The standard ICE interface is defined using AADL prototype feature groups which may be extended by particular ICE devices to include signals particular to those devices. These feature groups are depicted in Figures 3 and 4 as colored, rectangles.

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

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

[150] ASTM-F2761 uses the term ICE “Network”

[151] A formal standard for ICE interfaces has not been determined, but will implement the intent of ASTM F2761-09 Subclause 4.4 ICE Equipment Interface.

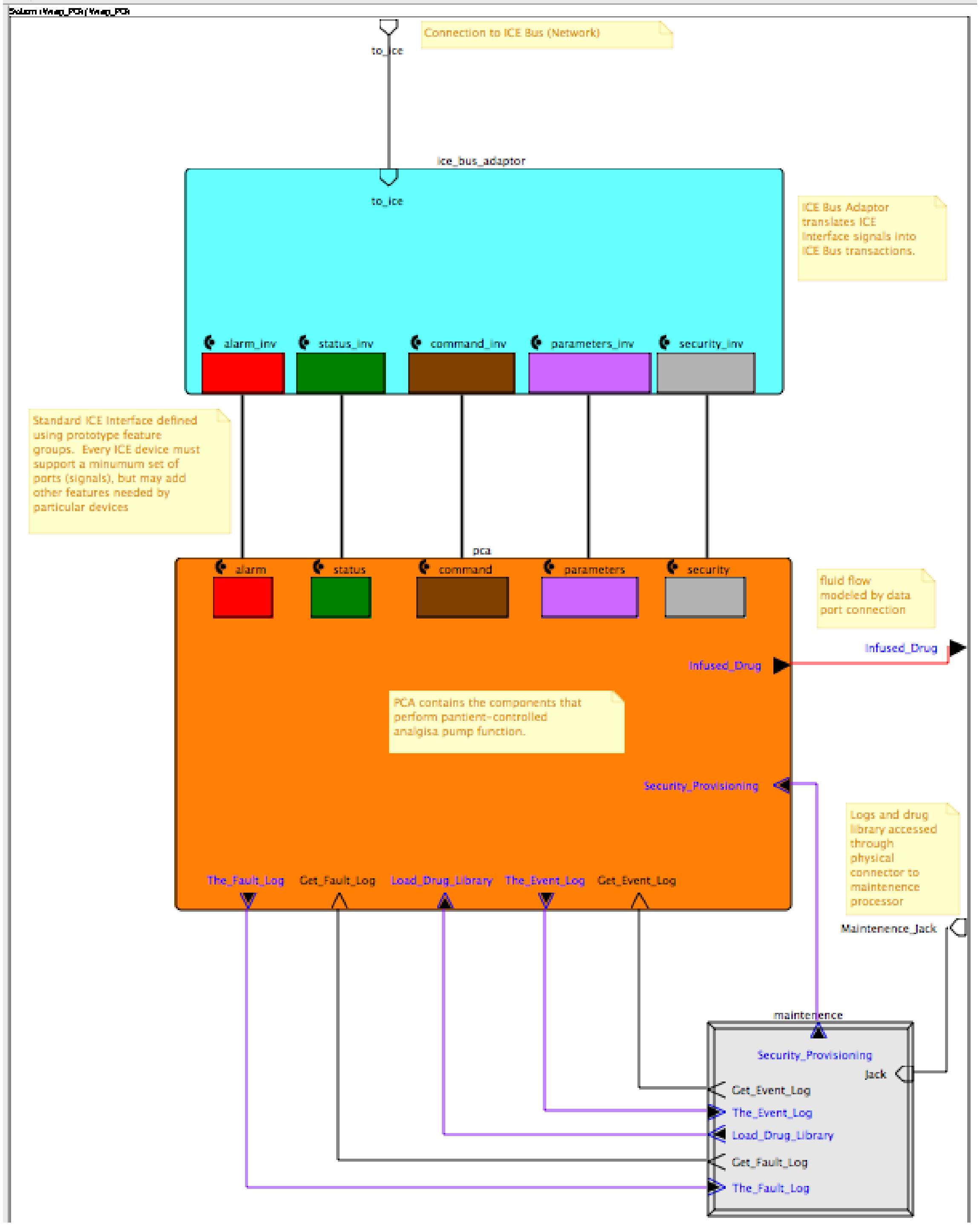
System : Wrap_PCA / Wrap_PCA
to_ice
Connection to ICE Bus (Network)
ice_bus_adaptor
to_ice
ICE Bus Adaptor translates ICE Interface signals into ICE Bus transactions.
alarm_inv
status_inv
command_inv
parameters_inv
security_inv
Standard ICE Interface defined using prototype feature groups. Every ICE device must support a minumum set of ports (signals), but may add other features needed by particular devices
pca
alarm
status
command
parameters
security
fluid flow modeled by data port connection
Infused_Drug
Infused_Drug
PCA contains the components that perform pantient-controlled analgisa pump function.
Security_Provisioning
Logs and drug library accessed through physical connector to maintenence processor
The_Fault_Log
Get_Fault_Log
Load_Drug_Library
The_Event_Log
Get_Event_Log
Maintenence_Jack
maintenence
Security_Provisioning
Jack
Get_Event_Log
The_Event_Log
Load_Drug_Library
Get_Fault_Log
The_Fault_Log

Figure 3: PCA Pump Functional Architecture Top-Level

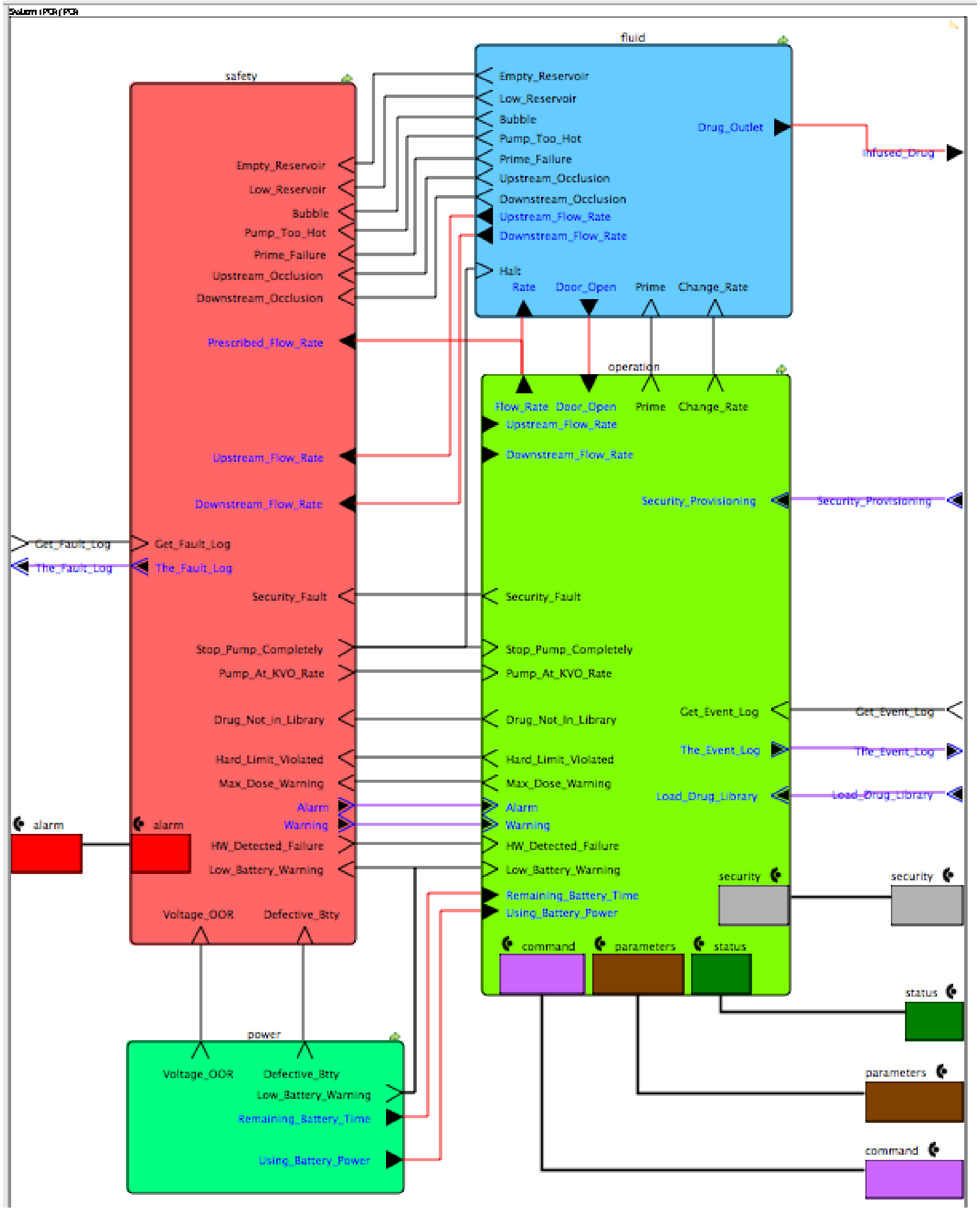

Figure 4: PCA Functional Components

R5.7.0(1) ICE operating status
R5.7.0(2) ICE alarms
R5.7.0(3) ICE bolus duration
R5.7.0(4) ICE KVO rate
R5.7.0(5) ICE resume infusion

10.2 Power Subsystem

The *power subsystem* consists of a battery, power control, and an implicit power supply as depicted in Figure 5.

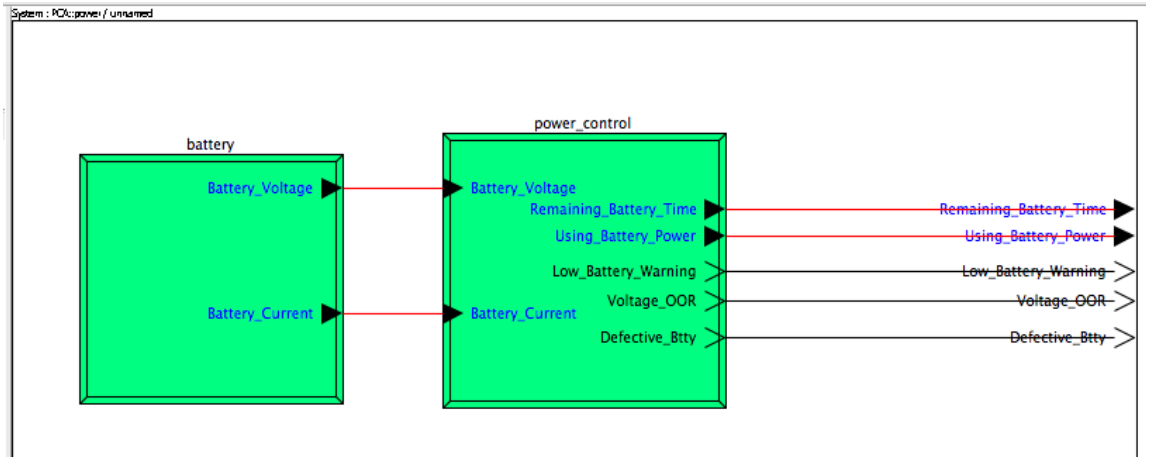

Figure 5: Power Subsystem

10.2.1 Battery

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

Allocated Requirements
R6.3.0(1) battery backup

10.2.2 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

10.3 Operation Subsystem

The *operation subsystem*, depicted in Figure 6, controls infusion, performs security operations, and operates the user interface. It also includes a scanner and patient button. The behaviors of each operation component are summarized in Table 9.

Table 9: Operation Components

Component	**Behavior**
control_panel	displays information sounds and displays alarms and warnings senses finger touch for pump control
operation_process	holds thread which controls operation
security	performs privacy and authentication
patient_button	patient request bolus
scanner	reads patient wristband, clinician badge, and drug label

10.3.1 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 an authorized clinician to start and stop infusion.[152]
- 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

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

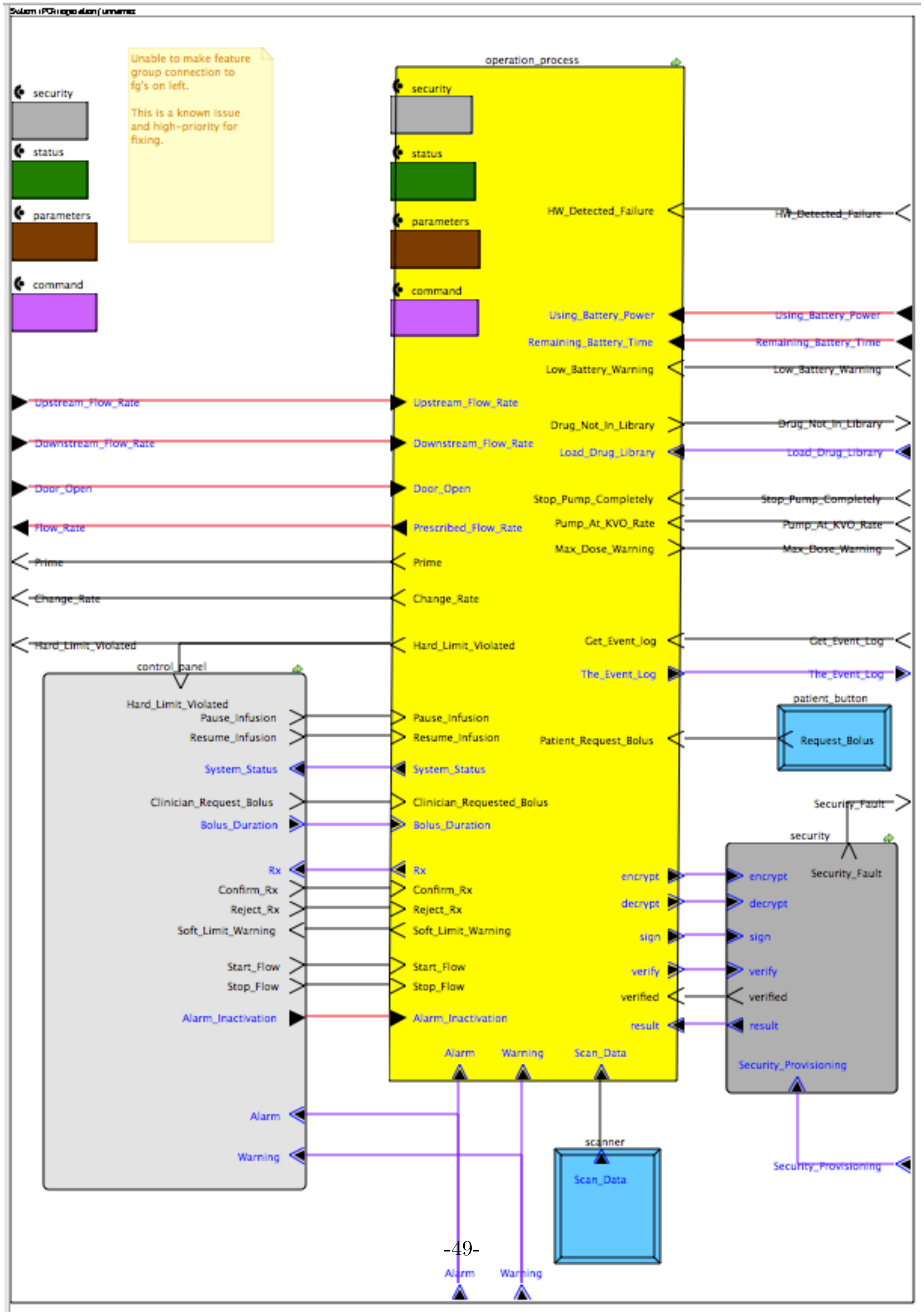

Figure 6: Operation Subsystem

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
R5.8.0(6) prescription confirmation
R5.9.0(5) hard limit
R5.9.0(6) soft limit

10.3.2 Operation Process

The *operation process* holds three threads for operation, drug library, and event logging as depicted in Figure 7.

10.3.3 Operation Thread

The *operation thread* performs primary pump operation control.

Allocated Requirements
R4.1.0(1) basal flow rate
R4.1.0(5) minimum KVO flow rate
R4.2.0(2) patient-requested bolus
R4.3.0(7) max dose warning
R5.2.0(2) halt pumping
R5.3.0(1) device parameters
R5.5.0(3) start infusion

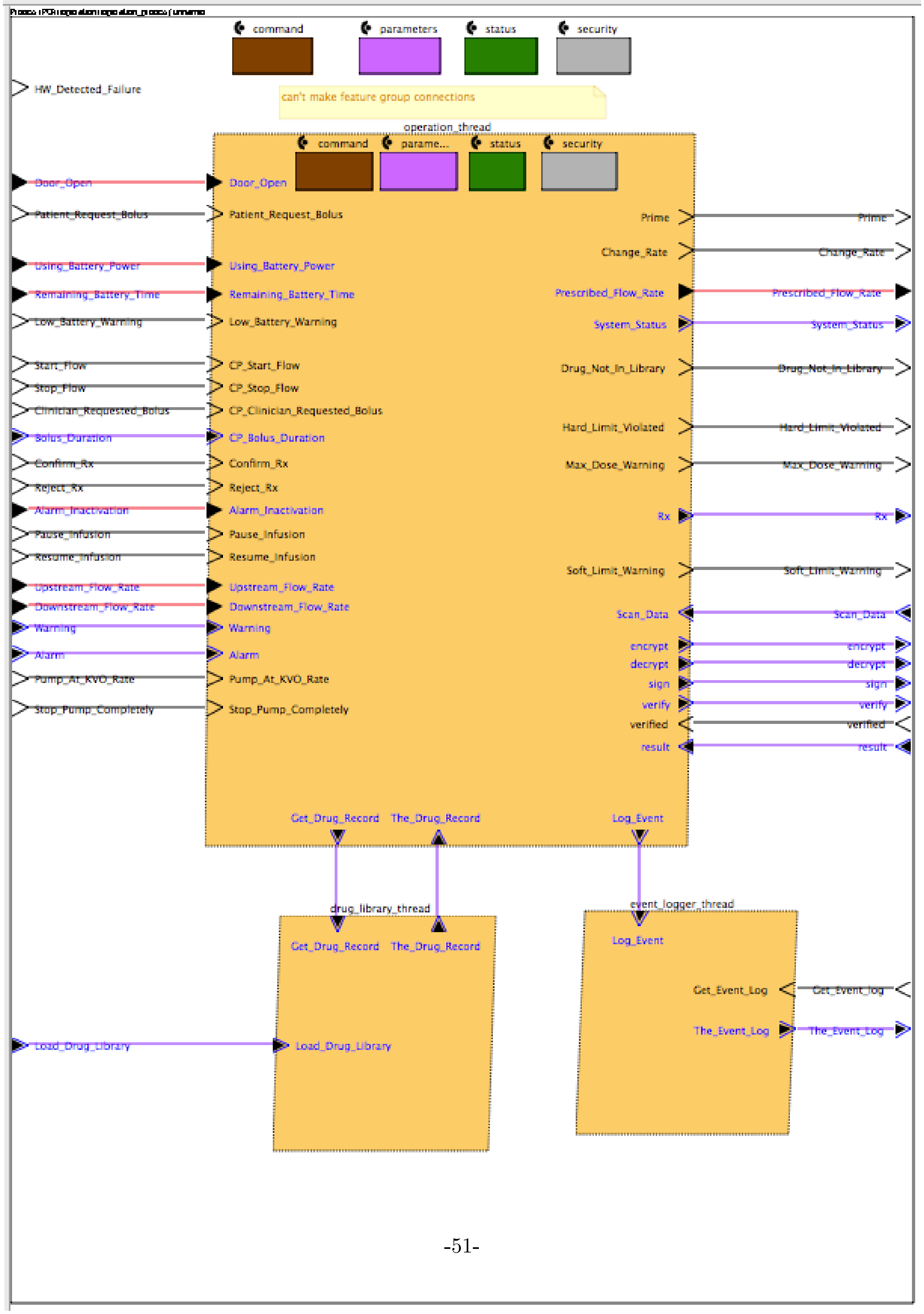

Figure 7: Operation, Drug Library, and Event Logger Threads

R5.5.0(6) stop infusion
R5.5.0(8) prescription confirmation
R5.5.0(9) soft limit confirmation
R5.5.0(10) hard limit
R5.6.0(4) prescription retention
R5.8.0(6) prescription confirmation
R5.8.0(8) drug in library
R5.9.0(3) drug library checking
R5.9.0(4) unknown drug
R5.9.0(5) hard limit
R5.9.0(6) soft limit
R6.2.0(6) occlusion alarm

10.3.4 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.

Allocated Requirements
R5.9.0(1) drug library
R5.9.0(2) drug library entry
R5.5.0(10) hard limit

10.3.5 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

10.3.6 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

10.4 Security Subsystem

The *security subsystem*, depicted in Figure 8 performs authentication calculations of patient wrist bands, clinician badges, prescription labels, drug libraries, and messages with ICE. 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.[153]

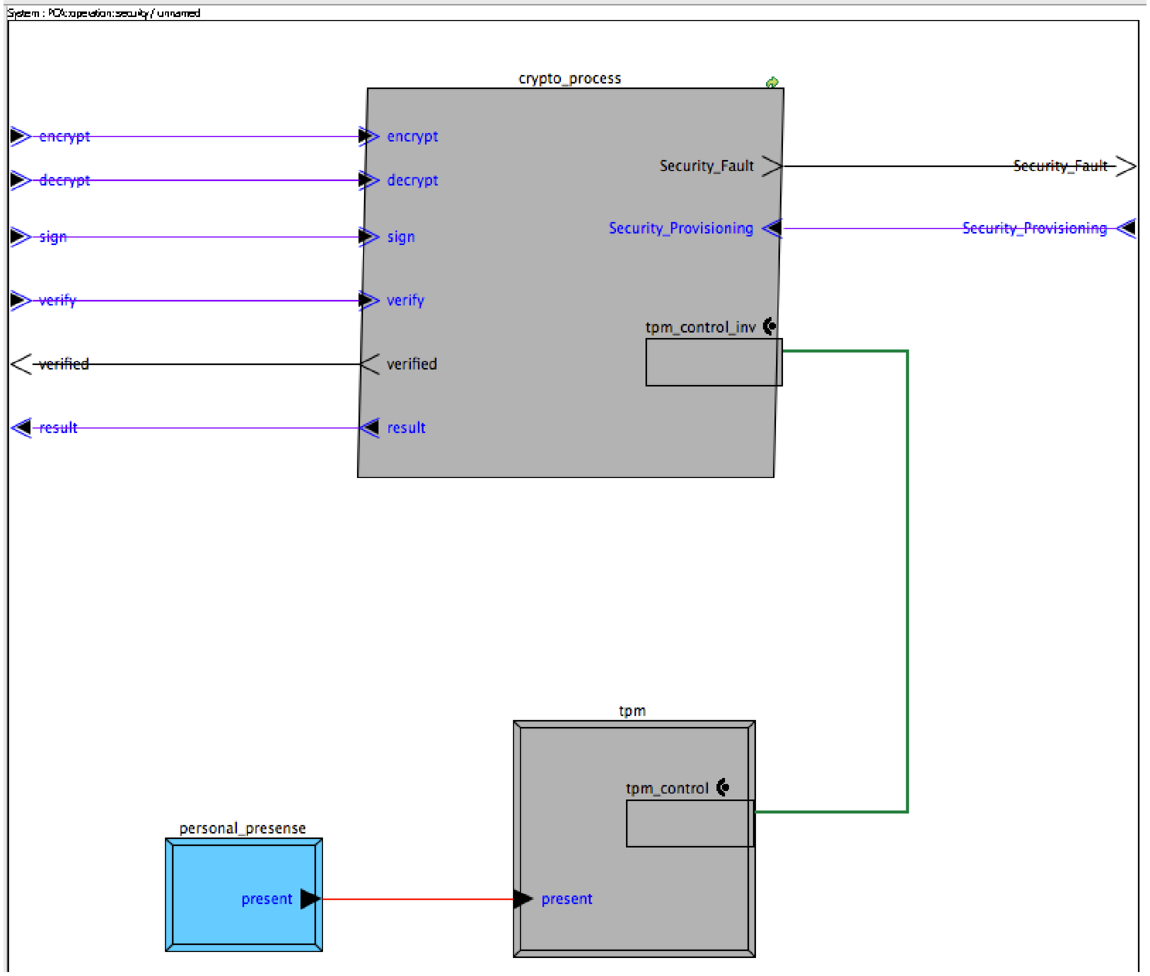

Figure 8: Security Subsystem

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

[153] Provisioning?

R7.1.0(3) prescription authentication
R7.1.0(4) drug library authentication
R7.2.0(1) confidentiality

10.5 Fluid Subsystem

The *fluid subsystem* moves drug from the reservoir to the line to the patient and is depicted in Figure 9. The drug flows from the reservoir, through the upstream monitor to the pump, then through the downstream monitor to the tube to the patient.

10.5.1 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

10.5.2 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

10.5.3 Downstream Monitor

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

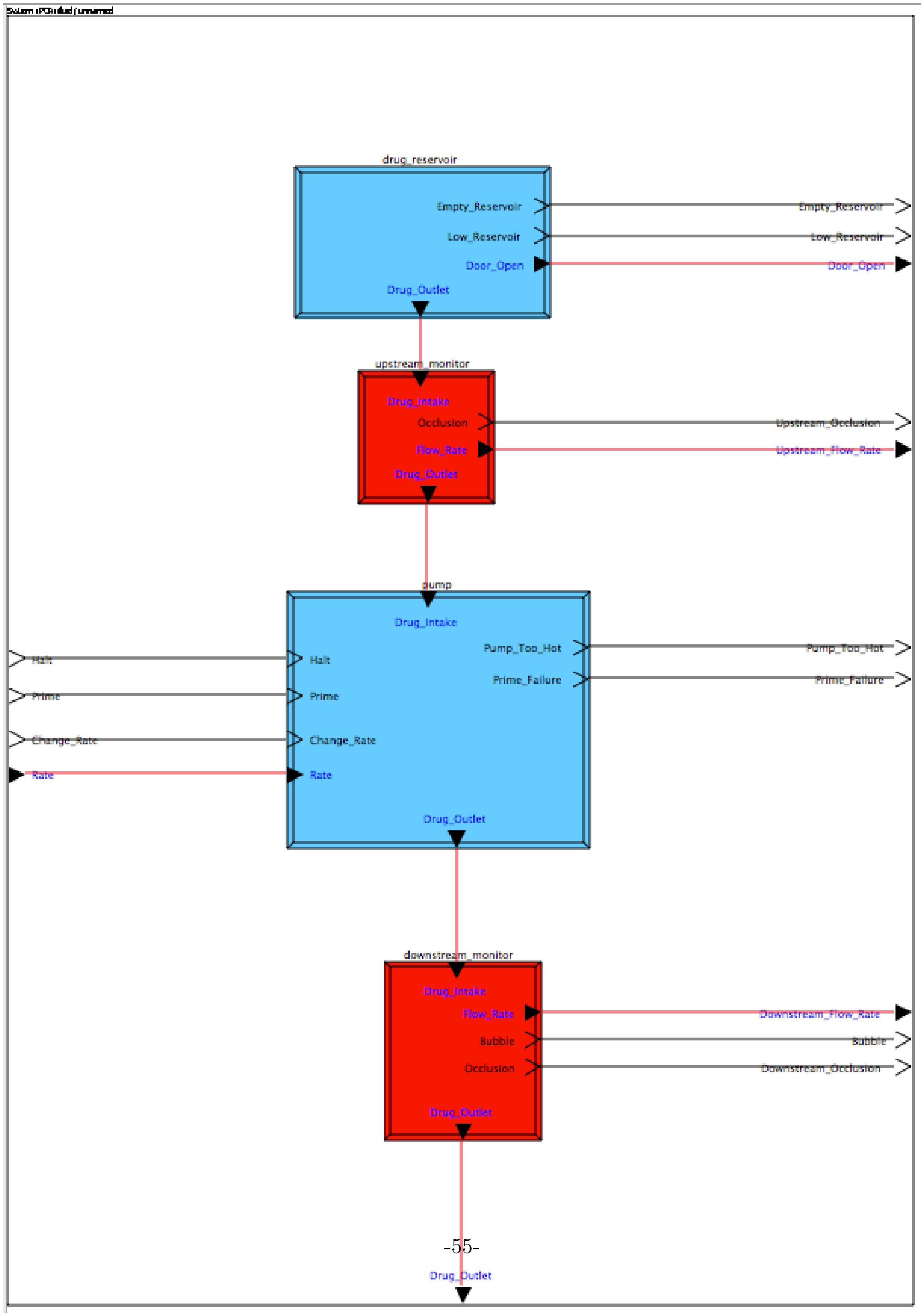

Figure 9: Fluid Subsystem

10.5.4 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

10.5.5 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.

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

10.6 Safety Subsystem

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 10, and depicted in Figure 10.

Table 10: 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

Allocated Requirements
R6.1.0(1) safety architecture

10.6.1 Failure LED

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

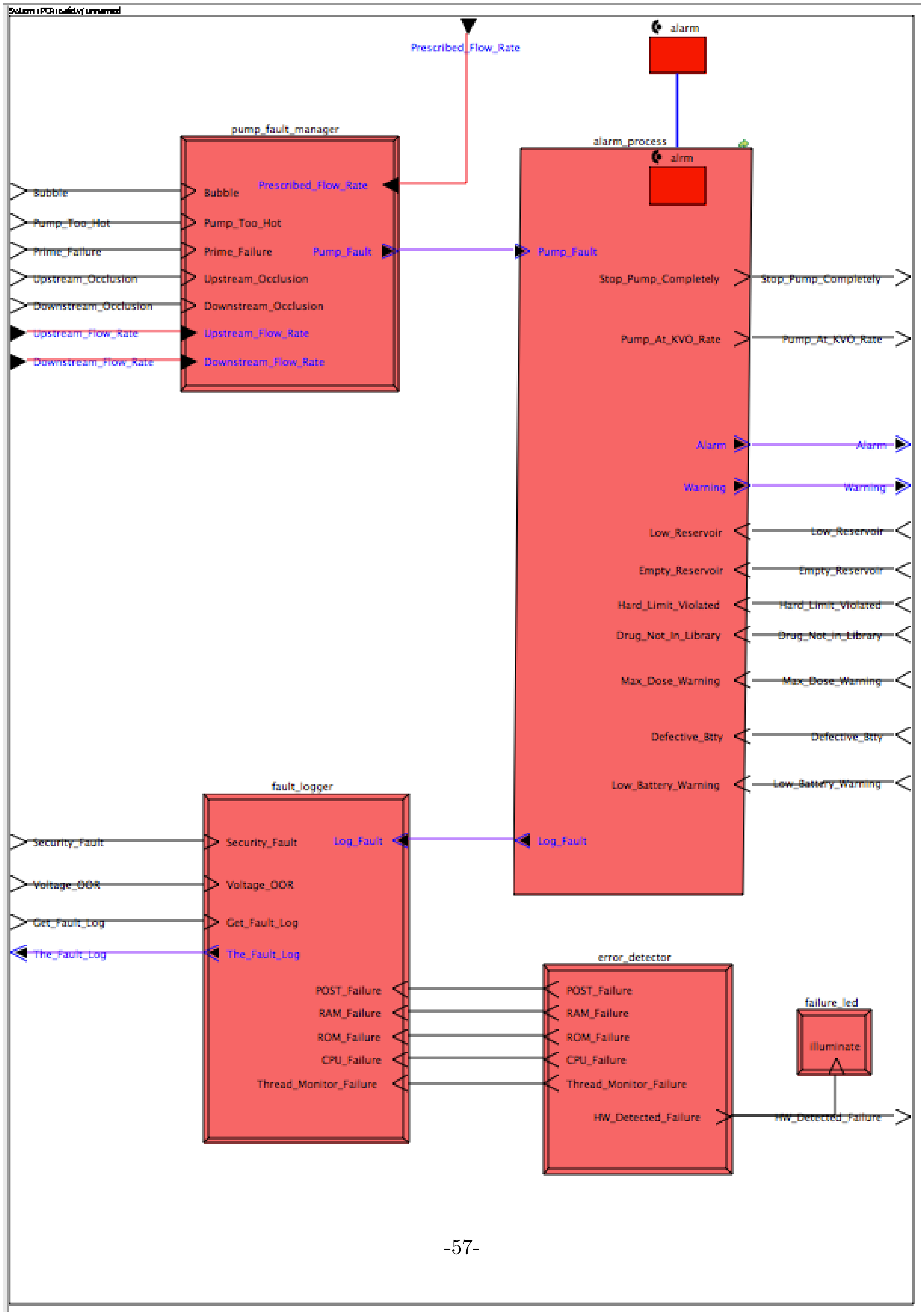

Figure 10: Safety Subsystem

Allocated Requirements
R6.4.0(7) hardware fault indicator

10.6.2 Alarm Thread

The *alarm thread* (within the alarm process) 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
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
R6.4.0(6) unmasked faults

10.6.3 Pump Fault Manager

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
R5.4.0(8) pump overheated alarm

10.6.4 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(3) continuous fault-detection
R6.4.0(4) single-event upsets

10.6.5 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 ICE 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
R5.6.0(8) real-time clock

10.7 Functional Safety Architecture

The functional *safety architecture* separates operation from error/fault detection, with a few exceptions.[154] This allows safety requirements to be more easily achieved and verified. Components comprising the functional safety architecture are:

- Upstream Monitor
- Downstream Monitor
- Pump Fault Manager
- Alarm Thread
- Error Detector
- Fault Logger
- Failure LED
- Power Control

Because a single touch screen is required, the control panel handles alarm and warning visual display, audible alert, and alarm inactivation. The "alarm" feature group of the ICE interface relays alarm and warning indications when thread execution is possible. The alarm thread determines if the event warrants change in flow rate, and if so, signals the infusion thread to halt infusion completely, or pump at the keep-vein-open rate.

[154] like detecting the pump is too hot

Allocated Requirements
R6.1.0(1) safety architecture

10.8 ICE Bus Adaptor

The *ICE bus adaptor* converts events and data on the ICE interface into network transactions on the ICE Bus.

10.9 Maintenance Processor

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

11 Initialization and Configuration

The PCA pump initializes automatically upon power-on, performing a power-on self test (POST). It is configured by loading an authenticated drug library, and scanning and authenticating the patient and clinician for their identity, and the drug container for the prescription provenance before it is loaded into the drug reservoir. Duration of clinician-requested bolus may be entered either on the control panel, or through the ICE interface.

12 Rationale

This section is meant to provide reasons for requirements so that they may be known, but not clutter the expression of the requirements with they reasons. Because this document was written to provide a public example of requirements using FAA's Requirements Engineering Management Handbook, not to build actual medical devices, the reason for requirements is merely what the author thought best. The rationale for a real device may be so voluminous to best reside in its own document with this section merely referencing it.

Index

Document Change Log

Converted from generic patient-controlled analgesia pump to ICE. Added ICE interface and reorganized document structure to follow the Requirements Engineering Management Handbook. 2/8/2012 brl

Requirements numbering, scanner, tables, use and exception cases added 3/2/2012 brl

References, functional architecture, rationale, initialization and safety architecture added 3/26/2012 brl

Requirements allocated to functional architecture 3/27/2012 brl

Architecture reorganized to separate safety architecture from operational elements; crypto processor added; exception cases for authentication failure added; functional architecture rewritten. 3/30/2012 brl

Added sound to POST, crypto_control thread, open door alarm, reverse flow, EMC, 4/5/2012 brl

Added additional security information 9/3/2012 eyv

Security provisioning channel added; all diagrams in functional architecture replaced from Adele visual architecture 9/19/2012 brl