Department of Computer & Information Science

Technical Reports (CIS)

University of Pennsylvania *Year* 2009

Generic Infusion Pump Hazard Analysis and Safety Requirements Version 1.0

David E. Arney[*] Raoul Jetley[†] Paul Jones[‡]
Insup Lee[**] Arnab Ray[††]
Oleg Sokolsky[‡‡] Yi Zhang[§]

[*]University of Pennsylvania
[†]Office of Science and Engineering Laboratories, Food and Drug Administration
[‡]Office of Science and Engineering Laboratories, Food and Drug Administration
[**]University of Pennsylvania, lee@cis.upenn.edu
[††]Fraunhofer Center for Experimental Software Engineering
[‡‡]University of Pennsylvania, sokolsky@cis.upenn.edu
[§]Office of Science and Engineering Laboratories, Food and Drug Administration

Generic Infusion Pump Hazard Analysis and Safety Requirements Version 1.0

David Arney[1], Raoul Jetley[2], Paul Jones[2], Insup Lee[1], Arnab Ray[3], Oleg Sokolsky[1], Yi Zhang[2]
1 University of Pennsylvania
2 Office of Science and Engineering Laboratories, Food and Drug Administration
3 Fraunhofer Center for Experimental Software Engineering

February 6, 2009

Abstract

The Generic Infusion Pump (or GIP) project is an effort to make generic formal models of infusion pump systems. Our process of building these formal models started with requirements elicitation and hazard analysis. This document contains the informal requirements and hazard analysis used to create a generic pump model.

We plan to use these models and properties to generate tests which can be used for conformance testing infusion pump implementations. Our future work will focus on extending these pump models with additional safety requirements and exploring the use of test generation for conformance testing real pump implementations.

Contents

1 Introduction

The goal of the Generic Infusion Pump (GIP) project is to develop a set of models and reference specifications of generic infusion pumps to verify the correct functioning of software for different types of infusion pumps submitted for FDA approval. The project defines a reference specification of a generic infusion pump which device manufacturers could use to develop more specialized pumps. Using a recognized reference specification would allow device manufacturers to concentrate on the specialized functionality of their particular pump devices and simplify the verification process. In addition, the generic infusion pump itself can be extended to provide reference specifications of more specialized pumps, such as volumetric and patient controlled analgesic (PCA) pumps. The purpose of this document is to supply a hazard analysis and define requirements of a generic infusion pump.

2 Hazard Analysis

2.1 Hazards

Hazardous or potentially harmful situations for the generic infusion pump can be classified under the following categories

1. Operational Hazards
2. Environmental Hazards
3. Electrical Hazards
4. Hardware Hazards
5. Software Hazards
6. Mechanical Hazards (Physical Hazards)
7. Biological and Chemical Hazards
8. Use Hazards

2.2 Alarms and Alerts

Pump Actions In response to a hazardous event, the pump can perform the following (software) actions:

- Alarm (p): An alarm consists of audio and video signals. 'p' indicates a specific type of alarm, e.g., occlusion.
- Alert (p): A warning issued to the user. Typically just a visual signal. Infusion should not be stopped.
- Log (): An entry made in the pump log.
- Stop (): Pump stops infusion.

The following alarms are defined for the generic infusion pump:

1. Occlusion
2. Air-in-line
3. Dead battery / No power
4. Empty Reservoir
5. No reservoir
6. Dose limit / Bolus limit Exceeded
7. Key pressed alarm
8. POST failure issued when one of the POST tests fails

    a CPU test failure
    b ROM / RAM CRC test failure
    c Battery test failure
    d Stuck key test failure
    e Watchdog test failure

f Real Time Clock test failure
g Tone test failure

9. Watchdog alarm issued when the watchdog timer/counter reaches zero
10. Overheating
11. Channel disconnected
12. Sensor failure
13. Defective battery / Battery cannot be charged
14. A-to-D conversion failed
15. System failure issued when one of the system checks fails

The alerts for the generic infusion pump include the following:

1. Low battery
2. Dose out of range / Check dose settings
3. Low Reservoir
4. Panel unlocked / door open
5. Infusion set not loaded properly
6. Dose error reduction check failed / Dose set out of range
7. Key press required (a key input is required, while the pump is idle for ¿5minutes)

2.3 Pump Checks

Apart from these responses to hazardous situations, the generic infusion pump also has the following safety mechanisms to prevent, or detect, anomalies:

- POST checks
- Watchdog interrupt tests
- (Periodic) System checks
- Sensor checks
- Dose error reduction tests

2.3.1 POST Checks

Power On Self Tests (POST) are done at startup to check whether the device's hardware is functional.

1. CPU test
2. ROM / RAM CRC test
3. Battery test
4. Stuck key test
5. Watchdog test
6. Real Time Clock test
7. Tone test

2.3.2 (Periodic) System Checks

a System checks
b A RAM test shall periodically check different sections of the RAM through low-level drivers.
c A ROM CRC test shall periodically check different sections of the ROM through low-level drivers.
d A CPU test shall be performed once every 60 minutes to check the processors code register.
e A Communications test shall be performed during all RF/wireless communication, checking the CRC for each packet received. A packet that is dropped shall be re-transmitted at least n times.
f A System failure alarm shall be issued if any of the system checks fail.

2.4 Hazard Analysis

2.4.1 Operational Hazards

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
1.1	Overinfusion	All	Programmed flow rate too high	Alarm(); Log()	Drug library	1.1, 1.4.4, 1.4.11
1.2	Overinfusion	All	Dose limit exceeded due to too many bolus requests	Alarm(); Log()	Flow sensor	1.4, 3.4.6
1.3	Overinfusion	All	(Programmed) Bolus volume/concentration too high	Alarm(); Log()	Drug library	1.4, 3.4.6
1.4	Overinfusion/ Underinfusion	All	Incorrect drug concentration specified	Alarm(); Log()	Barcode scanner	1.1, 6.1.3, 6.1.4
1.5	Underinfusion	All	Programmed flow rate too low	Alarm(); Log()	Drug library	1.1, 6.1.3, 6.1.4
1.6	Underinfusion	FRN	Air in line	Alarm(); Log()	Flow sensor	1.9
1.7	Underinfusion	FRN	Occlusion (supply side and patient side)	Alarm(); Log()	Flow sensor	1.10
1.8	Underinfusion	FRN	Reservoir empty Alarm(); Log()	Flow sensor;	Drug library	1.5
1.9	Underinfusion	FRN	Reservoir low Alert(); Log()	Flow sensor;	Drug library	1.5
1.10	Underinfusion	All	Flow rate does not match programmed rate	Alarm(); Log()	Flow sensor	1.2, 6.1.3, 6.1.4
1.11	Deflation issue	FRN	Inability of device and/or device components to release gas or air	Alert(); Log()		
1.12	Filling problem	All	Inability to Auto fill	Alert(); Log()		
1.13	Improper flow	FRN	Free flow of drug	Alarm(); Log()	Flow sensor	1.2.2
1.14	Improper flow	FRN	Bleed back; Reflux within device	Alarm(); Log()	Flow sensor	1.8
1.15	Improper flow	FRN	Fluctuation of Tidal Volume	Alarm(); Log()		
1.16	Improper flow	All	Inaccurate flow rate; Infusion intermittent	Alarm(); Log()	Flow sensor	1.2
1.17	Inflation issue	FRN	Inability of device and/or device components to expand or enlarge with gas or air	Alert(); Log()		
1.18	Low Pressure	All	Decrease in Pressure; No Pressure	Alarm(); Log()		1.10.3, 1.10.4, 1.10.5

1.19	High Pressure	All	Increase in Pressure	Alarm(); Log()		1.10.3, 1.10.4, 1.10.5
1.20	Low Pump speed	All	Decreased pump speed; Pumping stopped	Alarm(); Log()	Flow sensor	1.1.5, 1.1.8, 1.2.3
1.21	High Pump speed	All	Increased pump speed	Alarm(); Log()	Flow sensor	1.2.3
1.22	Failure to alarm	All	Defective alarm unit; Delayed alarm detection	Log()		
1.23	False alarm	All	Log()			
1.24	Failure to prime	FRN	Air in line	Alert(); Log()	Flow sensor	1.9
1.25	Incorrect therapy	FRN	Prescription/dosage values fall out of default value range	Alert(); Log()	Drug library; Barcode scanner	5.1
1.26	False alarm	FRN	Inappropriate prompts	Log()		
1.27	Air bubble introduced in blood stream	All	Air in line	Alarm(); Log()	Flow sensor	1.9
1.28	Incorrect therapy	FRN	Rate or Dose cannot be read from order			
1.28	Underinfusion	FRN	Pump programmed but 'start' not pressed	Alert(); Log();		

2.4.2 Environmental Hazards

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
2.1	Failure to operate/ Pump malfunction	All	Temperature /Humidity/ Air pressure too high or too low			7.1
2.2	Contamination	FRN	Contamination due to spillage / exposure to toxins			
2.3	Incorrect therapy	FRN	Patient is underweight; Patient is overweight; Patient has medical condition that disallows use of specific pump	Alert(); Log()	Barcode scanner	5.1.1
2.4	Failure to attend alarm	All	Background noise (may cause alarms not being heard by medic)			3.2.3
2.5	Failure to attend alarm	FRN	Patient muffles alarm (ambulatory/portable pump)			3.2.3

2.6	Failure to attend alarm	FRN	Inaudible or no voice prompts			3.2.3
2.7	Tampering	FRN	Patient tampers with pump settings without authorization			2.1
2.8	Tampering	FRN	Panel lock broken or opened during infusion	Alert(); Stop()		2.1, 3.3
2.9	Tampering	FRN	Panel/door opened during infusion; Infusion started when door open	Alert(); Log()		2.1, 3.3
2.10	Interference	All	Electrical interference from cell phones, ESD etc.			6.1
2.11	Interference	FRN	Inadequate shielding provided			6.1
2.12	Overheating	FRN	Fire			7.1.2
2.13	Contamination	FRN	Battery leak			
2.14	Tampering	FRN	Children or animals pull tubing, press buttons			

2.4.3 Electrical Hazards

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
3.1	Overheating	FRN	Incorrect or loose interconnections between devices channel error;	Alarm(); Log()		7.1.2
3.2	Overheating	FRN	Supply processor charge too high; Insufficient cooling/faulty heat sink; Unintended magnet quench	Alarm(); Log()		7.1.2, 7.3
3.3	Charge Error	All	Battery could not be charged	Alarm(); Log()		4.1.8
3.4	Supply Voltage Error	FRN	Supply voltage too high; Supply voltage too low; Battery voltage exceeds limits			7.3
3.5	Battery Failure	FRN	Battery voltage too low; Battery depleted	Alarm(); Log()		4.1
3.6	A-to-D conversion Failure	All	A-to-D conversion failed			
3.7	Electric shock	FRN	Leakage Current too high (pump could be source of electric shock)			4.2.1

3.8	Electric shock	FRN	Electrical power failure;	Power surge		4.1.9
3.9	Electric shock	All	Inadequate resistance;	Loss of resistance		
3.10	Circuit failure	FRN	Electrical shorting;	High impedance; Low impedance		4.1.9
3.11	Electromagnetic compatibility issue	FRN	Electromagnetic interference; Electrostatic discharge; Radiofrequency interference			

2.4.4 Hardware Hazards

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
4.1	System failure	All	Malfunctioning component	Alarm(); Log()		3.3, 3.5
4.2	System failure	FRN	System malfunction RTC not synchronized (date/time register not same as the RTC); Clock frequency check failed			3.3, 3.4
4.3	System failure	All	CPU test failed; One or more of the system components failed			3.3, 3.4
4.4	System failure	All	Synchronization error between pump components		Drug library	3.3.4
4.5	Channel error	FRN	synchronization problem between channels on a multi-channel pump			3.5
4.6	Network error	FRN	Pump not compatible with networked / integrated device			3.3.4
4.7	Memory failure	FRN	System malfunction RAM test failed; Attempted write to memory failed; Critical value data integrity error			3.3, 3.4
4.8	Memory failure	FRN	System malfunction ROM (or external flash memory) CRC test failed			3.3, 3.4

4.9	Watchdog failure	All	System malfunction Watchdog timer test failed; Watchdog not interrupted in 90 seconds			3.4.4.5
4.10	False alarm	All	False watchdog interrupt			
4.11	Incorrect test results	All	False negative test result; False positive test result; Incorrect measurement; Test result inaccurate			
4.12	Incorrect dose value entered	FRN	Key debounce not detected		Drug library	2.3
4.13	Failure to alarm	All	Sensor failure			

2.4.5 Software Hazards

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
5.1	Data error	FRN	Failure to backup; Data retrieval error; Could not write to pump log			1.7.1
5.2	Data error	FRN	Unable to retrieve data from drug library; Failure to transmit record			
5.3	Incorrect version	FRN	Software updates not installed; Incorrect version installed		Barcode scanner	5.1.8
5.4	Failure to alarm	All	Communication problem between channels	Log()		
5.5	Pump could not be silenced	FRN	Alarm priority set incorrectly	Log()		
5.6	Incorrect dose administered	FRN	Incorrect drug library; Old version of drug library			5.1.8
5.7	Channel error	FRN	Failure to recognize new channels added to pump			
5.8	Communication error	All	System malfunction RF Communication test failed			3.3.4
5.9	Pump failed to startup	FRN	One or more of the POST tests failed			3.4.5
5.10	Pump failed to shut down	All	Failure to auto-stop (following a critical failure that requires pump to be stopped)			

5.11	Pump reverts to default dose values	All	Programmed dose set incorrectly; Inappropriate reset to default		Drug library	5.1.3
5.12	Incorrect test results	All	False negative test result; False positive test result; Incorrect measurement; Test result inaccurate			

2.4.6 Mechanical Hazards (Physical Hazards)

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
6.1	Unable to set dose, start/ stop/ reset pump, silence alarm	FRN	Broken part (e.g., broken keypad)		Alert()	3.3
6.2	Incorrect dose value entered	FRN	Key stuck / depressed		Alarm()	2.3
6.3	No alarm signal	FRN	Speaker / Audio unit failure		Log()	3.3
6.4	Physical Damage to pump	All	Falling; Shear; Stress			
6.5	Injury to medic/patient	FRN	Sharp edges			
6.6	Pump stops infusion	All	Pump motor fails; Pump unable to stroke		Flow sensor	3.5
6.7	Physical Damage to pump	All	Chemical damage from cleaning fluid			
6.8	Physical Damage to pump	All	Fluid ingress			

2.4.7 Biological and Chemical Hazards

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
7.1	Biological / Chemical Hazard	FRN	Device contaminated during use; Device contaminated by blood-/leaking fluid			
7.2	Biological / Chemical Hazard	FRN	Inadequate device cleaning; Residue after contamination; Failure to flush; Failure to disinfect			

2.4.8 Use Hazards

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
8.1	Overfill	All	Incorrect fill volume specified Alert(); Log()		Barcode scanner	
8.2	Short fill	All	Incorrect fill volume specified Alert(); Log()		Barcode scanner	
8.3	Knowledge-based failure	All	Operating instructions incomplete; Inaccurate labeling		Barcode scanner	
8.4	Knowledge-based failure	FRN	Medic fails to recognize hazardous situation			
8.5	Knowledge-based failure	FRN	Pump does not display adequate dosage information on the display			
8.6	Rule-based failure	FRN	Incorrect prescription given to patient; Incorrect drug library loaded		Barcode scanner	2.2, 5.1.8
8.7	Overinfusion	FRN	User / Patient change infusion settings inadvertently		Drug library	2.2, 5.1
8.8	Underinfusion	FRN	User / Patient change infusion settings inadvertently		Drug library	2.2, 5.1
8.9	Patient incapacitated	FRN	Home care patient unable to administer dosage/service alarm condition			
8.10	Attentional failure	All	Incorrect prescription entered			2.2, 5.1
8.11	Memory failure	FRN		Too few doses administered; Patient given multiple doses	Flow sensor	
8.12	Incorrect dose settings	FRN	Key pressed too long	Alarm()		2.3.1
8.13	Inadequate training	All	User not trained to use pump; User not familiar with pump			
8.14	Incorrect dose mode	FRN	Incorrect units used for specifying dose parameters (e.g., ml/hr instead of mcg/hr)		Barcode scanner	

3 Safety Requirements

This Section lists safety requirements for the generic infusion pump (GIP) model. The requirements include safety features and constraints for a general-purpose infusion pump. Configuration parameters for the model are identified and enumerated based on these requirements.

1 Infusion Control

1.1 Flow rate

1.1.1 The flow rate for the pump (for both primary and secondary infusions) shall be programmable.

1.1.2 At minimum, the pump shall be able to deliver primary (basal) infusion at flows throughout the range of 0.1 to 999 ml/hr.

1.1.3 For a Small-volume pump (i.e., pumps that provide microinfusion flows as low as 0.1 ml/hr), the maximum flow rate shall be limited to 99.9 ml/hr.

1.1.4 For a Large-volume pump (i.e., pumps that provide macroinfusion flows up to 999 ml/hr), the minimum flow rate shall be at least 1 ml/hr.

1.1.5 Flow discontinuity at low flows (1 ml/hr or less) should be minimal.

1.1.6 The basal delivery rate shall be programmable for durations of up to 24 hours.

1.1.7 An active basal shall continue to be delivered without change while programming basal rates.

1.1.8 The pump should maintain a minimum KVO (keep vein open) rate of x ml/hr at all times during infusion.

1.2 Flow rate accuracy

1.2.1 During extended operation, the flow rate shall remain accurate within 5% of the rate setting for at least 72 hours of continuous use.

1.2.2 If the pump is equipped with a flow rate sensor and the flow rate exceeds the programmed rate setting by more than 10% over a period of more than 15 minutes, or if the pump goes into free flow, the pump shall issue an alarm to indicate overinfusion of the patient. [identify hazards that may result in flow rate $> 110\%$]

1.2.3 If the pump is equipped with a flow rate sensor and the flow rate is less than 90% of the programmed rate setting over a period of 15 minutes, the pump shall issue an alarm to indicate underinfusion of the patient. [identify hazards that may result in flow rate $< 90\%$]

1.3 Volume to be infused (VTBI)

1.3.1 For small-volume pumps (i.e., pumps that provide microinfusion flows as low as 0.1 ml/hr), VTBI (Volume to be Infused) settings shall cover the range from 0.1 to 999 ml.

1.3.2 For large volume pumps, VTBI (Volume to be Infused) settings shall cover the range from 1 to 9,999 ml.

1.3.3 For small-volume pumps, the user shall be able to set the VTBI in 0.1 ml increments for volumes below 1 ml.

1.3.4 For large-volume pumps, the user shall be able to set the VTBI in 1 ml increments for volumes below 100 ml.

1.3.5 For small-volume pumps, the user shall be able to set the VTBI in 10 ml increments for volumes above 100 ml.

1.3.6 For large-volume pumps, the user shall be able to set the VTBI in 100 ml increments for volumes above 1000 ml.

1.4 Bolus Dose

1.4.1 A normal bolus dose shall be given when requested by the patient .A square bolus may be programmed to be administered over a period of time.

1.4.2 The flow rate for normal and square bolus doses shall be separately programmable.

1.4.3 The combined flow rate (basal rate + maximum of programmed normal and square bolus dose rates) shall be limited by the maximum flow rate for the pump.

1.4.4 A bolus dose shall not change the programmed (basal) flow rate.

1.4.5 A normal bolus shall take precedence over a programmed square bolus. The square bolus shall be suspended while the normal bolus dose is administered.

1.4.6 At the completion of the normal bolus dose, the square bolus shall continue delivery.

1.4.7 Delivery of a square bolus shall be distributed evenly over the duration of the bolus.

1.4.8 The pump cannot be programmed to have more than one square bolus at a time.

1.4.9 The maximum programmable duration for a square bolus shall be limited to x hrs.

1.4.10 The maximum programmable period for a square bolus shall be limited to x hrs.

1.4.11 No normal bolus doses should be administered when the pump is alarming (in an error state).

1.4.12 If a bolus request causes the bolus dose to exceed the maximum permissible limit (for a given time period), the pump shall issue a Dose limit exceeded alarm.

1.5 Drug reservoir

1.5.1 The reservoir volume and time remaining shall be calculated initially before an infusion is started.

1.5.2 The calculated reservoir time shall be accurate to 3 minutes.

1.5.3 The reservoir time remaining shall be re-calculated every time the current basal flow rate is changed.

1.5.4 The reservoir time remaining shall be re-calculated at the beginning of every bolus dose.

1.5.5 If the current value / calculated volume of the reservoir is less than x ml, and an infusion is in progress, a Low Reservoir alert shall be issued.

1.5.6 If the current value / calculated volume of the reservoir is 0 ml, and an infusion is in progress, an Empty Reservoir alarm shall be issued.

1.6 Pump suspend

1.6.1 When the option to suspend the pump is selected, the current pump stroke shall be completed prior to suspending the pump.

1.6.2 If the suspend occurs due to a fault condition, the pump shall be stopped immediately without completing the current pump stroke.

1.7 Data retention

1.7.1 If the pump is turned off, it shall retain the programmed dose settings and patient data for at least 4 hours.

1.8 Reverse delivery

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

1.9 Air-in-line alarm

1.9.1 An air-in-line alarm shall be triggered if air bubbles larger than 200 μL are detected.

1.9.2 In enteral pumps, the air-in-line alarm shall be triggered if air bubbles larger than 50 L are detected for a period of x minutes.

1.10 Occlusion alarm

1.10.1 An upstream occlusion alarm shall be triggered if the pump senses an upstream (fluid-container side) occlusion.

1.10.2 A downstream occlusion alarm shall be triggered if the pump senses a downstream (patient side) occlusion.

1.10.3 The downstream occlusion pressure limit shall be less than 20 psi (1034 mm Hg).

1.10.4 The upstream occlusion pressure limit shall be greater than y psi (z mm Hg).

1.10.5 When an occlusion occurs, the pump shall stop flow and alarm as quickly as possible (within a maximum delay time of x seconds).

1.10.6 When an occlusion occurs, the pump should release any built-up pressure in the tubing set. This may require reversing the pump mechanism momentarily.

1.10.7 After the occlusion is removed, the bolus volume released should be most 0.5 ml.

2 User Interface

2.1 Resistance to tampering and accidents

2.1.1 To avoid accidental tampering of the pumps settings such as the flow rate/VTBI, at least two steps should be required to change the settings.

2.1.2 Changing settings, such as the patients weight or infusion duration, while the pump is infusing, should either not be allowed, or at least require confirmation.

2.1.3 The administration set should be designed to prevent compromising patient safety or cause an unacceptable flow error.

2.1.4 There shall be no multiple-key legal values. That is, there should be no legal inputs that require multiple keys to be pressed simultaneously.

2.1.5 If the numeric keypad cover is broken or unlocked during infusion, the pump should issue an alarm to indicate illegal tampering.

2.2 User input

2.2.1 If the pump is in a state where user input is required, the pump shall issue periodic alerts/indications every 15 minutes till the required input is provided.

2.2.2 The pump shall issue an alert if paused for more than x minutes

2.2.3 Clearing of the pump settings and resetting of the pump shall require confirmation.

2.2.4 If the pump is idle for 5 minutes while programming a dose setting, the pump shall issue an alert to indicate that the user needs to finish programming/start infusion

2.2.5 If the pump is idle for more than 10 minutes while programming a dose setting, the pump shall issue an alarm and clear the dose parameters defined.

2.2.6 Each time the pump is turned on, the system should require the user to indicate whether the pump is being used on a new patient and to select (or confirm, if not a new patient) the current clinical location.

2.2.7 For a multi-channel pump:

2.2.7.1 The pump should display the drug/solution name and dose being infused by each channel.

2.2.7.2 The system should trigger an alert if the same drug or solution is programmed on more than one channel. It should be possible to override the alert if the programming is intentional.

2.3 Keypad

2.3.1 If a key that is not functioning as a repeating key is held down for one minute, either through a fault condition, purposely by the user, or by inadvertently contacting another surface, the pump shall issue a Key depressed alarm.

2.3.2 A key that is depressed shall not be identified as a distinct key press for a period of 1 second (i.e., a key must be pressed for more than 1 second to recognize it as a distinct input)
[More requirements to be added]

3 Error Handling

3.1 Alarm signaling

3.1.1 An alarm condition shall be indicated through both audio and visual signals.

3.1.2 Alarms should clearly indicate the specific problem causing the alarm condition.

3.1.3 Upon encountering an error condition, the remainder of any active bolus shall be cancelled.

3.2 Alarm silencing

3.2.1 It shall be possible to temporarily disable audible alarm signals; however, after silencing, the alarm should automatically reactivate after 2 minutes or less.

3.2.2 It shall not be possible to permanently disable audible alarm signals.

3.2.3 Audible alarm signals shall be in the range of 20 dB to 100 dB.

3.2.4 There shall be an audio alert on an invalid/illegal input to the pump.

3.3 Safety checks

3.3.1 A RAM test shall periodically check different sections of the RAM through low-level drivers.

3.3.2 A ROM CRC test shall periodically check different sections of the ROM through low-level drivers.

3.3.3 A CPU test shall be performed once every 60 minutes to check the processors code register.

3.3.4 A System failure alarm shall be issued if any of the safety checks fail.

3.4 POST (Power On Self Test)

3.4.1 On being powered on, the pump shall undergo a POST / power on self-test.

3.4.2 The system shall perform power-on self-tests (POST) for all devices and subassemblies possible without degrading normal operation.

3.4.3 The POST shall take no longer than 1 minute 10 seconds.

3.4.4 The POST shall include the execution of the following tests:

3.4.4.1 CPU test

3.4.4.2 ROM / RAM CRC test

3.4.4.3 Battery test

3.4.4.4 Stuck key test

3.4.4.5 Watchdog test

3.4.4.6 Real Time Clock test

3.4.4.7 Tone test

3.4.5 Any failure of a test step during POST shall abort the remaining test steps and generate the appropriate alarm for the failure.

3.4.6 No bolus dose shall be possible during the POST.

3.5 Watchdog

3.5.1 Each task involved in the pump delivery (or infusion) shall have a watchdog timer or counter associated with it to catch and stop run-away, or stalled processes.

3.5.2 The watchdog timer shall interrupt the pump if it ceases/suspends normal operation, or does not respond to user input for 90 seconds.

3.5.3 The watchdog timer shall check that each of the other tasks has responded within the last 90 seconds.

3.5.4 If any task does not respond to a watchdog test for more than 3 minutes, a Watchdog alarm shall be raised.

3.5.5 A watchdog test shall be performed by calling a low-level driver and shall generate a Watchdog Test Failure alarm upon failure.

4 Event and Error Logging

4.1 Log data

4.1.1 The pump shall maintain an electronic log to record each external (user) event.

4.1.2 The pump shall maintain an electronic log to record each fault condition, and the associated alarm and/or alert issued.

4.1.3 Each log entry shall be stamped with a corresponding date/time value.

4.1.4 Information from the logs shall not be lost when the pump is turned off.

5 Power and Battery Operations

5.1 Battery voltage

5.1.1 An active battery voltage shall be measured for the pump throughout its operation at a frequency no less than once every 3 minutes.

5.1.2 The active battery voltage shall be calculated as an average of 10 consecutive battery voltage readings.

5.1.3 The amount of battery life remaining shall be calculated as a function of the active battery voltage.

5.1.4 If the battery life remaining is less than 15 minutes, the pump shall issue a Low battery alarm. [WAS: An active battery voltage greater than 0.80 V and less than or equal to 0.95 V shall trigger a Low battery alarm.]

5.1.5 The low battery alarm shall be silenced when the pump is connected to an external power supply.

5.1.6 If the battery life remaining is less than 5 minutes, the pump shall issue a Battery depleted alarm. [WAS: An active battery voltage less than or equal to 0.80 V shall trigger a Battery depleted /No power alarm.]

5.1.7 The depleted battery alarm shall be silenced when the pump is connected to an external power supply.

5.1.8 If the pump voltage does not increase to $>$1V within 30 minutes (15 minutes when pump is idle), the pump shall issue a defective battery alarm to indicate that the battery could not be charged.

5.2 Leakage current

5.2.1 If patient leakage current greater than x mA is detected, the pump shall issue a Patient Leakage Current alarm.

5.3 Auto-off / Sleep mode

5.3.1 The pump shall transition into sleep mode if no infusion is taking place and no alarm is active and the programmed duration elapses without a key press on the user interface.

5.3.2 The pump shall transition out of the sleep mode when a user event is detected (e.g., when a key is pressed on the user interface).

5.3.3 The auto-off time duration shall be programmable in the range 0 to 24 hours in increments of 1 hour.

5.3.4 The auto-off time duration must be greater than the user input idle time (2.2.4).

6 Dose Error Reduction

6.1 Drug library

6.1.1 The pump shall include a programmable drug library configurable according to patient type (adult, pediatric, etc.) and care area (home care, ambulatory, clinic, etc.).

6.1.2 The drug library shall consist of the following entries:

6.1.2.1 List of all drugs that can be used with the pump.

6.1.2.2 The amount of drug to be infused, diluent volume and/or the drug concentration.

6.1.2.3 The dose mode for infusion (e.g., ml/hr, mg/min)

6.1.2.4 Hard and soft limits for an infusion

6.1.2.5 Hard and soft limits for a bolus dose

6.1.2.6 Hard and soft limits for a loading dose

6.1.2.7 The volume to be infused (VTBI), where applicable

6.1.3 If the programmed infusion value is out of range of the upper or lower hard limit, the pump shall issue an incorrect dose entered warning and prompt the user to re-enter the infusion value.

6.1.4 If the programmed infusion value is out of range of the upper or lower soft limit, the pump shall issue a warning indicating that a soft limit has been violated, and prompt the user for confirmation before starting the infusion. Indication of an overridden limit should be observable at least every few seconds.

6.1.5 The patient shall not be able to change the drug profile or settings for a drug in the drug library.

6.1.6 The pump should maintain a history log of drug library entries and the dates they were enabled.

6.1.7 A clear indication should be displayed any time the drug library is not in use.

6.2 Infusion settings

6.2.1 Changing the drug type shall stop any active infusion.

6.2.2 Changing the drug type shall force a restart of the infusion. The reservoir time and volume shall be recomputed.

6.3 Pump defaults

6.3.1 The pump shall have certain in-built default settings corresponding to dose and flow rate parameters.

6.3.2 The user/patient shall not be able to change the default settings.

6.3.3 The defaults shall only be modified or configured by a pump administrator.

6.3.4 The administrator screens shall be protected by a secure login/password.

6.3.5 The defaults may consist of the following (not an exhaustive list): default basal flow rate, maximum flow rate, bolus units, time display format, minimum/maximum patient weight, minimum/maximum VTBI, default drug concentrations, minimum/maximum pressure ratings.

7 System Environment

7.1 Operating conditions

7.1.1 The pump should be able to operate within a temperature range of 5 to 45 degrees C (35-40 deg C for implanted pumps).

7.1.2 If the pump gets overheated to more than x degrees Centigrade, the pump shall issue a Pump Overheated alarm.

7.1.3 The pump should be able to withstand and operate under atmospheric pressure ranging from 500 to 5000 mmHg.

7.1.4 The (external) pump should be able to operate at relative humidity ranging from 20% to 90% (non-condensing).

7.2 RF signals

7.2.1 Pumps using RF waves or other wireless technology for communication shall be constructed in accordance with FDA guidance on wireless communication and ensure that commonly encountered electromagnetic signals are unlikely to cause disruption to the infusion of fluid from the pump.

7.3 Vibration

7.3.1 Implantable pumps shall be able to withstand random vibration in accordance with EN 60068.2.64, Test Fh, under the following conditions:

7.3.1.1 test frequency range: 5 Hz to 500 Hz

7.3.1.2 acceleration spectral density: 0.7 (m/s2)2/Hz.

7.3.1.3 shape of acceleration spectral density curve: flat horizontal, 5 Hz to 500 Hz.

4 Conclusion and Future Work

We began by enumerating the large number of hazards associated with the operation of an infusion pump. This hazard analysis was the basis for the safety requirements we then developed.

We plan to use these requirements to build formal models of the generic infusion pump, which can then be analyzed for correctness based on properties from the hazard analysis, as well as structural properties such as completeness and consistency. We also plan to extend this document, for instance adding hazards and requirements related to a network connection or those specific to particular types of pumps such as PCA pumps.