CIS 890: High-Assurance Systems

Open PCA Pump and ISOSCELES Projects

Lecture PCA Pump: Open PCA Pump Architecture Overview

Objectives

- Understand the primary subsystems of a PCA Pump
- Understand the architectural decomposition of the Open PCA Pump (OPCAP) so as to enable more detailed study and research on the Open PCA Pump

Outline

- OPCAP Architecture – purpose and perspective
- Primary subsystems of the OPCAP Architecture
- Fluid Subsystem
- Power Subsystem
- Operation Subsystem
- Safety Subsystem
- Conclusion

Open PCA Pump

Purpose and Perspective

- The OPCAP artifacts are meant to present a "realistic" context for safety-critical systems and interoperable medical devices
- There is currently no real hardware corresponding to the OPCAP artifacts, but the ISOSCELES project is adapting the artifacts for a low-cost open source platform
- Compared to PCA Pumps on the market, the scope of the artifacts includes the most common and important features related to safety engineer and high assurance software development
  - *Does not capture every feature in every available pump!*

Primary Subsystems

Fluid Subsystem

- Provides low-level hardware control of pump
- Detects fault conditions associated with pump (e.g., blockage of fluid flow)

Operational Subsystem

- Controls device modes of operation and rate of pump
- Operator input/output

Safety Subsystem

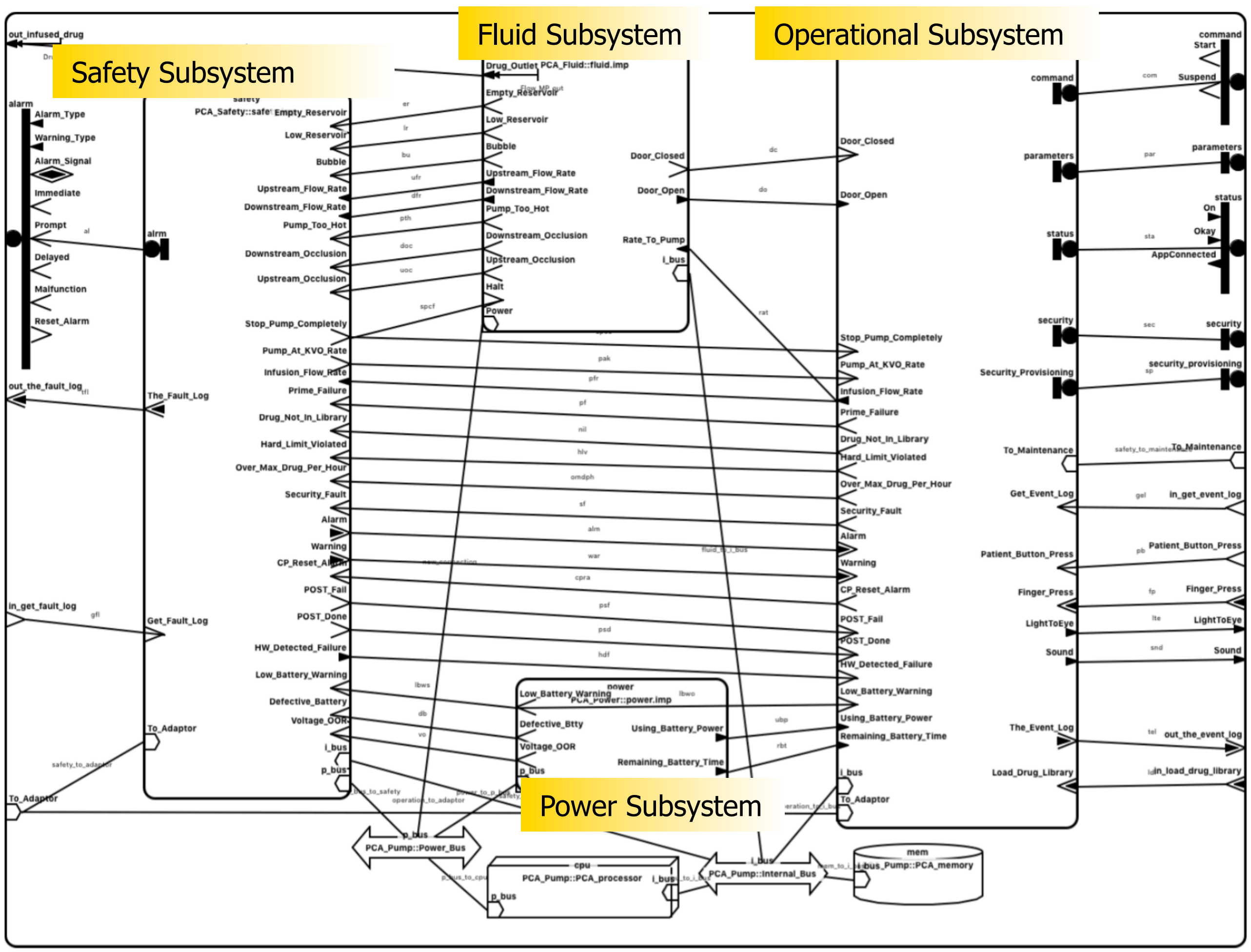
- Monitors condition of computational resources (processor, memory)
- Receives health/fault reports from other subsystems and determines if alarms should be raised
- Logs reports of problems/issues that occur during operation (including attempts to tamper with pump)

Power Subsystem

- Mostly hardware, including power supply and battery backup
- Power control logic to detect problems (e.g., voltage out of range) and to switch to battery when main power supply is disrupted

Pump Architecture

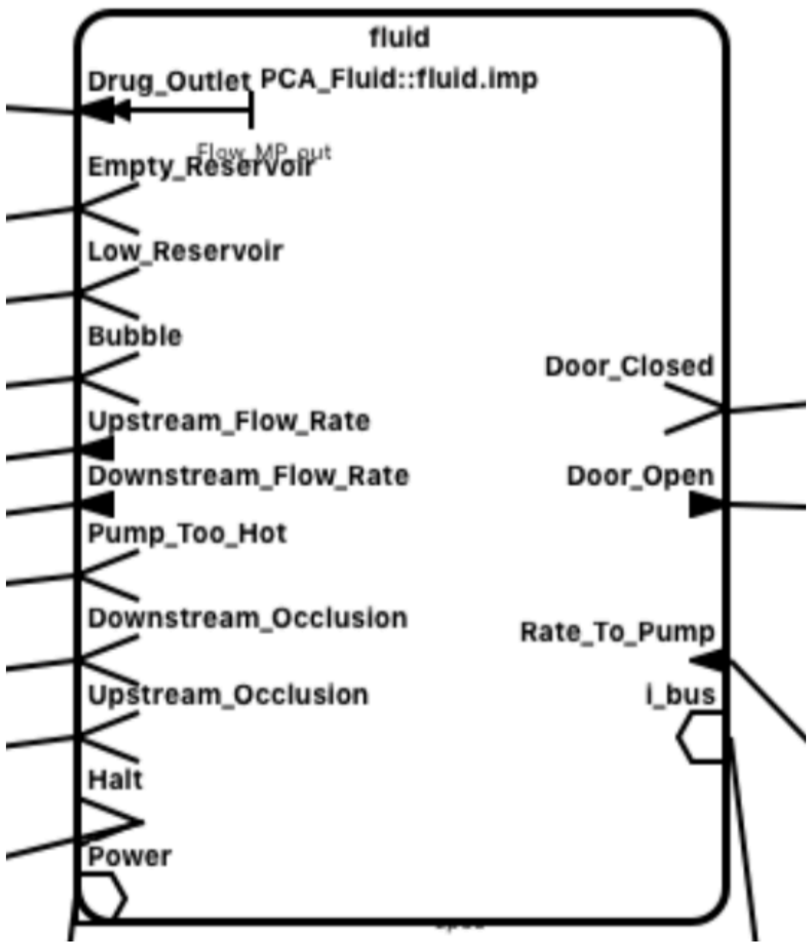
AADL Graphical View of the primary subsystems of the PCA Device



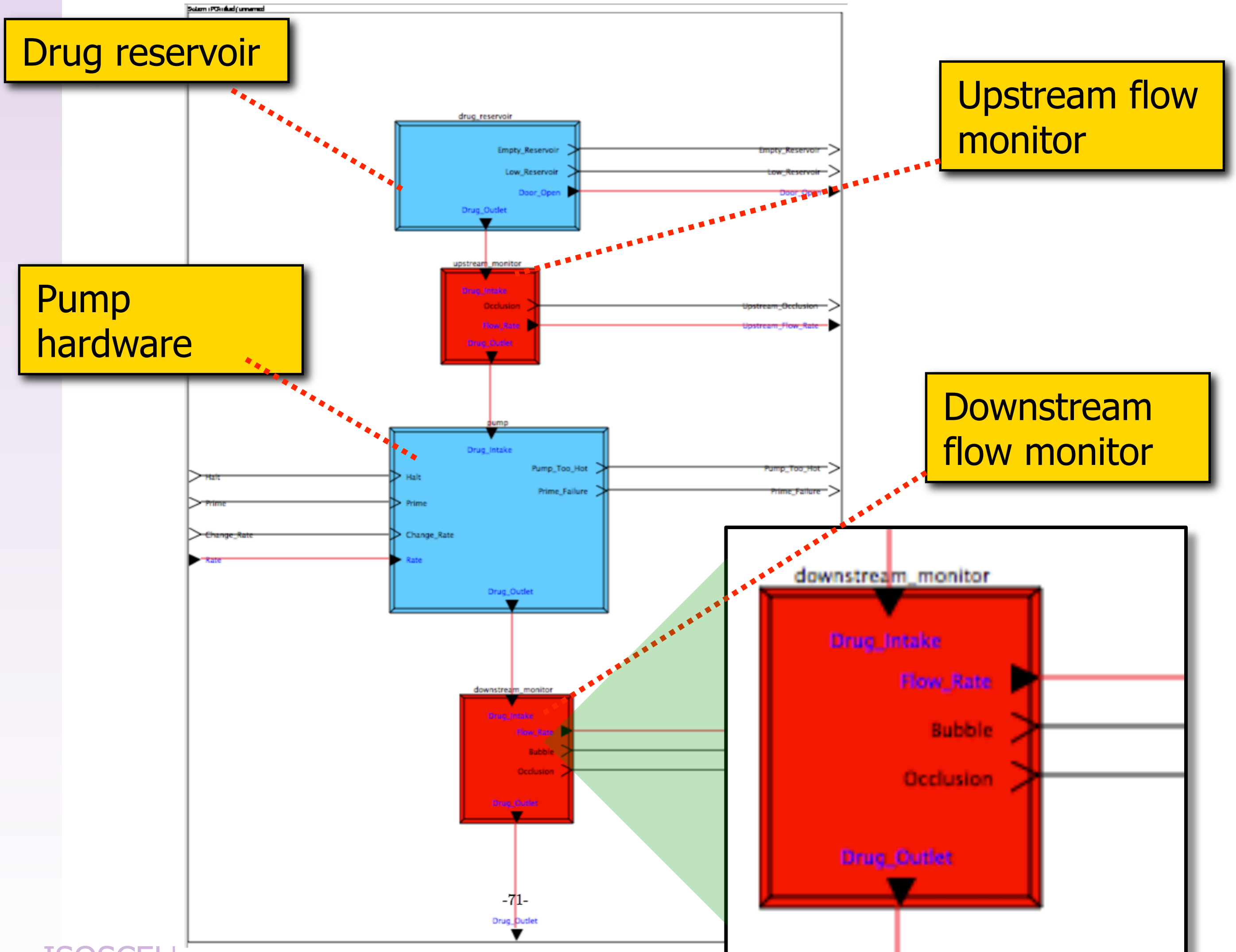
You are not expected to be able to read the details of this diagram. We are only giving pointers to important elements and relationships.

Fluid Subsystem

AADL Graphical View of the interface of the Fluid Subsystem



Fluid Subsystem



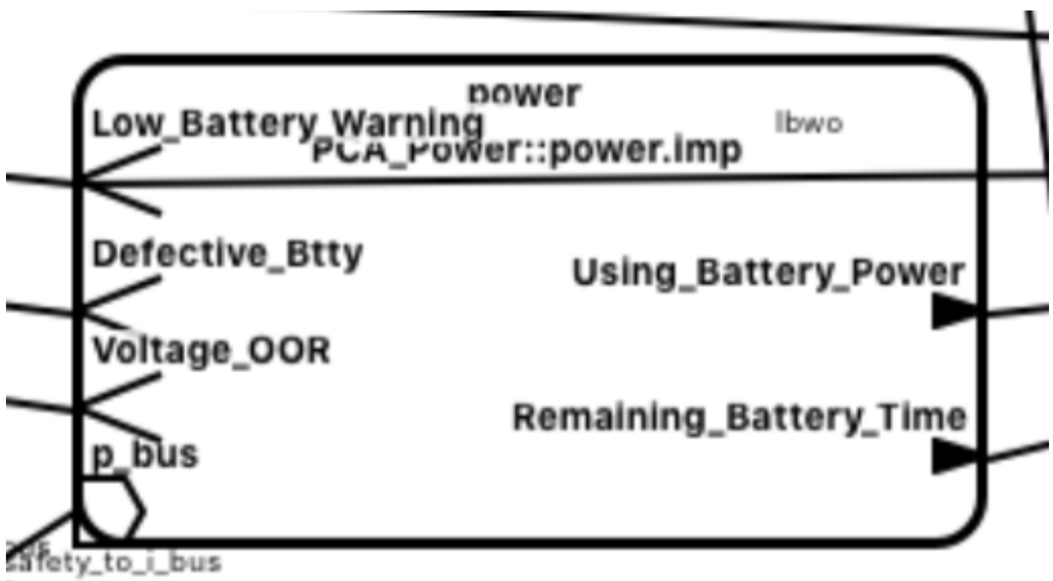
-71-

Fluid Subsystem

- The fluid subsystem moves drug from the reservoir to the IV line to the patient
- Inputs to the fluid subsystem include the flow rate and commands to start, stop, and prime the pump
- The fluid subsystem includes both upstream and downstream monitors that measure flow rate, occlusion (pressure differentials indicates blockage)
- Outputs from the fluid subsystem include
  - outputs from both flow monitors (flow rate values, occlusion indicators, bubble detected)
  - reservoir indicators (reservoir low/empty, door open)
  - pump indicators (pump too hot, prime failure)

Power Subsystem

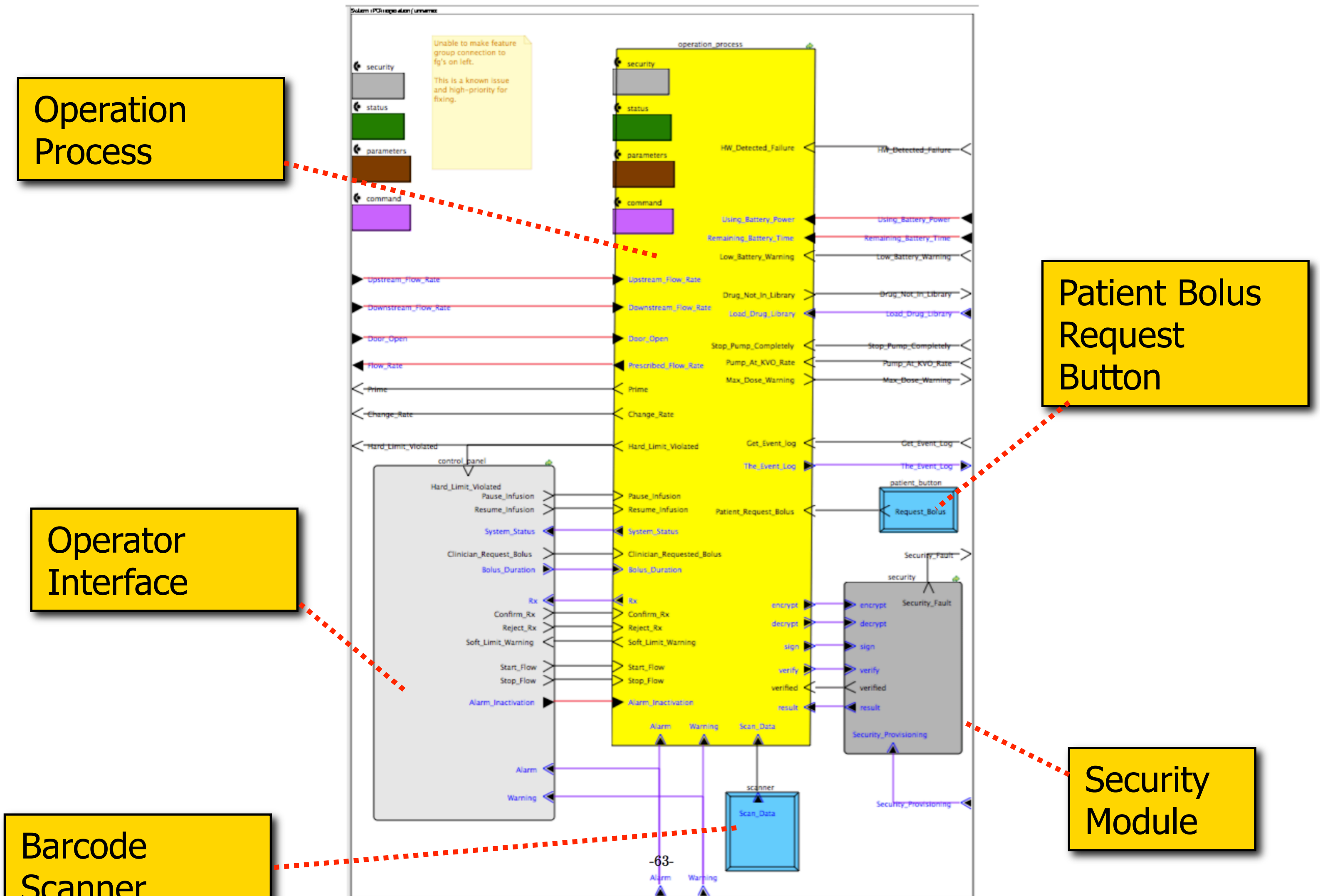
AADL Graphical View of the interface of the Power Subsystem



Power Subsystem

- The power subsystem consists of a battery, power control, and a power supply (not shown in diagram)
- Inputs -- there are no programmatic inputs to the power subsystem
- The power control switches between battery-backup and mains supply, and detects anomalies like voltage out-of-range
- Outputs from the power subsystem include
  - Battery indicators (low battery, defective battery)
  - Voltage out-of-range (OOR) indicator
  - Report of remaining minutes on battery power

Operational Subsystem



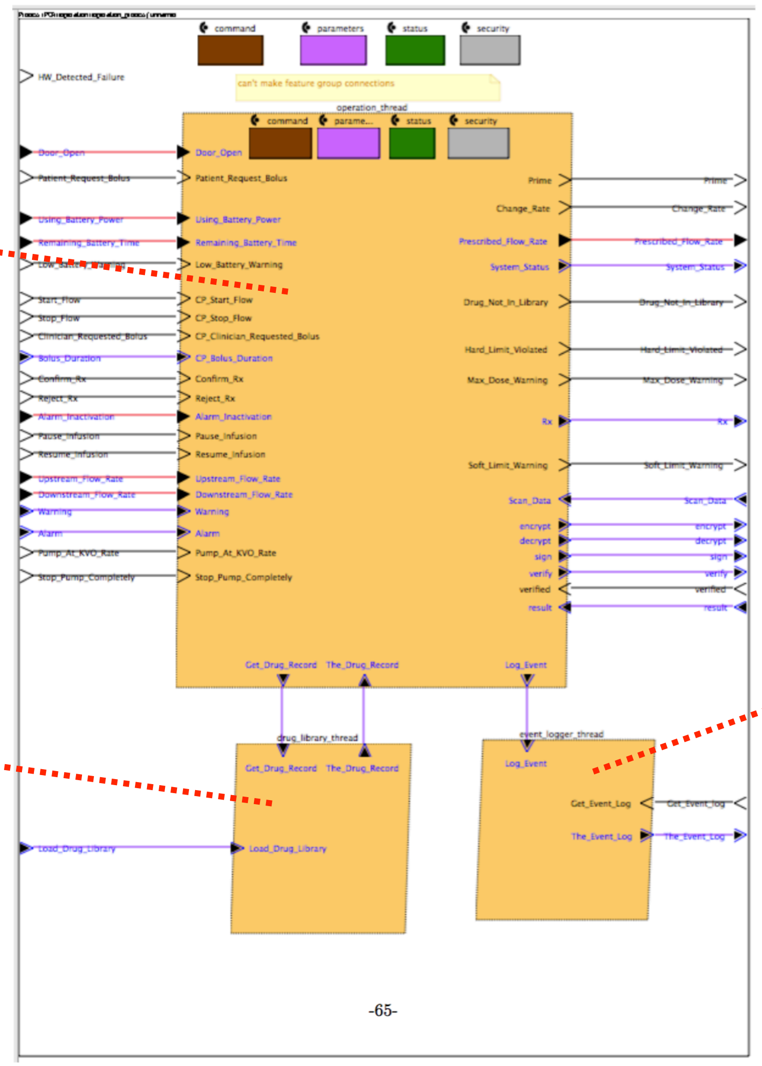
Operational Subsystem

Details of Operation Process

Operation Thread

Drug Library Thread

Event Logging Thread



Operator Interface / Control Panel

Provides the mechanism for clinician to interact with pump…

- Enables "programming of the pump"
  - Drug, patient bolus, basal rate, etc. with lockout and max volume infused
- Alternatively, confirm program obtained through barcode reader
- Start/stop infusion program
- Reports infusion program status and device status
- Allows clinician to request patient bolus
- Annunciates alarms and supports clinician response to alarms

Drug Library

The drug library is used to detect pump programming errors by comparing the operator configured program with typical doses, infusion rates, etc. for a particular drug

- The drug library includes a table of drugs along with common prescription/programming information for each drug
- As a "sanity check" (more precisely, an input validation step), the entered "program" for an infusion is compared with the values in the drug library
  - Soft limits – operator must manually confirm infusion if the program parameters lie outside of the soft limits
  - Hard limits – the device cannot run the infusion program with the program parameters lie outside of the hard limits

Drug Library

The following table shows the contents of a record within the drug library…

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

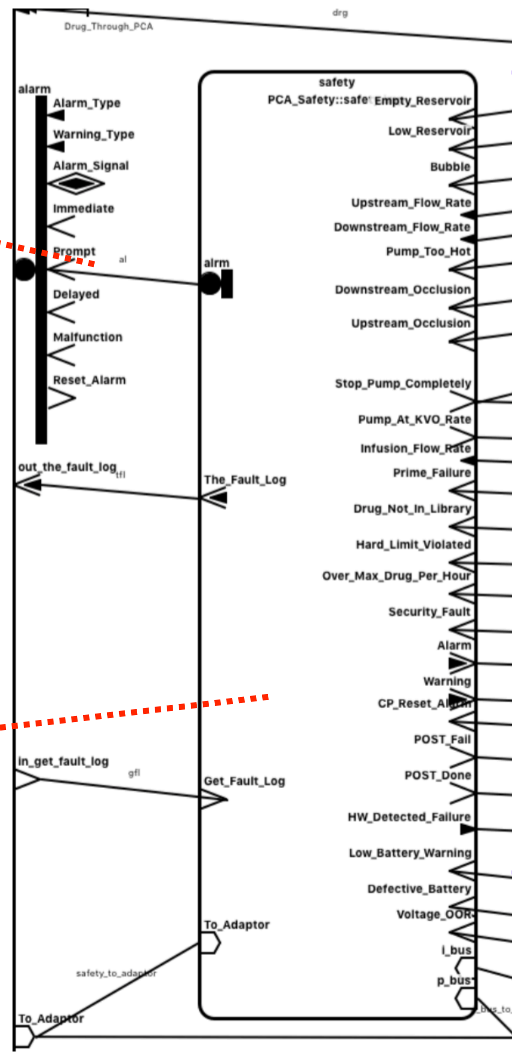
Operation Thread

Provides the logic for the primary medical functions of the device…

- Processes "pump program" to determine the rate and time for running the pump
- Implements mode logic for transitioning between different infusion modes of the pump as well as safety modes
- Analyzes the provided program against the drug library
- Compares current state and infusion history against limits (e.g., total hourly volume to be infused)
- Receives and processes fault information that may cause transitions to safe states

Safety Subsystem

Controls the annunciation of alarms via audio/visual outputs on the device control panel



Events indicating violations of operating constraints from other processes/ threads

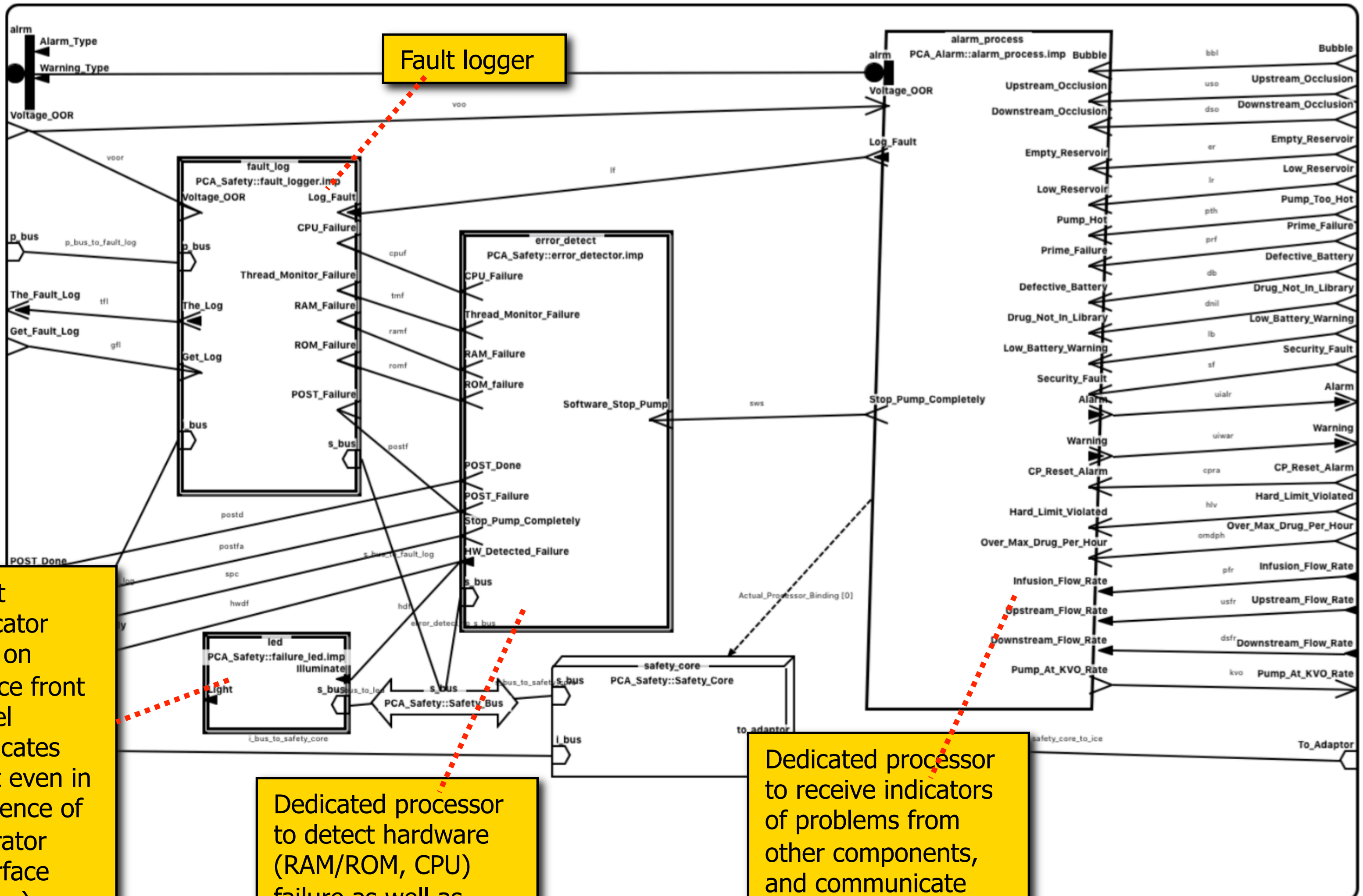
Internal components monitor for hardware failures of processor, memory, and other safety-critical components

Safety Subsystem Goals

The Safety Subsystem has four thematic goals…

- **Detect** – continuously monitoring the device for undesired states
  - E.g., detection of RAM/ROM or CPU failure
- **Notify** -- raising an internally handled exception or an externally visiable alarm or warning that includes information sufficient to enable an appropriate mitigation
  - E.g., alarm annunciation informing operator of above failures
- **Mitigate** -- the function of reducing the risk of an undesired device state to an acceptable level of risk state
  - E.g., move the device to a safe state, i.e., pump stopped or in "keep vein open" mode.
- **Record** -- the function of saving enough state information (logging) to reconstruct events leading to an undesired state
  - E.g., log problematic event

Safety Subsystem



Fault logger

Fault indicator LED on device front panel (indicates fault even in presence of operator interface failure)

Dedicated processor to detect hardware (RAM/ROM, CPU) failure as well as Power On System Test (POST)

Dedicated processor to receive indicators of problems from other components, and communicate operator-appropriate alarms/alerts to operator interface.

Conclusions

- The presented architecture provides a rationale decomposition of medical functions, safety functions, and operator interface functions on the device
- Caveats..
  - The presentation does not address the physical features of the device nor many details of the hardware
  - The architecture has not yet been validated in an actual end-to-end development (this is in progress in the ISOSCELES project)
- Many of details in the figures cannot be read in this presentation. The goal was to simply the primary entities and relationships.
  - The details of the figures are provided in text-based AADL models

For You To Do

- Browse the PCA device operator and service manuals found on the Open PCA Pump website and compare/contrast the features in the OPCAP to those found in commercially available systems