Requirements on the Physical Side of Cyber-Physical Systems

Mats Heimdahl

Professor, Computer Science and Engineering

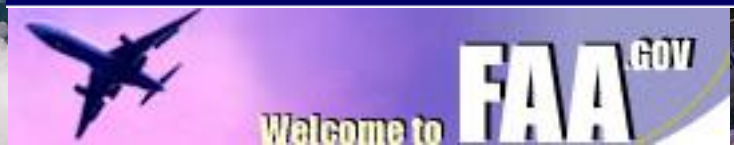
Director, University of Minnesota Software Engineering Center

UNIVERSITY OF MINNESOTA

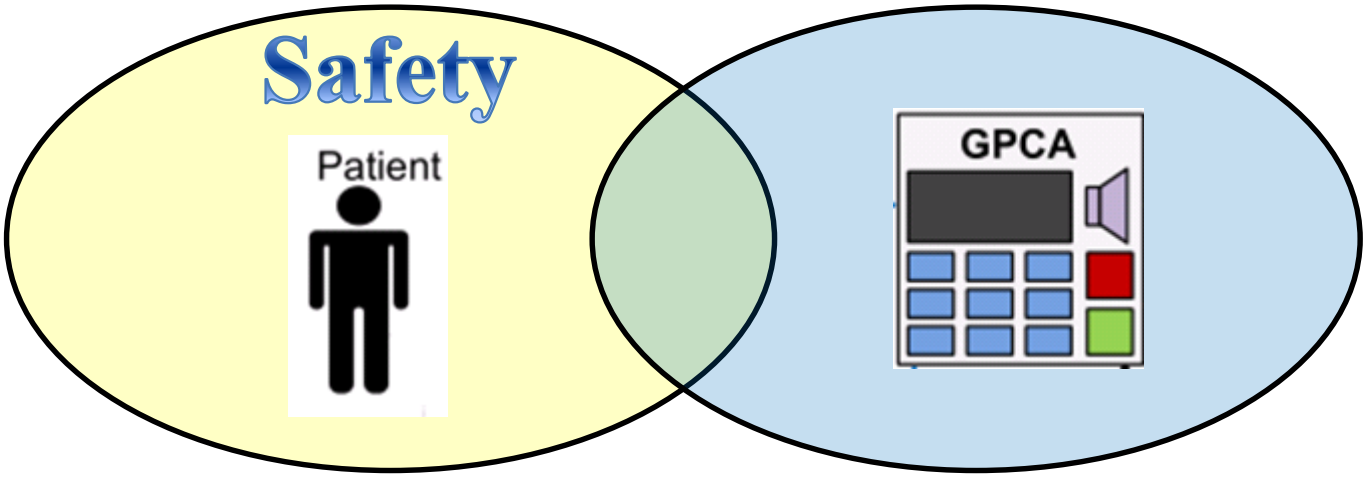
Software Engineering Center

Critical Systems

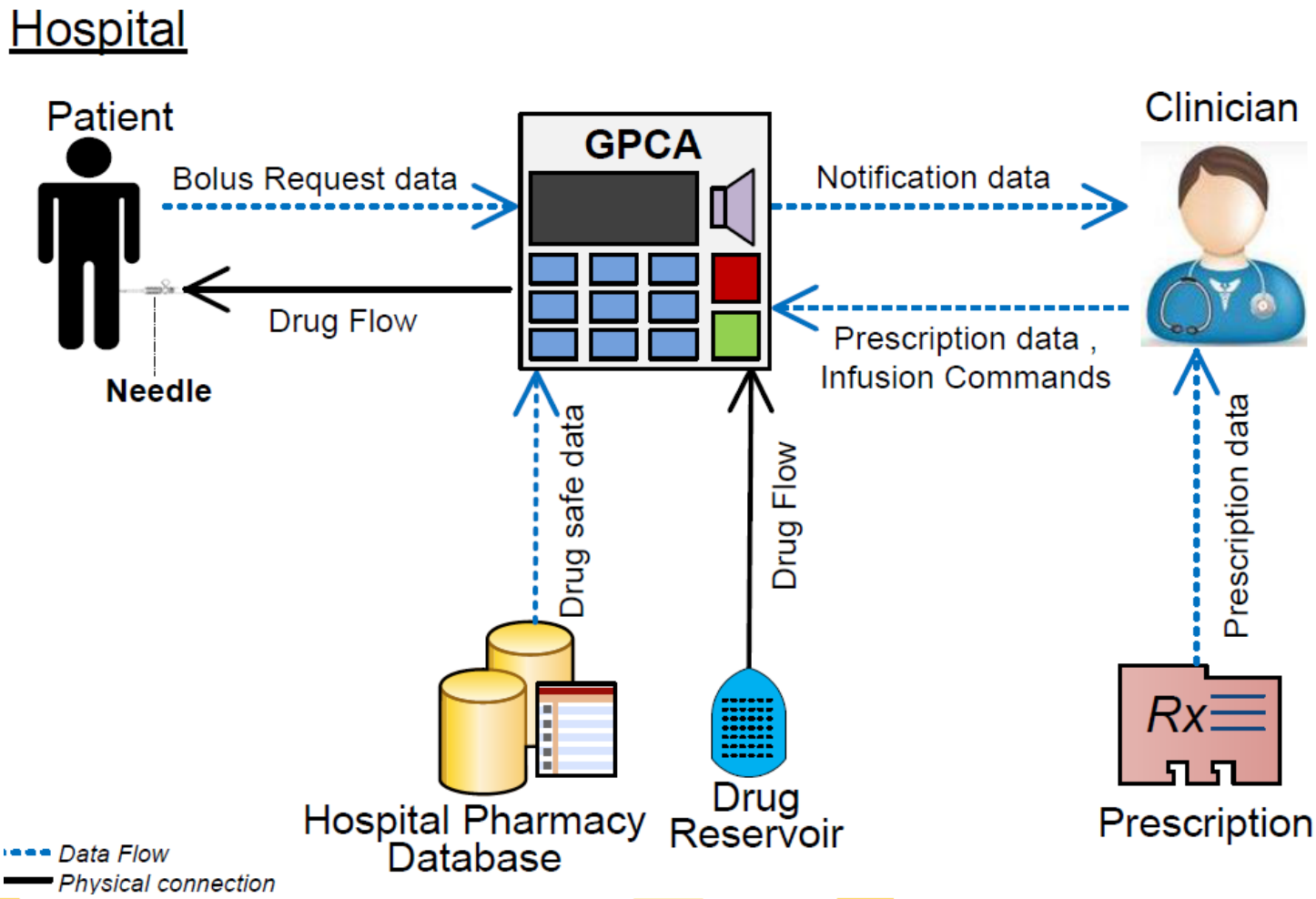
FDA U.S. Food and Drug Administration



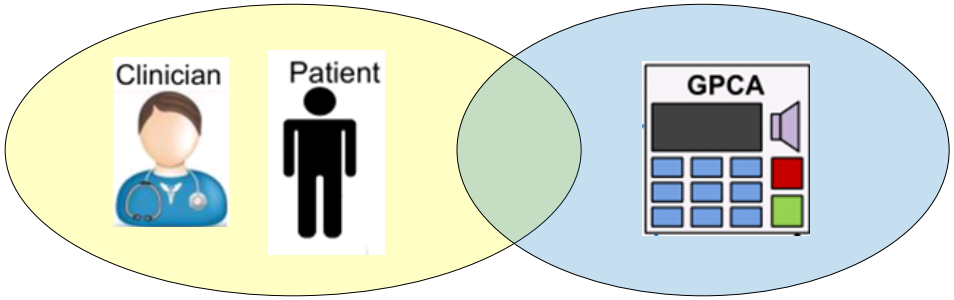
Assurance



Patient Controlled Analgesia Pump



Argument for No Under-Infusion(1)



Physical World System

No Under-Infusion

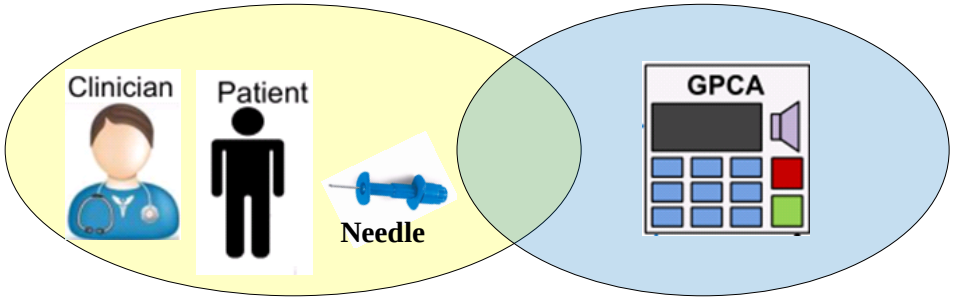
because

Device always delivers the drug through the needle at the programmed rate +/- 5%.

Given

The clinician connects the device to the patient as per instructions and enters the prescribed rate accurately.

Argument for No Under-Infusion(2)



Physical World System

No Under-Infusion

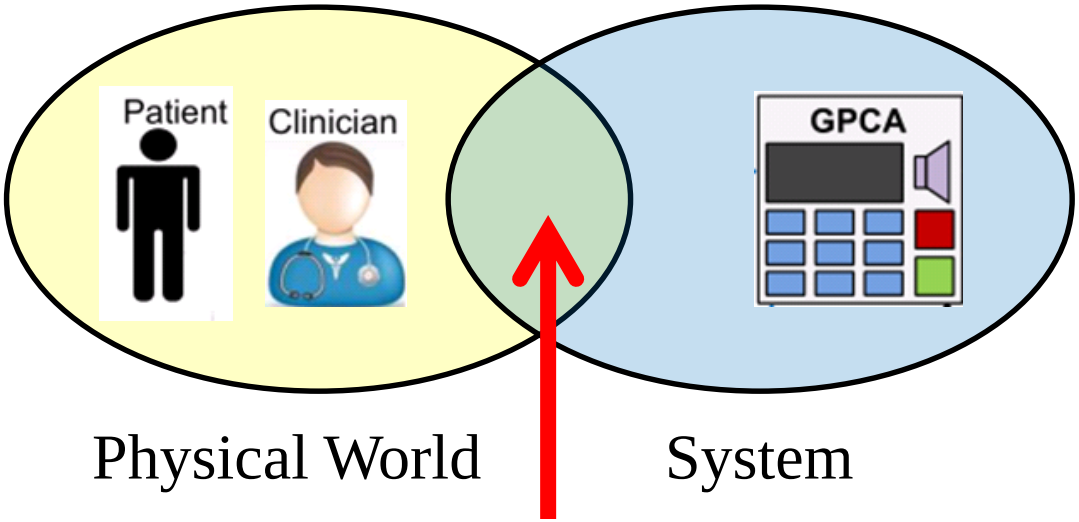
because

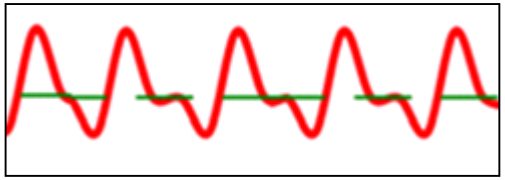
Device always delivers the drug through the hose at the programmed rate +/- 5%.

Given

The clinician connects the hose to the needle as per instructions, clinician ensures that needle is inserted appropriately into the patient and enters the prescribed rate accurately.

Continuous Quantities





Flow rate of drug

Three Immediate Challenges

- Appropriately "scoping" the requirements
  - Where is the system boundary?
- Writing requirements over the continuous and continual nature of (most) critical systems
  - How much do we need to capture?
- Providing the trace-links needed for assurance
  - What links and how many are needed?

Challenge 1 : System Scope

"Patient-requested bolus shall not be delivered more often than a prescribed number of minutes…"

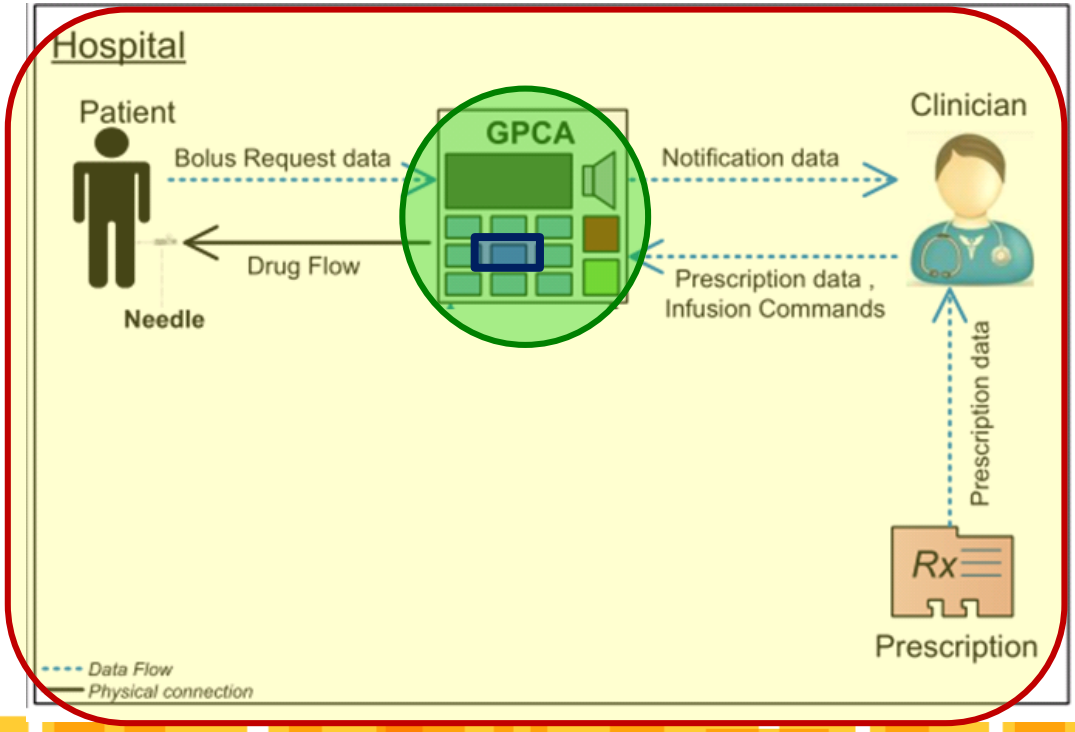
"An upstream occlusion alarm shall be triggered if the system senses an upstream occlusion."

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

“Scoping” Requirements

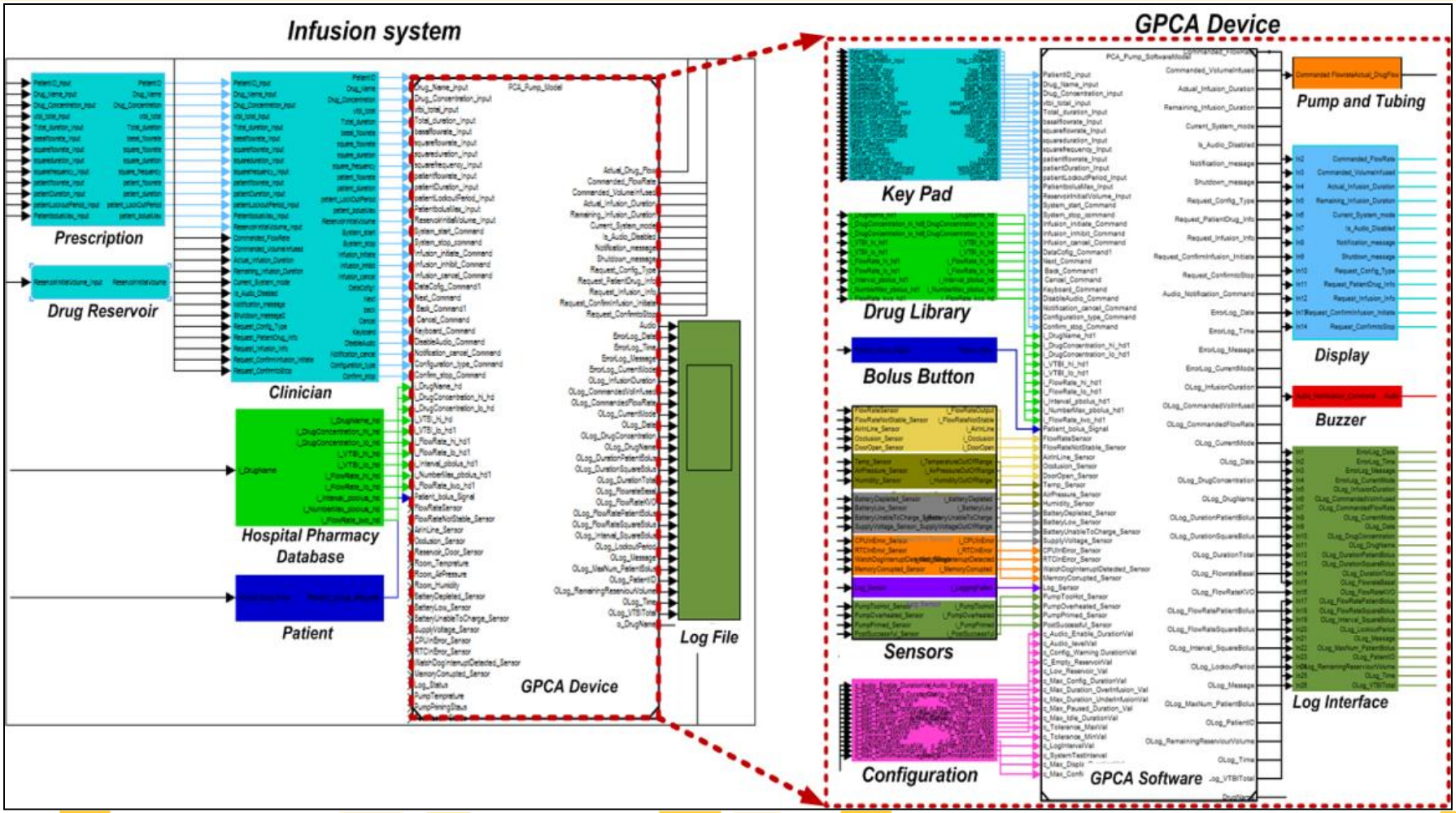
Patient-requested bolus shall not be delivered more often than a prescribed number of minutes

An upstream occlusion alarm shall be triggered if the system senses an upstream occlusion.



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

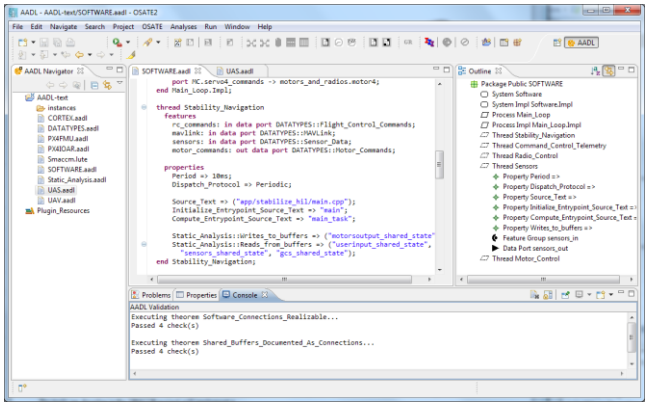
Aid—Architectural Models



Common Tools: Formal Methods Workbench

OSATE

Trusted Build



Resolute

Assurance Case

AGREE

Behavioral Analysis

Lute

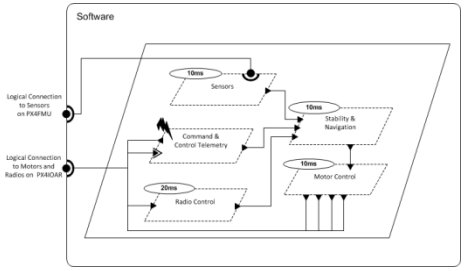
Structural Analysis

Architecture Models

Architecture Translation

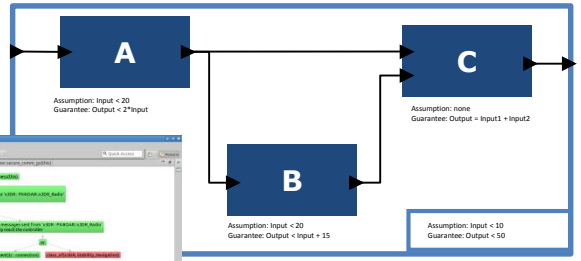
Architecture Analysis

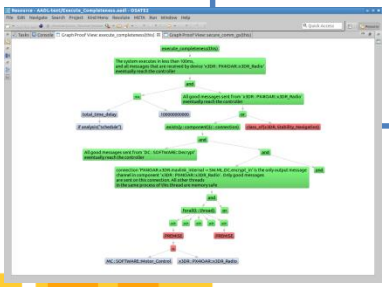
AADL



seL4

eChronos





Kind/JKind

Challenge 2: The Physical Side

Typical Requirements

"When the driver requests the cruise control to resume, the cruise control shall be engaged and bring the vehicle's speed to the target speed."

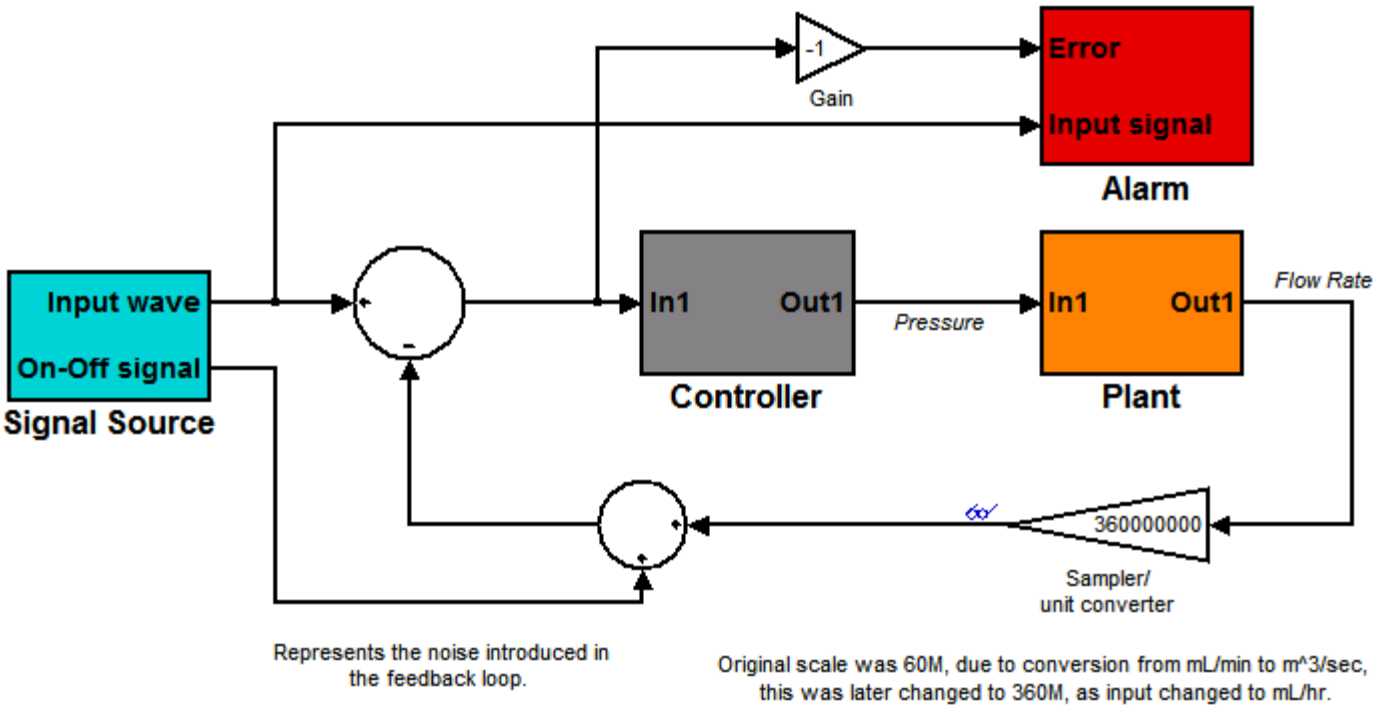
"A patient bolus dose shall be given when requested by the patient."

More Typical Requirements

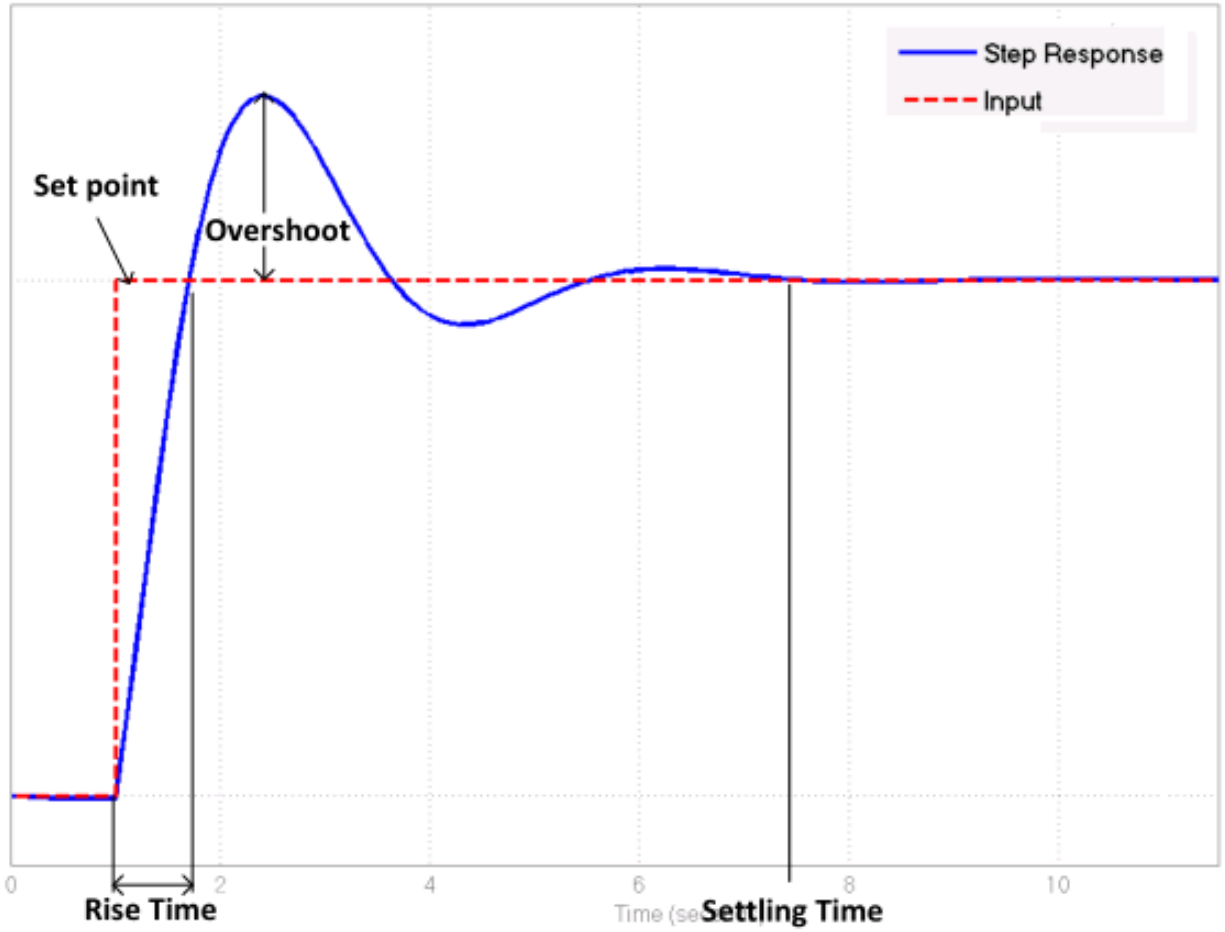
"The actual speed of the vehicle must be within ±5% of the target speed."

"The actual flow-rate must be within ±5% of the target flow-rate."

Aid—System Models



Step Response



Initial Classification

- Accuracy
- Rise Time and Drop Time
- Rate of Change
- Overshoot (maximum deviation)
- Settling Time
- Cumulative Error

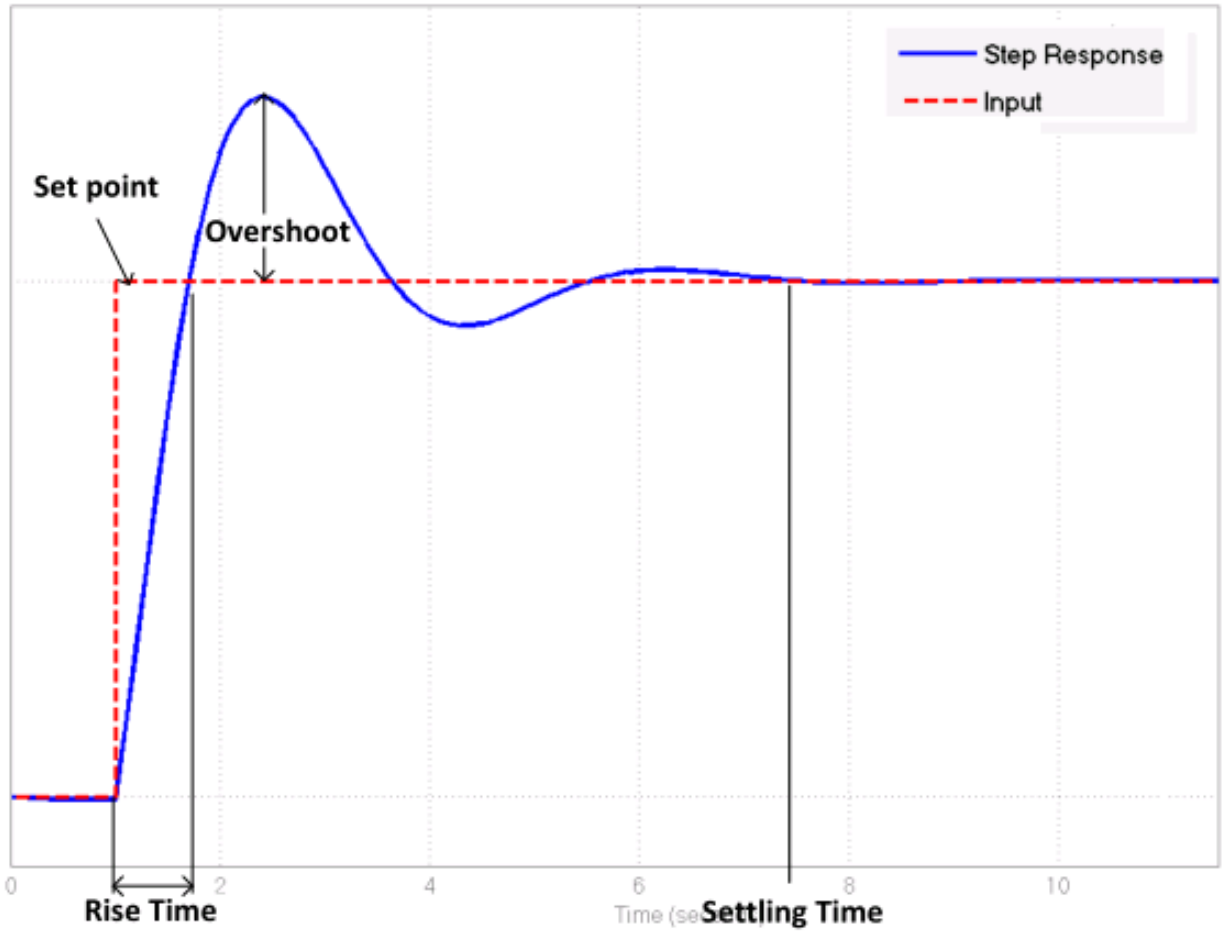
Accuracy

"The actual flow-rate (f) during normal operation shall be within ±5% of the target flow-rate (tfr): 0.95· tfr ≤ f ≤ 1.05· tfr."

Rise Time

"The duration between the time at which a new target flow-rate (tfr) is commanded and the time at which the actual flow-rate (f) reaches within ±5% of the target flow rate shall be shall be less than 1.0 s."

Step Response



Rate of Change

"The rate of change in the actual flow-rate (f) shall not exceed 0.5 ml/s²: $\dot{f} \leq 0.5\ ml/s^2$*."*

Overshoot

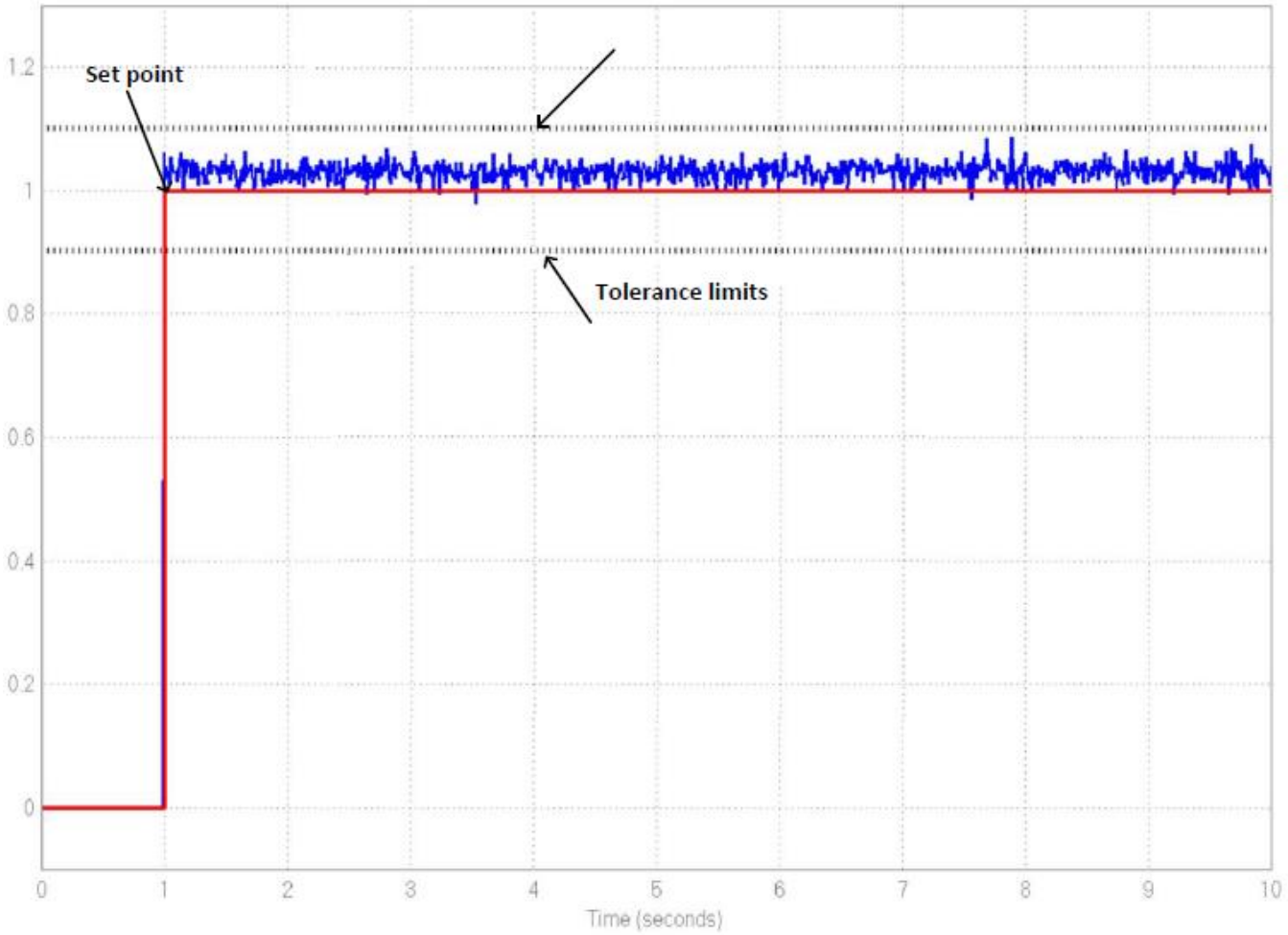
"The actual flow-rate (f) shall never exceed 10% of the target flow-rate (tfr): $f \leq tfr + 10\%$."

"The actual flow-rate (f) shall never exceed 10 ml/h: $f \leq 10$ ml/h."

Settling Time

"The time between when a new target flow-rate (tfr) is commanded and the time the actual flow rate (f) settles shall be less than 1.2 s."

Cumulative Error



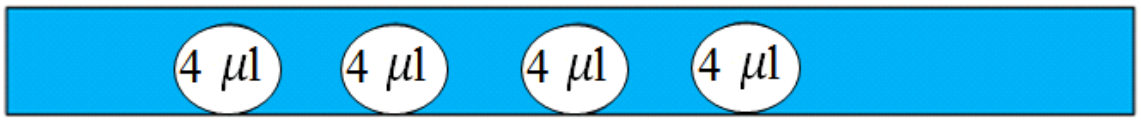
Cumulative Error

"The actual volume infused over a time interval of δ cannot exceed the commanded volume to be infused by more than 0.1 ml:

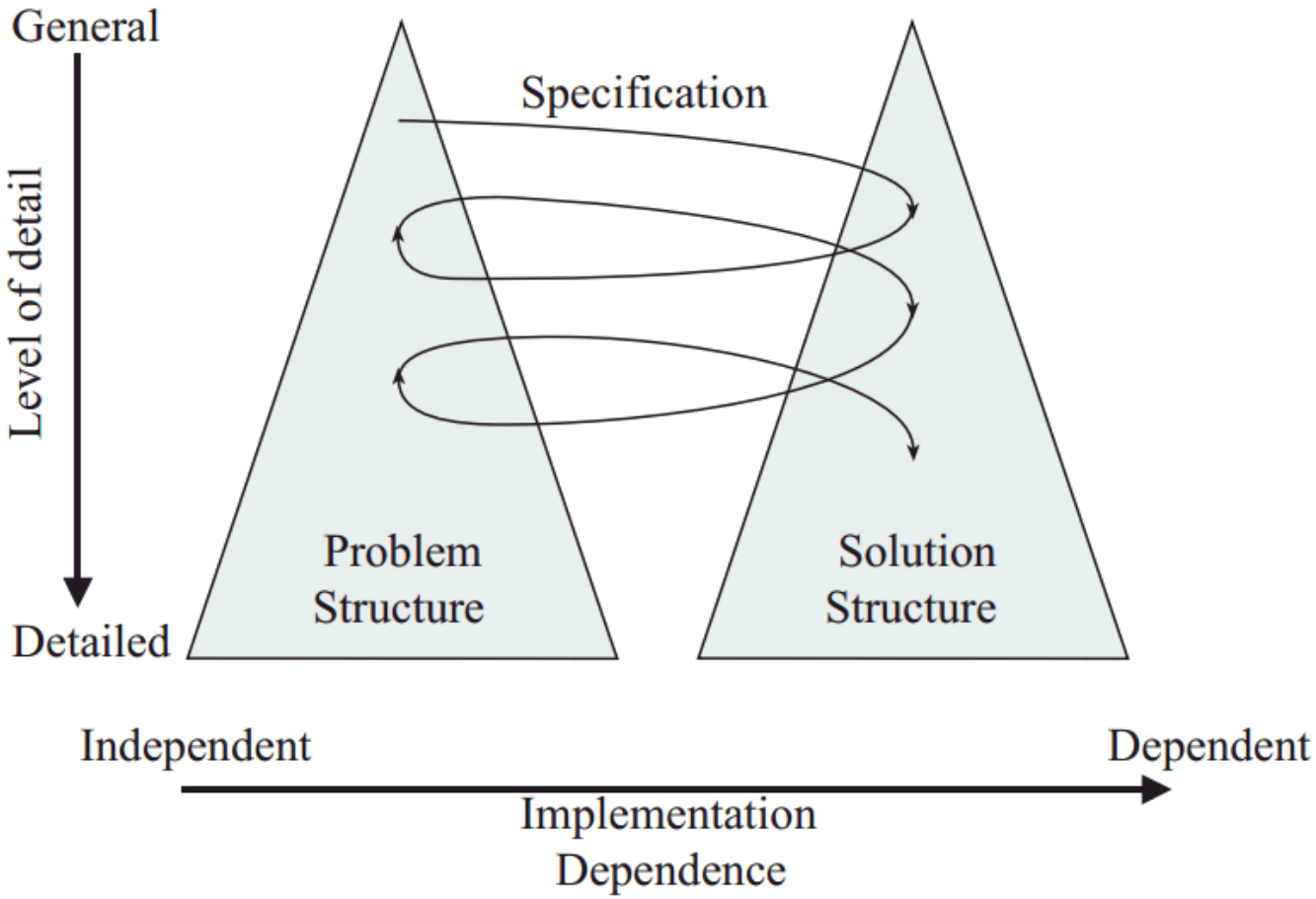
$$\int_{t}^{t+\delta} f\,dt \leq \int_{t}^{t+\delta} tfr\,dt + 0.1\ ml."$$

Cumulative Error

*"An **air-in-line alarm** shall be triggered if **air bubbles larger than 5 μl** are passing through the delivery hose."*



"Twin Peaks" Model by Bashar Nuseibeh



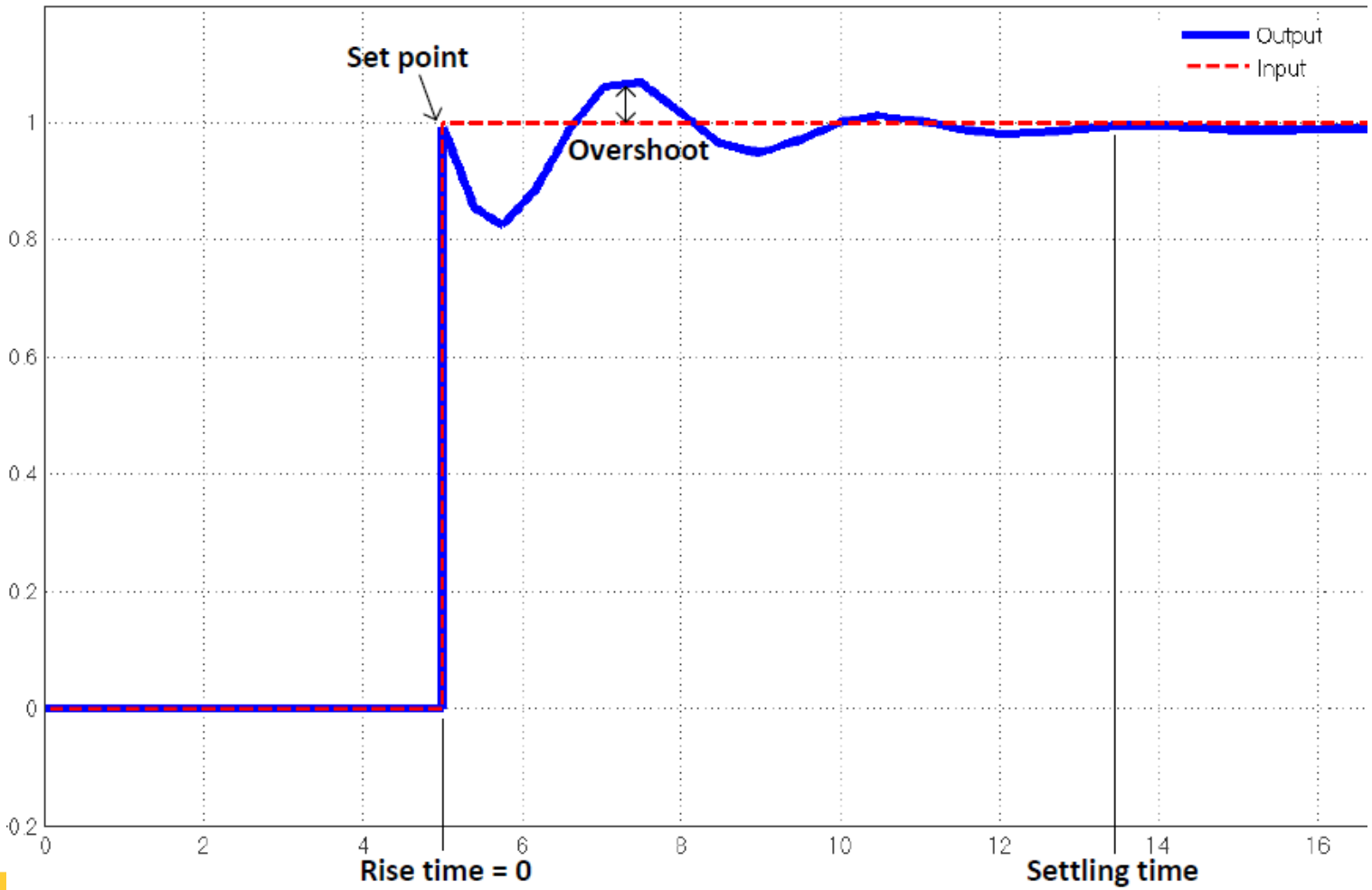
Summary

- Well defined component boundaries essential
  - Good requirements
  - Compositional assurance
- Bring control concerns to the requirements domain
  - Codify “good enough”
- How much is really needed?
- How to define and constrain acceptable mode-switching behavior?

Thank You

Funded by CNS-0931931 and CNS-1035715

Discussion


Set point
Overshoot
Output
Input
1
0.8
0.6
0.4
0.2
0
-0.2
0
2
4
6
8
10
12
14
16
Rise time = 0
Settling time