Complex Medical Processes as Context for Embedded Systems

George S. Avrunin[1] Lori A. Clarke[1]
Elizabeth A. Henneman[2] Leon J. Osterweil[1]

[1]Department of Computer Science
University of Massachusetts Amherst

[2]School of Nursing
University of Massachusetts Amherst

Certification issues

Goal is to ensure that

- (safety) requirements are appropriate and complete
- device/system satisfies the requirements

This is hard even for systems where requirements are clear and unchanging

Certification issues

Goal is to ensure that

- (safety) requirements are appropriate and complete
- device/system satisfies the requirements

This is hard even for systems where requirements are clear and unchanging

- But many systems (e.g., medical devices) are used in complex processes where requirements depend on details of the processes
- Certification must take these details into account

An example: "smart" infusion pumps

- Infusion pumps used over wide range of dosages and rates (3 orders of magnitude), may have several channels with different medications
- Errors in setting pumps can lead to serious and rapid over- or underdose of medication

An example: "smart" infusion pumps

- Infusion pumps used over wide range of dosages and rates (3 orders of magnitude), may have several channels with different medications
- Errors in setting pumps can lead to serious and rapid over- or underdose of medication
- New smart pumps intended to reduce such risks
  - Programmed with libraries of drugs used in divisions of hospital
    - libraries determine allowable medications, concentrations, units, dosing limits, alarms, possibility of clinician overriding stored settings, etc.
    - patient monitoring, drug interaction alerts
  - Clinician designates area of use when turning pump on, then programs drug, concentration, etc.
  - Pump alerts clinician if dose exceeds pre-set limits, drug already being administered

Safe use of pumps depends on details of process

For instance,

- pump settings are most liberal in OR—same dosages normally not allowed in ICU and some medications not used at all outside special units
  - special drugs used for anesthesia, etc.
  - anesthesiologist is both ordering and administering the medication
- pumps not usually taken out of OR, but there are special cases
  - e.g., patients don't usually go directly from OR to ICU, but critically ill patients may be moved from ICU to OR and back to ICU
  - usually patient is taken off all IV medication when moved to OR, but some medications must be maintained and pump goes with the patient to OR and back

Medical processes

Medical processes are

- highly concurrent
- exception-rich
- resource-constrained
- typically involve multiple agents (each participating in several processes at once)

Medical processes

Medical processes are

- highly concurrent
- exception-rich
- resource-constrained
- typically involve multiple agents (each participating in several processes at once)
- and they're usually poorly specified—when descriptions exist, they
  - give standard path of care, but not what to do in nonstandard situations that arise
  - are vague, allowing different participants to arrive at different understandings of specifics

Medical processes

Medical processes are

- highly concurrent
- exception-rich
- resource-constrained
- typically involve multiple agents (each participating in several processes at once)
- and they're usually poorly specified—when descriptions exist, they
  - give standard path of care, but not what to do in nonstandard situations that arise
  - are vague, allowing different participants to arrive at different understandings of specifics

Approaches to certification that assume the requirements are fixed and well-understood are inadequate in such settings

Certification depends on good description and analysis of the processes in which devices are used

Will describe some research directed at these issues

- formal definitions of complex medical processes
- formal statements of requirements they are intended to satisfy
  - precise and rigorous enough to support analysis methods that can, e.g., identify safety problems such as process executions on which infusion pump not correctly reset

This work can provide a basis for more complete understanding of the behavior of medical devices in the context of the processes in which they are used.

Process definition example

[demo with Little-JIL definitions of in-patient blood transfusion process]

Requirements for processes

- We want to apply rigorous analysis methods to process definitions to identify potential sources of medical errors.
  - also interested in automation, efficiency, clarifying roles of agents, etc.
- For safety analysis, need clear statements of properties process is supposed to enforce—those statements need to be
  - understandable to domain experts
  - formal and precise enough to support analysis
  - carefully elucidated so that critical details are addressed correctly and completely
- But it's hard to achieve this!

Tool support for requirements elucidation

[demo of Propel tool and blood transfusion properties]

Analyzing process definitions

- Finite-state verification methods
  - construct model from process definition
    - still some issues in modeling failure not recognized by agent, etc.
  - verify properties formulated using Propel
    - applying several different FSV tools
- Other kinds of analysis
  - simulation
  - fault tree (and other hazard analysis approaches)

How does this support certification of medical devices?

Once we have a good way to represent the process in which the device will be used, we can

- Introduce model of device into into analysis of process properties
  - represent device as agent in Little-JIL or compose (possibly abstract) finite-state model of device with model of process and then
    - check safety properties of process with device
    - identify requirements device must satisfy to work safely in given process
- Introduce (possibly abstract) model of process into analysis of device
  - show that device behaves safely as long as process satisfies certain constraints
  - certify device within a "process envelope"