

Hazard Analysis of Health Information Systems Using System-Theoretic Process Analysis (STPA)

Eugenia Kim (eugenk23@mit.edu)

Massachusetts Institute of Technology

MIT STAMP Workshop | March 25, 2025

Electronic Health Records

Base EHR Capabilities

Patient demographic and clinical health information

Clinical decision support

Physician order entry

Capture and query of health care quality information

Capacity to exchange with and integrate health information from other sources

Desired Impacts / Benefits

Patient care

Patient participation

Care coordination

Diagnostics and patient outcomes

Efficiencies and cost savings

Losses and Hazards

Losses

L-1: Loss of life or serious injury to the patient, resulting in patient harm and/or decline in the patient's quality of life (QoL)

L-2: Loss or reduction in providers' quality of work life (burnout)

L-3: Loss of reputation of the healthcare organization

L-4: Loss of patient throughput (efficiency)

L-5: Loss or reduction of ability to work with peer and academic institutions

L-6: Loss of financial feasibility or sustainability (unacceptable cost of care)

Hazards

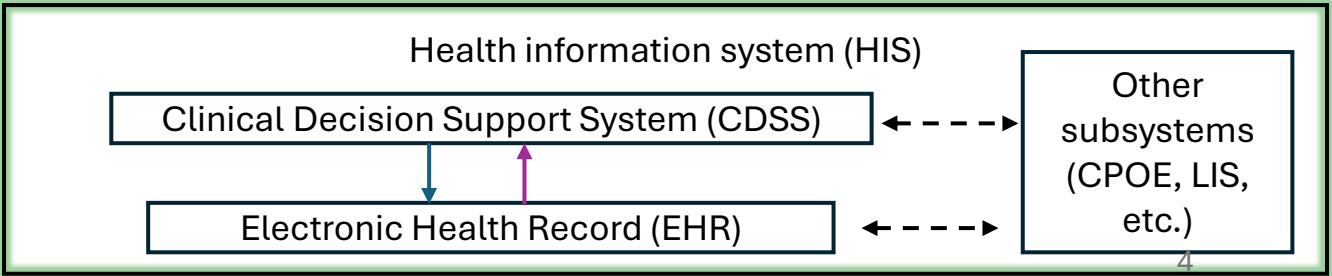
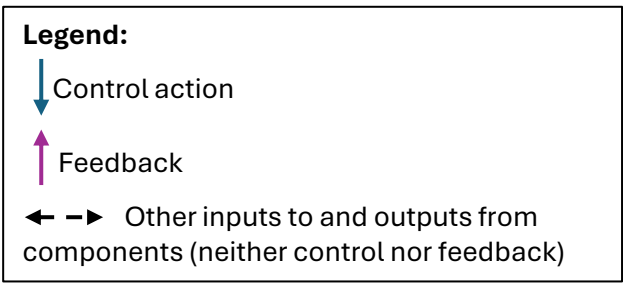
H-1: Patient receives less than acceptable standard of care

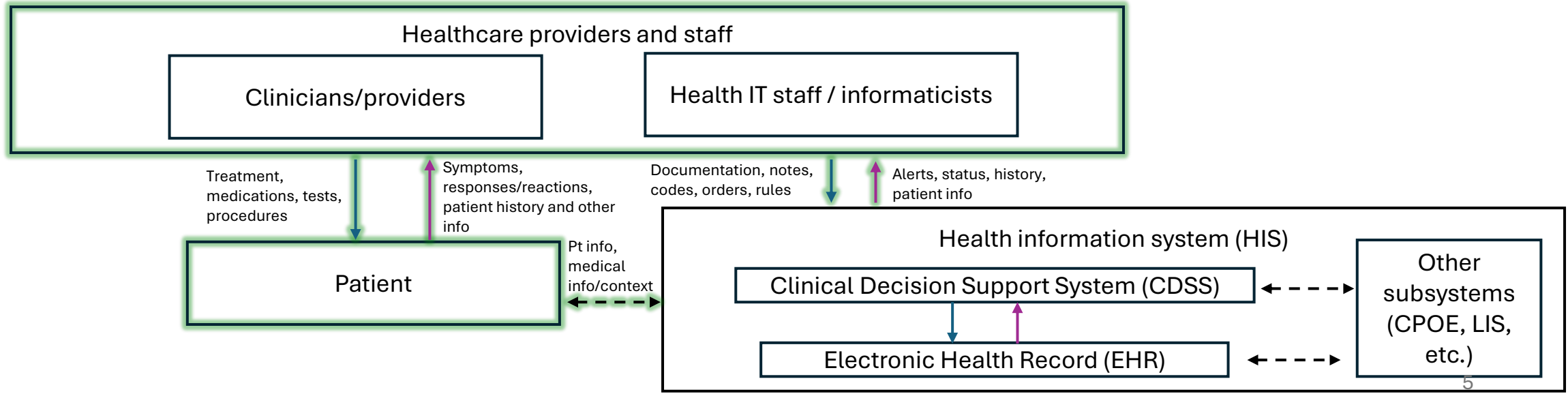
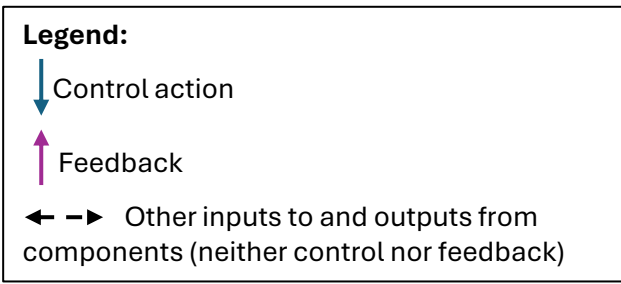
- H-1-1: EHR does not reflect patient's condition accurately
- H-1-2: EHR degrades provider QoL, leading to reduced staffing levels for providing acceptable care

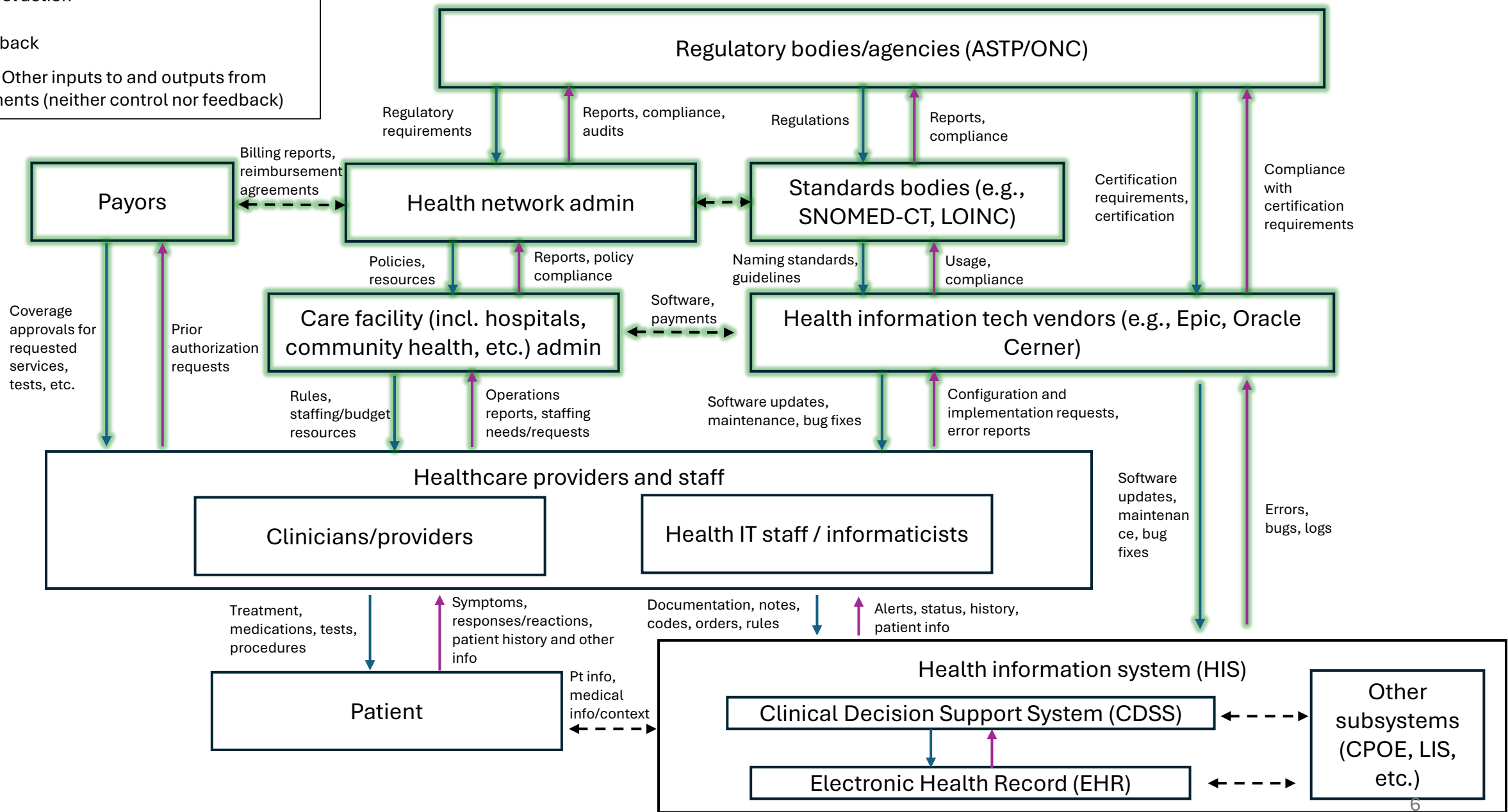
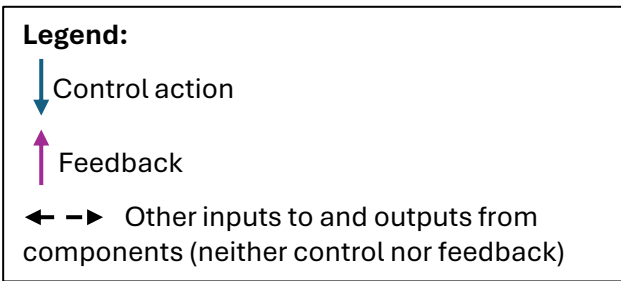
H-2: EHR is not usable in operational, clinical contexts

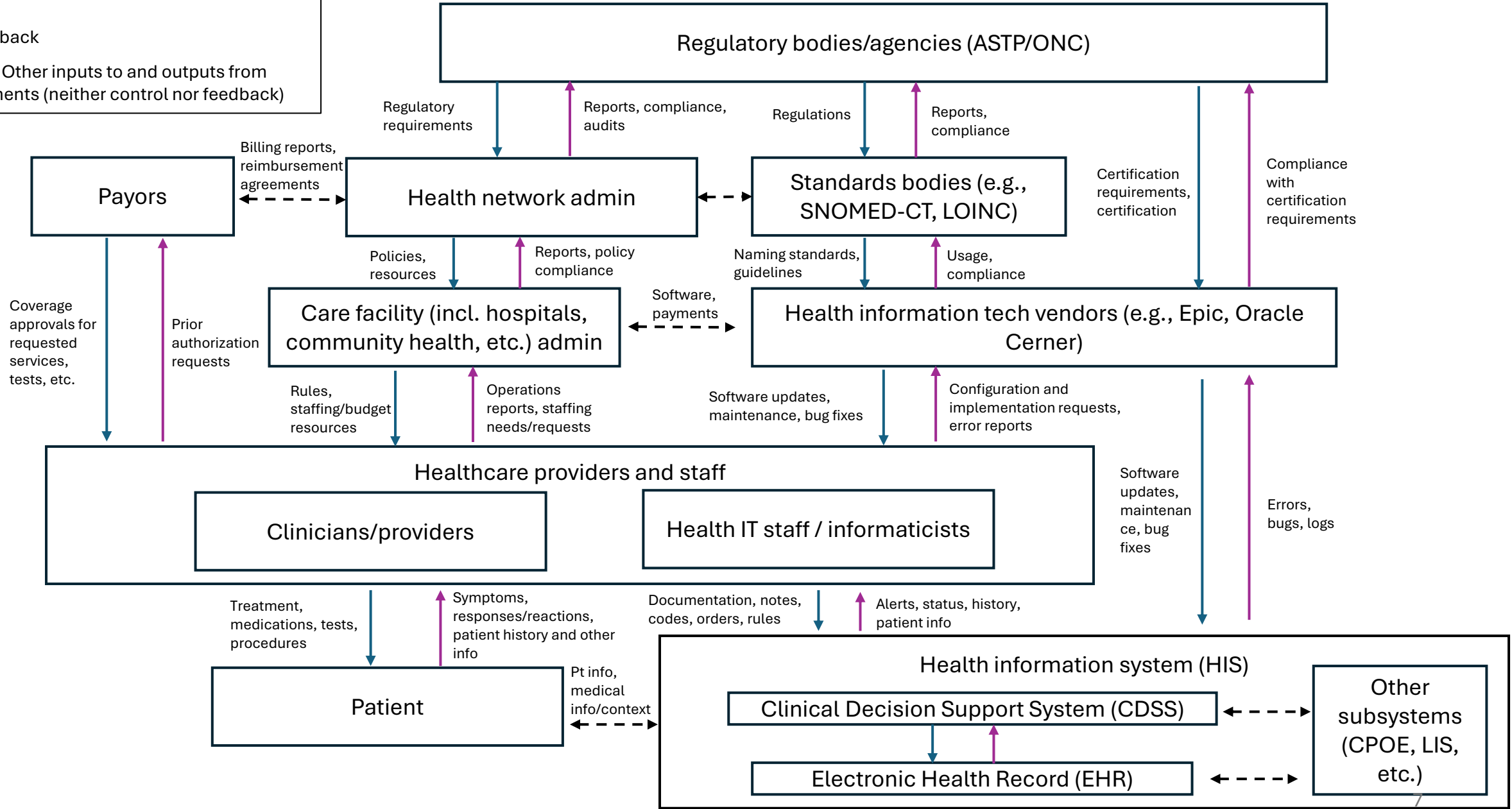
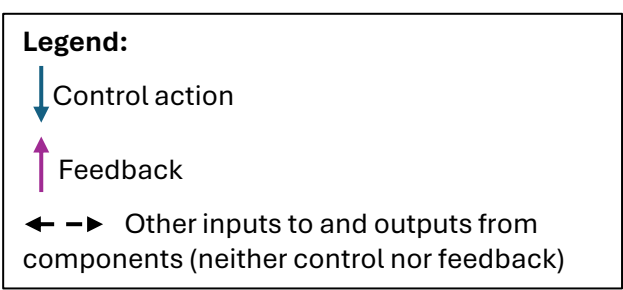
- H-2-1: Necessary EHR data cannot be accessed and entered in a timely manner (in an intuitive manner)
- H-2-2: EHR data is misinterpreted by the user(s)

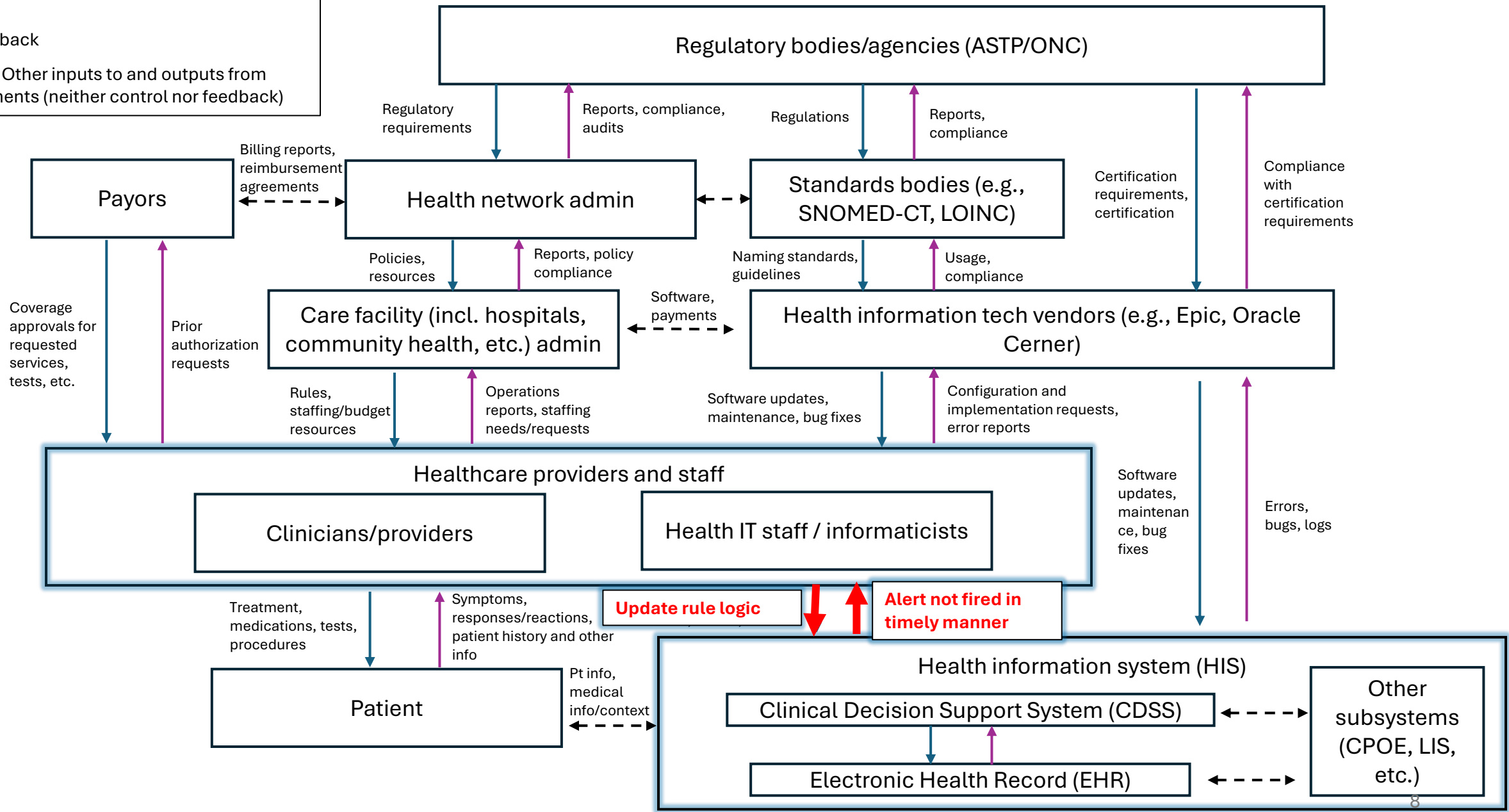
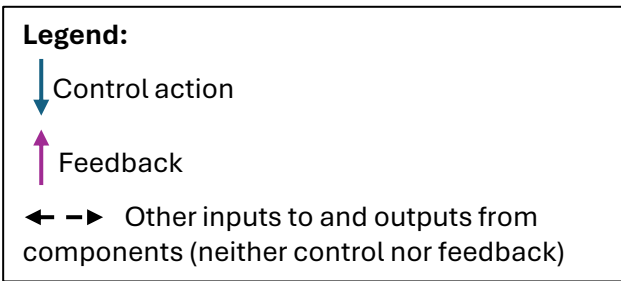
H-3: Patient data is accessed and used by unauthorized parties









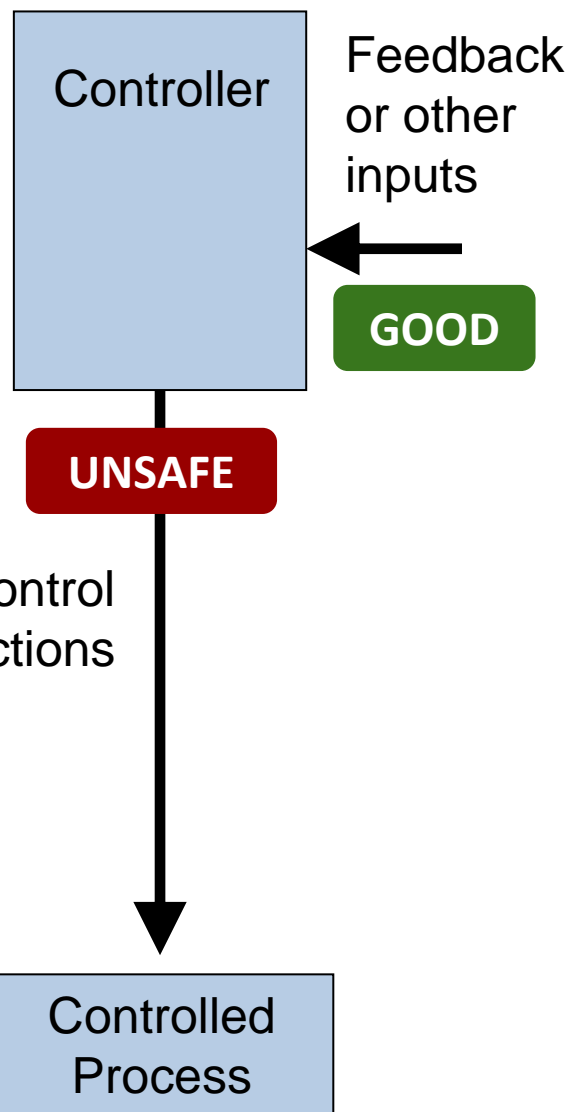


Examples of Unsafe Control Actions (UCAs) for Human Operators

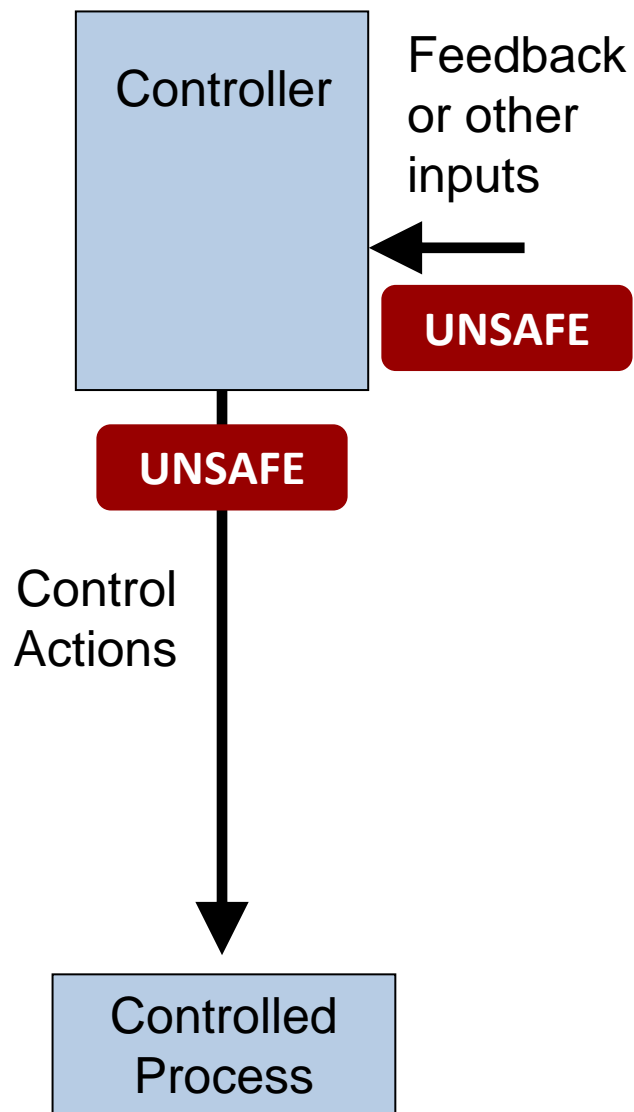
Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Health IT team creates an alert/flag for a lab test.	UCA-1.1: Health IT team does not create a lab test alert/flag for when the patient has been on a drug for <x time> and has not had a test within the clinical guidelines [H-1, H-2]	UCA-1.2: Health IT team creates an alert/flag for an unnecessary lab test when the patient does not require one [H-1, H-2]	UCA-1.3: Health IT team creates an alert/flag for a lab test too late after a system downtime [H-1, H-2]	N/A as this is a discrete control action and not a continuous one
Health IT team updates CDSS rule logic for a lab test alert.	UCA-2.1: Health IT team does not provide an update to the CDSS rule logic for an alert when the EHR's internal drug ID code has changed [H-1, H-2]	UCA-2.2: Health IT team updates the rule logic for a lab test alert with incorrect data (dosage, timing, lab) after a drug dictionary change [H-1, H-2]	UCA-2.3: Health IT team updates rule logic for lab test too late after the EHR's internal drug ID code has changed [H-1, H-2]	N/A as this is a discrete control action and not a continuous one

STPA: Four Classes of Formal Scenarios

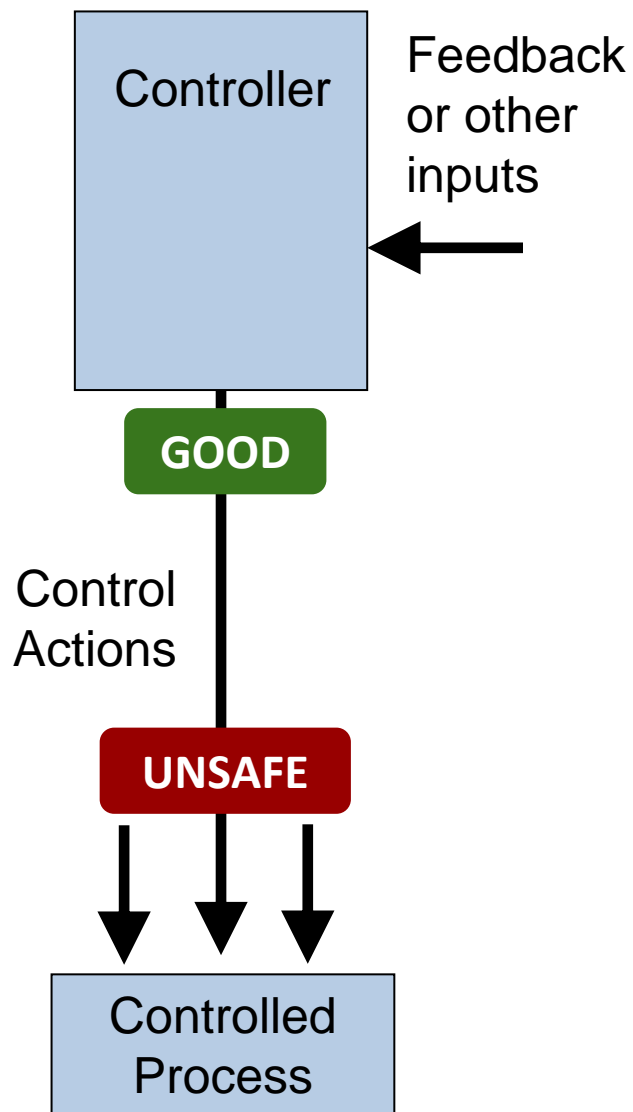
Class 1



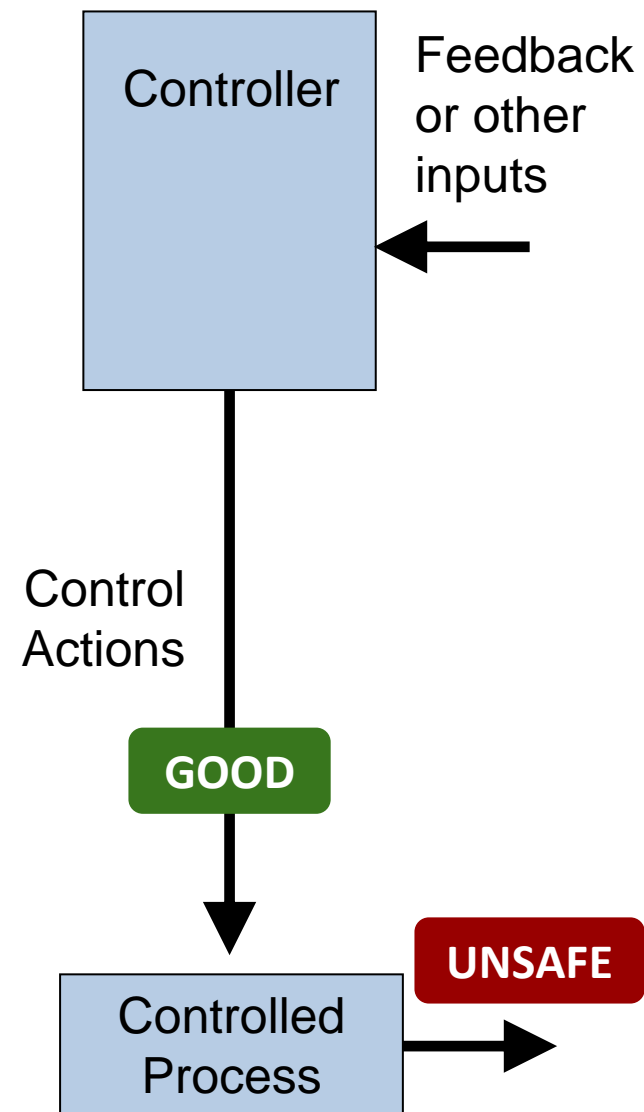
Class 2



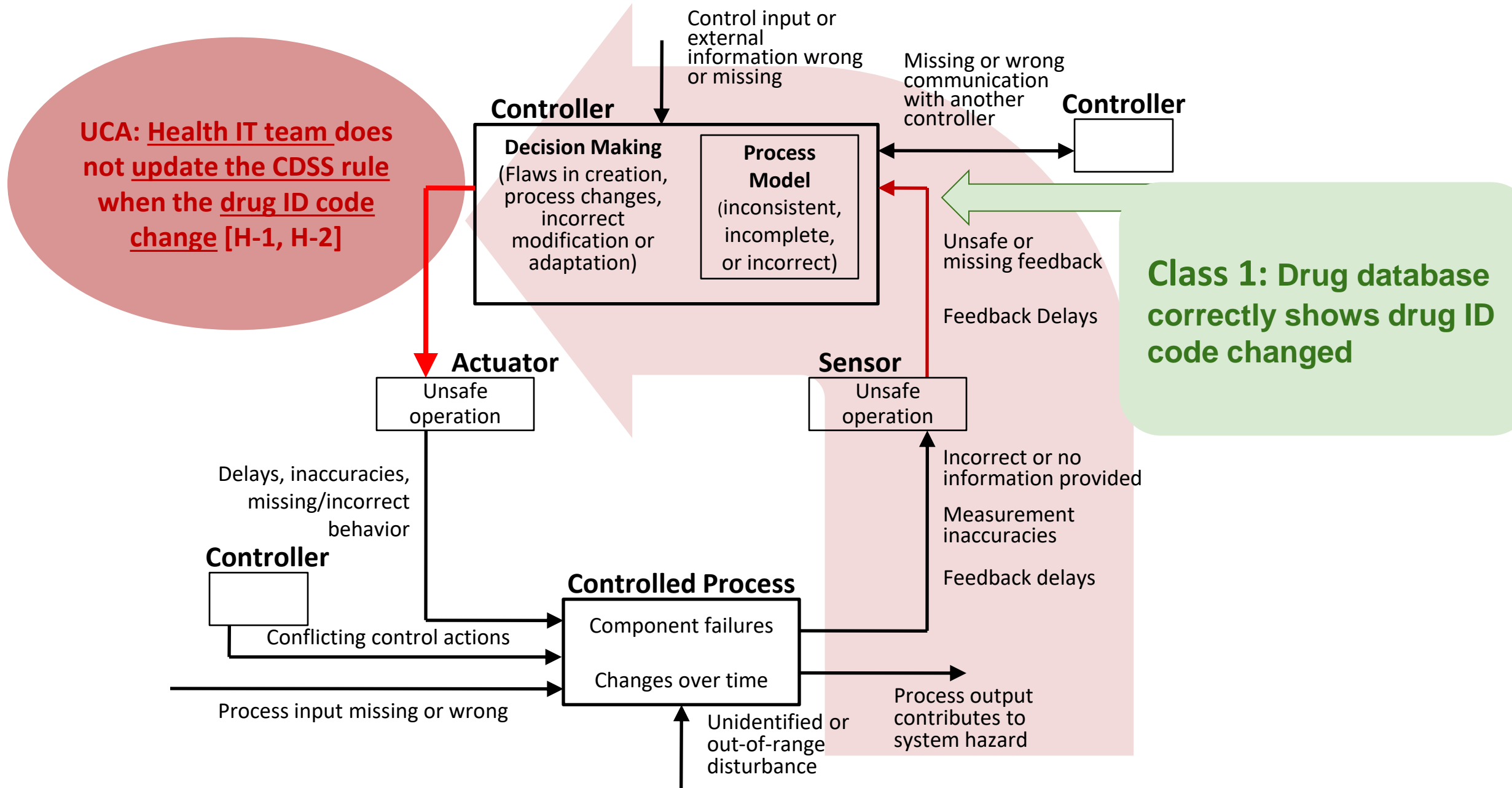
Class 3



Class 4



STPA: Class 1 Scenario Archetype



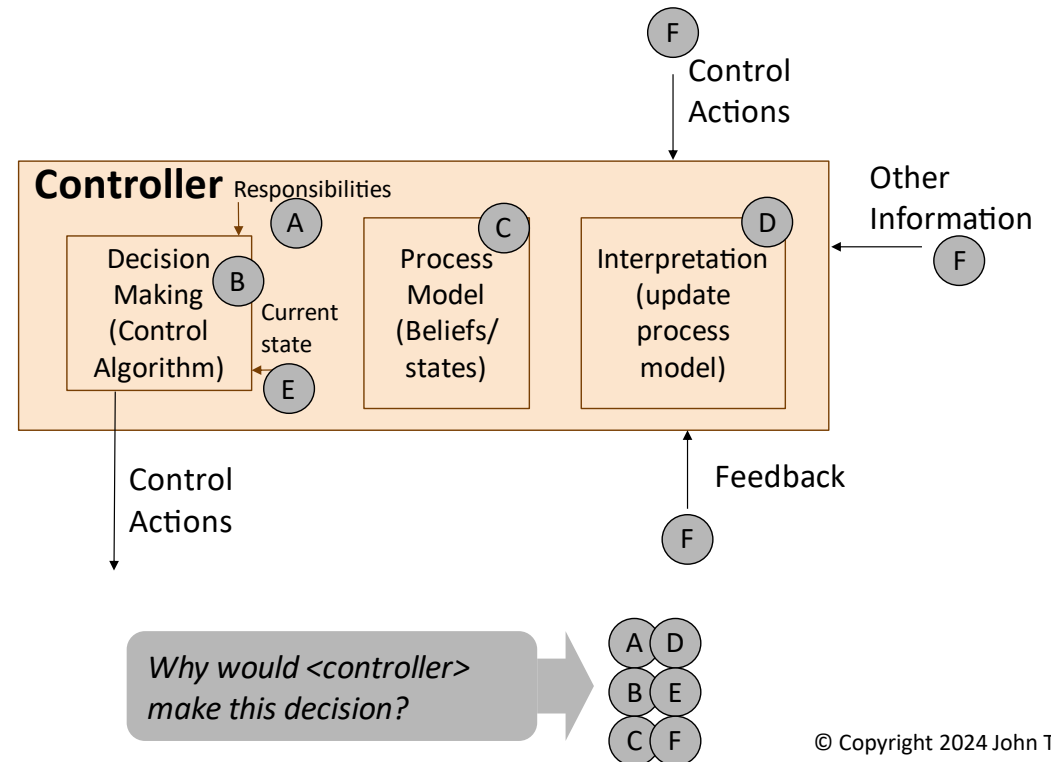
Class 1 Scenario Archetype: Unsafe Controller Behavior

The feedback/input was adequate, BUT the control action was unsafe.

“Simple” Causes

- Example:
 - There was a network service disruption that prevented the health IT team from receiving the input the EHR internal ID code had changed
 - E.g., Distributed Denial of Service (DDoS) attack

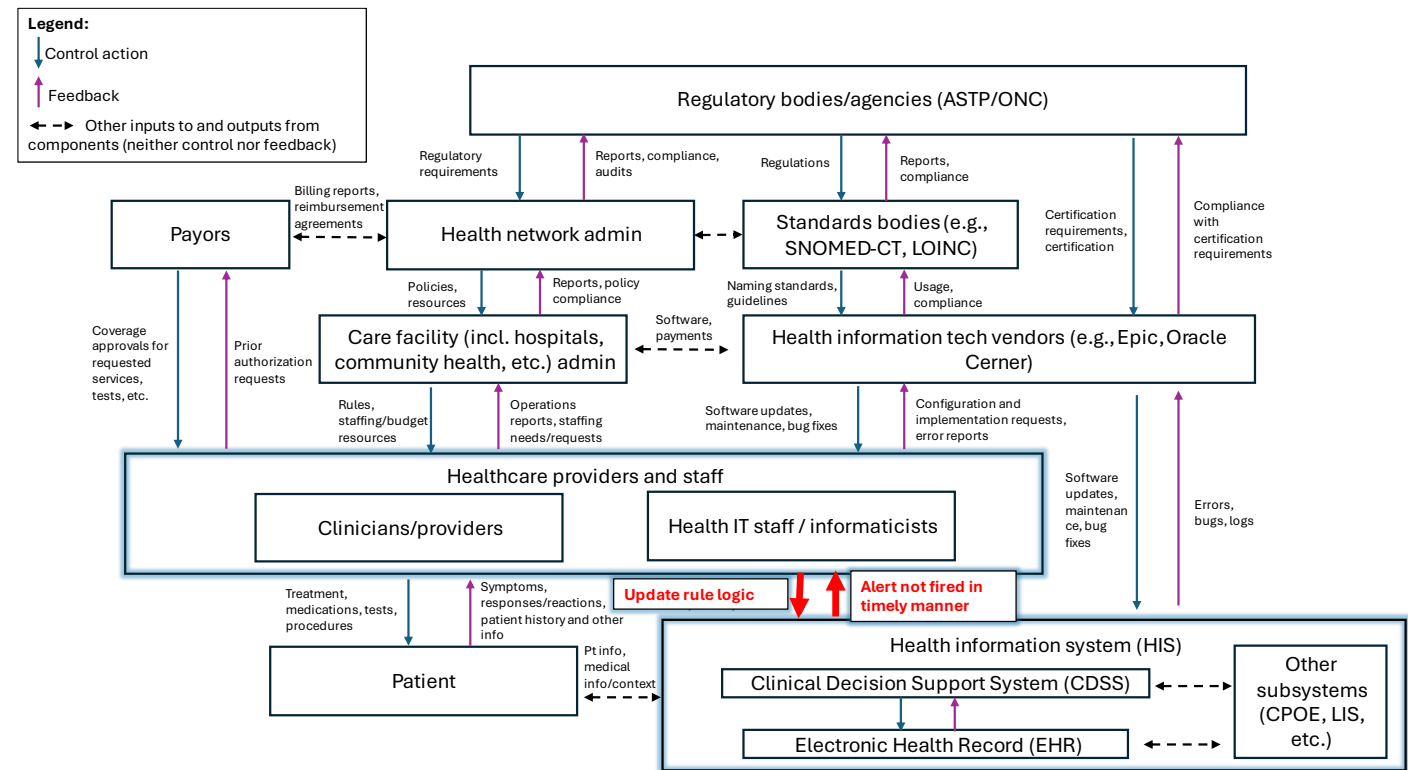
More Complex Causes



© Copyright 2024 John Thomas

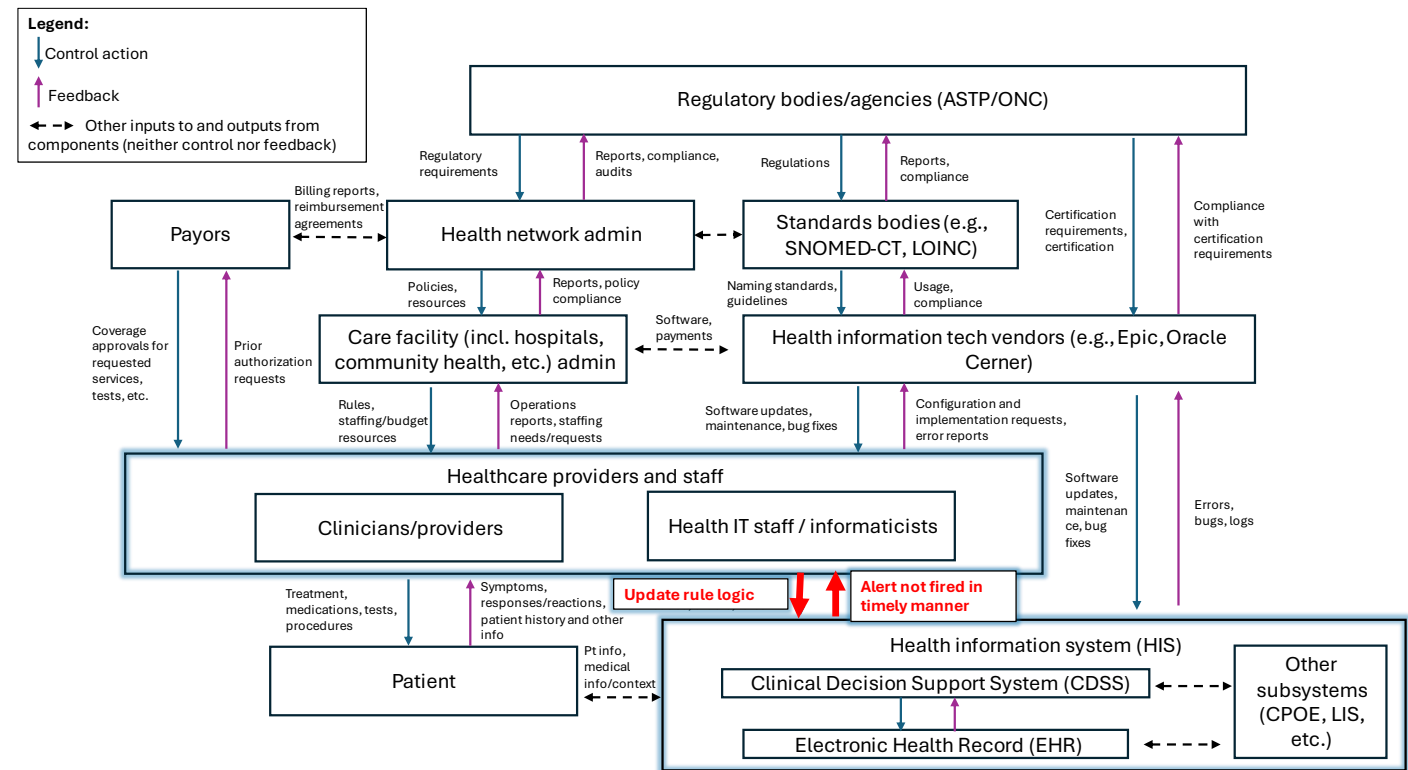
Class 1 Scenario Archetype: Unsafe Controller Behavior Causes without failure examples

- Responsibilities
 - R-1: Health IT team might not feel like it's their responsibility or under their purview
 - R-2: Health IT team might not have an interface to other teams, creating a gap in responsibilities and communication breakdown
 - R-3: Health IT team might have another responsibility that takes precedence over updating (e.g., direct order to freeze any and all updates/changes)
- Control algorithms (tech) or decision-making rationale (human)
 - DM-1: The health IT team implements but doesn't validate the rule (e.g., hard coding to only include the brand name but not the generic)



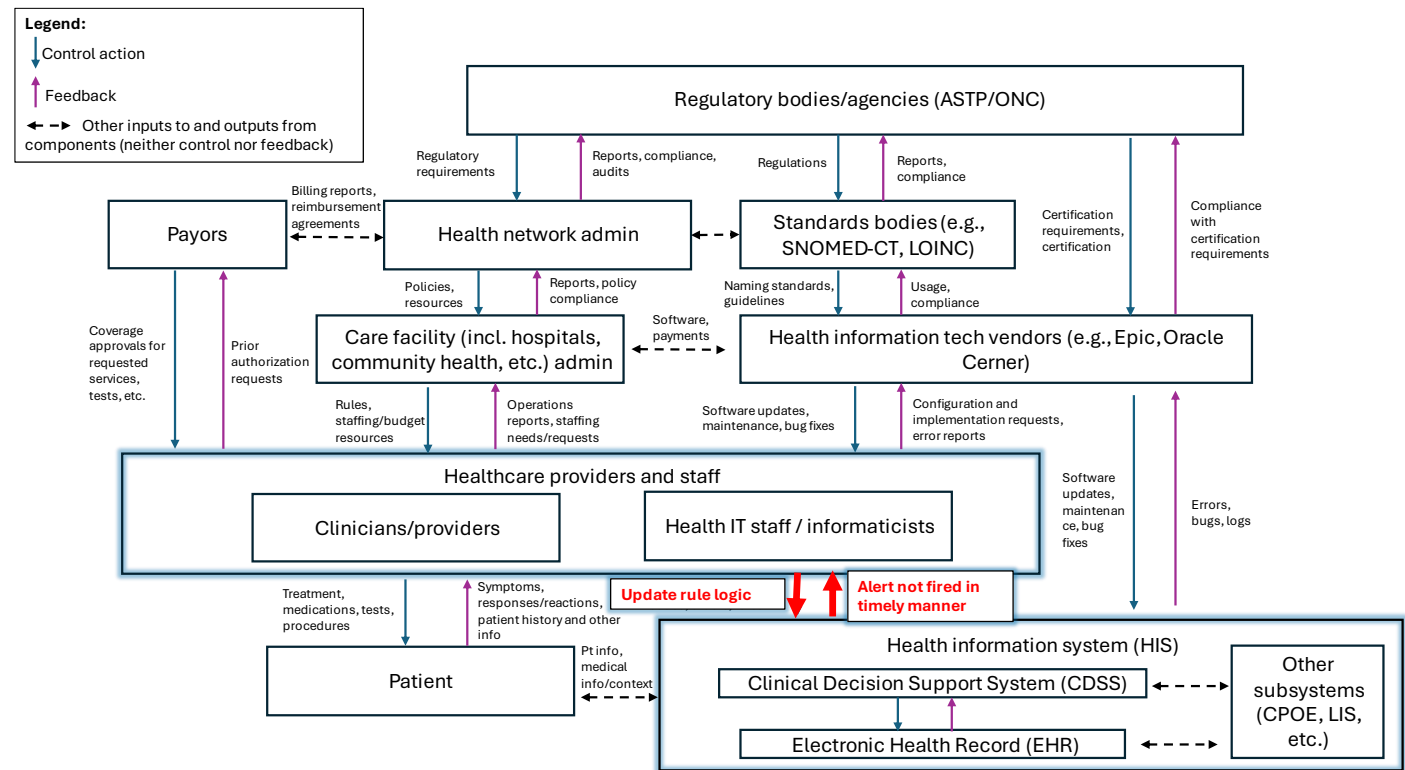
Class 1 Scenario Archetype: Unsafe Controller Behavior Causes without failure examples

- Process models (beliefs/states)
 - PM-1: The health IT team incorrectly believes that the rule logic accounts for the cases/equivalents of the same drug
 - PM-2: The health IT team incorrectly believes the other internal group has already conducted the change/update to the rule logic
- Interpretation or process model updates
 - PMU-1: Process model is too late because there was a lengthy approval process (red tape)
 - PMU-2: When the alert is not triggered, the health IT team may assume that the CDSS rule is working as intended



Class 1 Scenario Archetype: Unsafe Controller Behavior Causes without failure examples

- Internal controller states
 - CS-2: If the Health IT team is overburdened with other priorities as part of workload, it will continue to not update the CDSS rule logic for an alert
 - CS-3: If communication connections are disabled, then the health IT team can miss notifications or requests for the rule logic to be updated
 - CS-4: If problems are not identified as critical priorities, the health IT team may not know to prioritize



Class 1 Scenario Archetype: Unsafe Controller Behavior

Solution Examples

Responsibilities

- Health IT team is responsible for ensuring EHR aligns to/complies with data standards across all data types
- Health IT team is responsible for architecting the HIS
- Health IT team is responsible for maintaining the subsystems of the HIS (e.g., EHR, algorithms, models, databases, data pipelines, interfaces)

Interpretation or process model updates

- Address lengthy approval process delays via a safety management system (SMS)
- Provide warning through communications as part of the SMS that if a rule is not updated, it should not be used/relied on

Why Apply STPA to Health Information Systems?

Strengthen certification and accreditation processes

Inform more comprehensive testing strategies

Inform safer EHR procurement decisions

Guide robust system design and upgrades

Facilitate communication across stakeholders

Promote safer integration with third-party modules

Enhance existing guidelines and regulatory compliance

Align with broader safety and quality improvement frameworks



Questions?