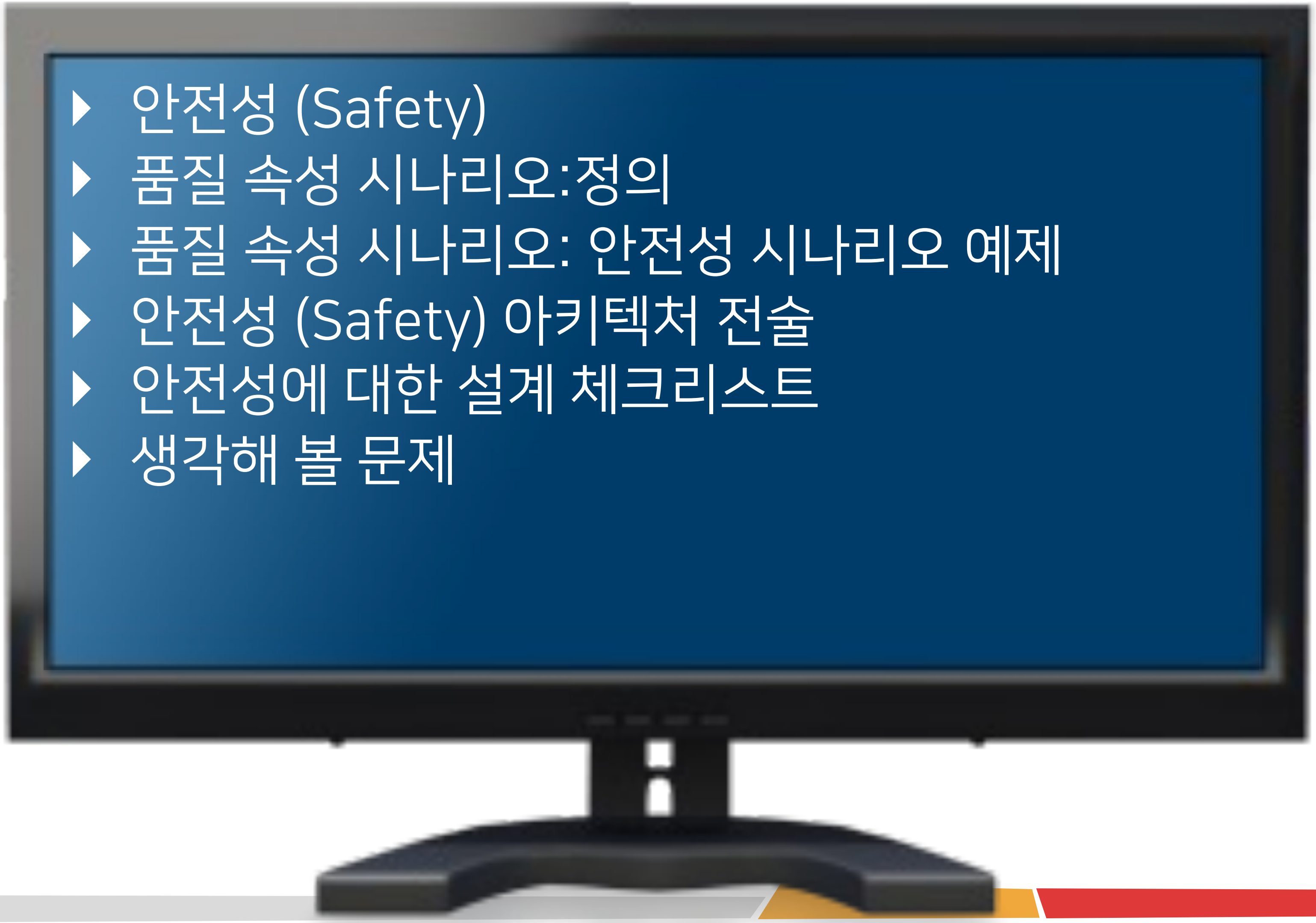
Summer 2022

Safety Tactics

Seonah Lee

Gyeongsang National University

안전성 (Safety) 아키텍처 전술



- 안전성 (Safety)
- 품질 속성 시나리오:정의
- 품질 속성 시나리오: 안전성 시나리오 예제
- 안전성 (Safety) 아키텍처 전술
- 안전성에 대한 설계 체크리스트
- 생각해 볼 문제

Safety

- 안전성 (Safety)
  - A system's ability to avoid astraying into states that cause or lead to damage, injury, or loss of life to actors in its environment

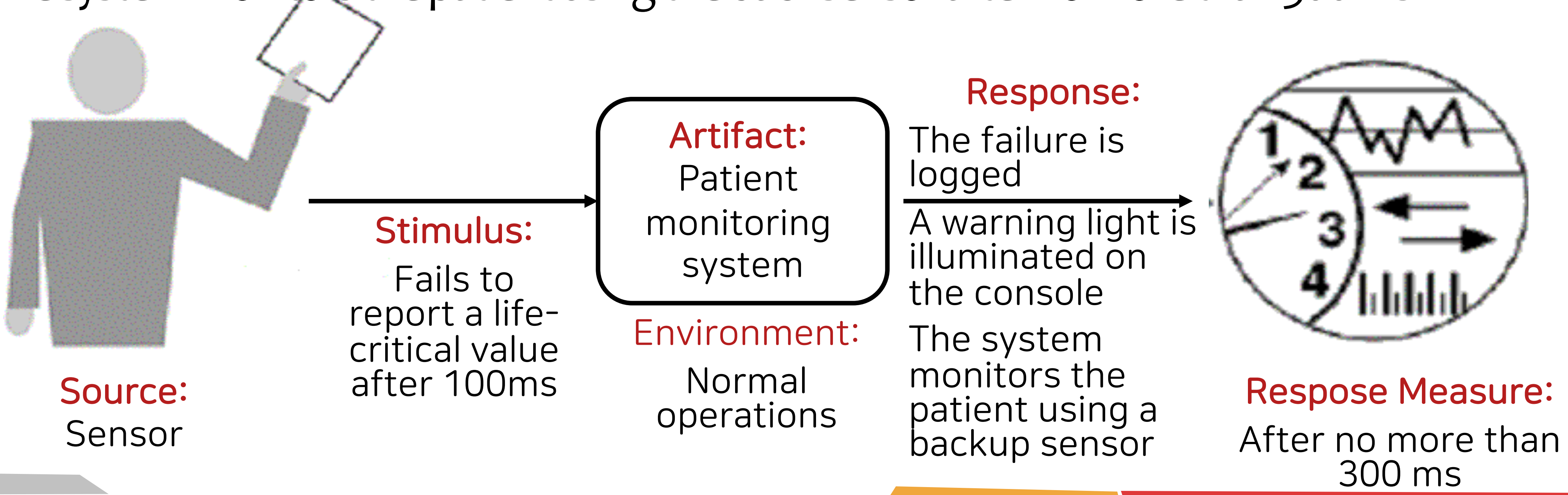
Unsafe States	Descriptions
Omissions	The failure of an event to occur
Commission	The spurious occurrence of an undesirable event
Timing	The occurrence of an event before (or after) the time required
Problems with system values	Incorrect but detectable values; Incorrect and undetectable values
Sequence omission and commission	An event is missing or an unexpected event is inserted
Out of sequence	A sequence of event arrive, not in the prescribed order

Quality Attribute Scenario for Safety

Component	Description
Source	A data source, a time source, or a user action
Stimulus	An omission, commission, or occurrence of incorrect data or timing
Environment	System operating mode
Artifact	Some part of the system
Response	The system does not leave a safe state space The system returns to a safe state space The system continues to operate in a degraded mode to minimize damage Users are advised of the unsafe state or the prevention The even is logged
Response Measure	Tine to return to safe state space Damage or injury caused

Quality Attribute Scenario Example for Safety

- A sensor in the patient monitoring system fails to report a life-critical value after 100 ms.
- The failure is logged, a warning light is illuminated on the console, and a backup (lower-fidelity) sensor is engaged.
- The system monitors the patient using the back sensor after no more than 300 ms.



Source: Sensor

Stimulus: Fails to report a life-critical value after 100ms

Artifact: Patient monitoring system

Environment: Normal operations

Response: The failure is logged

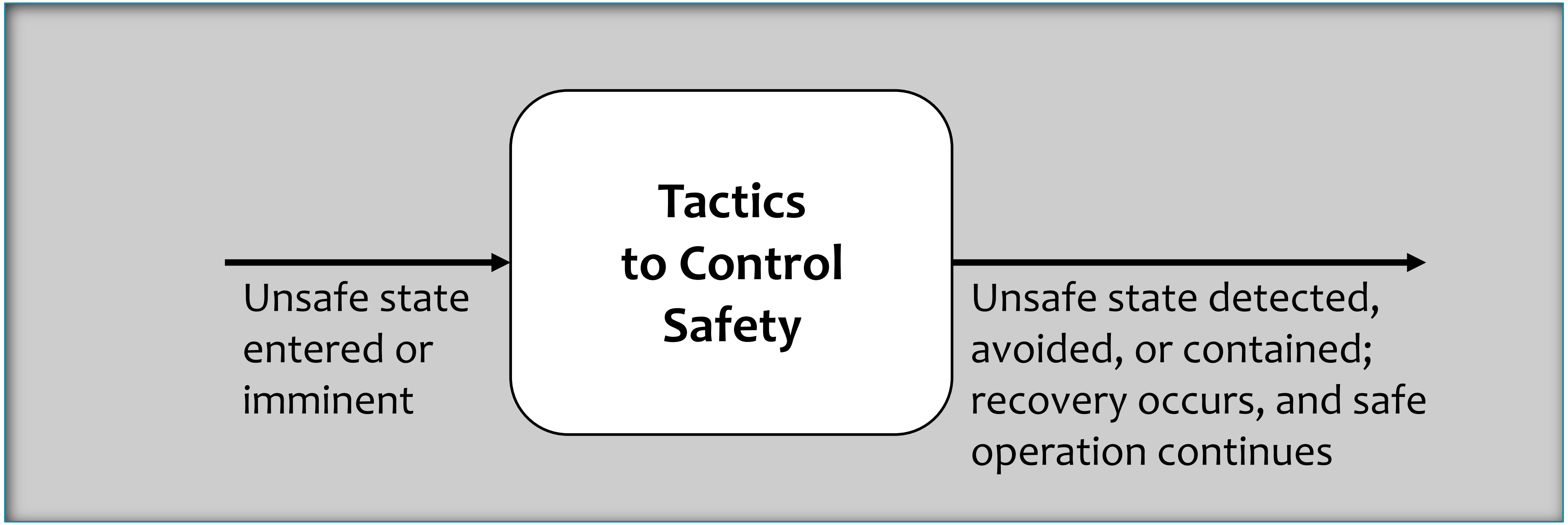
A warning light is illuminated on the console

The system monitors the patient using a backup sensor

Respose Measure: After no more than 300 ms

Safety Tactics

- Safety tactics may be broadly categorized as unsafe state avoidance, unsafe state detection, or unsafe state remediation.



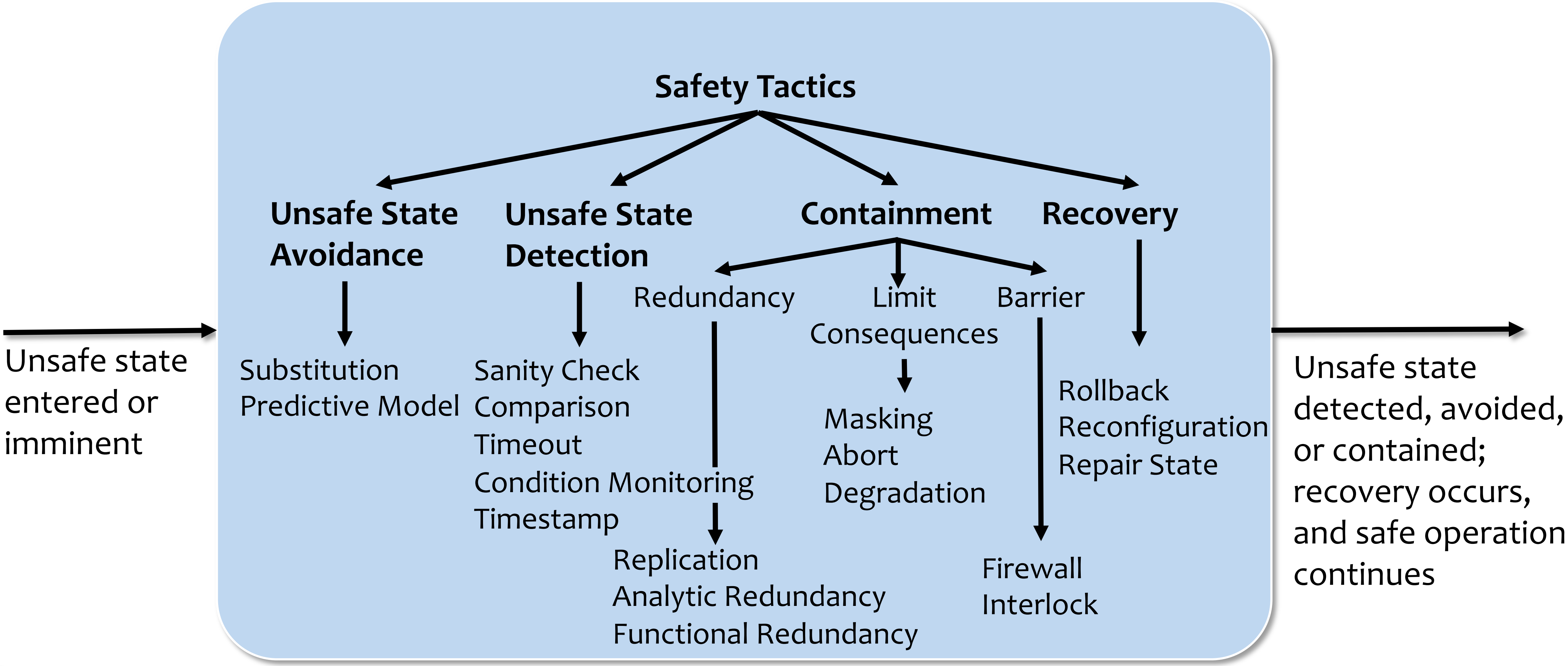
Unsafe state entered or imminent

Tactics to Control Safety

Unsafe state detected, avoided, or contained; recovery occurs, and safe operation continues

http://etutorials.org/Programming/Software+architecture+in+practice,+second+edition/

Safety Tactics



Unsafe state entered or imminent

Safety Tactics

Unsafe State Avoidance

Substitution
Predictive Model

Unsafe State Detection

Sanity Check
Comparison
Timeout
Condition Monitoring
Timestamp

Containment

Redundancy

Replication
Analytic Redundancy
Functional Redundancy

Limit Consequences

Masking
Abort
Degradation

Barrier

Firewall
Interlock

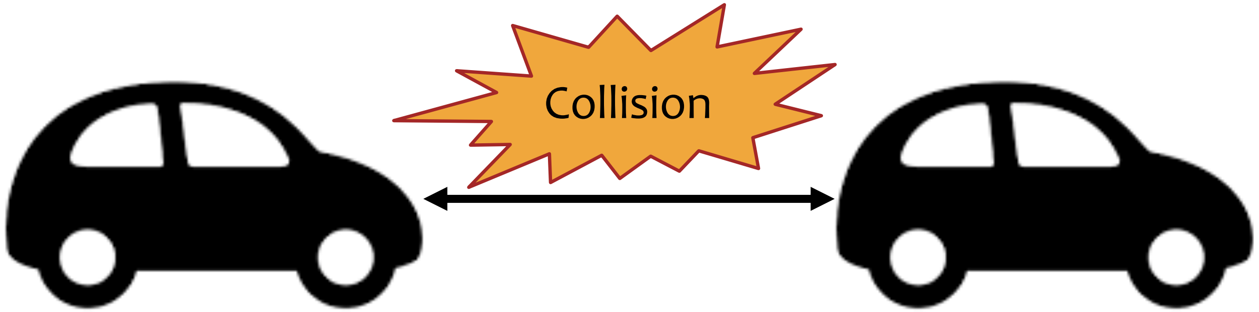
Recovery

Rollback
Reconfiguration
Repair State

Unsafe state detected, avoided, or contained; recovery occurs, and safe operation continues

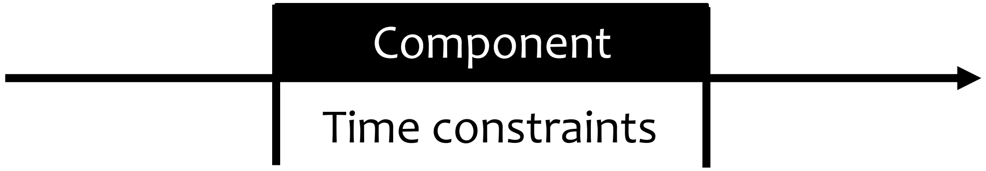
Safety Tactics

- Unsafe State Avoidance
  - Substitution
    - Protection mechanism for potentially dangerous software design features
      - Watchdogs, monitors, and interlocks
  - Predictive Model
    - A model that predicts the state of health of system processes, resources, or other properties

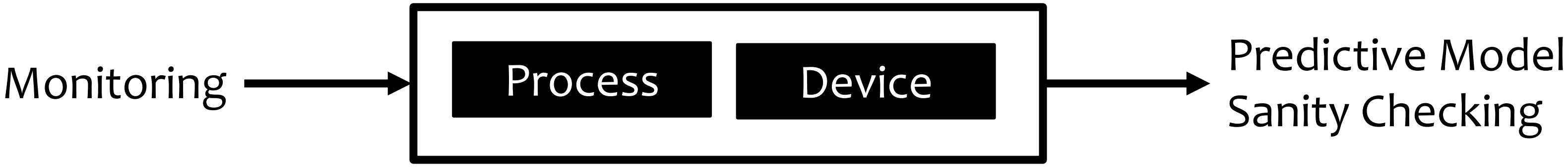


Safety Tactics

- Unsafe State Detection
  - Timeout
    - to determine whether the operation of a component is meeting its timing constraints

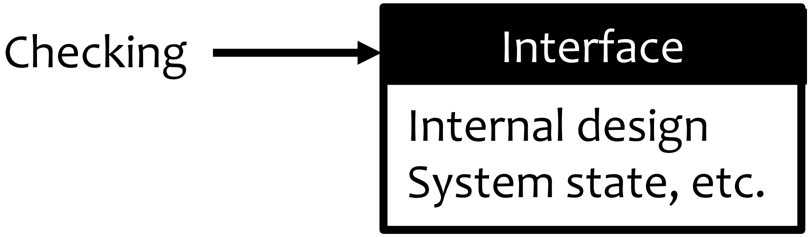


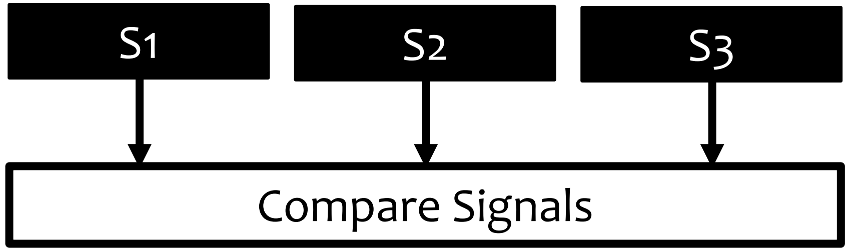
  - Timestamp
    - to detect incorrect sequences of events, primarily in distributed message-passing systems
  - Condition Monitoring
    - Condition monitoring identifies system states that may lead to hazardous behavior.



Safety Tactics

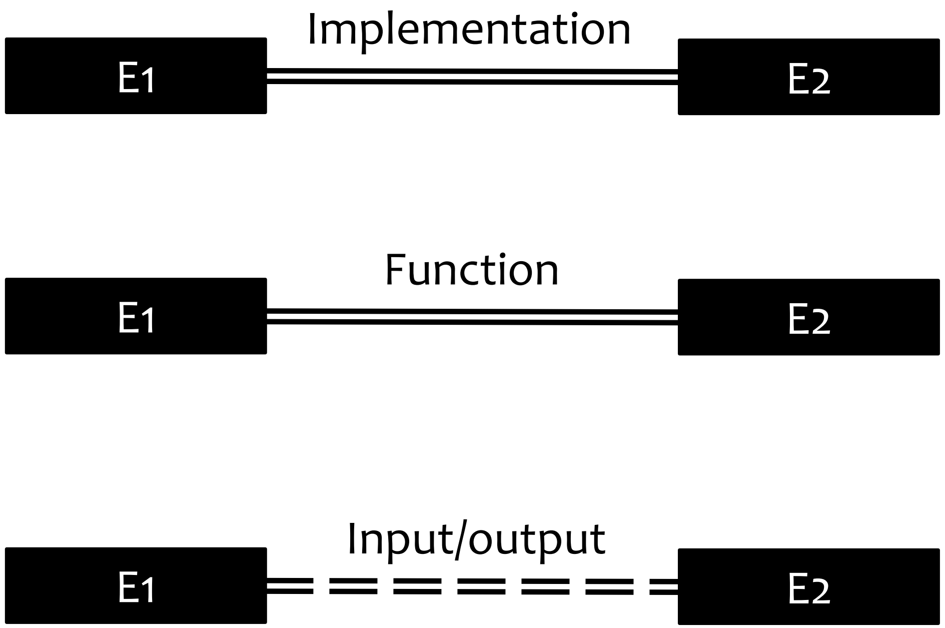
- ## Unsafe State Detection
  - ### Sanity Checking
    - The sanity checking tactic checks the validity or reasonableness of specific operation results, inputs or outputs of a component
  - ### Comparison
    - The comparison tactic allows the system to detect unsafe states by comparing the outputs produced by a number of synchronized or replicated elements.





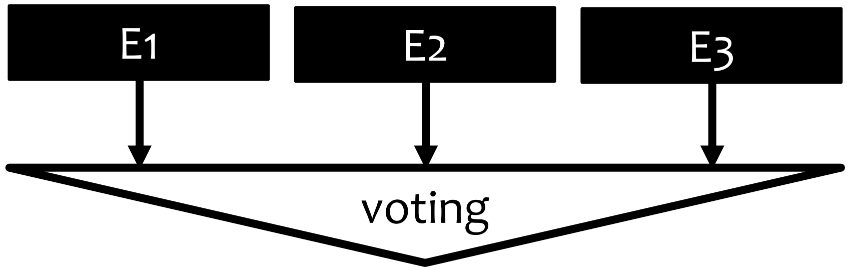
Safety Tactics

- **Containment: Redundancy**
  - **Replication**
    - It just involves having clones of a component
  - **Functional Redundancy**
    - It makes design diversity to address the issue of common mode failures in components
  - **Analytic Redundancy**
    - It permits not only diversity of components, but also a higher-level diversity that is visible at the input and output level



Safety Tactics

- **Containment: Limit Consequences**
  - **Masking**
    - It masks a fault by comparing components

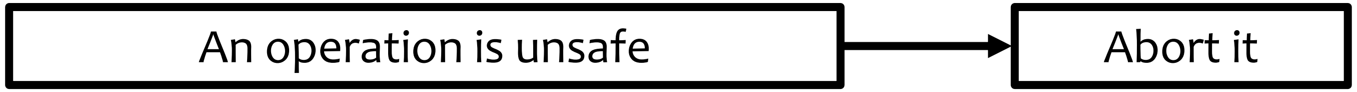

E1

E2

E3

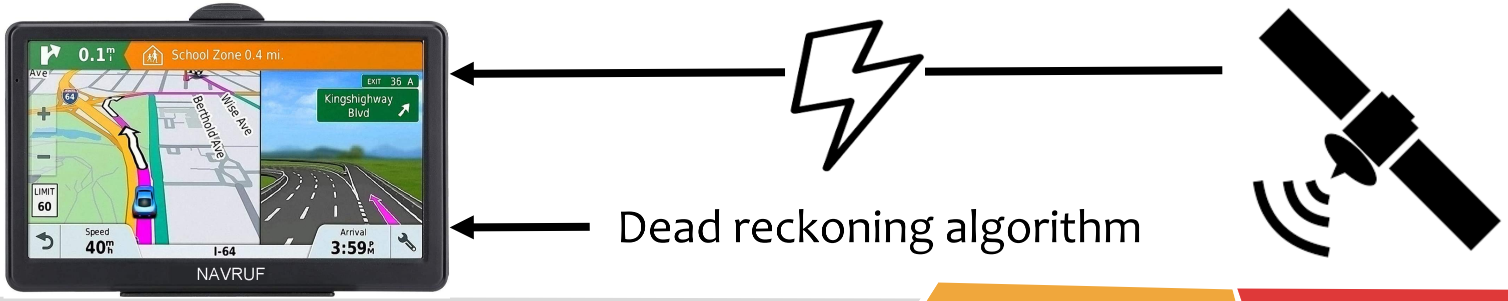
voting

  - **Abort**


An operation is unsafe

Abort it

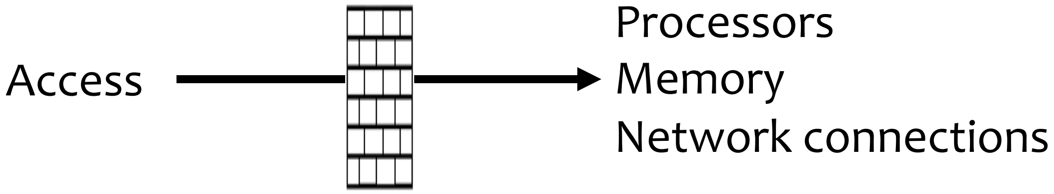
  - **Degradation**
    - maintains the most critical system functions in the presence of component failures

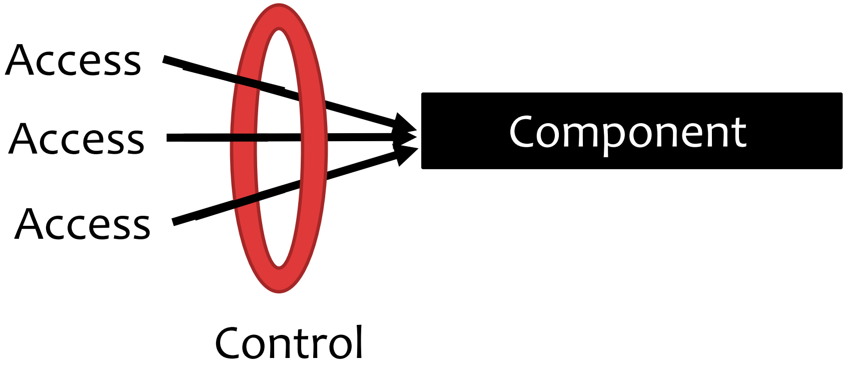


Dead reckoning algorithm

Safety Tactics

- **Containment: Barrier**
  - **Firewall**
    - A firewall limits access to specified resources
  - **Interlock**
    - The interlock protects against failures arising from incorrect sequencing of events.



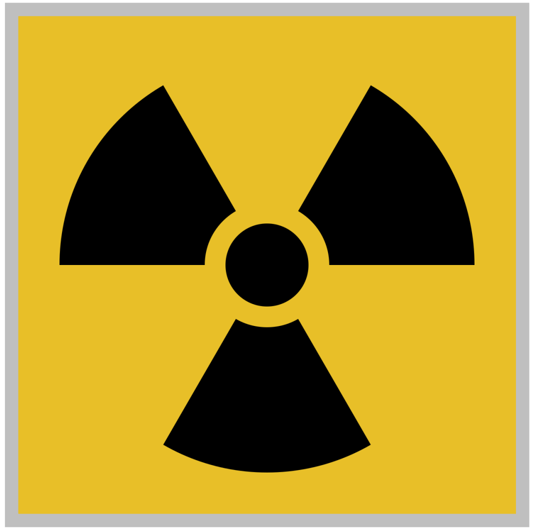


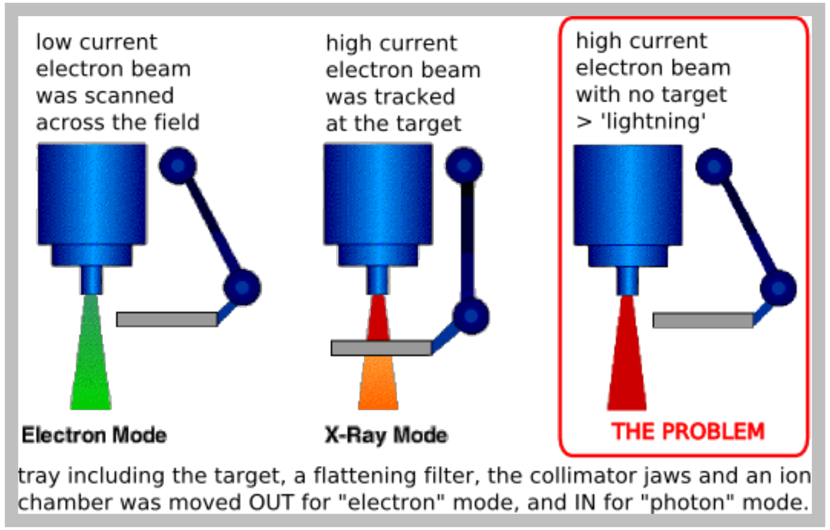
Safety Tactics

- Recovery
  - Rollback
    - It permits the system to revert to a saved copy of a previous known good state—the rollback line—upon the detection of a failure.
  - Reconfiguration
    - It attempts to recover from component failures by remapping the logical architecture onto the (potentially limited) resources left functioning.
  - Repair State
    - It repairs an erroneous state and then continues execution.
    - It increases the set of states that a component can handle competently, without failure

Radiation Therapy Machine

Therac - 25
(파생 모델 – 방사선 누출)





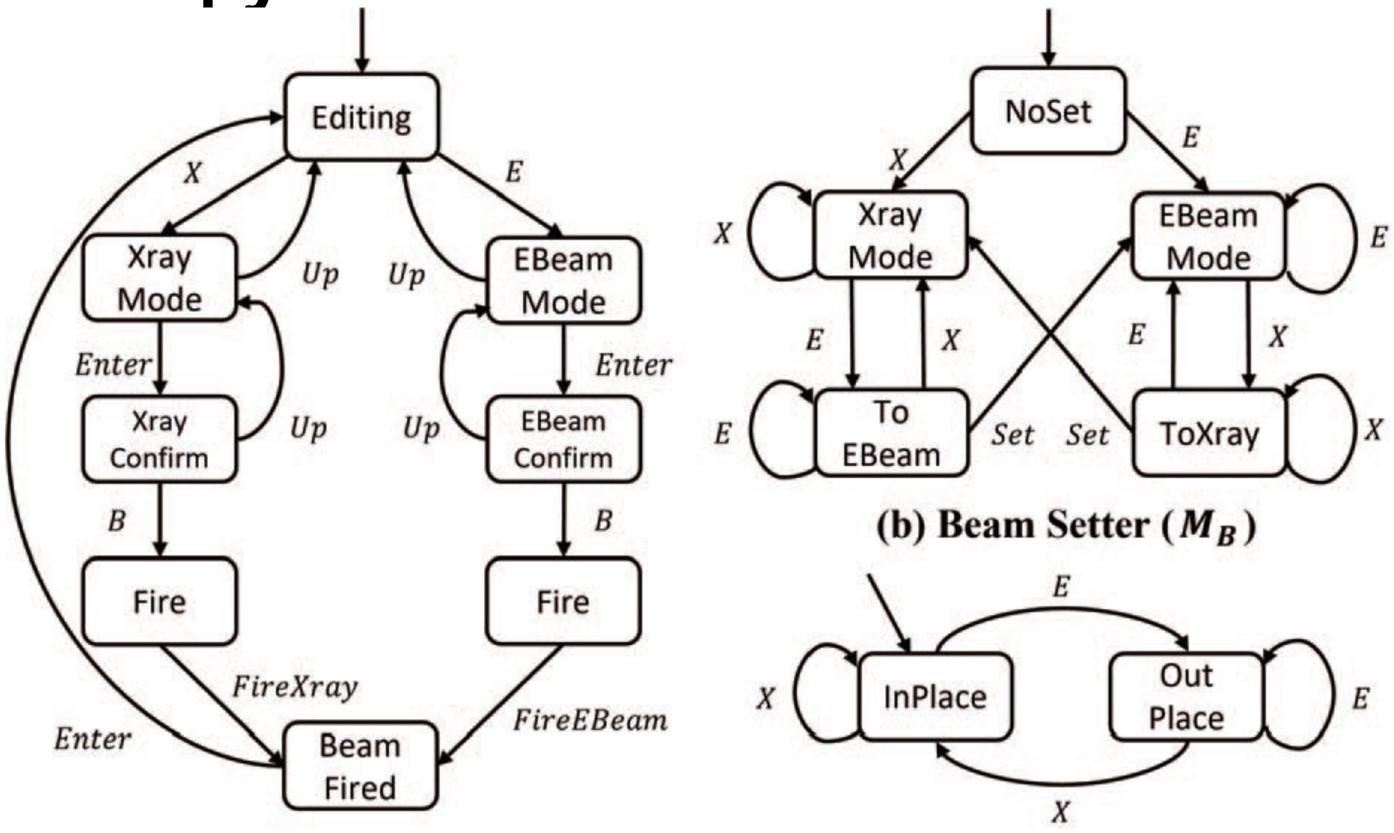
tray including the target, a flattening filter, the collimator jaws and an ion chamber was moved OUT for "electron" mode, and IN for "photon" mode.

- 암 종양 제거를 위한 방사선 치료기
- Therac-20의 SW를 재사용
- Therac-20에서 문제없었으나 Therac-25에서 문제 발생
  → HW 개선으로 속도가 빨라지면서 ' 잠재된 ' 버그가 동작

'이전에 안전했던
소스'가
안전을 담보하지 못함

Radiation Therapy Machine

- Radiation therapy machine



(b) **Beam Setter (M_B)**

(a) **Interface (M_I)**

(c) **Spreader (M_S)**

Zhang, Changjian, Taranj Saluja, Rômulo Meira-Góes, Matthew Bolton, David Garlan, and Eunsuk Kang. "Robustification of Behavioral Designs against Environmental Deviations." (2023).

Question?

Seonah Lee
saleese@gmail.com