STPA Exercise:
DoD Access Control Barrier

John Thomas

Access control barrier

System-Theoretic Process Analysis (STPA)

- Identify system accidents, hazards
- Draw functional control structure
- Identify unsafe control actions
- Identify accident scenarios

(Leveson, 2012)

Access Control Barrier

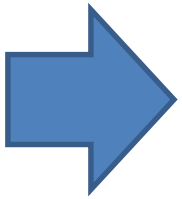
- Accidents (Mishaps)
  - A-1: People injured or killed (traditional safety)
  - ?

Access Control Barrier

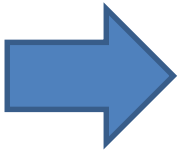
- Accidents (Mishaps)
  - A-1: People injured or killed (traditional safety)
  - A-2: Economic loss (damage to vehicle or barrier)
  - A-3: Unauthorized access
  - A-4: Authorized access not allowed

Access Control Barrier

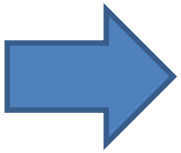
- Accidents (Mishaps)
  - A-1: People injured or killed
  - A-2: Economic loss (damage to vehicle or barrier)
  - A-3: Unauthorized access
  - A-4: Authorized access not allowed



Traditional Safety



Security



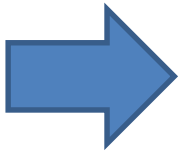
Functional

Access Control Barrier

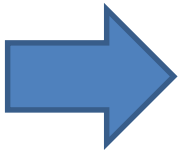
- Accidents
  - A-1: People injured or killed
  - A-2: Economic loss (damage to vehicle or barrier)
  - A-3: Unauthorized access
  - A-4: Authorized access not allowed
- Barrier System Hazards
  - H-1: Barrier damages authorized person/vehicle [A-1,A-2,A-4]
  - H-2: Barrier doesn't stop unauthorized vehicle [A-3]
  - H-3: Barrier prevents authorized access [A-4]

Access Control Barrier

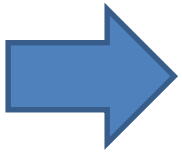
- System Hazards
  - H-1: Barrier damages authorized person/vehicle [A-1,A-2,A-4]
  - H-2: Barrier doesn't stop unauthorized vehicle [A-3]
  - H-3: Barrier prevents authorized access [A-4]



Traditional Safety



Security



Functional

System-Theoretic Process Analysis (STPA)

- Identify system accidents, hazards
- Draw functional control structure
- Identify unsafe control actions
- Identify accident scenarios

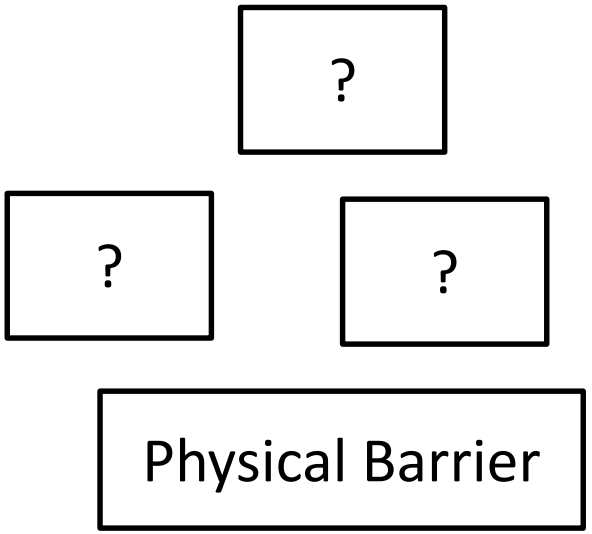
(Leveson, 2012)

Control structure

- Identify:
  - Physical Process
  - Controllers
  - Responsibilities
  - Control actions
  - Process Models

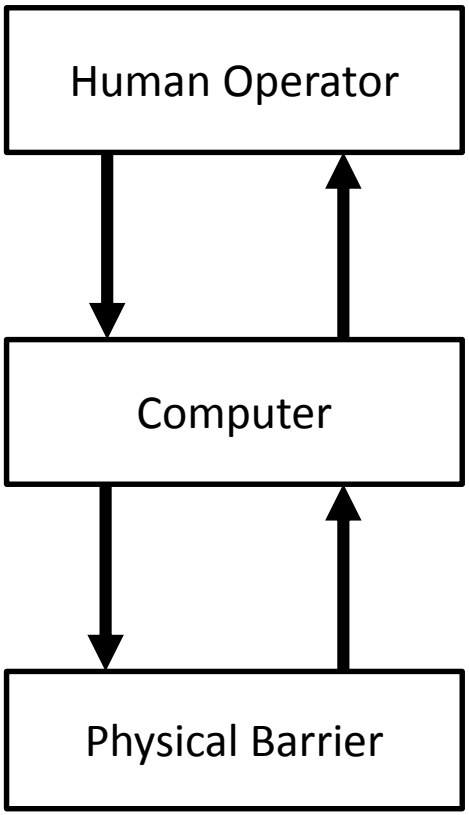
Control structure

- Identify:
  - Physical Process
  - Controllers
  - Responsibilities
  - Control actions
  - Process Models

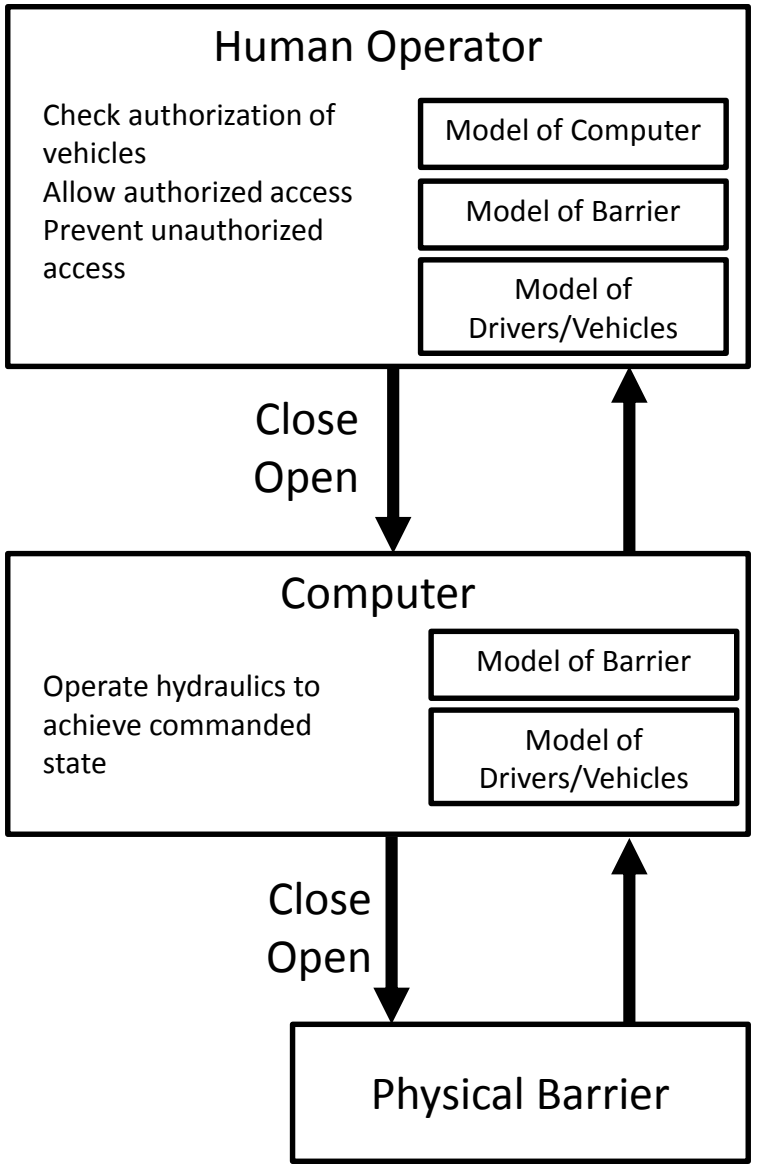


Control structure

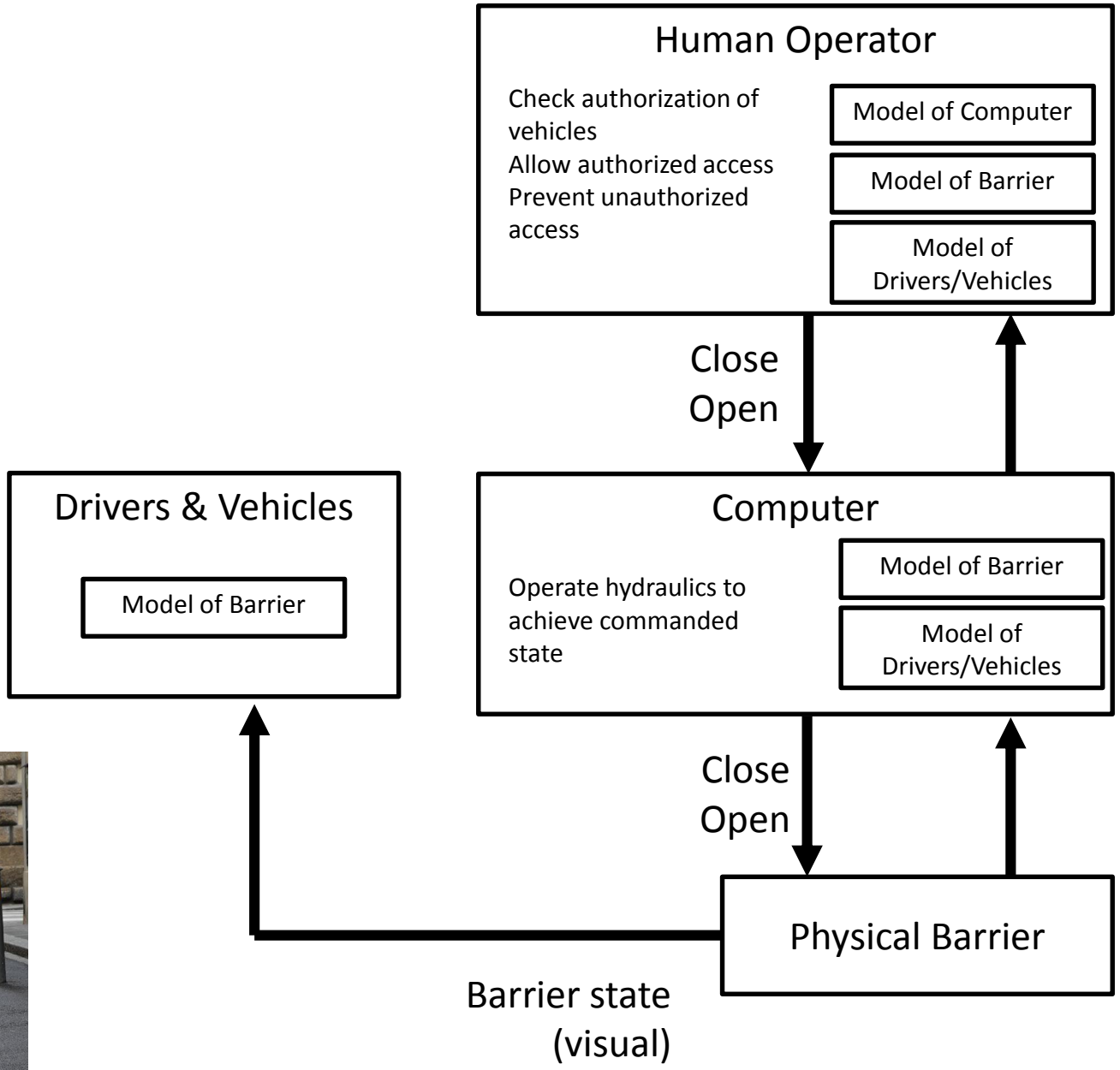
- Identify:
  - Physical Process
  - Controllers
  - Responsibilities
  - Control actions
  - Process Models



Access Control Barrier



Access Control Barrier

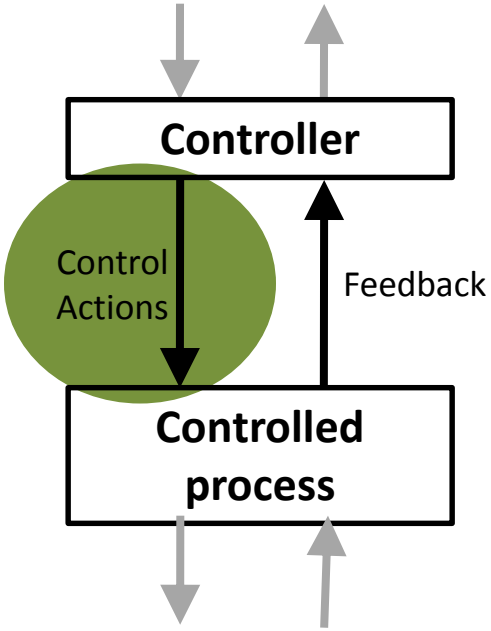


System-Theoretic Process Analysis (STPA)

- Identify system accidents, hazards
- Draw functional control structure
- Identify unsafe control actions
- Identify accident scenarios

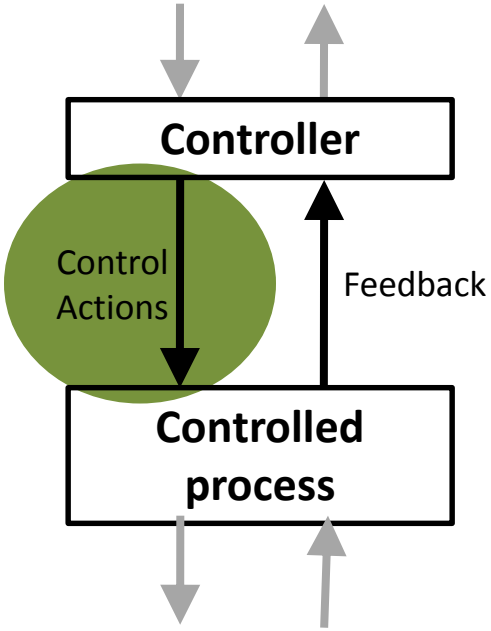
(Leveson, 2012)

Unsafe Control Actions (UCA)



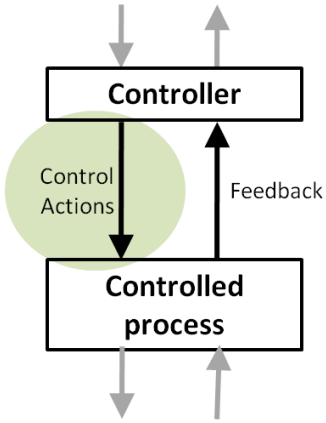
Command A				

Unsafe Control Actions (UCA)



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Command A	?	?	?	?

Structure of an Unsafe Control Action



Example:

"Operator does not provide Open Cmd when vehicle has been authorized" [H-3]

Source Controller

Type

Control Action

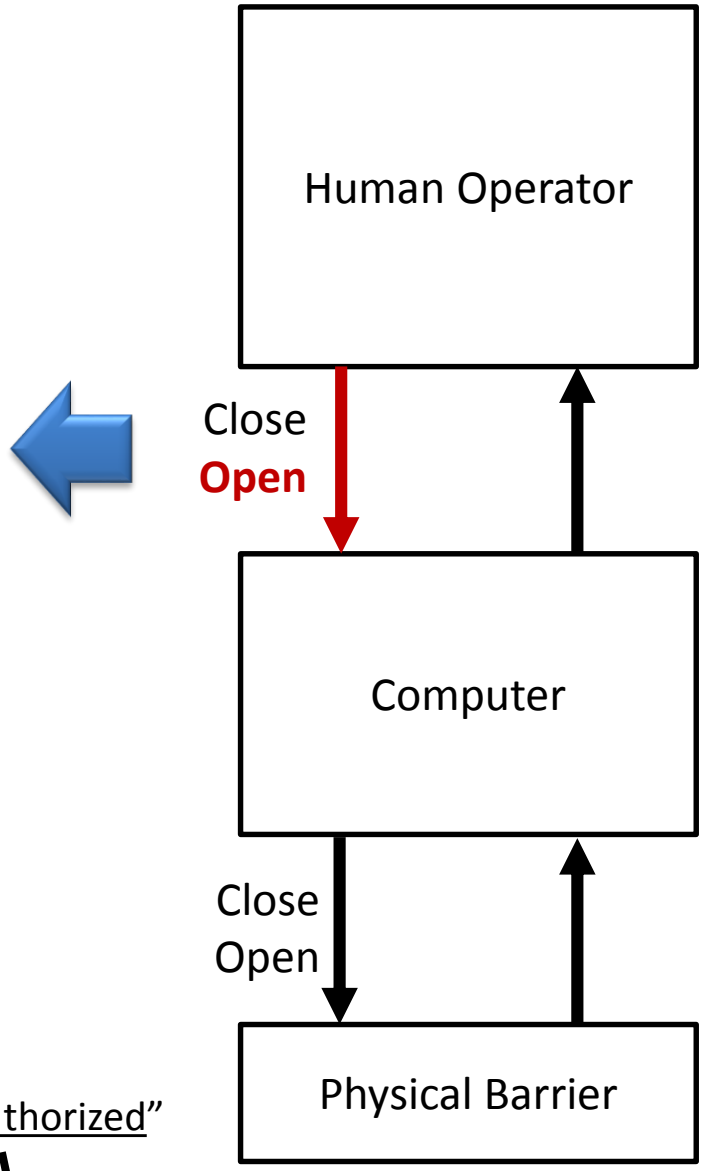
Context

Four parts of an unsafe control action

- Source Controller: the controller that can provide the control action
- Type: whether the control action was provided or not provided
- Control Action: the controller's command that was provided / missing
- Context: conditions for the hazard to occur
  - (system or environmental state in which command is provided)

Unsafe Control Actions

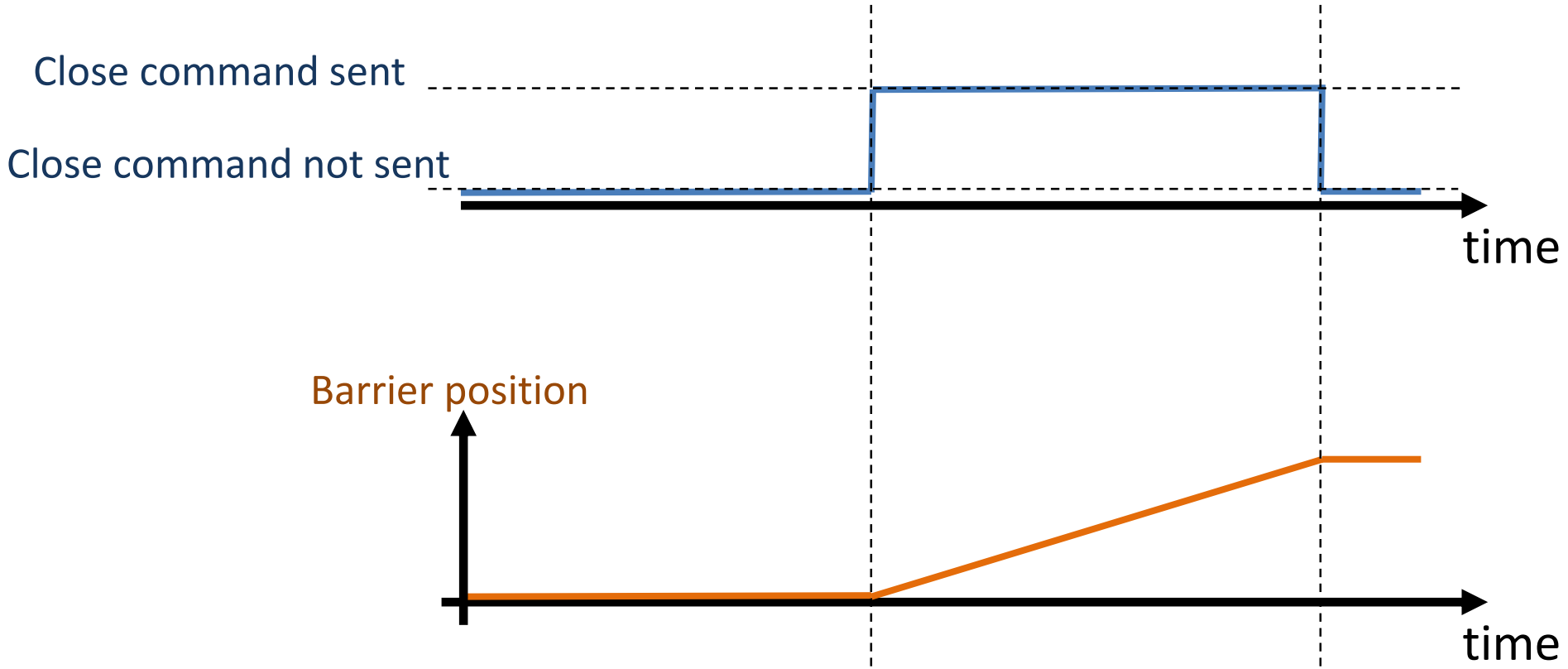
	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Open Cmd	**Operator does not provide Open Cmd when _____**	**Operator provides Open Cmd when _____**	**Operator provides Open Cmd too late after _____** **Operator provides Open Cmd too early before _____**	**Operator stops providing Open Cmd too soon before _____** **Operator continues applying Open Cmd too long after _____**



Example:
"Operator does not provide Open Cmd when vehicle has been authorized"

Source Controller — Type — Control Action — Context

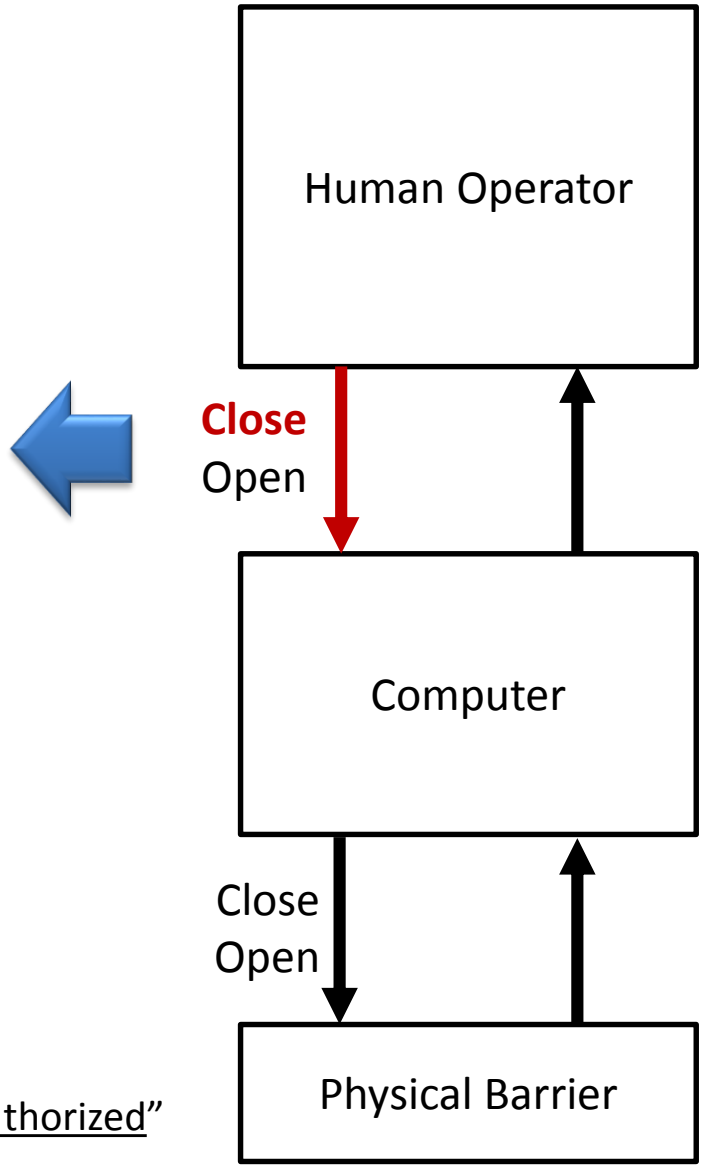
Commands with a duration



Stopped too soon, Applied too long refers to commands with a duration

Unsafe Control Actions

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Cmd	**Operator does not provide Close Cmd when _____**	**Operator provides Close Cmd when _____**	**Operator provides Close Cmd too late after _____** **Operator provides Close Cmd too early before _____**	**Operator stops providing Close Cmd too soon before _____** **Operator continues applying Close Cmd too long after _____**



Example:
"Operator does not provide Open Cmd when vehicle has been authorized"

Source Controller — Type — Control Action — Context

H-1: Barrier damages authorized person/vehicle
H-2: Barrier doesn't stop unauthorized vehicle
H-3: Barrier prevents authorized access

UCAs → Safety Constraints (Procedures)

Unsafe Control Action		Safety Constraint
Operator does not provide Open Cmd when vehicle is authorized [H-3]		Operators must provide Open Cmd once vehicle has been authorized [H-3]
		
		
		

System-Theoretic Process Analysis (STPA)

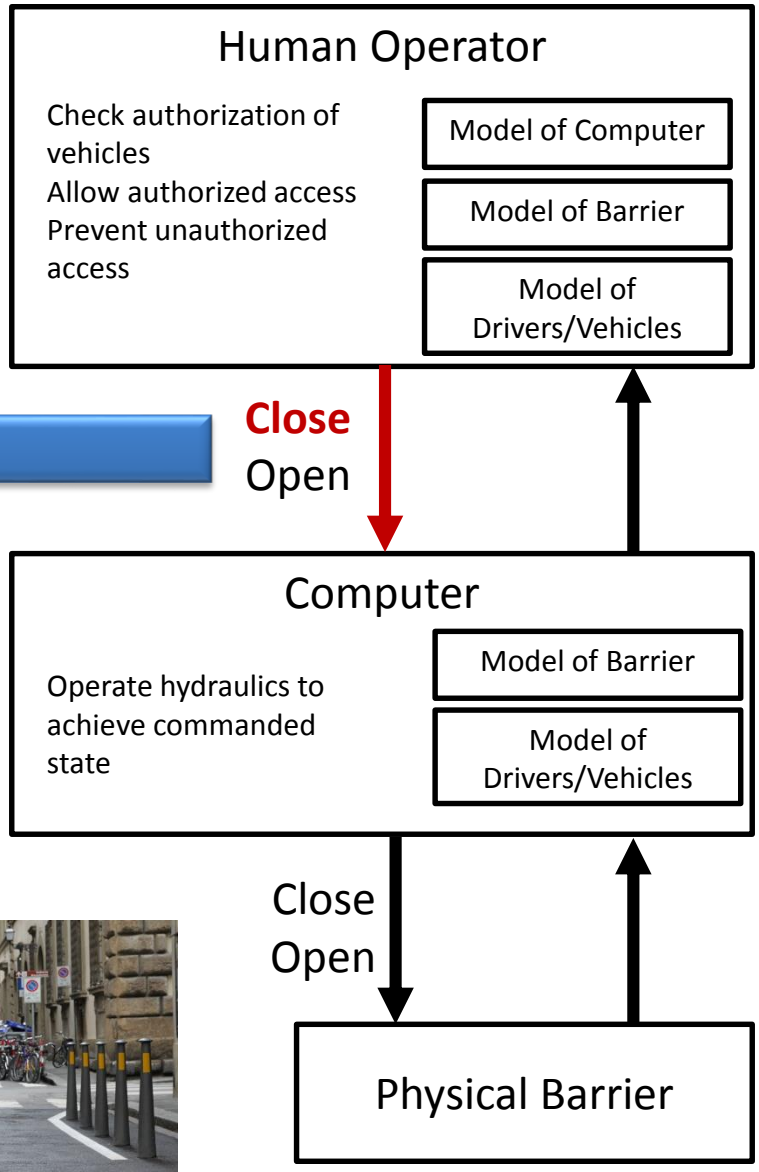
- Identify system accidents, hazards
- Draw functional control structure
- Identify unsafe control actions
- Identify accident scenarios

(Leveson, 2012)

Access Control Barrier

How could these UCAs occur?
(causal scenarios)

UCA-1: Operator does not provide Close Cmd before unauthorized vehicle passes through [H-2]



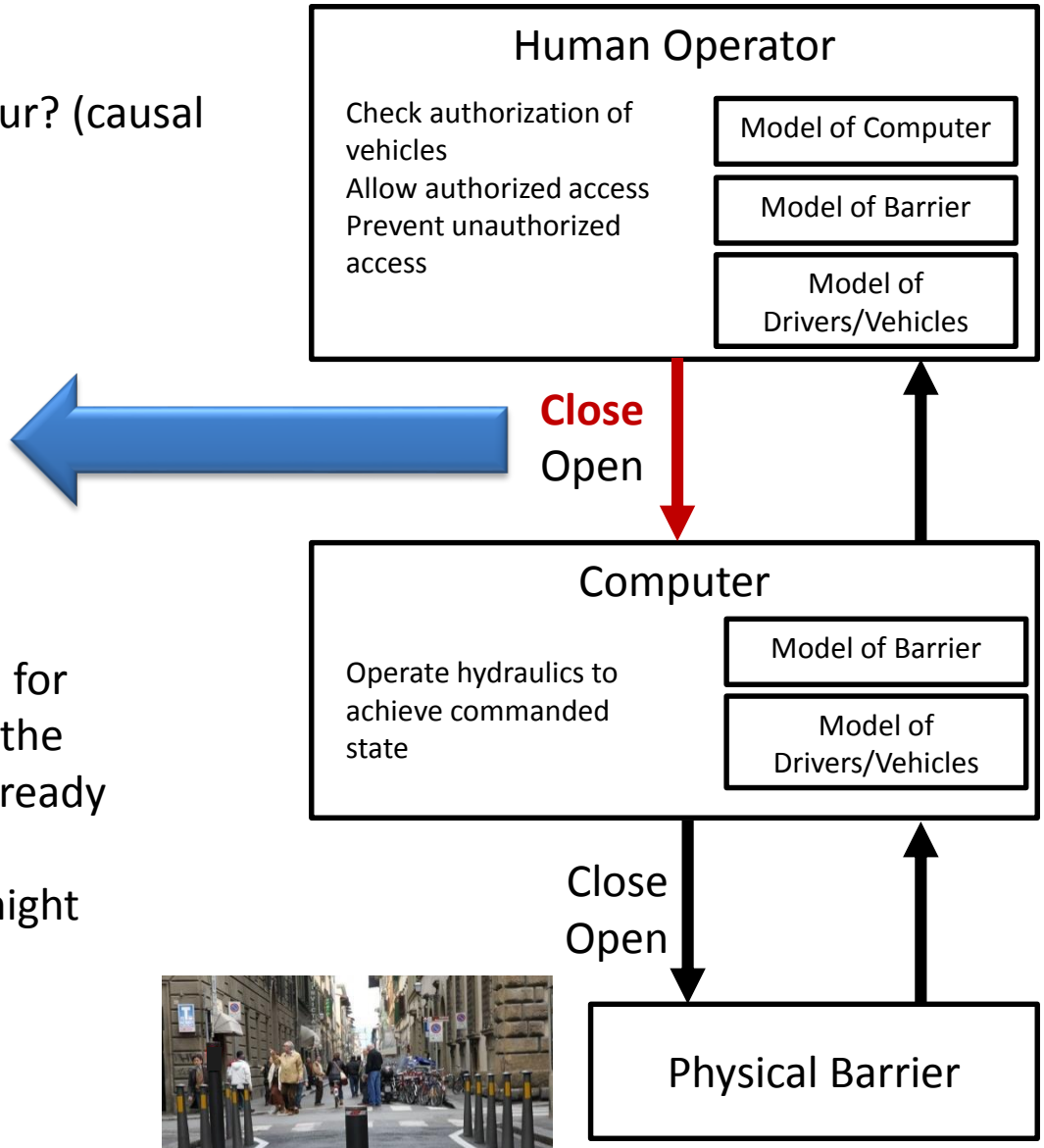
How can this happen?

- Incorrect operator beliefs? (process models)
- What might cause these flawed beliefs?
- Inadequate feedback?
- Operator procedures
- Other operators, supervisors
- Etc.

Access Control Barrier

How could those conditions occur? (causal scenarios)

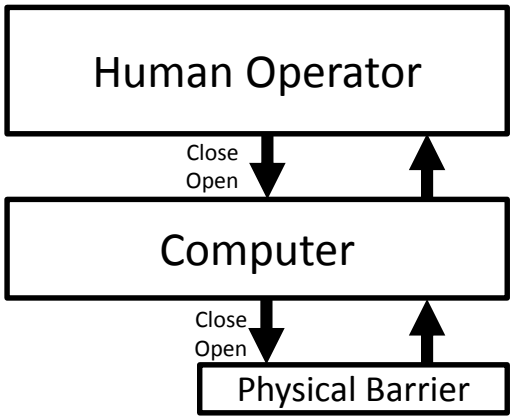
UCA-1: Operator does not provide Close Cmd before unauthorized vehicle passes through [H-2]



Example Scenarios:

- Operator did not provide Close Cmd for unauthorized vehicle [H-2] because the operator believed the barrier was already closed.
  - Why? What kind of feedback might cause this belief?

Identify Solutions for Scenarios



Example Scenarios:

- S-1: Operator did not provide Close Cmd for unauthorized vehicle [H-2] because the previous authorized vehicle passed through quicker than usual (reaction time)
- S-2: Operator did not provide the Close Cmd for unauthorized vehicle [H-2] because he was interrupted and forgot it had not been closed
- S-3: Operator provided the Close Cmd too early before authorized vehicle was clear [H-1,H-3] because he had learned to compensate for delayed system response
- S-4: Operator provided Close Cmd when authorized vehicle was on barrier [H-1,H-3] because he didn't expect vehicle to stop on barrier

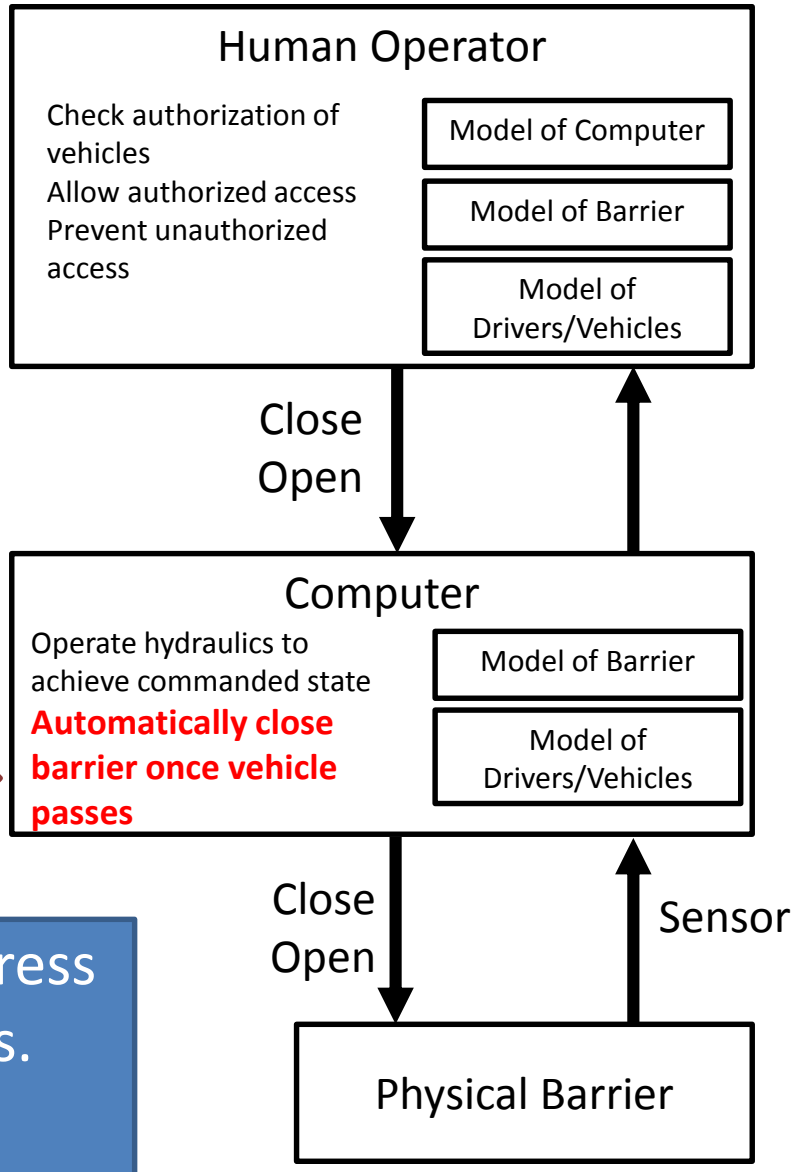
Potential Design Solutions:

- Make computer automatically close barrier once vehicles pass through [S-1,2,3]
- Provide feedback about barrier state. [S-2]
- Provide alert when barrier is opened for extended period [S-2]
- Add safety suppression loop, computer interlock [S-3,4]

Access Control Barrier

Potential Design Solutions:

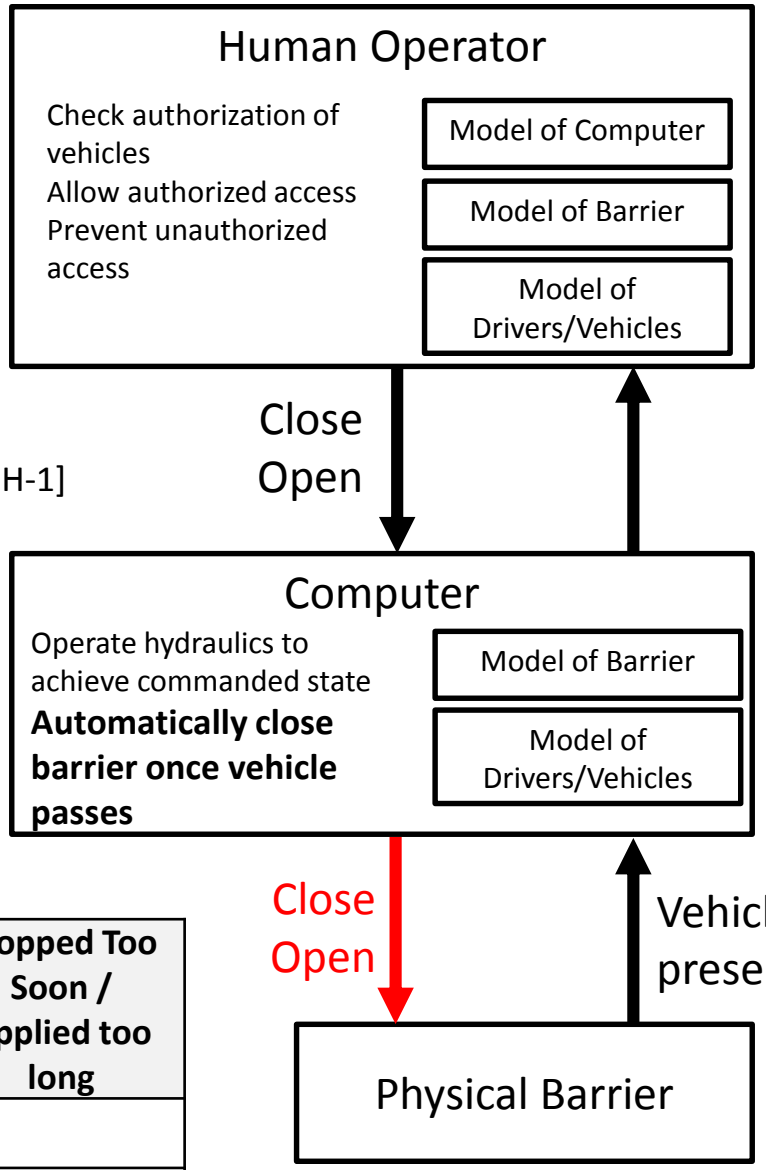
- Make computer automatically close barrier once vehicles pass through[S-1,2,3]



This technical solution could help address several human interaction problems.
Could it cause new problems?
Let's analyze the technical system!

Analyze the Computer

H-1: Barrier damages authorized person/vehicle
H-2: Barrier doesn't stop unauthorized vehicle
H-3: Barrier prevents authorized access



Example:
"Computer provides Close Cmd when vehicle is still over barrier" [H-1]

- Computer: Source Controller
- provides: Type
- Close Cmd: Control Action
- vehicle is still over barrier: Context

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close Cmd				
Open Cmd				

Access Control Barrier

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Close	Computer does not provide Close Cmd when commanded by operator and vehicle is not present [H-2]	Computer provides Close Cmd when authorized vehicle is on barrier [H-1] Computer provides Close Cmd when powered on (unknown state) Computer provides Close Cmd when not commanded by operator and no vehicle has passed through [H-1,H-3]	Computer provides Close Cmd too late to stop following vehicle [H-2] Computer provides Close Cmd too early, before authorized vehicle has passed through [H-1, H-3] Computer provides Close Cmd too early, before vehicle is authorized [H-1, H-3]	Computer keeps applying Close Cmd when Open Cmd is being issued Computer keeps applying Close Cmd Too long after barrier is already up [H-1]
Open				

Access Control Barrier

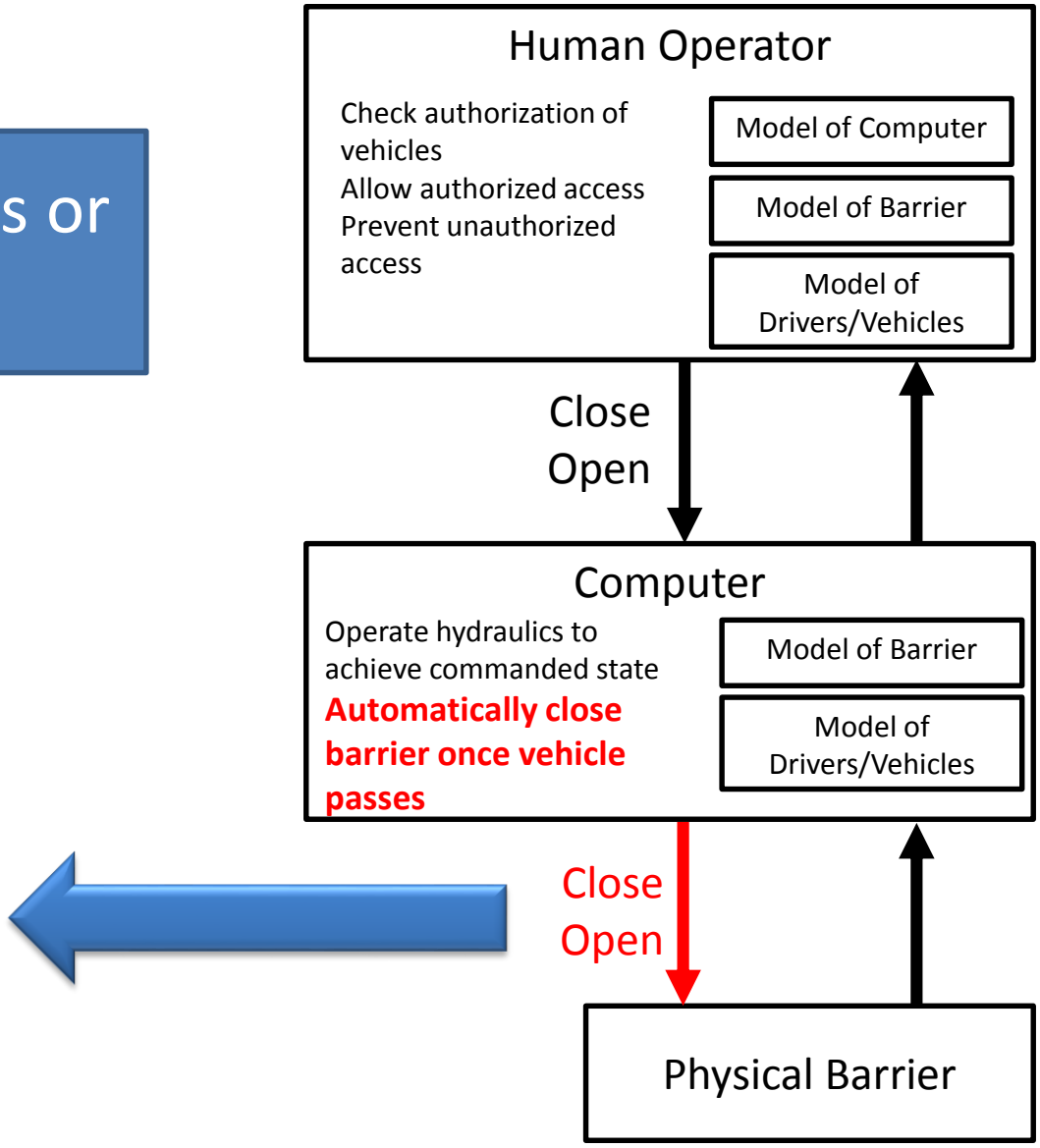
Are these safety issues or security issues?

UCA-1: Computer provides Close Cmd too early before authorized vehicle is clear [H-1]

UCA-2: Computer provides Close Cmd too late to stop the following vehicle [H-1,H-2]

UCA-3: Computer does not provide Close Cmd when commanded by operator [H-2]

Etc.



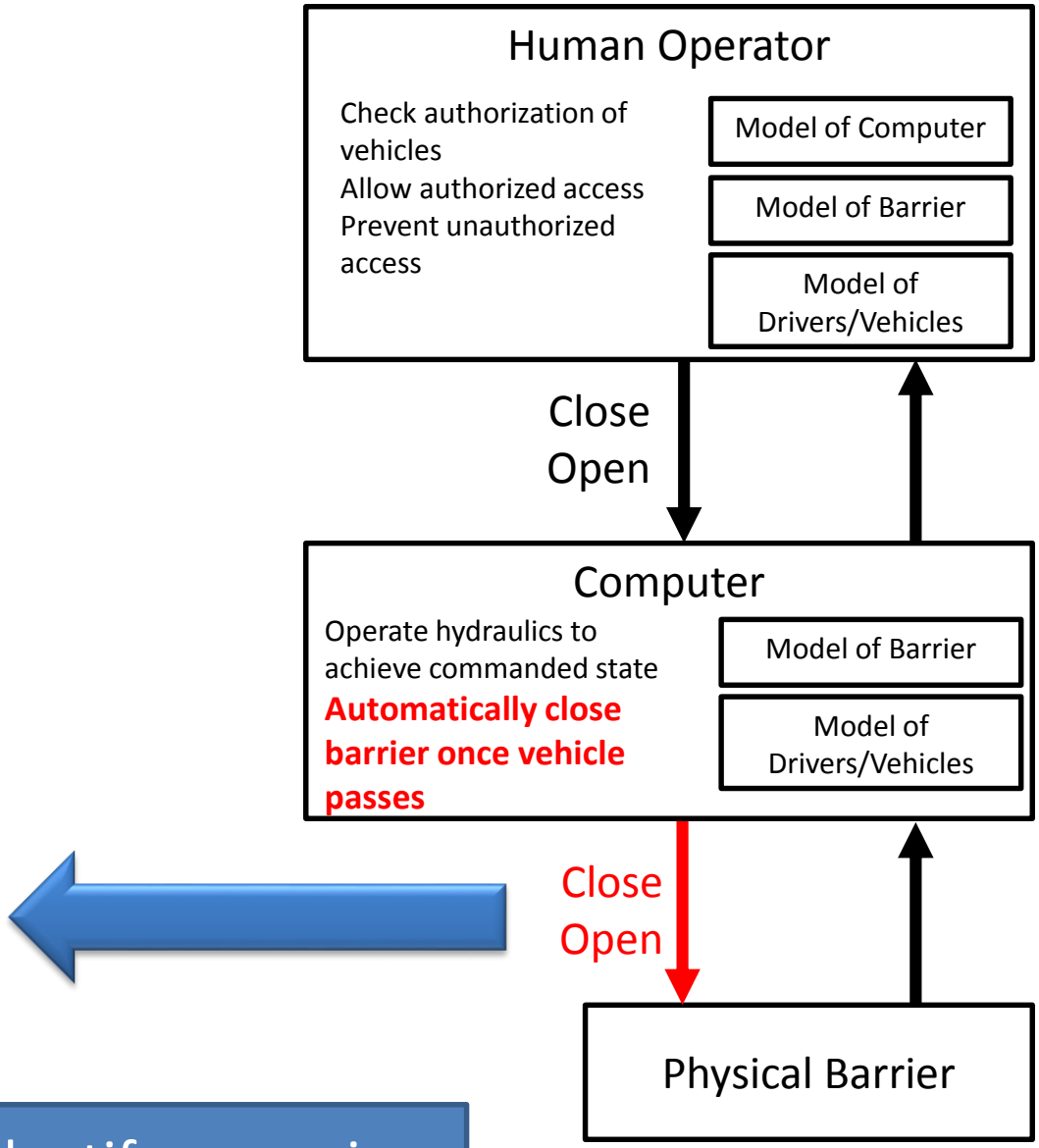
Access Control Barrier

UCA-1: Computer provides Close Cmd too early before authorized vehicle is clear [H-1]

UCA-2: Computer provides Close Cmd too late to stop the following vehicle [H-1,H-2]

UCA-3: Computer does not provide Close Cmd when commanded by operator [H-2]

Etc.



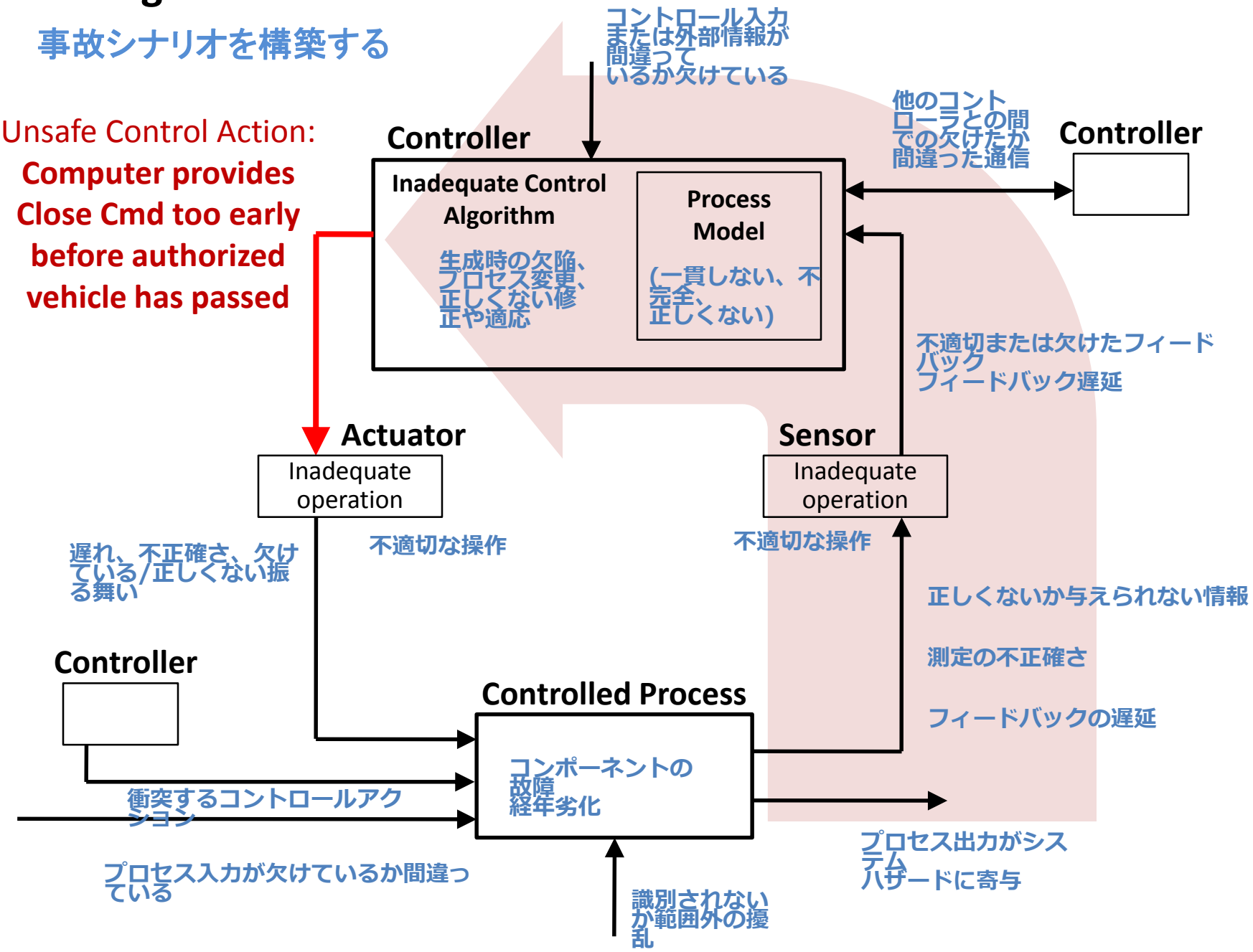
Identify scenarios

Building Accident Scenarios

事故シナリオを構築する

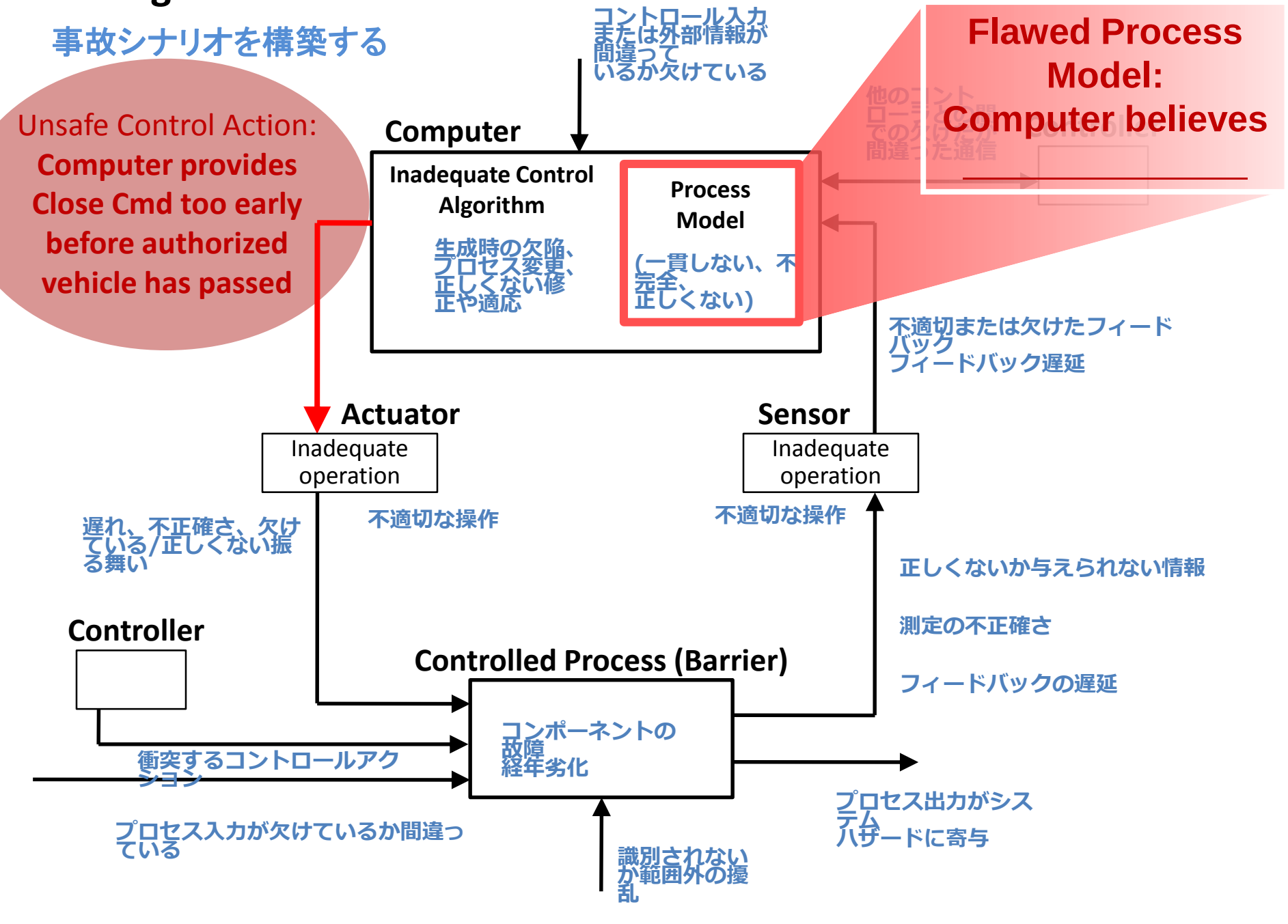
Unsafe Control Action:

Computer provides Close Cmd too early before authorized vehicle has passed



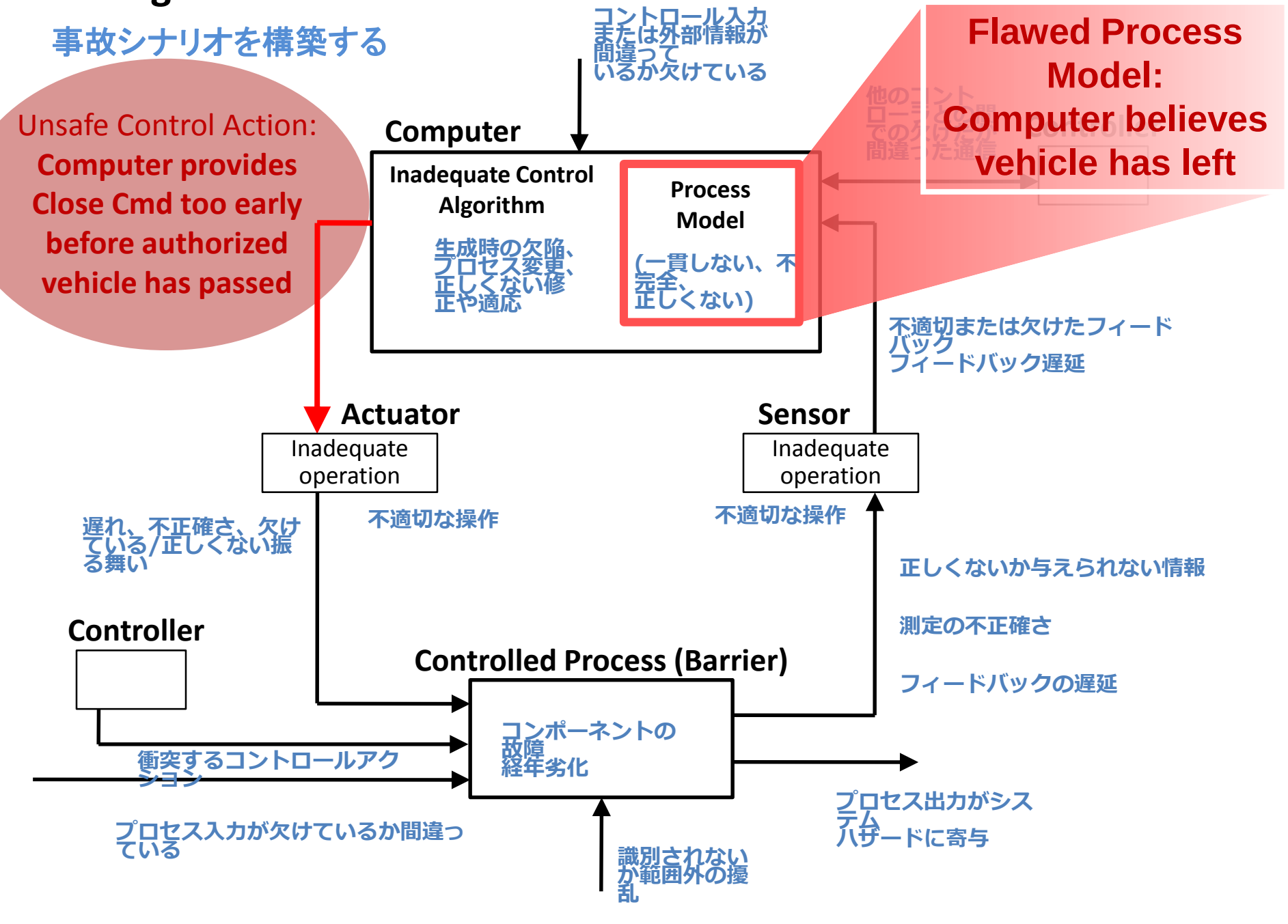
Building Accident Scenarios

事故シナリオを構築する



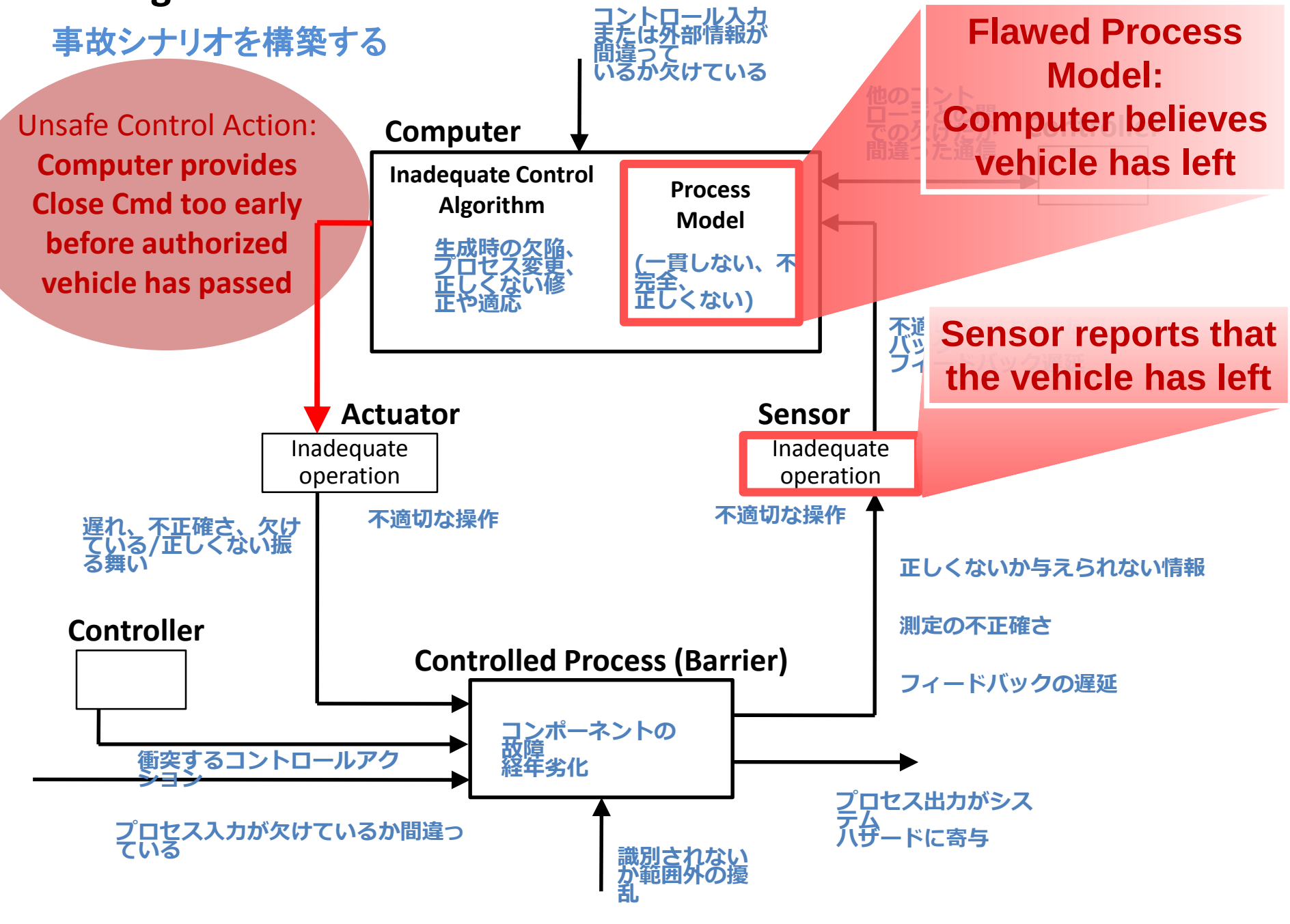
Building Accident Scenarios

事故シナリオを構築する



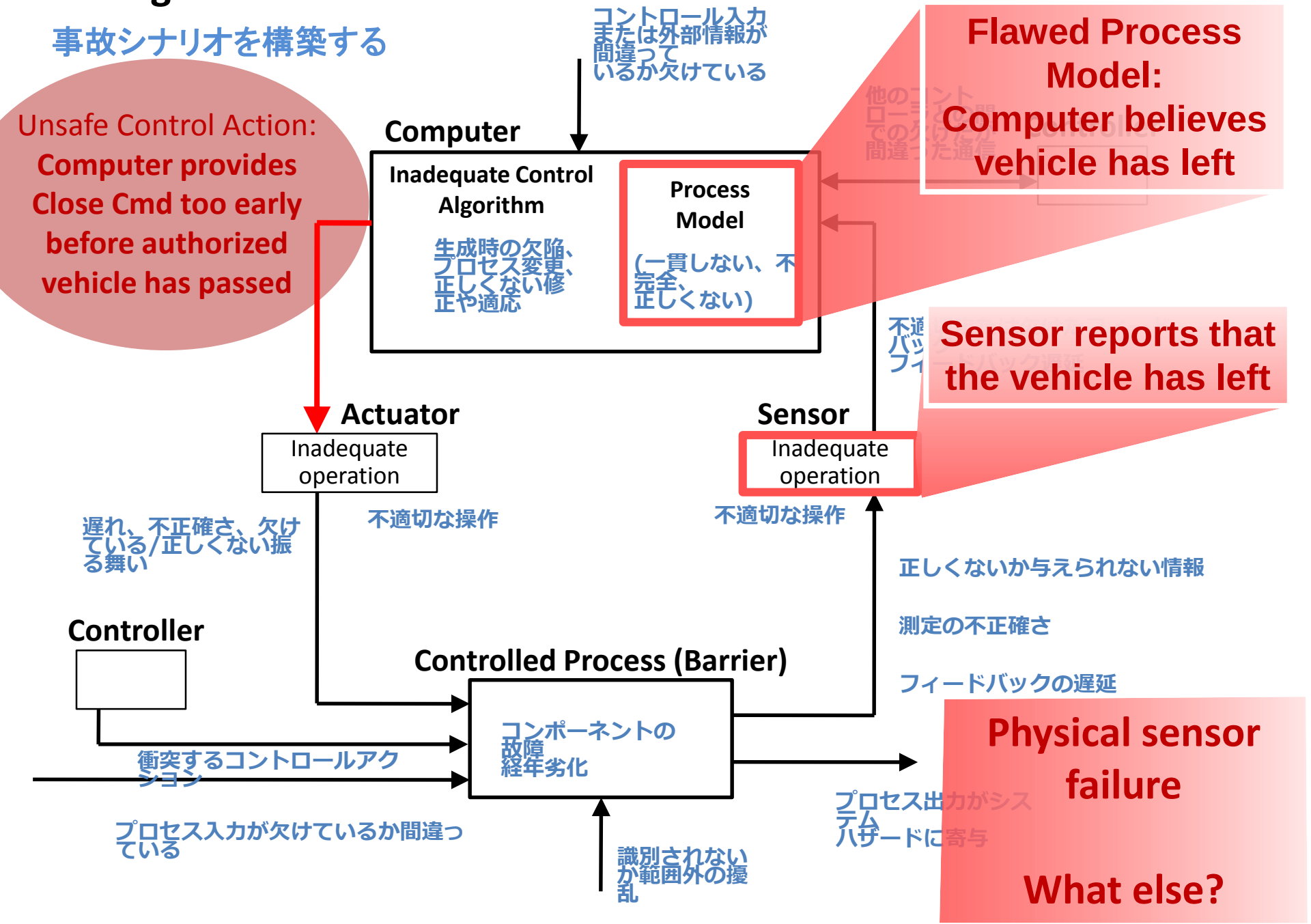
Building Accident Scenarios

事故シナリオを構築する



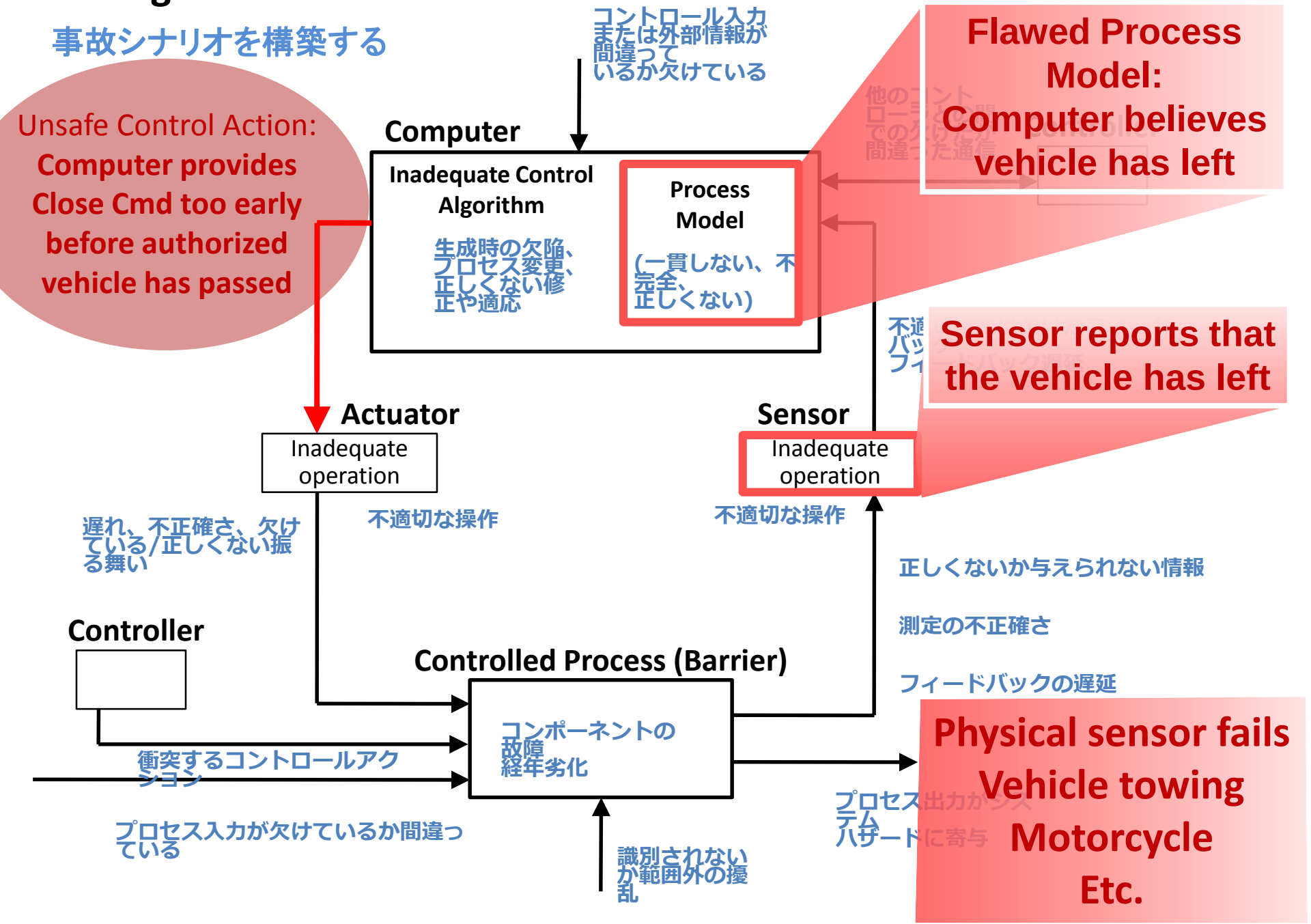
Building Accident Scenarios

事故シナリオを構築する



Building Accident Scenarios

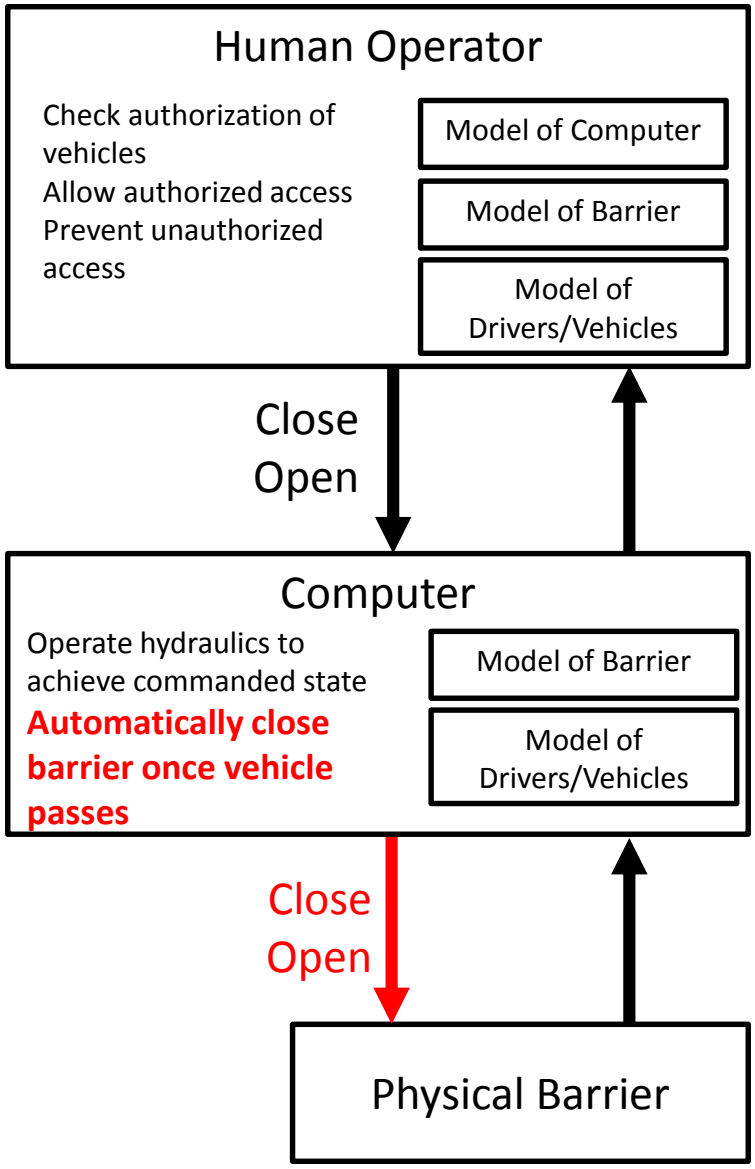
事故シナリオを構築する



Access Control Barrier

Example Scenarios:

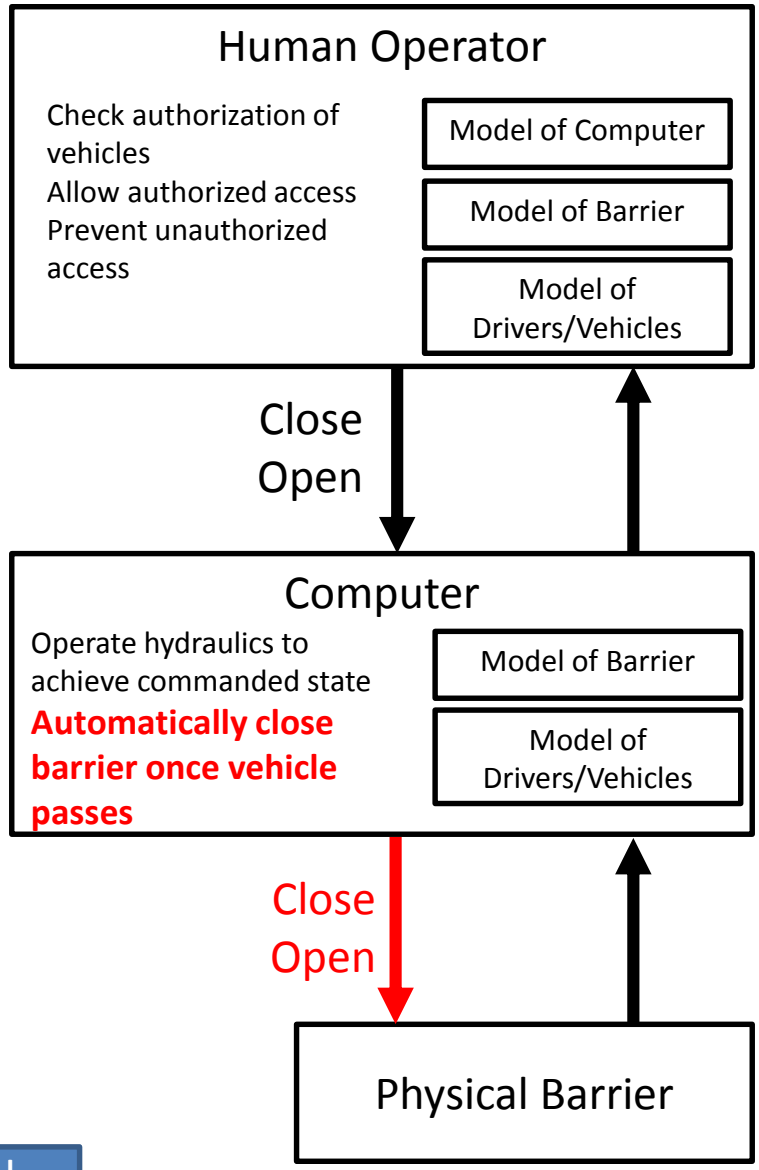
- Computer provides Close Cmd too early before authorized vehicle has passed because the computer incorrectly believes the authorized vehicle has left. This incorrect belief will occur if the loop sensor provides a false indication. A false indication may occur if the sensor fails or if the vehicle is towing another vehicle.



Access Control Barrier

Another example Scenario:

- Computer <u>does not provide Close</u> Cmd when commanded by Operator [H-2] because the computer incorrectly believes the previously authorized vehicle is still present. This incorrect belief will occur if the loop sensor provides false positive indication when there is no vehicle. False positive indication may occur due to:
  - Sensor failure
  - Delays in sensor response
  - Remote attack
  - Etc.

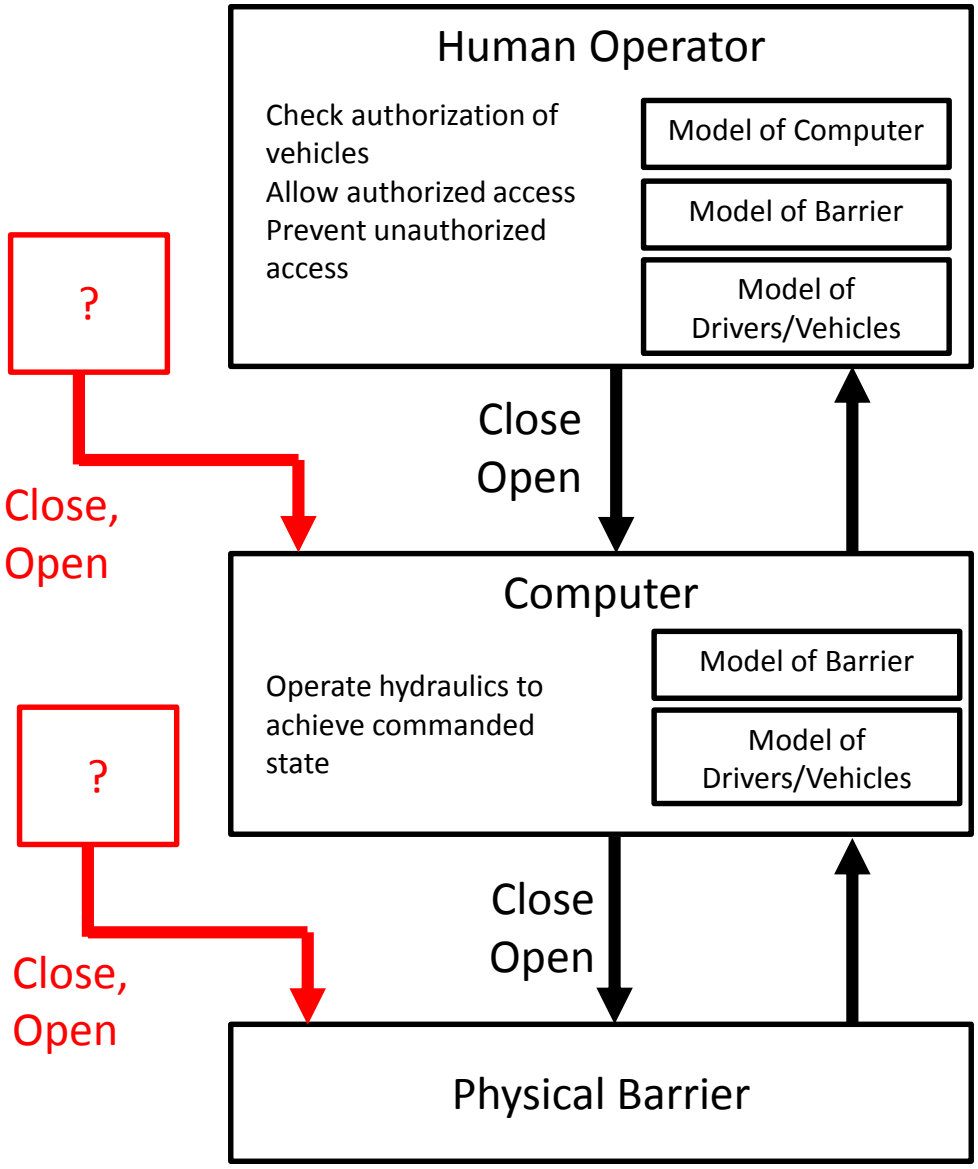


Identify Potential Solutions

Additional Security Considerations

Providing causes hazard
UCA-2: Operator provides Open Cmd when vehicle is not authorized [H-2]

UCA-3: **Adversary** provides Open Cmd when vehicle is not authorized [H-2]



Potential Design Solution:

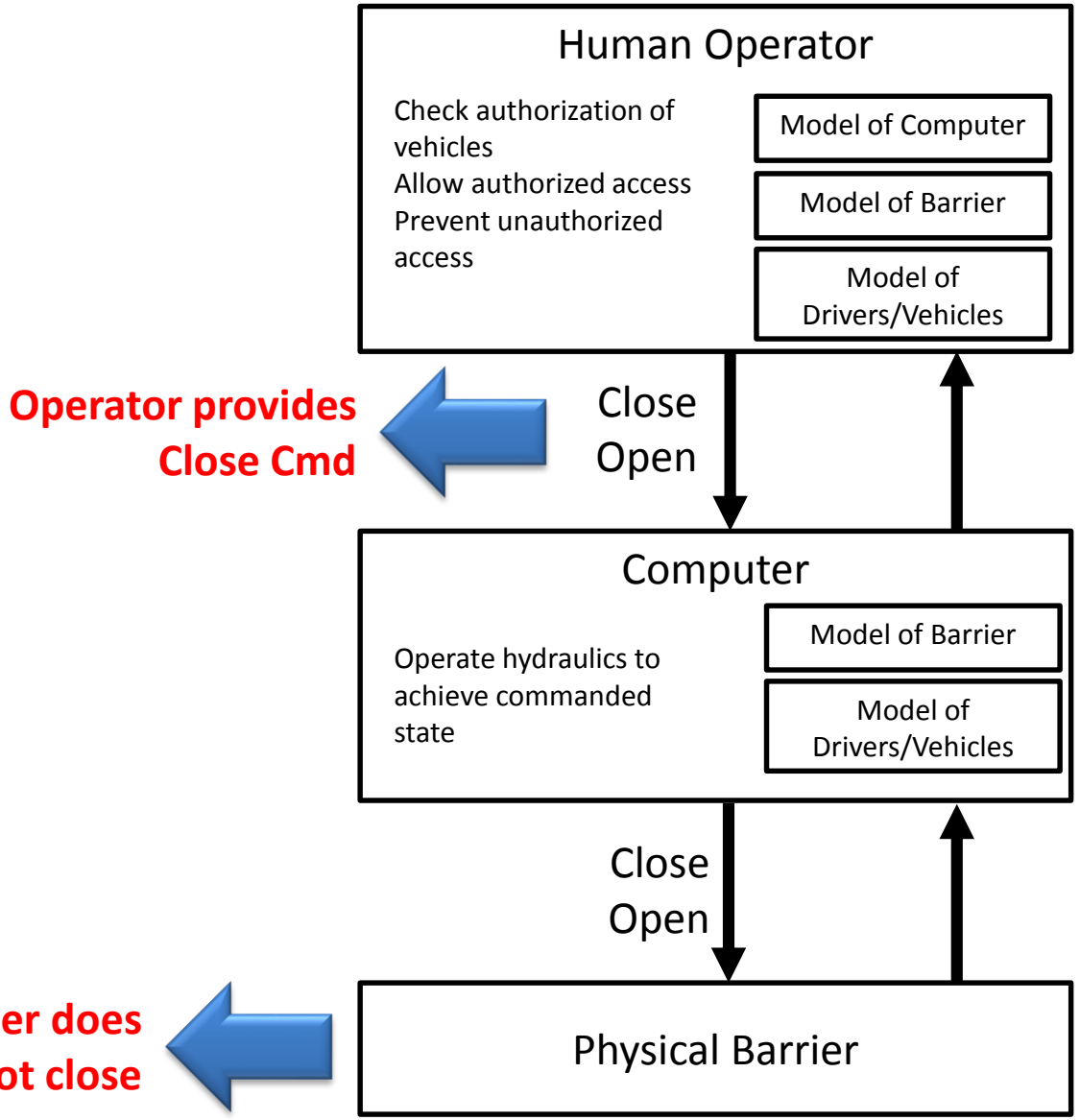
- Provide emergency lockout command

Command provided but not followed

Example Scenarios:

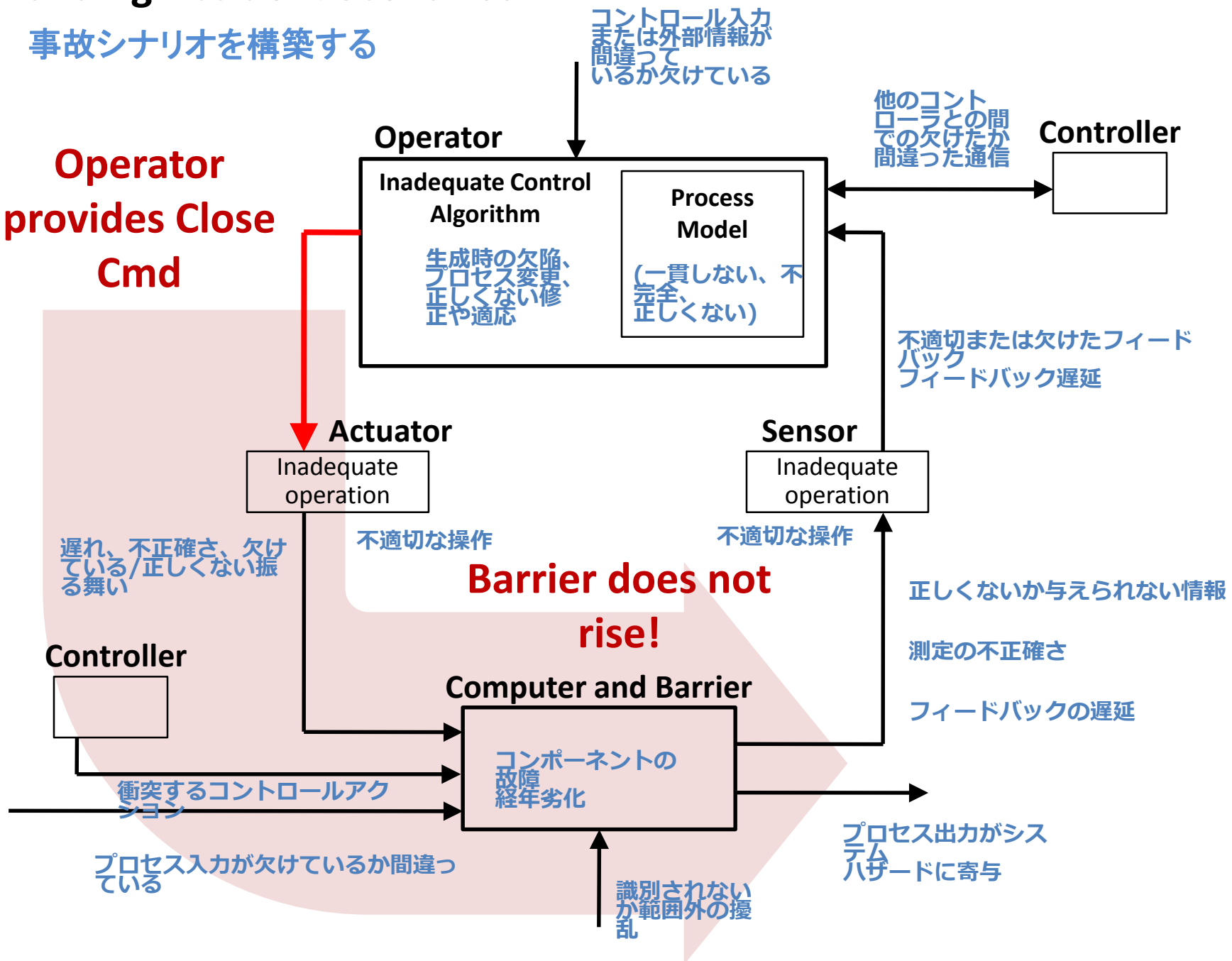
- Operator provides Close Cmd but barrier does not close because

_____



Building Accident Scenarios

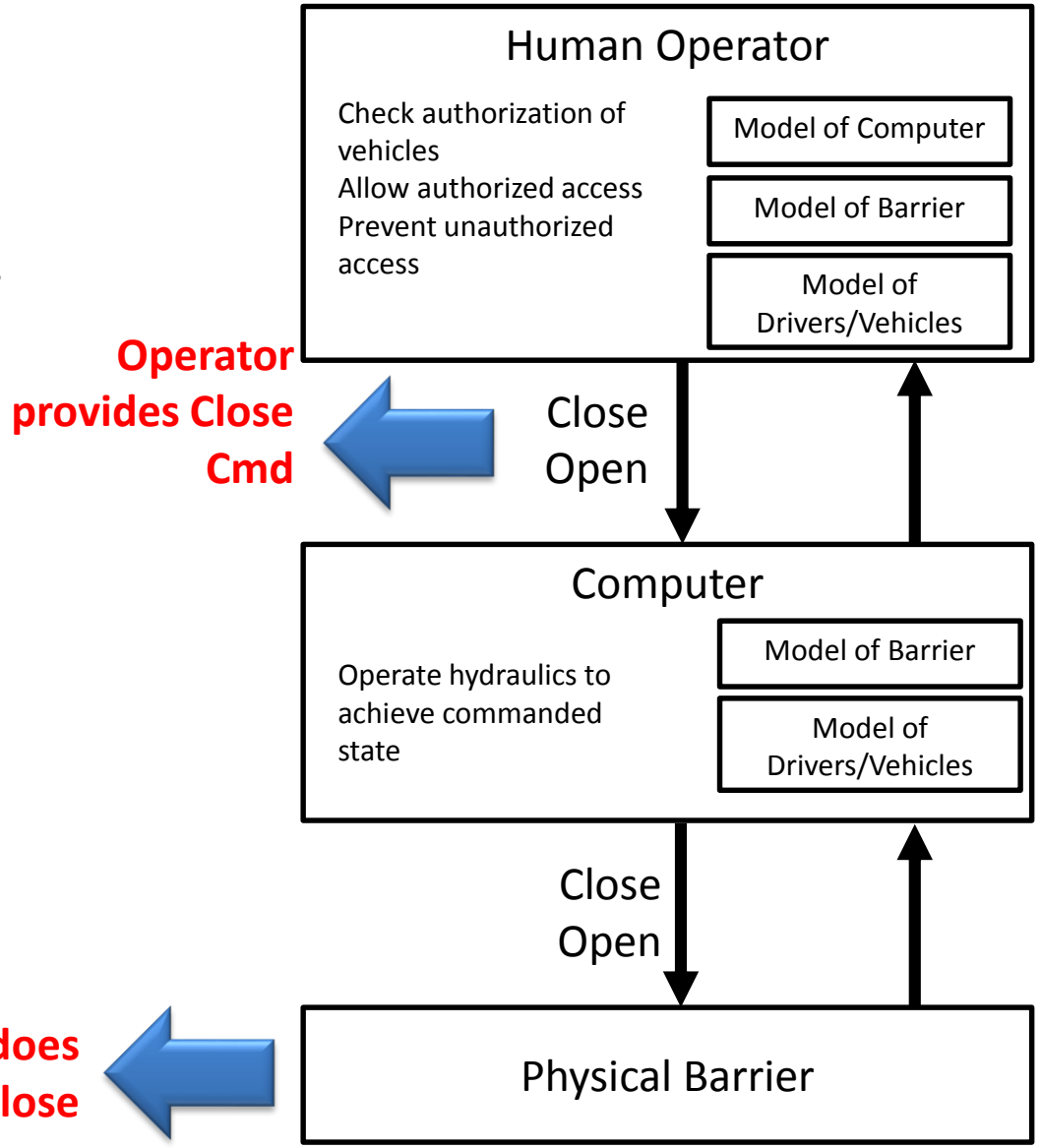
事故シナリオを構築する



Command provided but not followed

Example Scenarios:

- Operator provides Close Cmd but barrier does not close because power is lost [H-2]
- Operator provides Close Cmd but barrier does not close because hydraulic pump has failed [H-2]
- Operator provides Close Cmd but barrier does not rise fast enough to prevent unauthorized access [H-2]
- Operator provides Close Cmd but barrier does not close because temperature is too cold (e.g. ice, oil viscosity, etc.) [H-2]



Command provided but not followed

Example Scenarios:

- Operator provides Close Cmd but barrier does not close because power is lost [H-2]
- Operator provides Close Cmd but barrier does not close because hydraulic pump has failed [H-2]
- Operator provides Close Cmd but barrier does not rise fast enough to prevent unauthorized access [H-2]
- Operator provides Close Cmd but barrier does not close because temperature is too cold (e.g. ice, oil viscosity, etc.) [H-2]

Example Solutions:

- Add battery backup
- Add redundant pumps, hydraulic accumulator
- Provide Emergency Close function to close barrier quickly
- Include electric heaters

Command provided but not followed

Addressing safety or security?

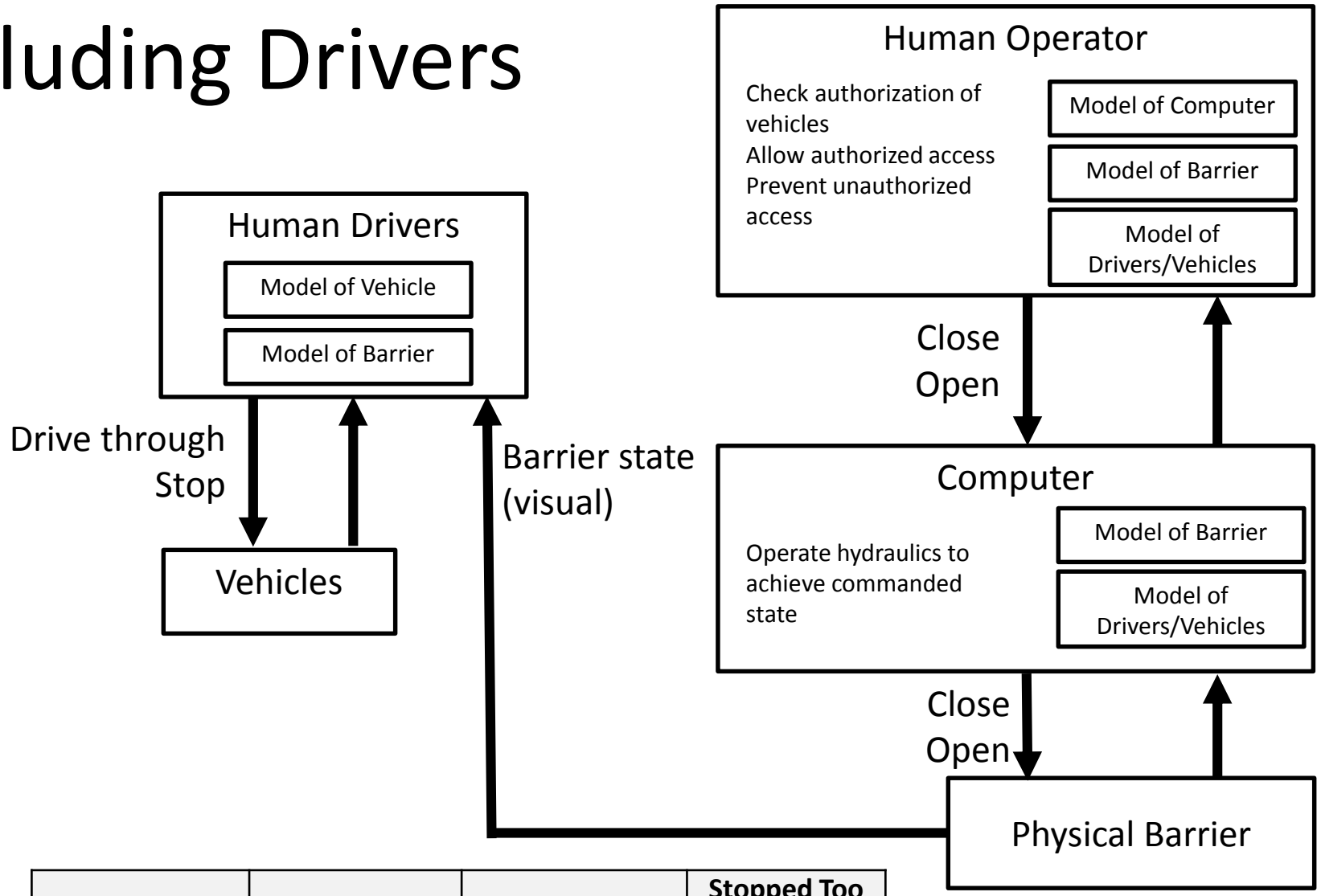
Example Scenarios:

- Operator provides Close Cmd but barrier does not close because power is lost [H-2]
- Operator provides Close Cmd but barrier does not close because hydraulic pump has failed [H-2]
- Operator provides Close Cmd but barrier does not rise fast enough to prevent unauthorized access [H-2]
- Operator provides Close Cmd but barrier does not close because temperature is too cold (e.g. ice, oil viscosity, etc.) [H-2]

Example Solutions:

- Add battery backup
- Add redundant pumps, hydraulic accumulator
- Provide Emergency Close function to close barrier quickly
- Include electric heaters

Including Drivers

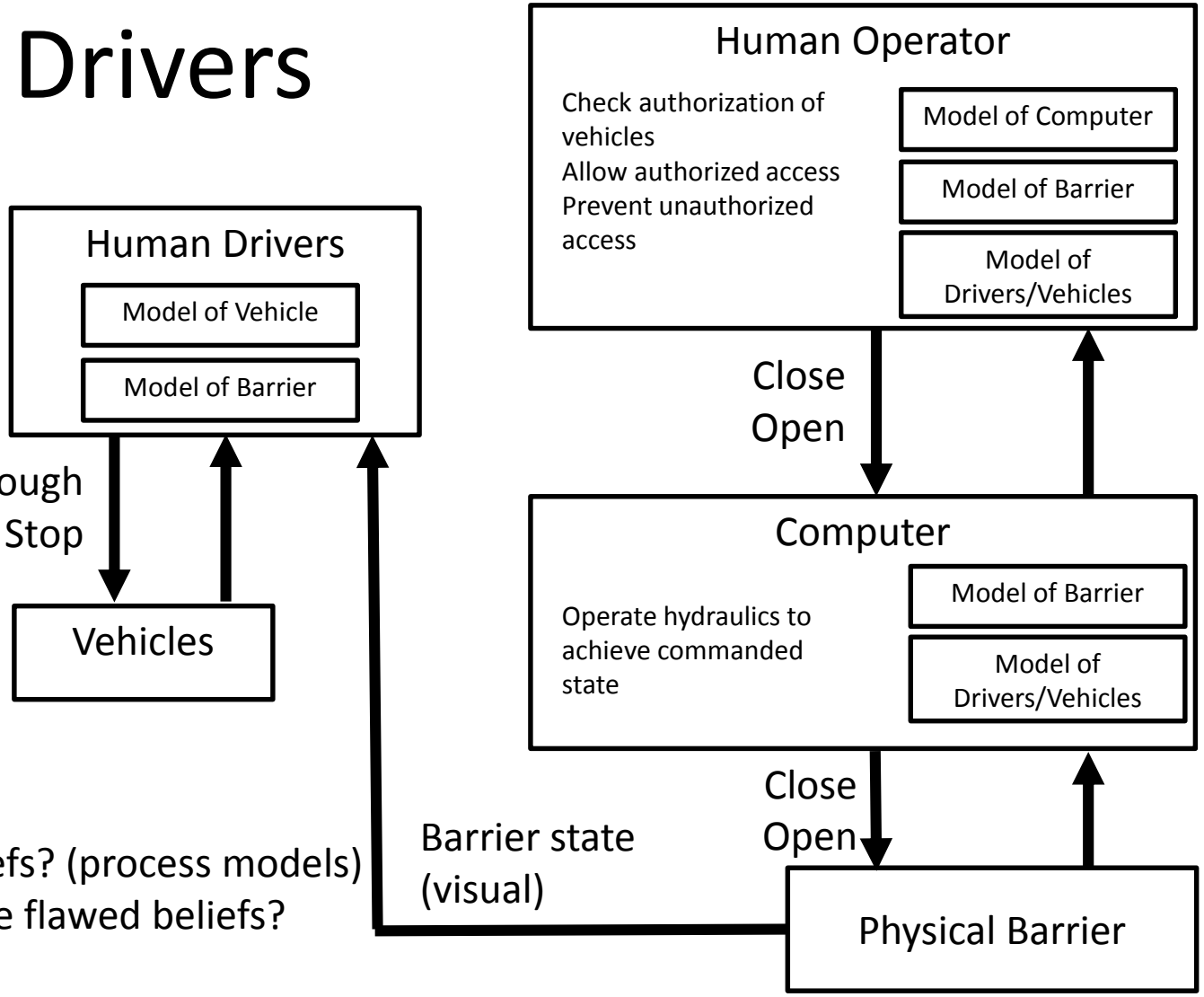


	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Drive through				
Stop				

Including Drivers

	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Drive Through	**UCA-D-1: Driver does not drive through when driver is authorized [H-3]**	**UCA-D-2: Driver drives through when barrier is Rising [H-1]** **Driver drives through when** _____		
Stop				

Including Drivers

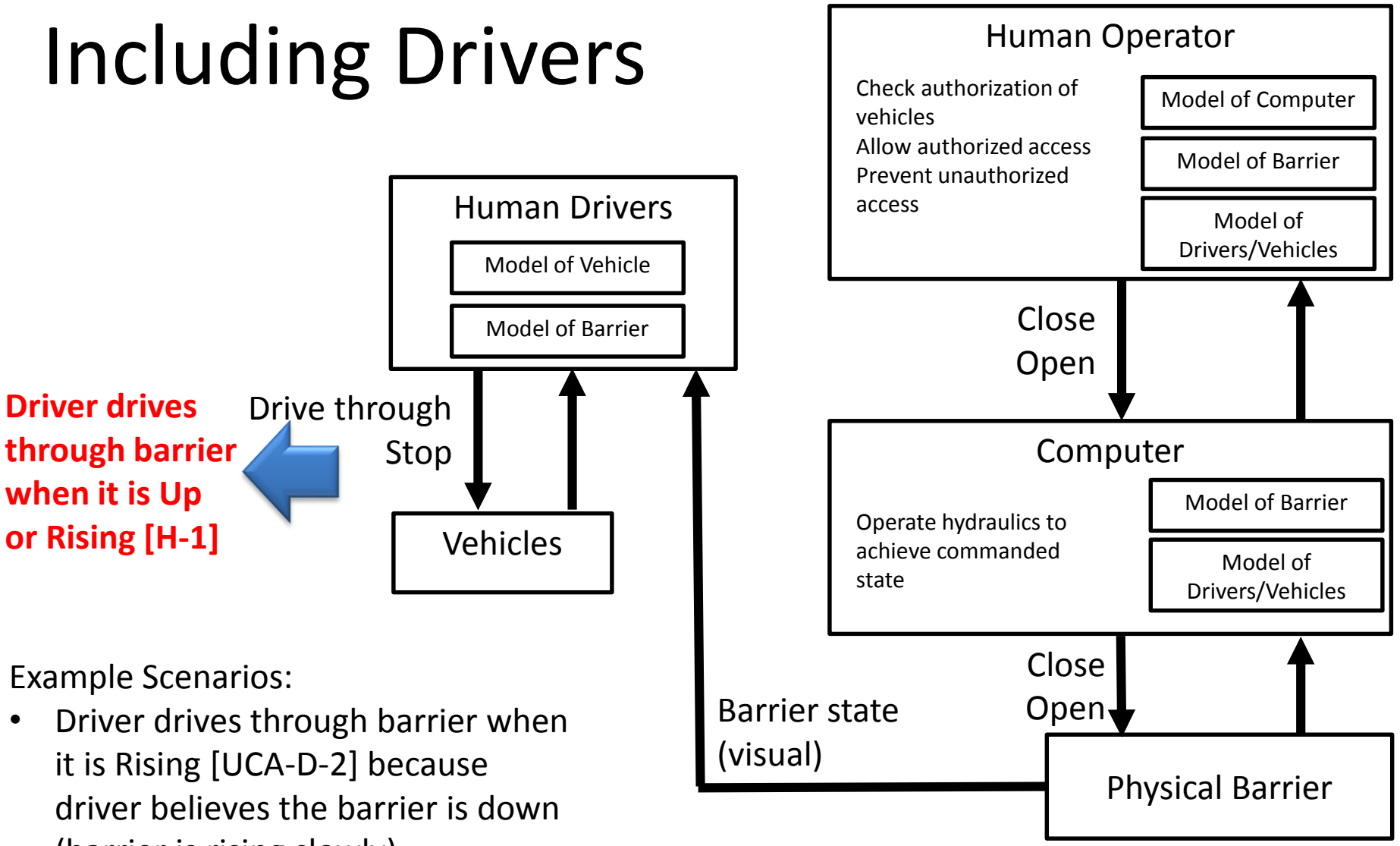


Driver drives through barrier when it is Up or Rising [H-1]

How can this happen?

- Incorrect operator beliefs? (process models)
- What might cause these flawed beliefs?
- Inadequate feedback?
- Operator procedures
- Other operators, supervisors
- Etc.

Including Drivers

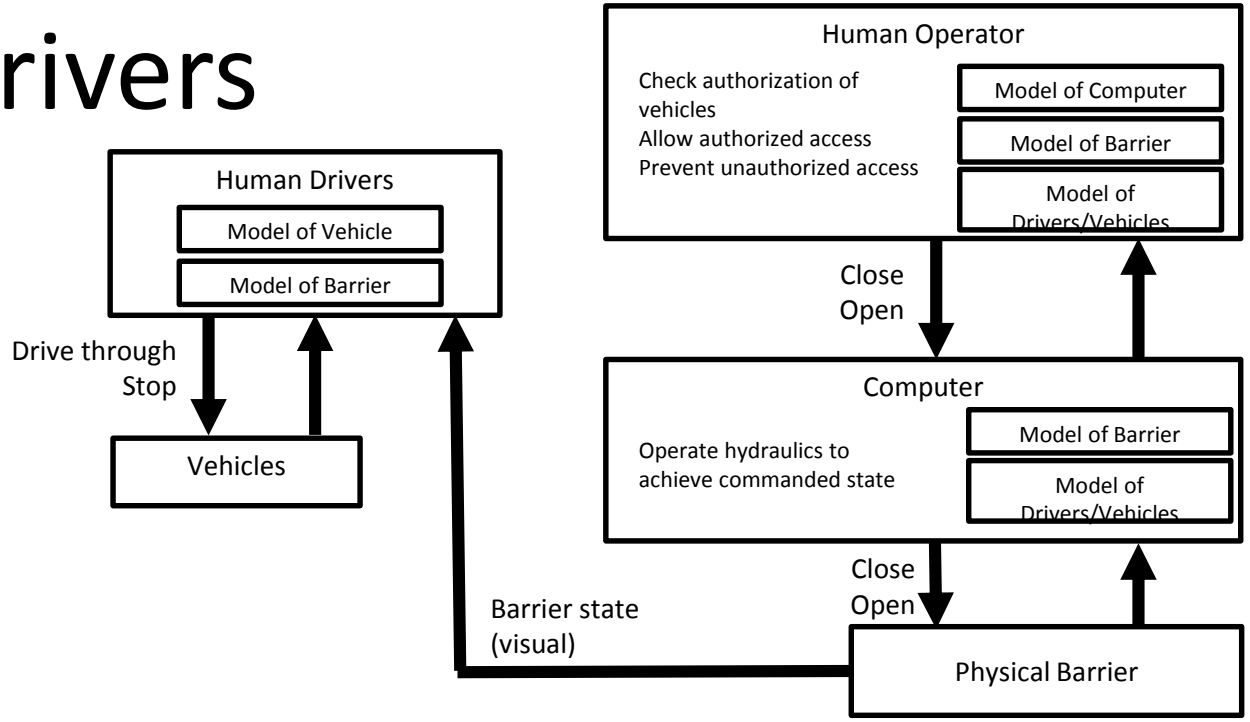


Example Scenarios:

- Driver drives through barrier when it is Rising [UCA-D-2] because driver believes the barrier is down (barrier is rising slowly)
- Driver drives through barrier when it is Up [UCA-D-3] because the driver can't see the barrier (e.g. blind spot, obscured by hood, etc.)

Identify potential solutions

Including Drivers



Example Scenarios:

- Driver drives through barrier when it is Rising [UCA-D-2] because driver believes the barrier is down (barrier is rising slowly)
- Driver drives through barrier when it is Up [UCA-D-3] because the driver can't see the barrier (e.g. blind spot, obscured by hood, etc.)

Potential Solutions:

- Provide Red/green lights to tell drivers when rising [UCA-D-2,3,4]
- Overhead gate for visual feedback [UCA-D-2,3,4]
- Put vehicle stopping location [X] feet before barrier to avoid blind spots [UCA-D-3]
- Etc.

Including Drivers

These overhead gates can't physically stop anything.
It's purely for feedback.

Example Scenarios:

- Driver drives through barrier when it is Rising [UCA-D-2] because driver believes the barrier is down (barrier is rising slowly)
- Driver drives through barrier when it is Up [UCA-D-3] because the driver can't see the barrier (e.g. blind spot, obscured by hood, etc.)

Potential Solutions:

- Provide Red/green lights to tell drivers when rising [UCA-D-2,3,4]
- Overhead gate for visual feedback [UCA-D-2,3,4]
- Put vehicle stopping location [X] feet before barrier to avoid blind spots [UCA-D-3]
- Etc.

Including Drivers

Under what conditions is the visual feedback needed?

Potential design solution

- Add overhead gate for visual feedback

UCA-D-2: Driver drives through when barrier is Rising [H-1]

UCA-D-3: Driver drives through when barrier is Up [H-1]

UCA-D-4: Driver drives through when barrier is Opening [H-1]

Requirements

- R-1: Overhead gate must be deployed when _____

Including Drivers

Aha! The sequence between gate/barrier matters!

Potential design solution

- Add overhead gate for visual feedback

UCA-D-2: Driver drives through when barrier is Rising [H-1]

UCA-D-3: Driver drives through when barrier is Up [H-1]

UCA-D-4: Driver drives through when barrier is Opening [H-1]

Requirements

- R-1: Overhead gate must be deployed when barrier is rising [UCA-D-2]
- R-2: Overhead gate must be deployed when barrier is Up [UCA-D-3]
- R-3: Overhead gate must be deployed when barrier is Opening [UCA-D-4]

System-Theoretic Process Analysis (STPA)

- Identify system accidents, hazards } What are the safety goals?
- Draw functional control structure
- Identify unsafe control actions } What can go wrong?
- Identify accident scenarios } How can that happen?

(Leveson, 2012)

Watch Videos

- Compare your design recommendations with actual barriers in operation
  - Did you identify features they implemented?
  - Did you identify additional features not implemented?
  - Do they have features you missed?
- Did you anticipate these accidents?

Wrap-up

MIT March Workshop (free)

Industries:
Automotive
Oil and Gas
Space
Aviation
Defense
Nuclear
Healthcare and Healthcare IT
Medical Devices
Academia
Insurance
Academia (Education)
Hydropower
Chemicals
Software/Computing
Government
Industrial Automation
Electric Utility
Security
Think Tank
Transportation
Maritime (security)
Environmental
Pharmaceuticals
Internet

Organizations:
General Motors
Ford
Nissan Motor Company
Toyota
Draper Lab
Volpe National Transportation Research Center
The Boeing Company
Boeing Environment Health and Safety
Boeing Engineering and Operations
Embraer
U.S. Nuclear Regulatory Commission
U.S. Army
GE Aviation
Sikorsky
Thoratec Corporation
University of Alabama in Huntsville
Liberty Mutual Safety Research Institute
ITA (Instituto Tecnologico de Aeronautica)
Jeppesen
Beijing Institute of Technology
TEGMA Gestao Logistica S.A.
Amsterdam University of Applied Sciences
Dutch Safety Agency
University of Stuttgart
BC Hydro
Therapeutic Goods Administration
Institute of Aeronautics and Space (IAE), Brazil
Shell Oil
University of Braunschweig
Stiki
Reykjavik University
National Nuclear Energy Commission, Brazil
FAA
U.S. Department of Transportation
U.S. Air Force
U.S. Navy
IPEV (Institute for Research and Flight Testing), Brazil
Japan Aerospace Exploration Agency (JAXA)
U.S. Department of Energy
Rockwell Automation
Democritus University of Thrace
Dependable Management
ILF Consulting Engineers
JETRO (Japan)
Alliance for Clinical Research Excellence and Safety
Washington CORE
Florida Institute of Technology
U.S. Navy Strategic Systems Programs
IPEN (Institute for Nuclear and Energy Research), Brazil
Duke Energy
Synensis
Japan MOT Society
Tufts University
Southern Company
U.S. Army Aviation Engineering
U.S. Army Corps of Engineers (Kansas City District)
University of Houston, Clear Lake
Lincoln Lab
Hanscom AFB
U.S. Army Research, Development, and Engineering Command
McMaster University
Bechtel
Kyushu University (Japan)
Analog Devices
Cummins
University of Massachusetts Dartmouth
Syracuse Safety Research
National Civil Aviation Agency (ANAC0, Brazil
State Nuclear Power Automation System Engineering Company (China)
Toyota Central R&D Labs
Massachusetts General Hospital
AstraZeneca
STM (Defense Technology Engineering and Trading Corp., Turkey)
Varian Medical Systems
Fort Hill Group
TUBITAK-UZAY (Scientific and Technological Research Council of TURKEY-Space Technologies Research Institute)
Cranfield University (U.K.)
U.S. Air Force Test Pilot School
NASA/Bastion Technologies
U.S. Customs and Border Protection
Second Curve Systems
Vequria
Akamai Technologies
Canadian Dept. of Defense (DND)
University of Virginia
MSAG
Novartis
U.S. Coast Guard
EPRI (Electric Power Research Institute)
Sandia National Laboratories
Lawrence Livermore National Laboratories
Tapestry Solutions
Kansas State University
Systems Planning and Analysis
Zurich University of Applied Sciences
IBM
Lawrence Berkeley National Laboratory (LBNL)
U.S. Navy School of Aviation Safety
JAMSS (Japanese Manned Space Systems)
U.S. Chemical Safety Board

mit.edu/psas

Countries: USA, Brazil, Japan, China, Netherlands, Germany, Canada, Australia, Iceland, Greece, United Kingdom, Turkey, Estonia, Australia

For more information

- Website: mit.edu/psas
  - Previous MIT STAMP workshop presentations
  - Industry-focused

- Email
  - JThomas4@mit.edu