Applying STPA to Automotive Cyber-Security (and Safety)

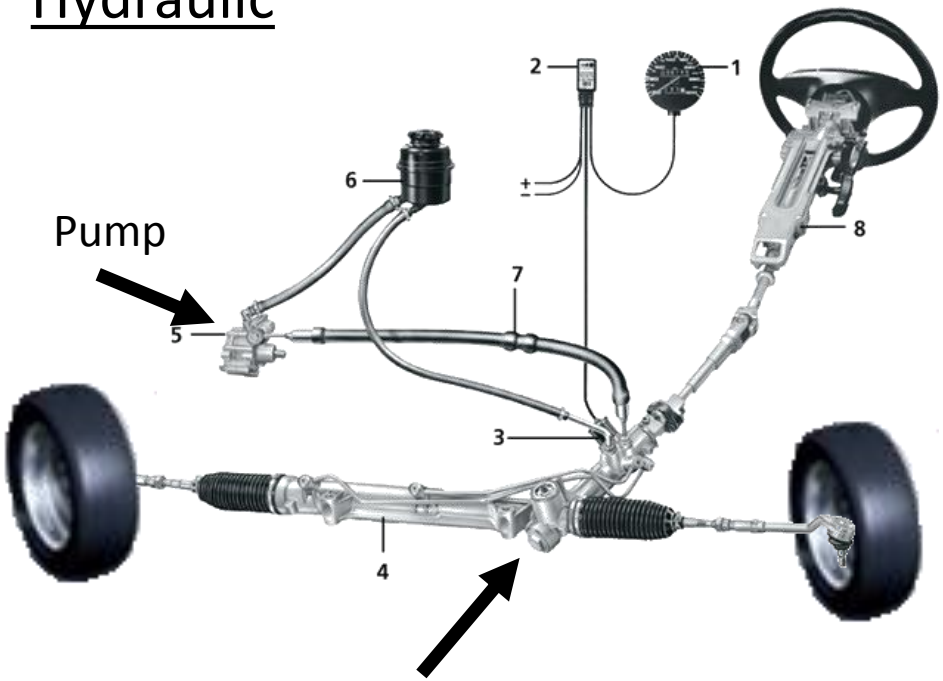
Mar 23, 2016

John Thomas, Hideki Nomoto,
Michihiro Matsumoto, Shigeyuki Kawana, Morihiro Kawamura ,
Shuichi Sato, Katsushi Sanda and Nancy Leveson

MIT, JAMSS, Toyota Motor Corp and Toyota Central R&D Labs

Power Steering

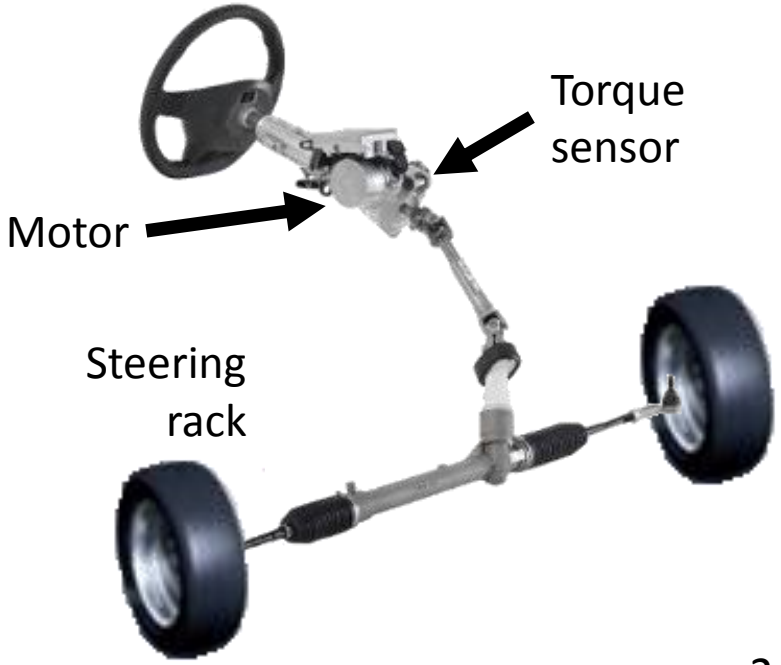
Hydraulic



Pump

Steering rack

Electric



Torque sensor

Motor

Steering rack

System Accidents

- A-1: Human injury or death
- A-2: Customers not satisfied

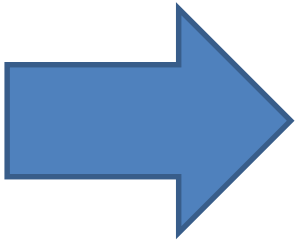
System Hazards

- H-1: Vehicle comes too close to cars, pedestrians, objects
- H-2: Vehicle behaves erratically

STPA
(System-Theoretic Process Analysis)

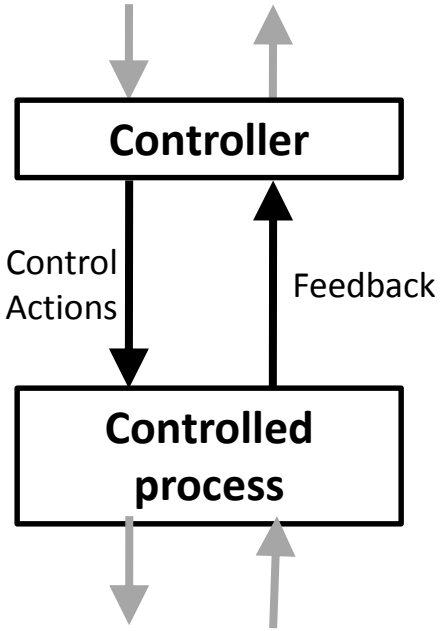


Identify accidents and hazards



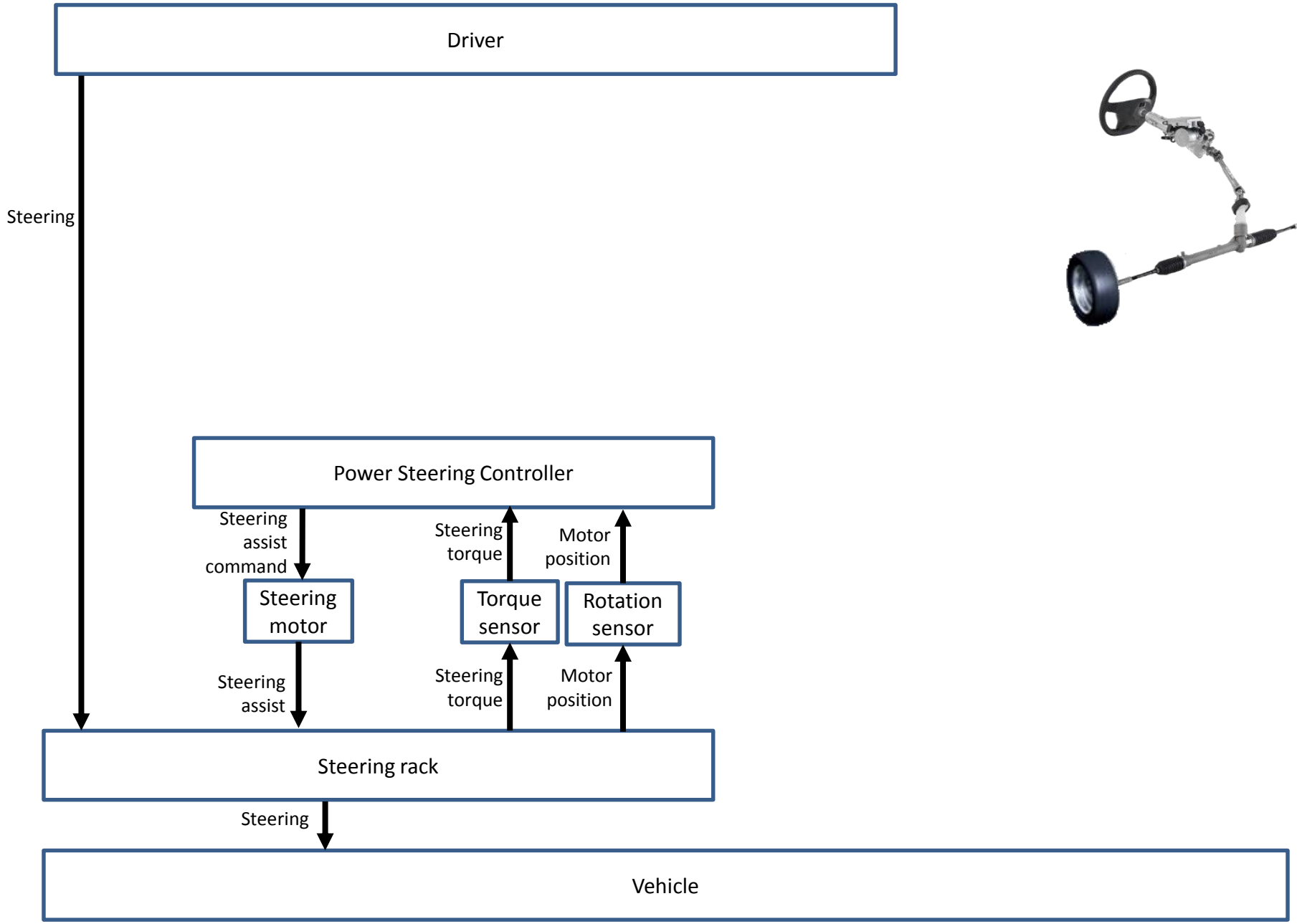
Draw the control structure

- Identify unsafe process behavior
- Identify causal scenarios



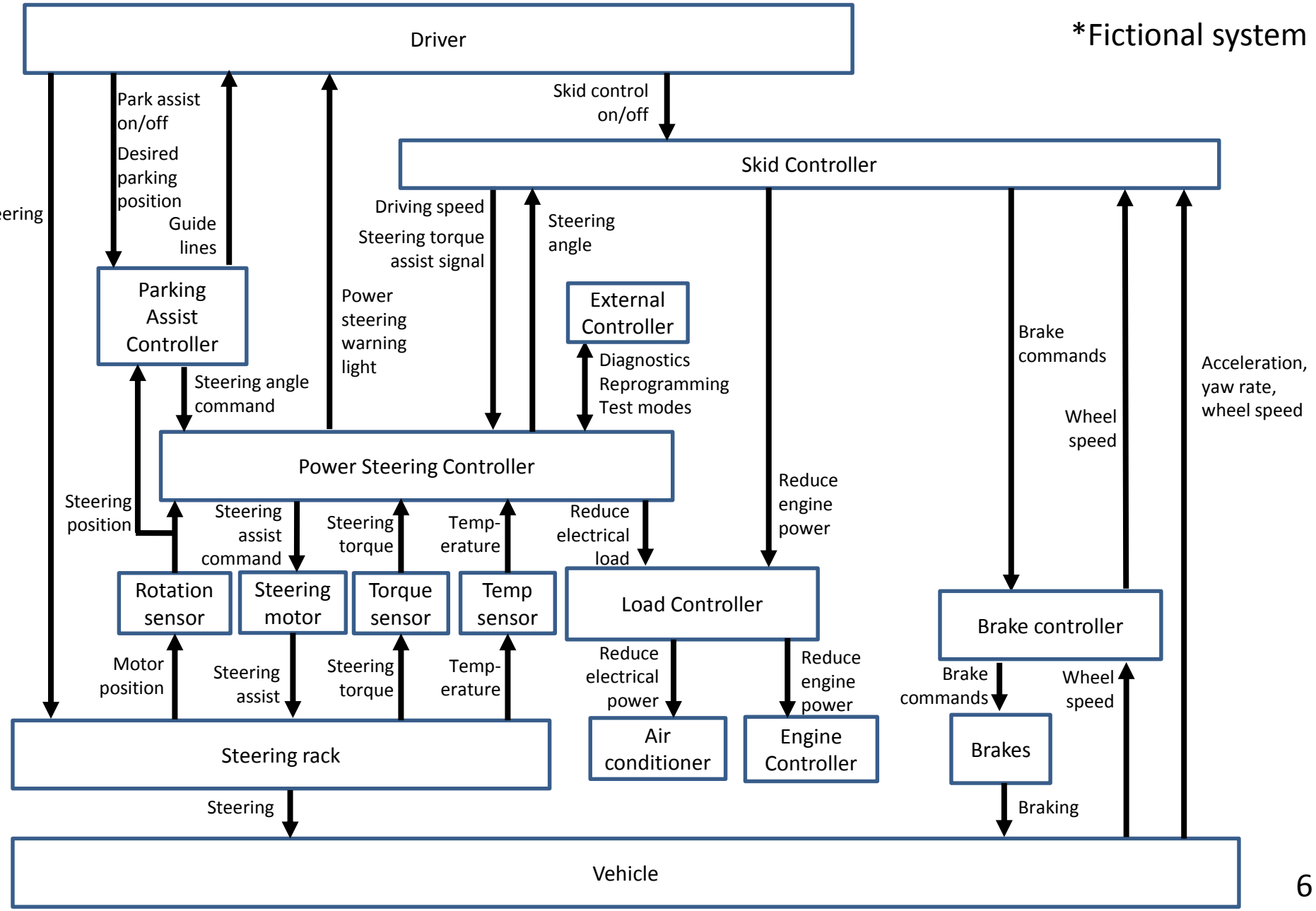
(Thomas, 2016)

Basic Control Structure



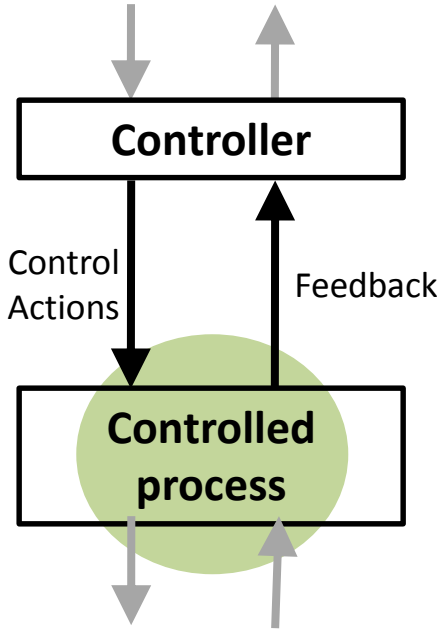
Detailed Control Structure

*Fictional system



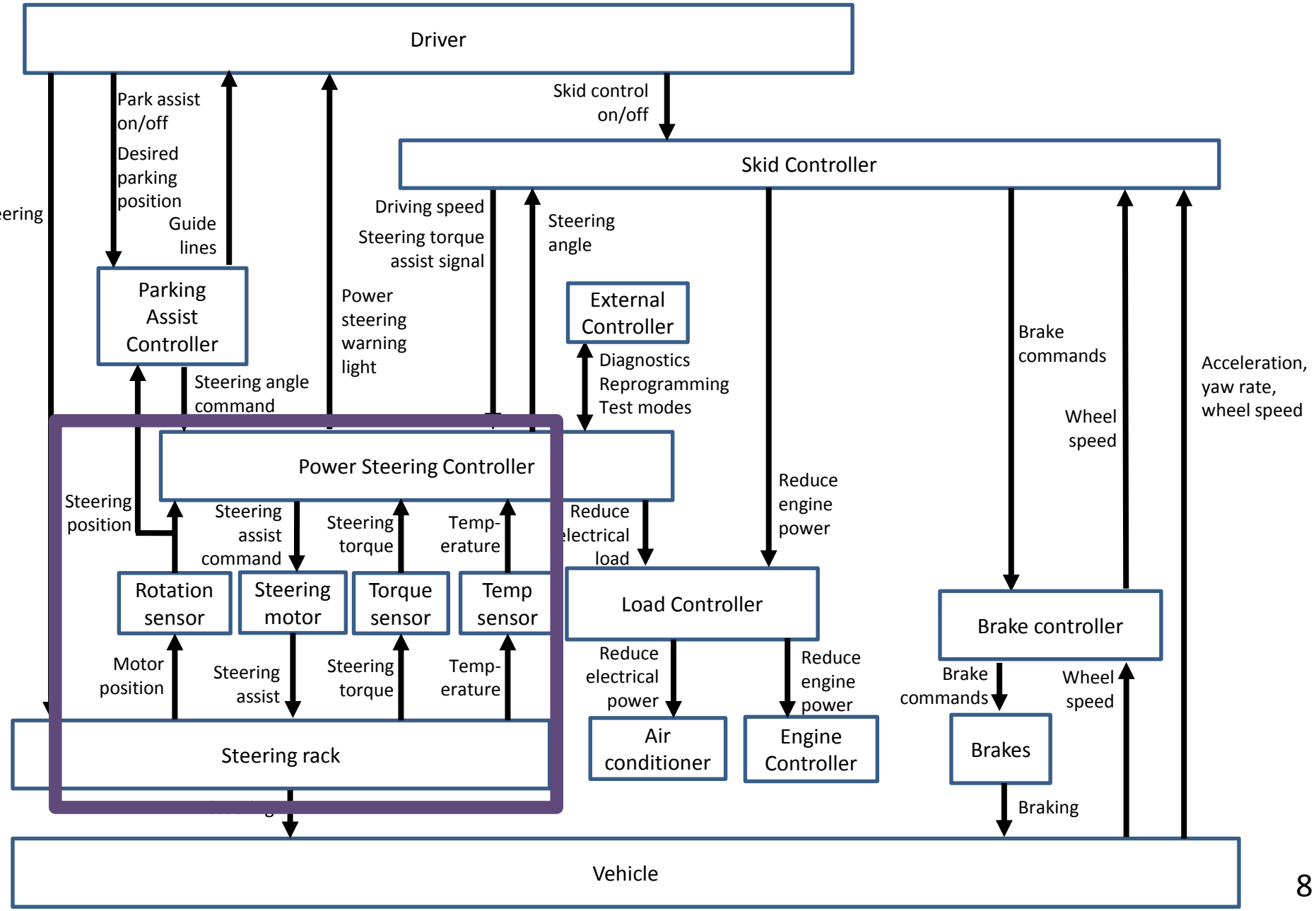
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Identify unsafe process behavior
- Identify causal scenarios

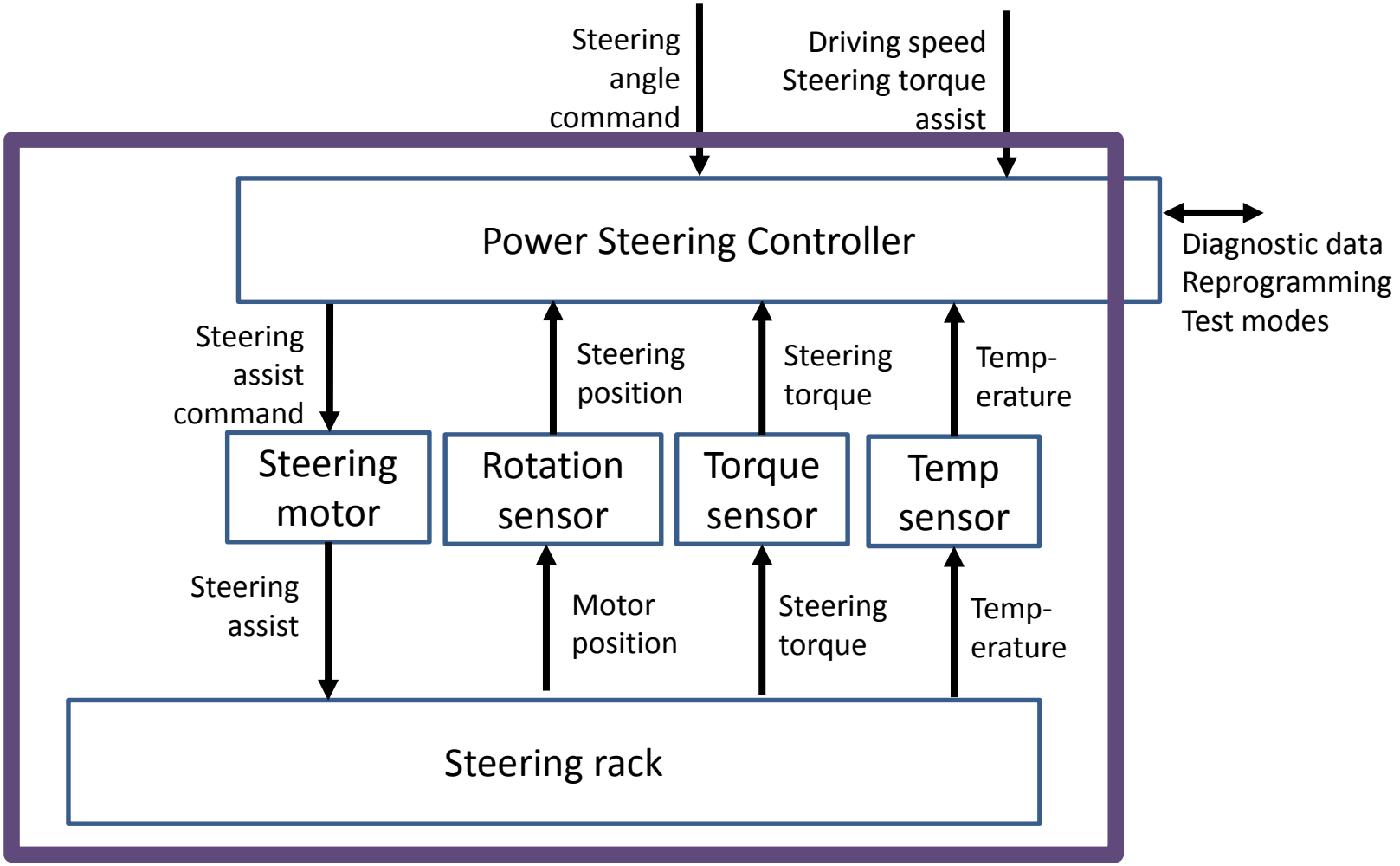


(Thomas, 2016)

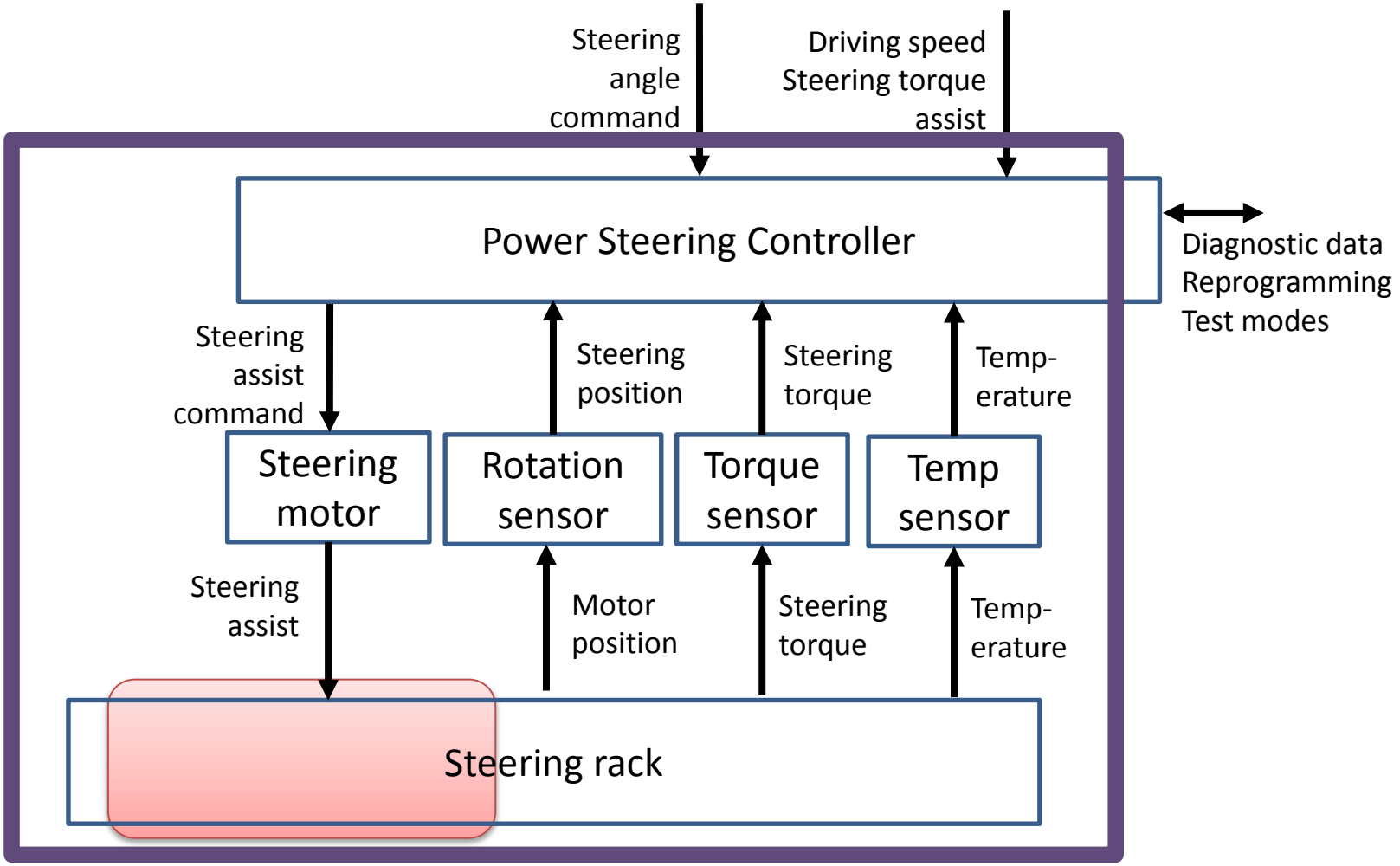
Detailed Control Structure



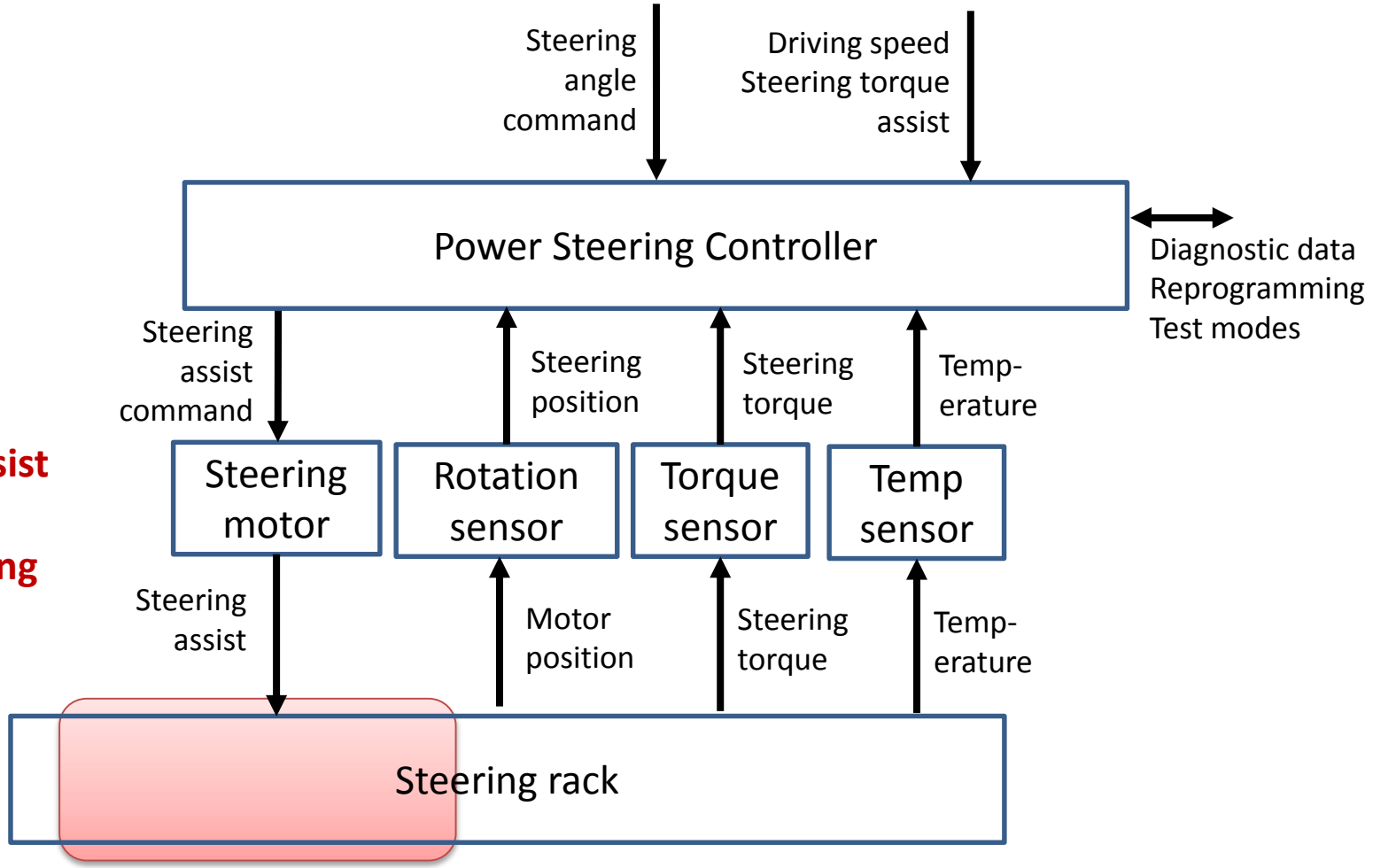
Main Control Loop



Main Control Loop



Identify Unsafe Control



UPB-1: No steering assist during low speed driving

Identify Unsafe Process Behavior

	Does not occur/not provided, causing hazard	Occurs/provided, causing hazard	Too early, too late, order	Stopped too soon, applied too long
Steering Assist	UPB-1: No steering assist during low speed driving UPB-2: No steering assist when steering torque is too high	UPB-3: Steering assist when there is no steering torque and park assist not used (excessive steering assist, steering wheel turns without driver input) UPB-4: Too little steering assist when steering torque is too high UPB-5: Steering assist in opposite direction the driver is steering in (e.g. fighting the driver) UPB-6: Too much steering assist when steering angle is at its limit	UPB-7: Steering assist too late after steering torque occurs UPB-8: Steering assist too late after commanded by park assist	UPB-9: Steering assist stops too soon while steering torque is still high UPB-10: Steering assist stops too soon before park assist command ends UPB-11: Steering assist for too long after steering torque becomes low UPB-12: Steering assist for too long after commanded by park assist

*Tables not complete

Identify Unsafe Process Behavior

	Does not occur/not provided, causing hazard	Occurs/provided, causing hazard	Too early, too late, order	Stopped too soon, applied too long
Steering Assist	UPB-1: No steering assist during low speed driving UPB-2: No steering assist when steering torque is too high	UPB-3: **Steering assist when there is no steering torque and park assist not used** (excessive steering assist, steering wheel turns without driver input) UP wh UP op st dr UPB-6: Too much steering assist when steering angle is at its limit	UPB-7: Steering assist too late after steering torque occurs UPB-8: Steering assist	UPB-9: Steering assist stops too soon while steering torque is still high UPB-10: Steering assist on before park and ends ering assist for er steering mes low ering assist for er commanded by park assist

Is this a security problem or a safety problem?

*Tables not complete

Process constraints

- Unsafe Process Behavior



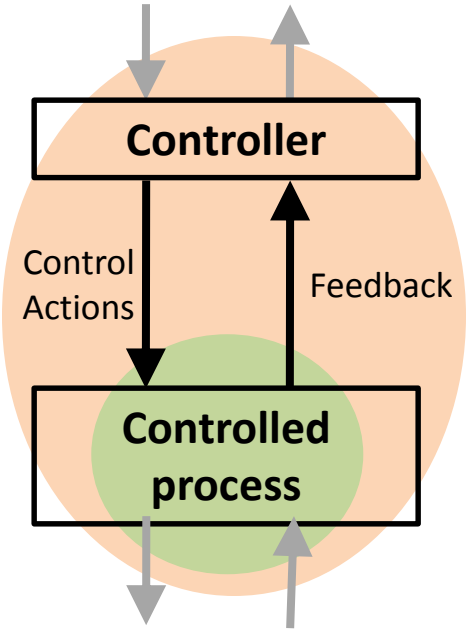
Process constraints (must be enforced by the control structure)

UPB-1: No steering assist during low speed driving

PC-1: Steering assistance must be provided during low speed driving

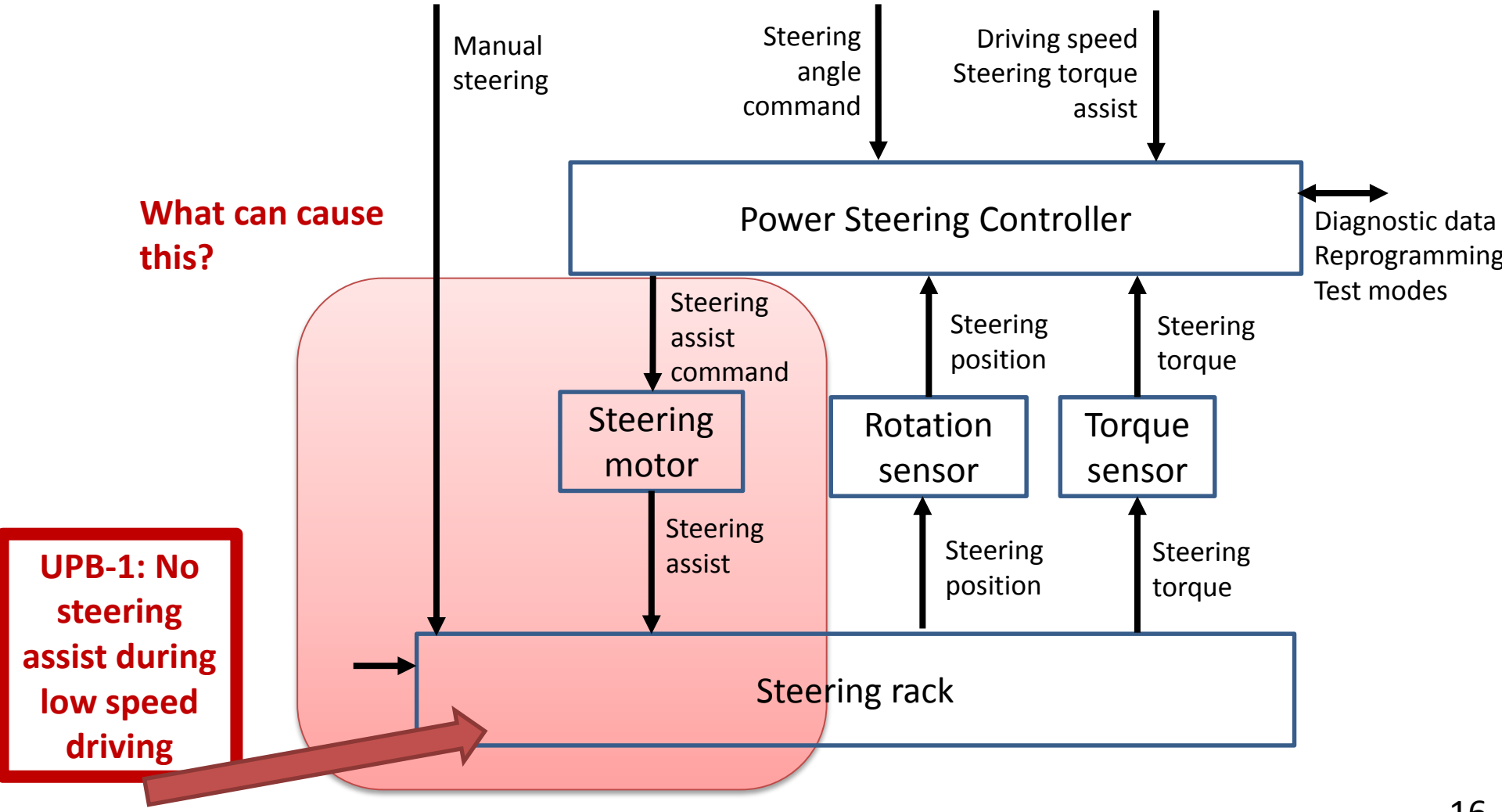
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Identify unsafe process behavior
- Identify causal scenarios

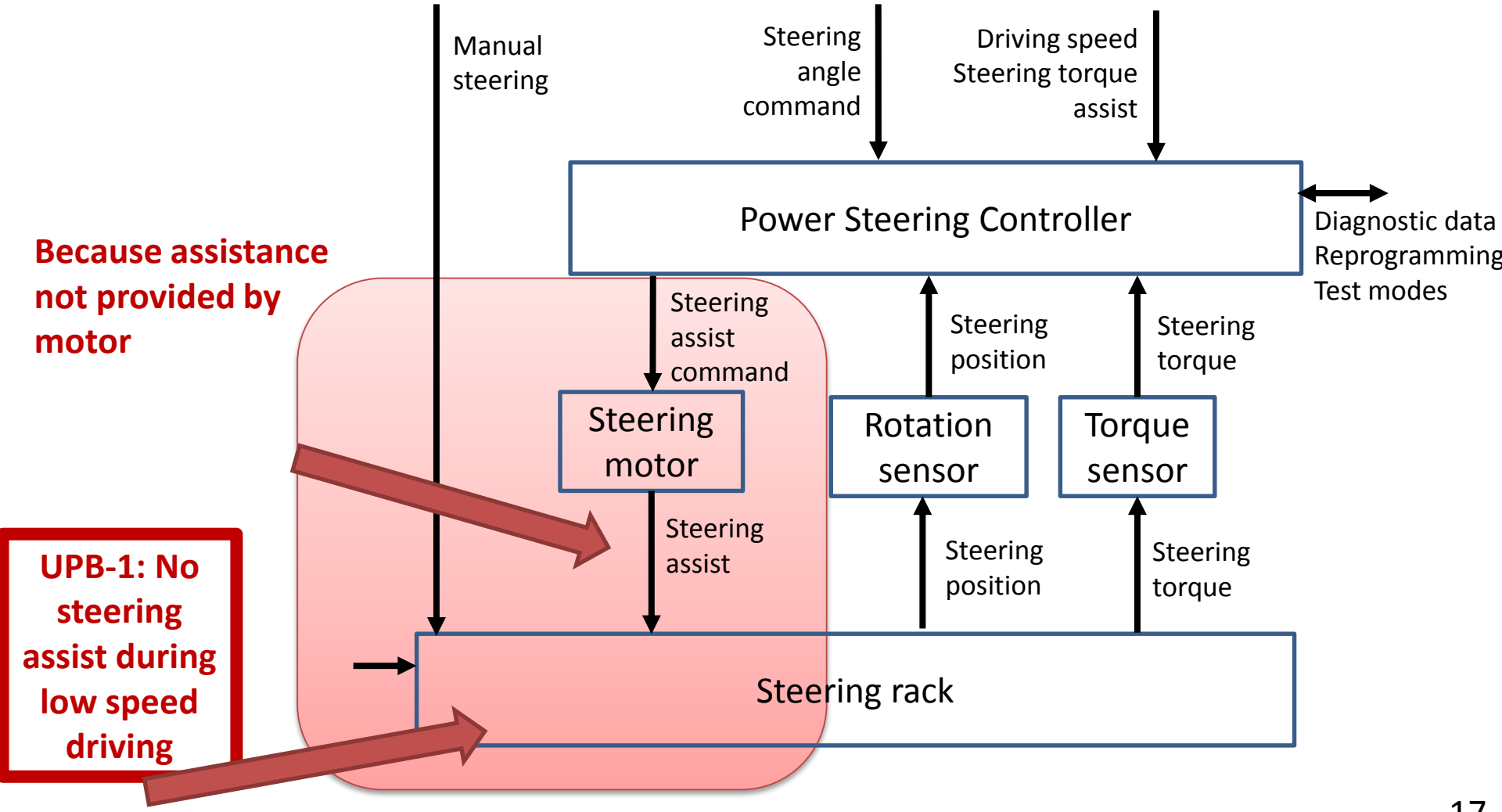


(Thomas, 2016)

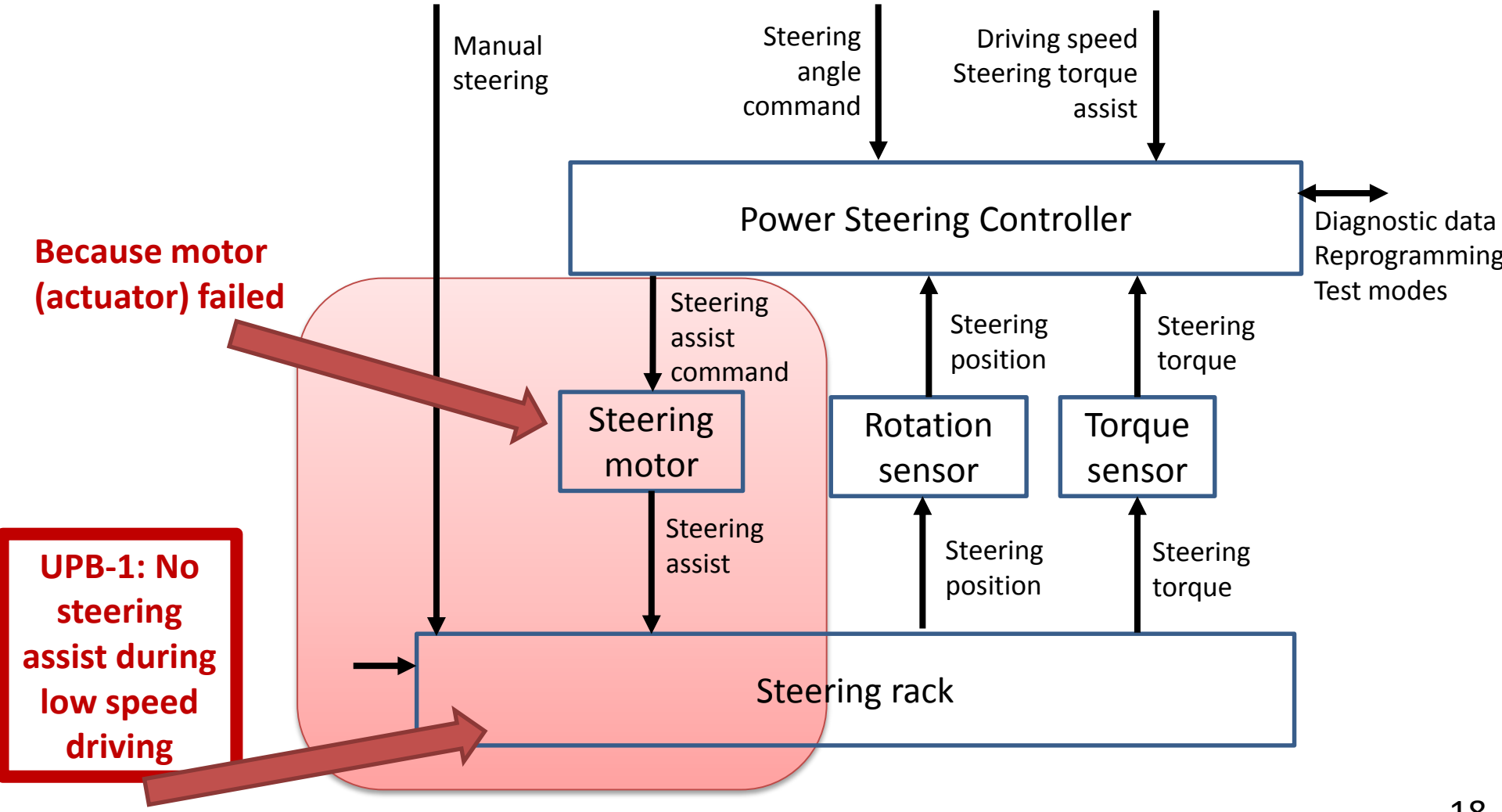
Identify Causal Scenarios



Identify Causal Scenarios

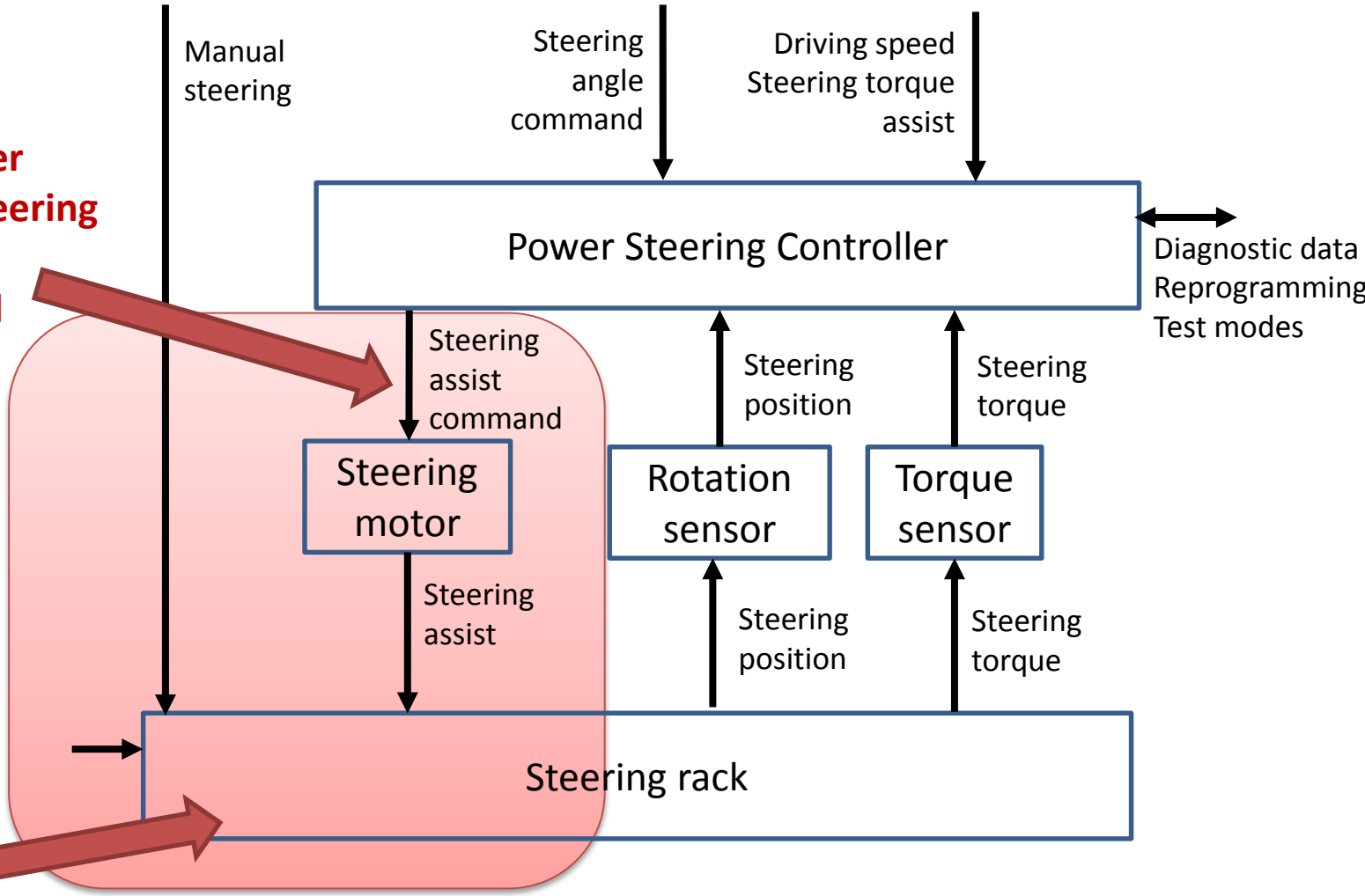


Identify Causal Scenarios



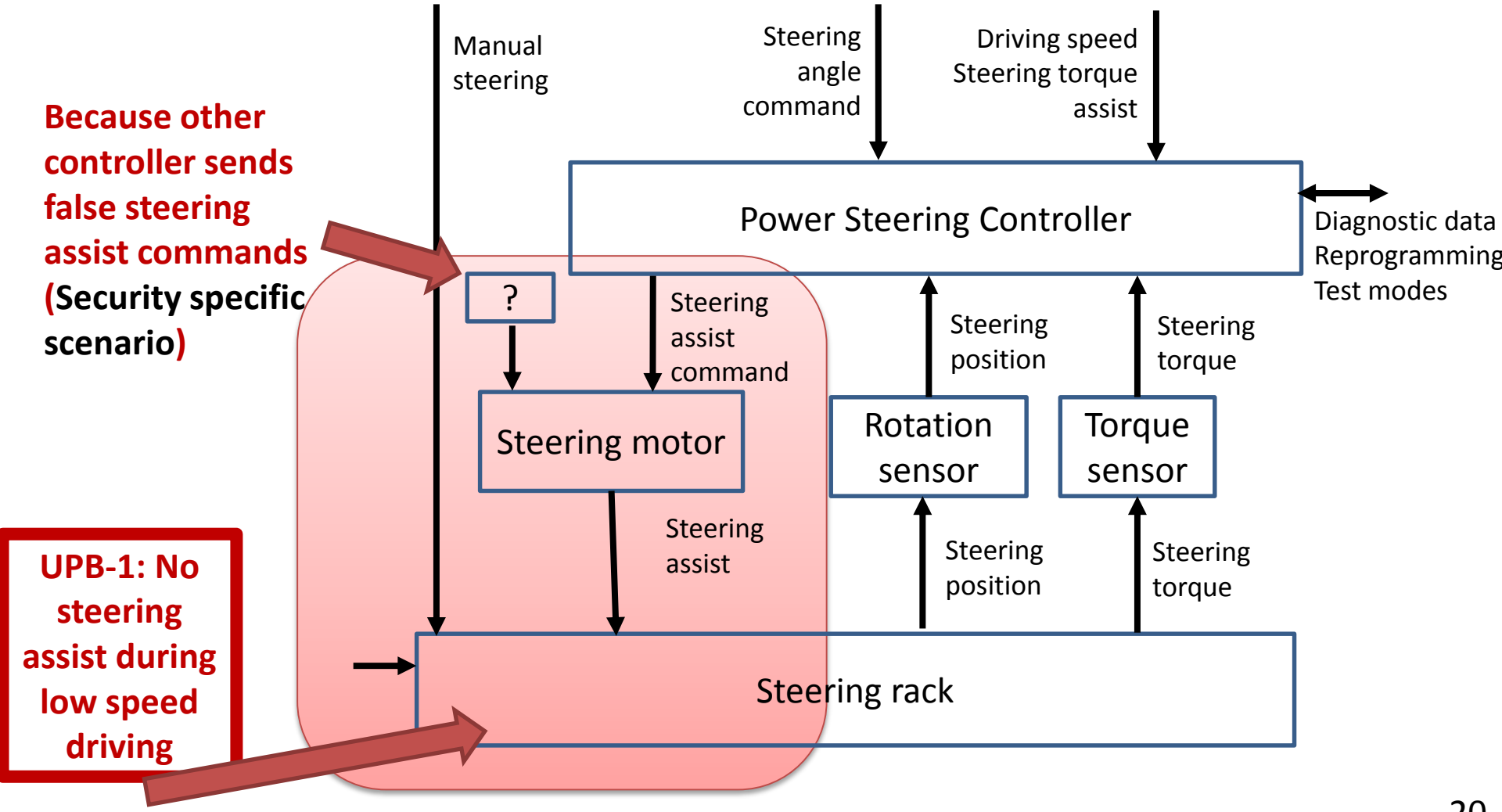
Identify Causal Scenarios

Because power steering controller does not send steering assist command during low speed driving (UCA-1)



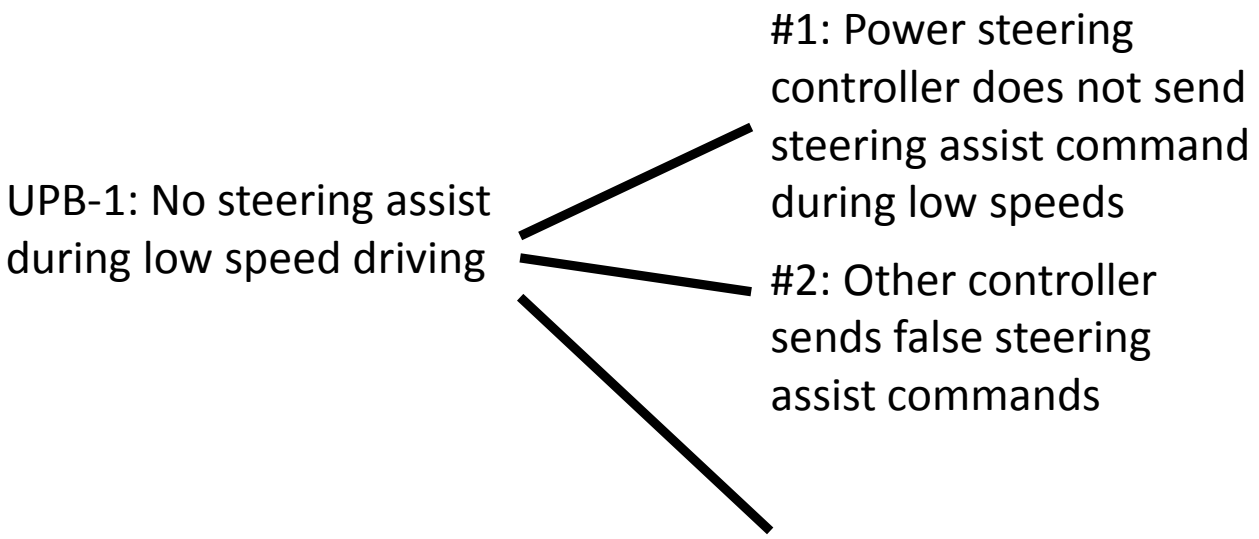
UPB-1: No steering assist during low speed driving

Identify Causal Scenarios



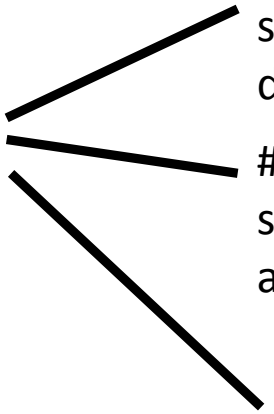
Identify causal scenarios

- Scenario: No steering assist during low speed driving (UPB-1) because power steering motor does not send steering command.
  - 1) Because power steering controller does not send steering assist command
  - 2) Because other controller sends false steering assist commands
- Etc.



Identify mitigations

UPB-1: Steering assist is not provided during low speed driving



#1: Power steering controller does not send steering assist command during low speeds

#2: Other controller sends false steering assist commands

Identify mitigations

UPB-1: Steering assist is not provided during low speed driving

#1: Power steering controller does not send steering assist command during low speeds

#2: Other controller sends false steering assist commands



Requirement #1: Steering motor must not accept commands from other controllers

Design example: Steering motor will be connected directly to power steering controller (no shared bus)

Identify mitigations

UPB-1: Steering assist is not provided during low speed driving

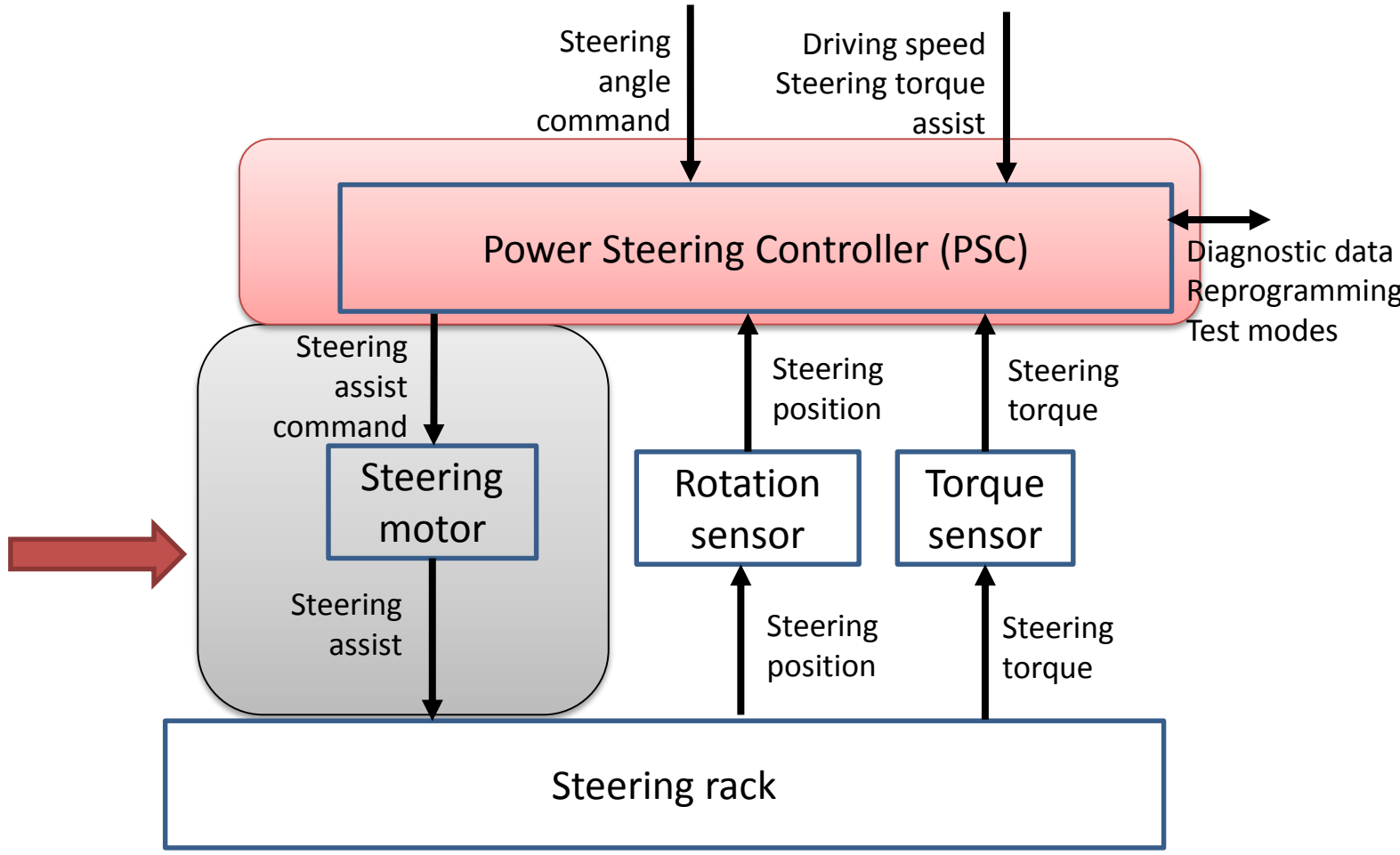
#1: Power steering controller does not send steering assist command during low speeds

How to prevent?

#2: Other controller sends false steering assist commands



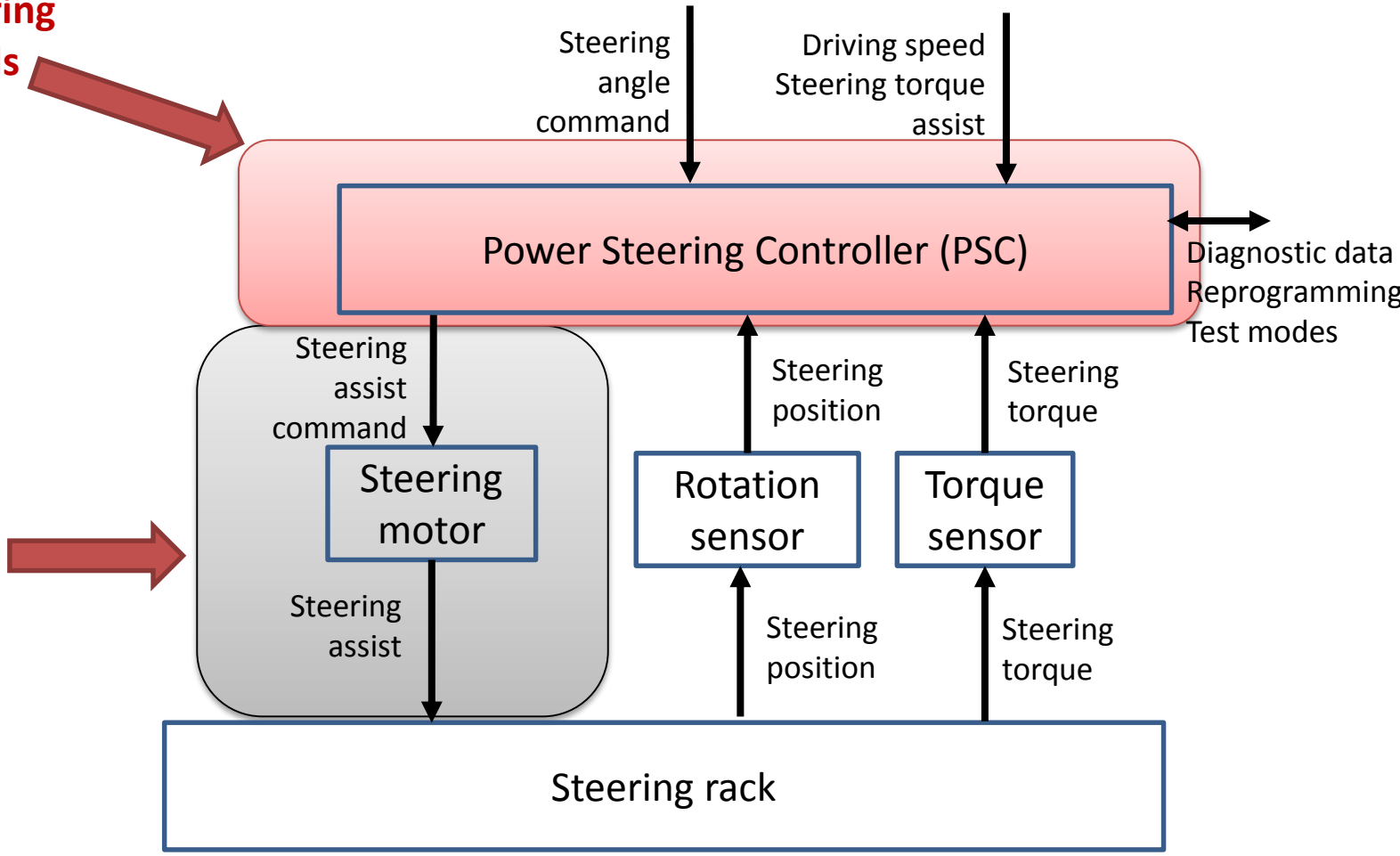
Identify causal scenarios



Scenario #1: PSC does not send steering assist command (UCA-1), no steering assist during low speed driving (UPB-1)

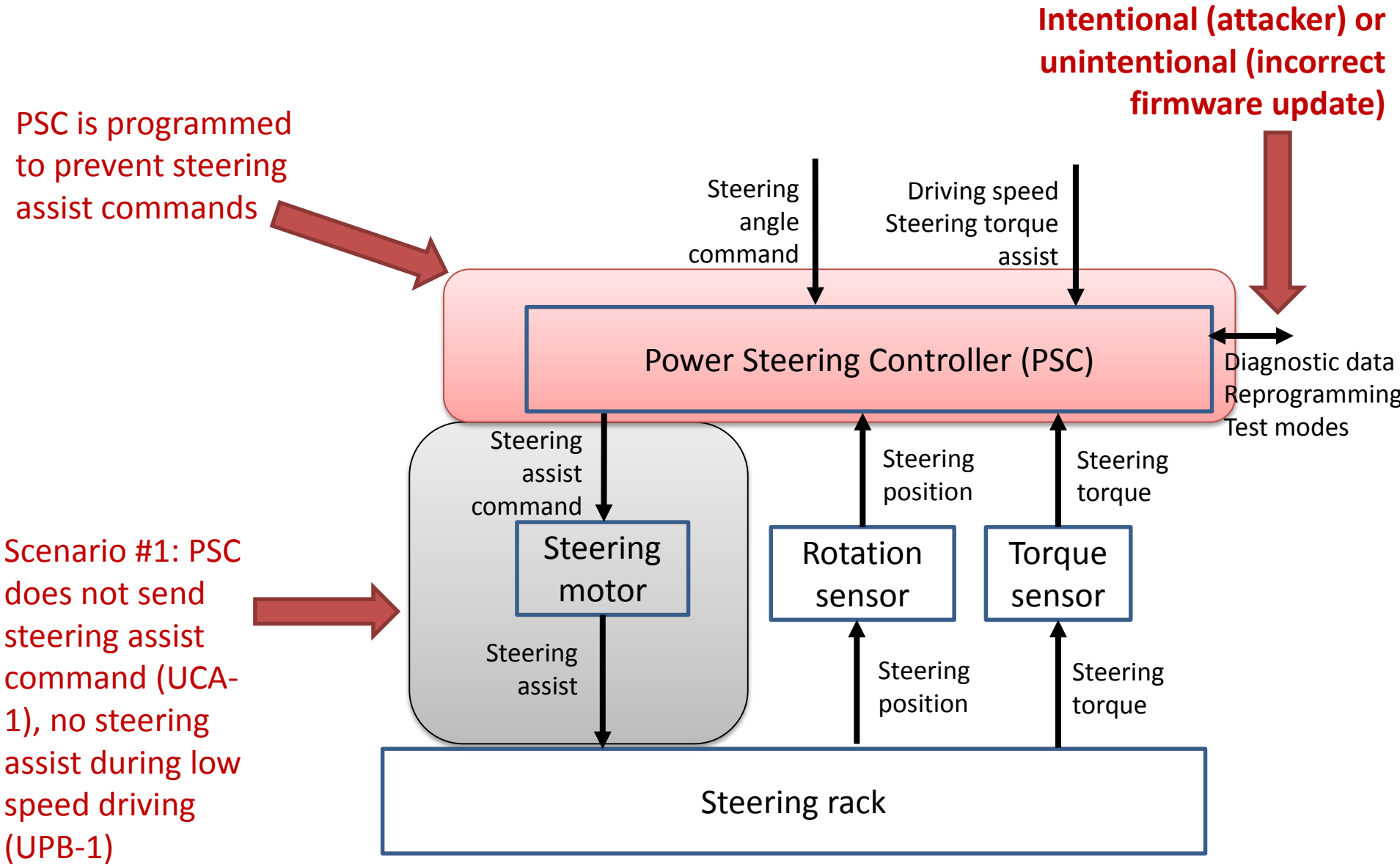
Identify causal scenarios

PSC is programmed to prevent steering assist commands



Scenario #1: PSC does not send steering assist command (UCA-1), no steering assist during low speed driving (UPB-1)

Identify causal scenarios



Identify mitigations

No steering assist during low speed driving
(Unsafe Process)

Power steering controller does not send steering assist command during low speeds
(Unsafe Control Action)

PSC is programmed to prevent steering assist commands
(Inadequate Control Algorithm)

Intentional (attacker)

Security Issue

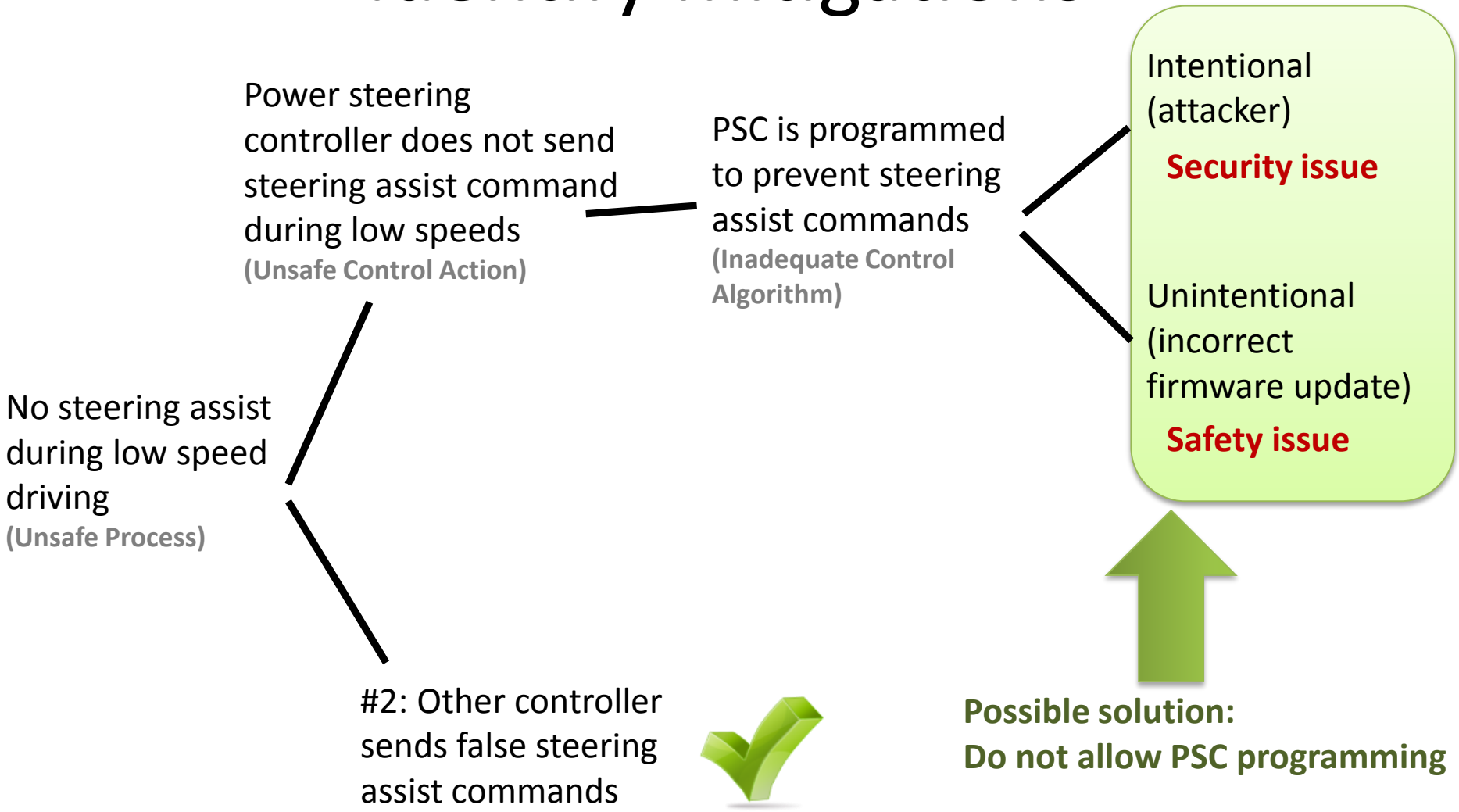
Unintentional (incorrect firmware update)

Safety Issue

#2: Other controller sends false steering assist commands



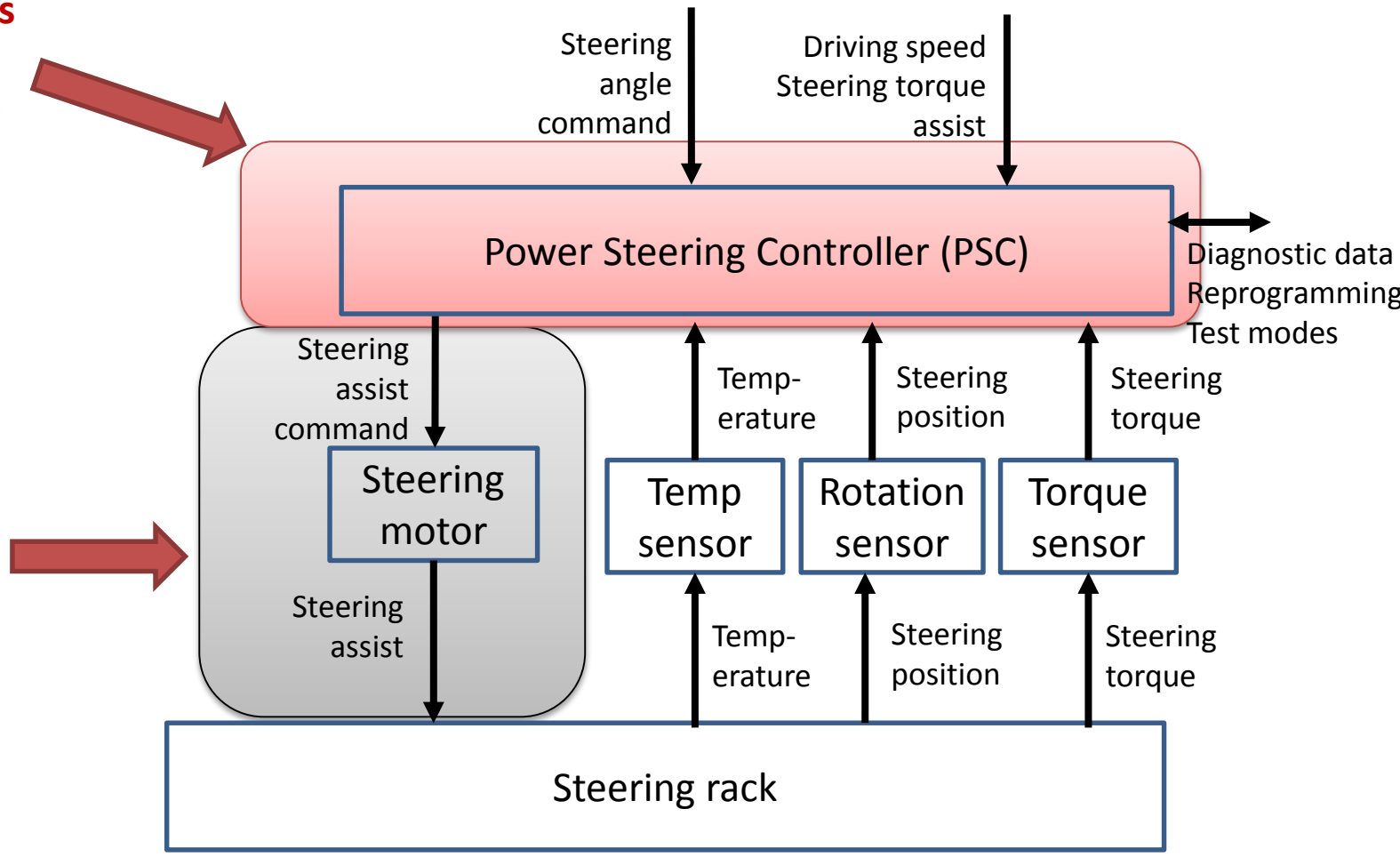
Identify mitigations



Identify causal scenarios

PSC incorrectly believes motor is overheating
(Process model flaw)

Scenario #1: PSC does not send steering assist command (UCA-1), no steering assist during low speed driving (UPB-1)

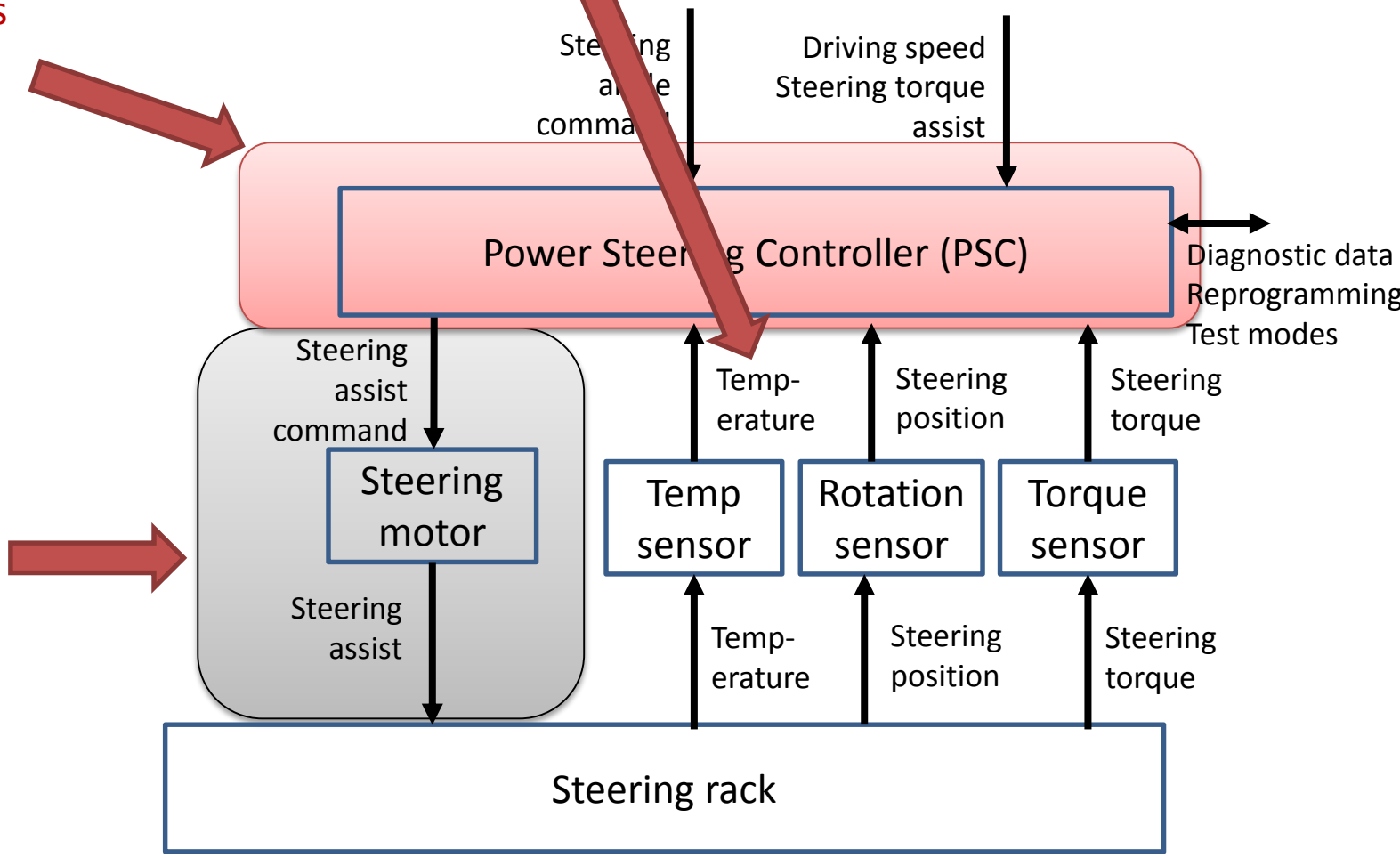


Identify causal scenarios

Temperature reading is incorrect (Incorrect feedback)

PSC incorrectly believes motor is overheating (Process model flaw)

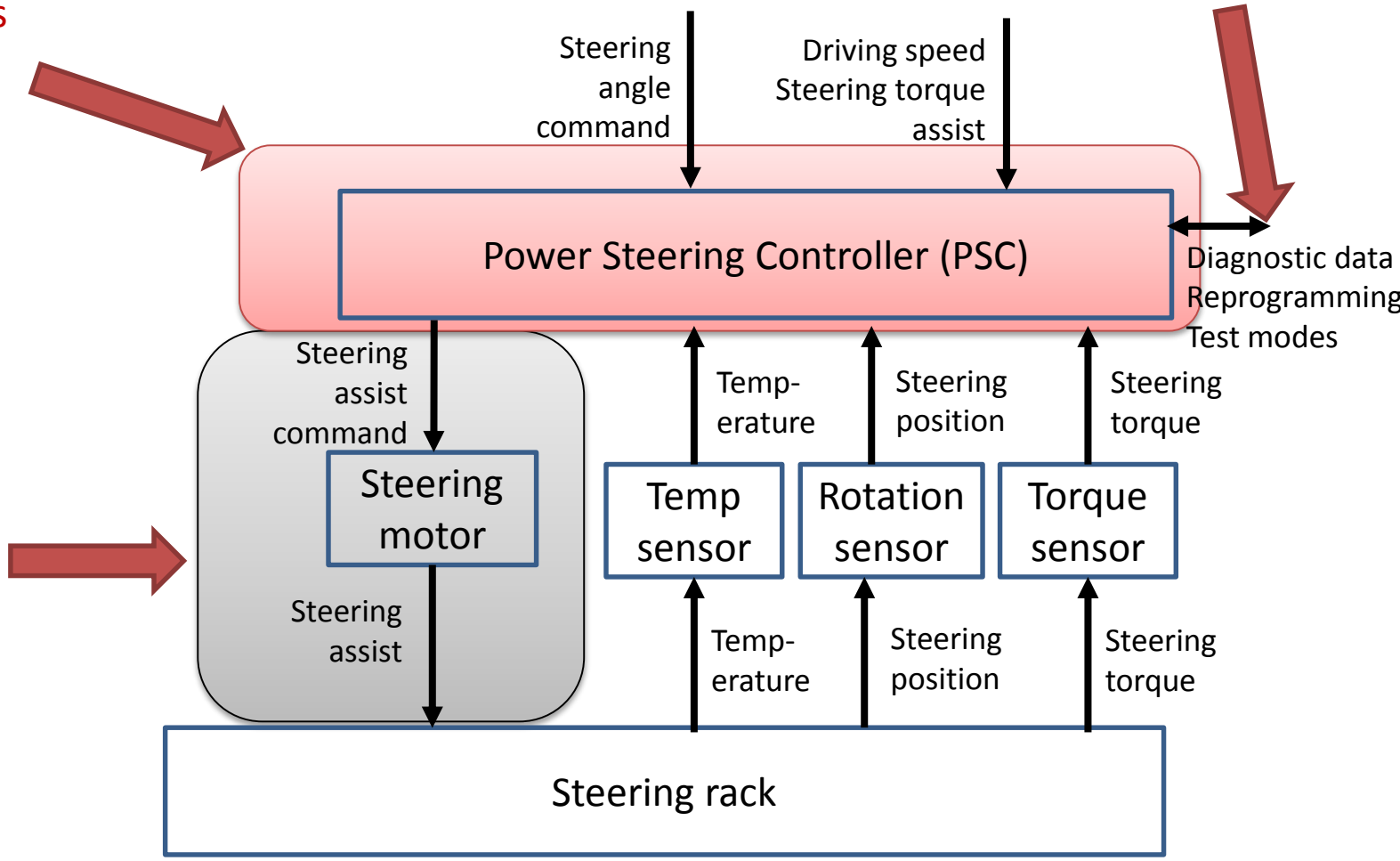
Scenario #1: PSC does not send steering assist command (UCA-1), no steering assist during low speed driving (UPB-1)



Identify causal scenarios

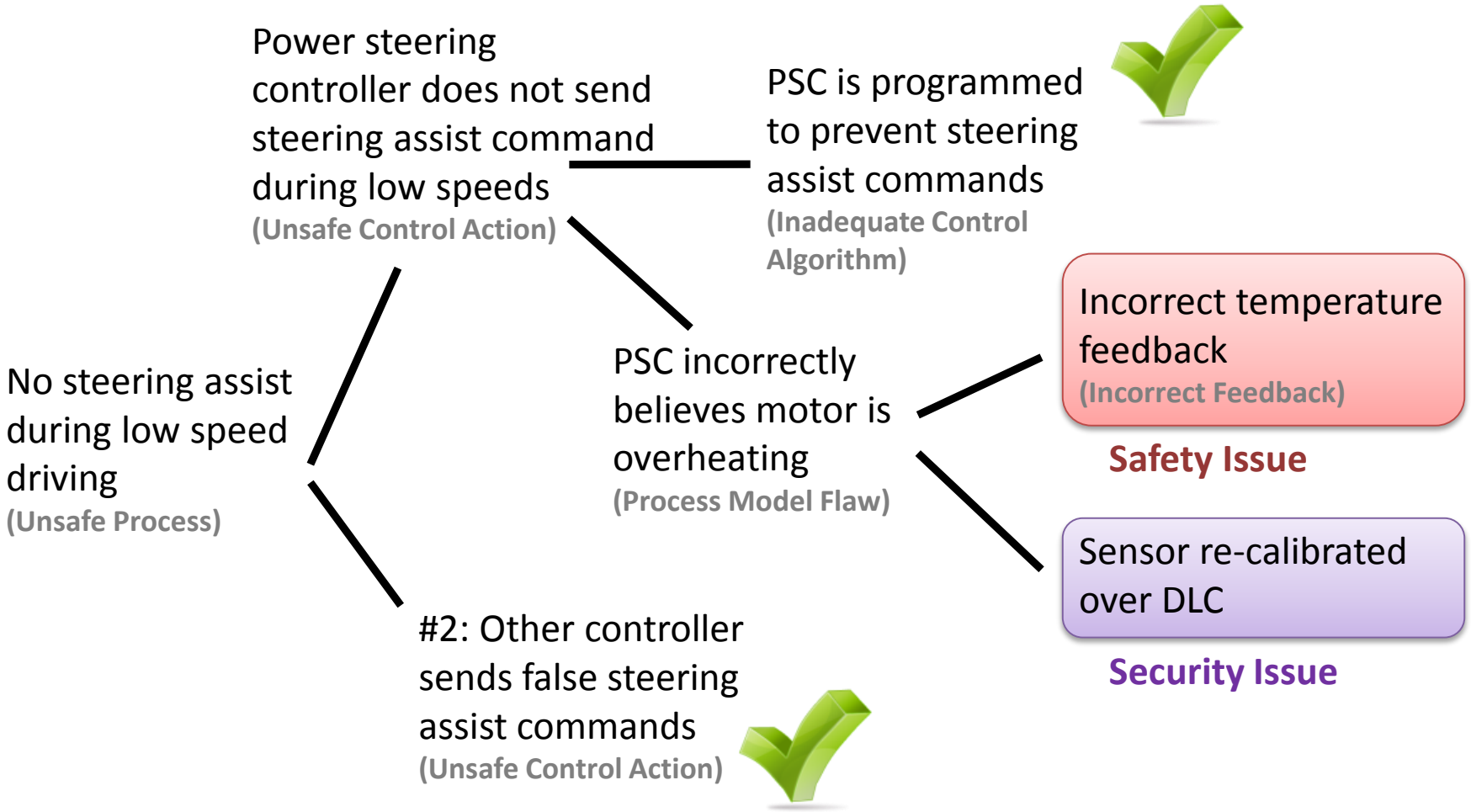
Temperature sensor calibrated incorrectly

PSC incorrectly believes motor is overheating
(Process model flaw)

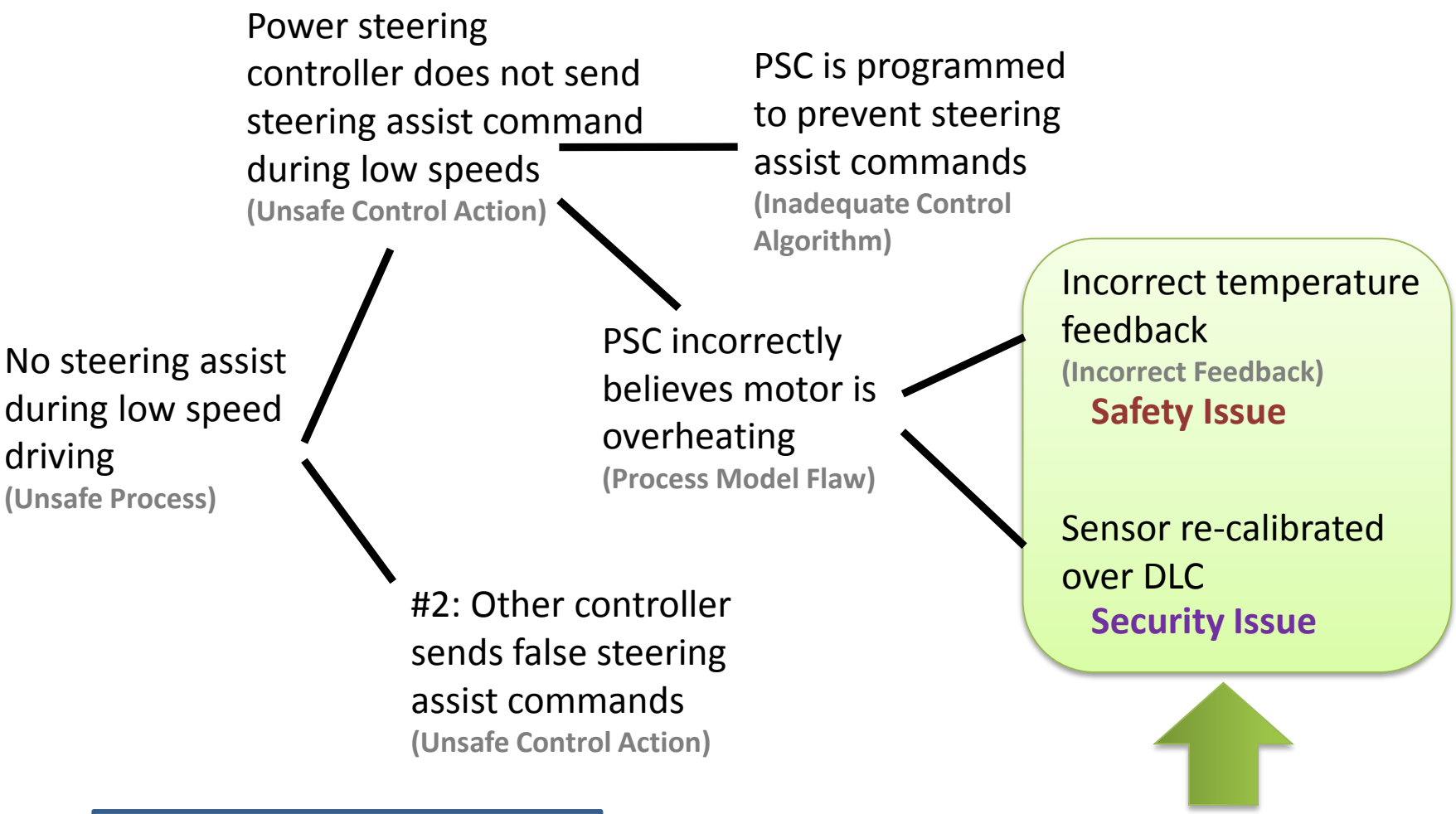


Scenario #1: PSC does not send steering assist command (UCA-1), no steering assist during low speed driving (UPB-1)

Capturing both safety and security issues



Capturing both safety and security issues



These scenarios can be generated automatically!

Possible solution:
Prevent overheating without active temperature monitoring

Another Scenario

- UPB-3: Excessive steering assist when driver did not enable park assist
  - UCA-3: Power Steering Controller provides excessive steering assist when driver did not enable park assist
    - Process Model Flaw #2: Power Steering Controller incorrectly believes park assist is enabled

Security Issue

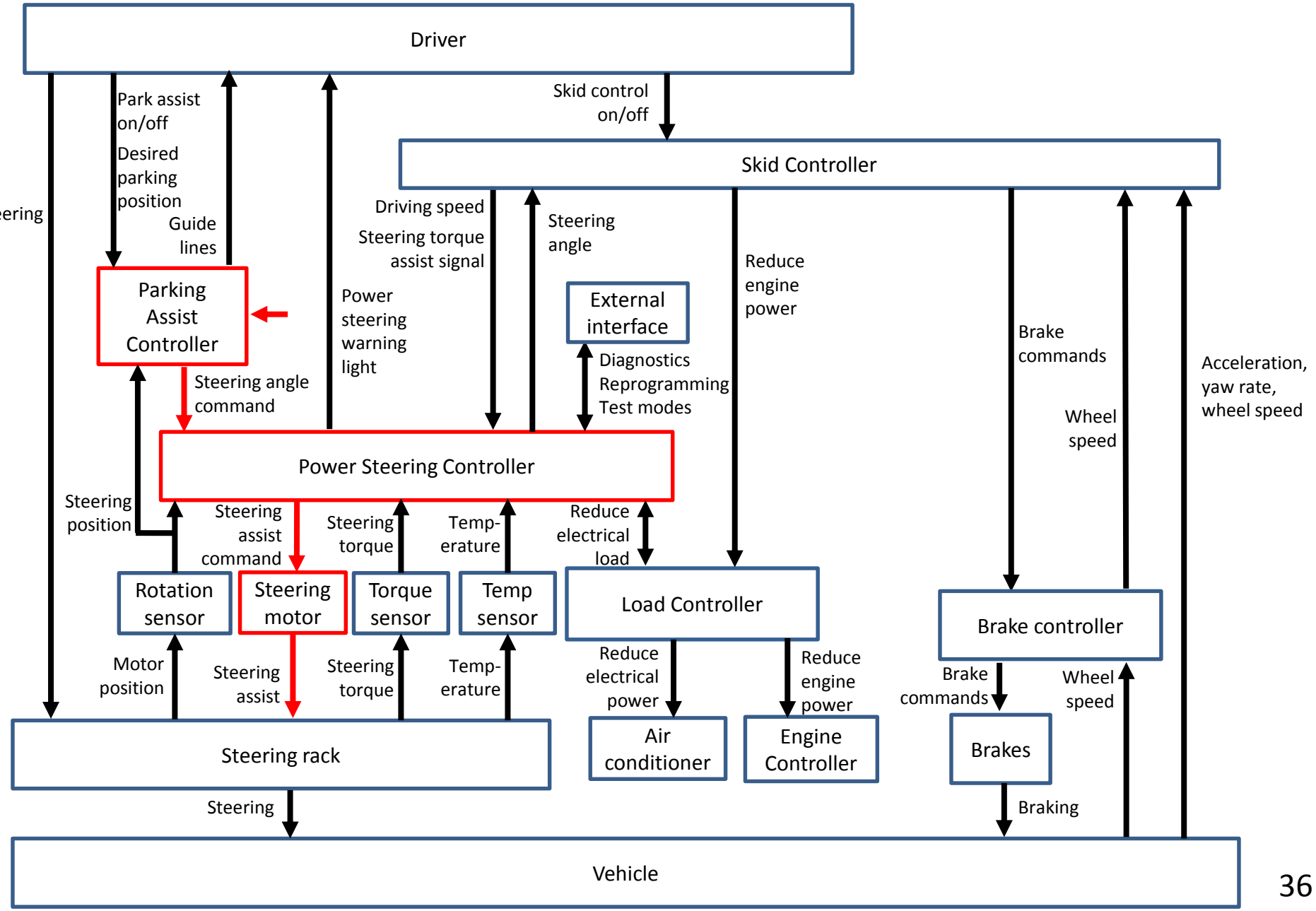
- Attacker injects false park assist command, resulting in incorrect steering angle commands

Safety Issue

- Park assist command from the driver is delayed during transmission, resulting in incorrect steering angle commands much later than intended

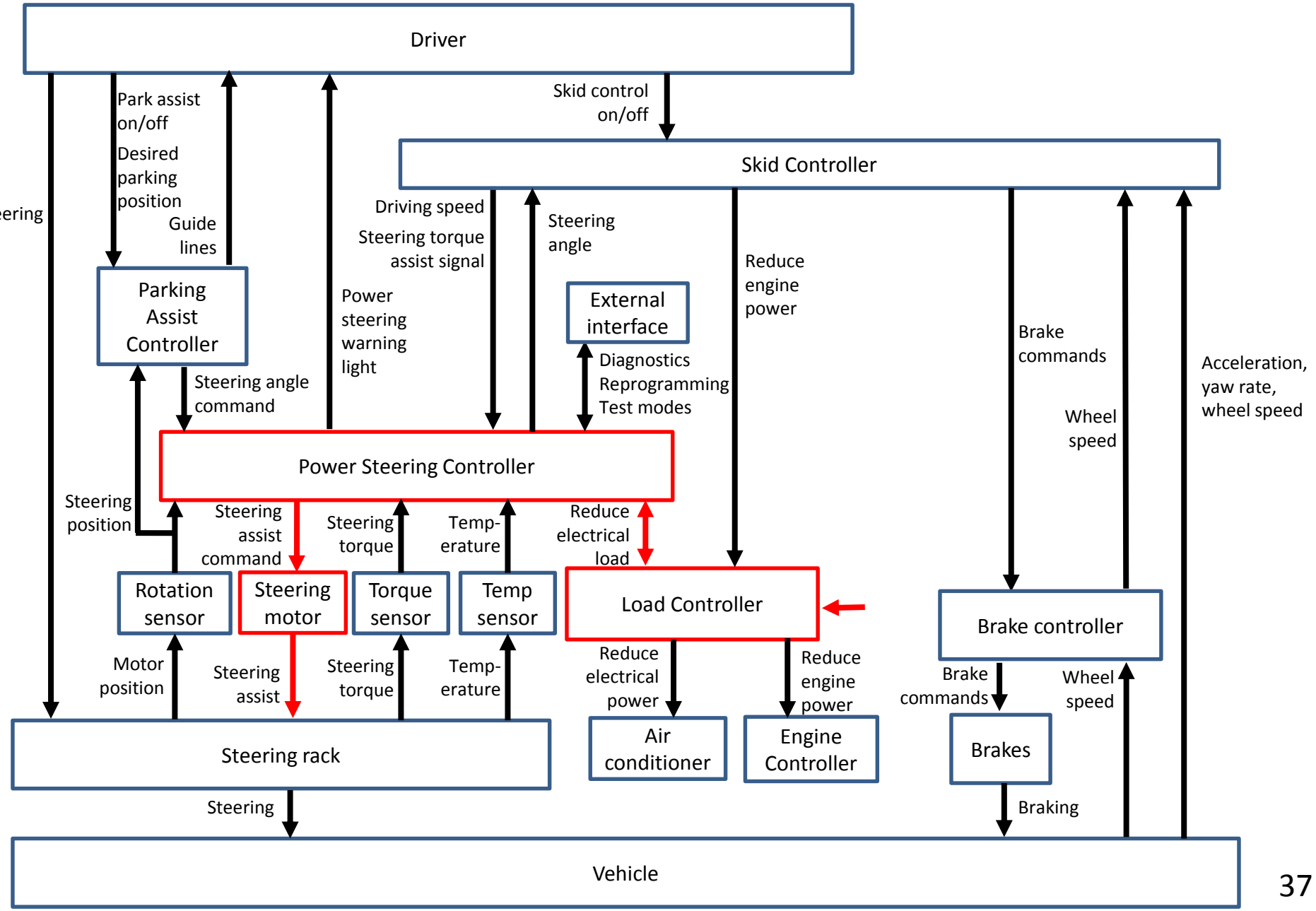
Copyright © John Thomas 2016

Detailed Control Structure



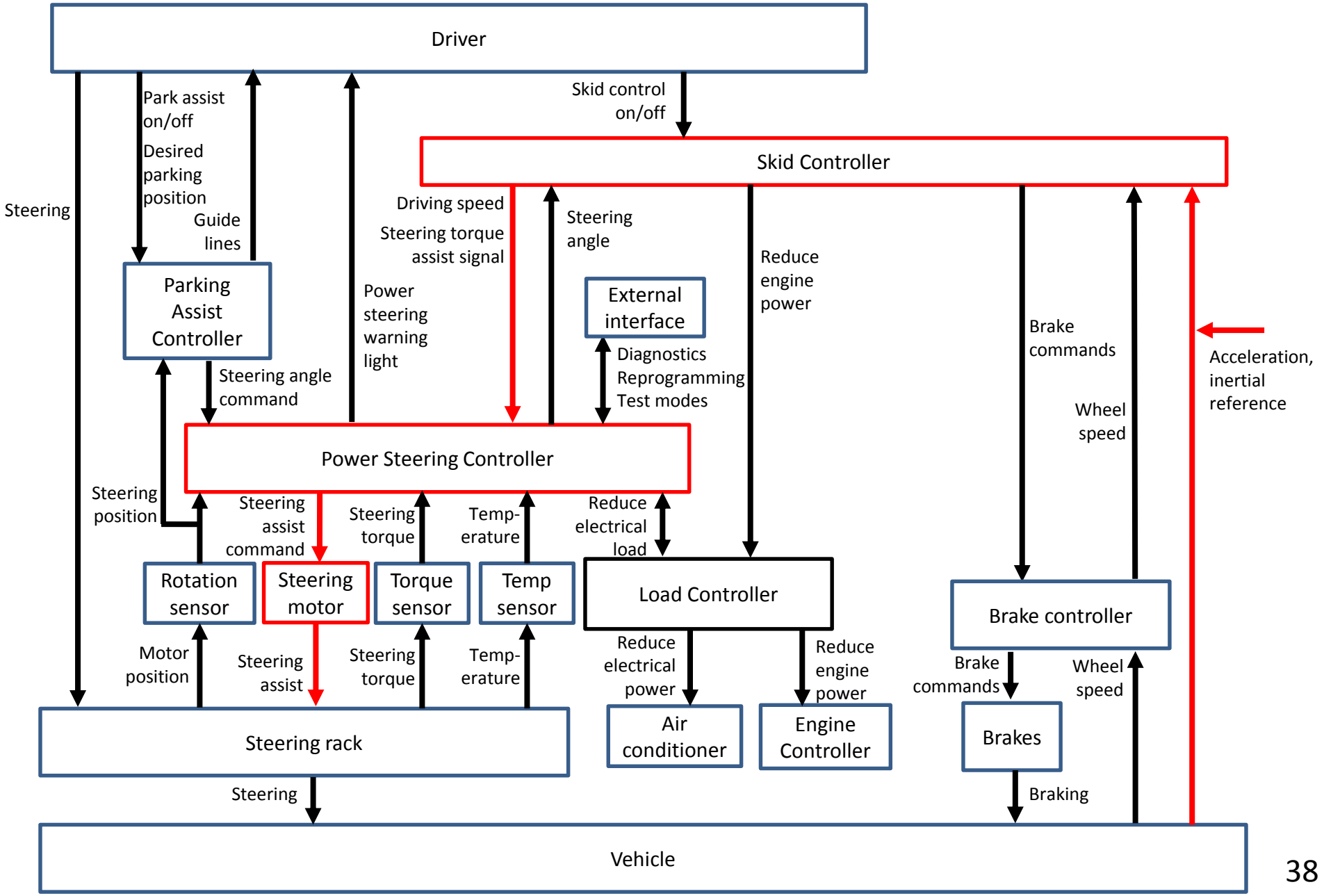
Copyright © John Thomas 2016

Detailed Control Structure



Copyright © John Thomas 2016

Detailed Control Structure



Conclusions

- Process applicable to both safety and security
  - The control structure is the same
  - The UCAs are the same
  - The process model flaws are the same
  - The final causes may be different for safety vs. security
- Safety + security together for increased efficiency
  - When used for security, safety issues can be added with very little extra effort
  - Separate analyses are not required
  - Can reduce time and effort
- Different starting point
  - Start in the controlled process, work backward
  - Same results as starting with Step 1 UCAs, Step 2A/B