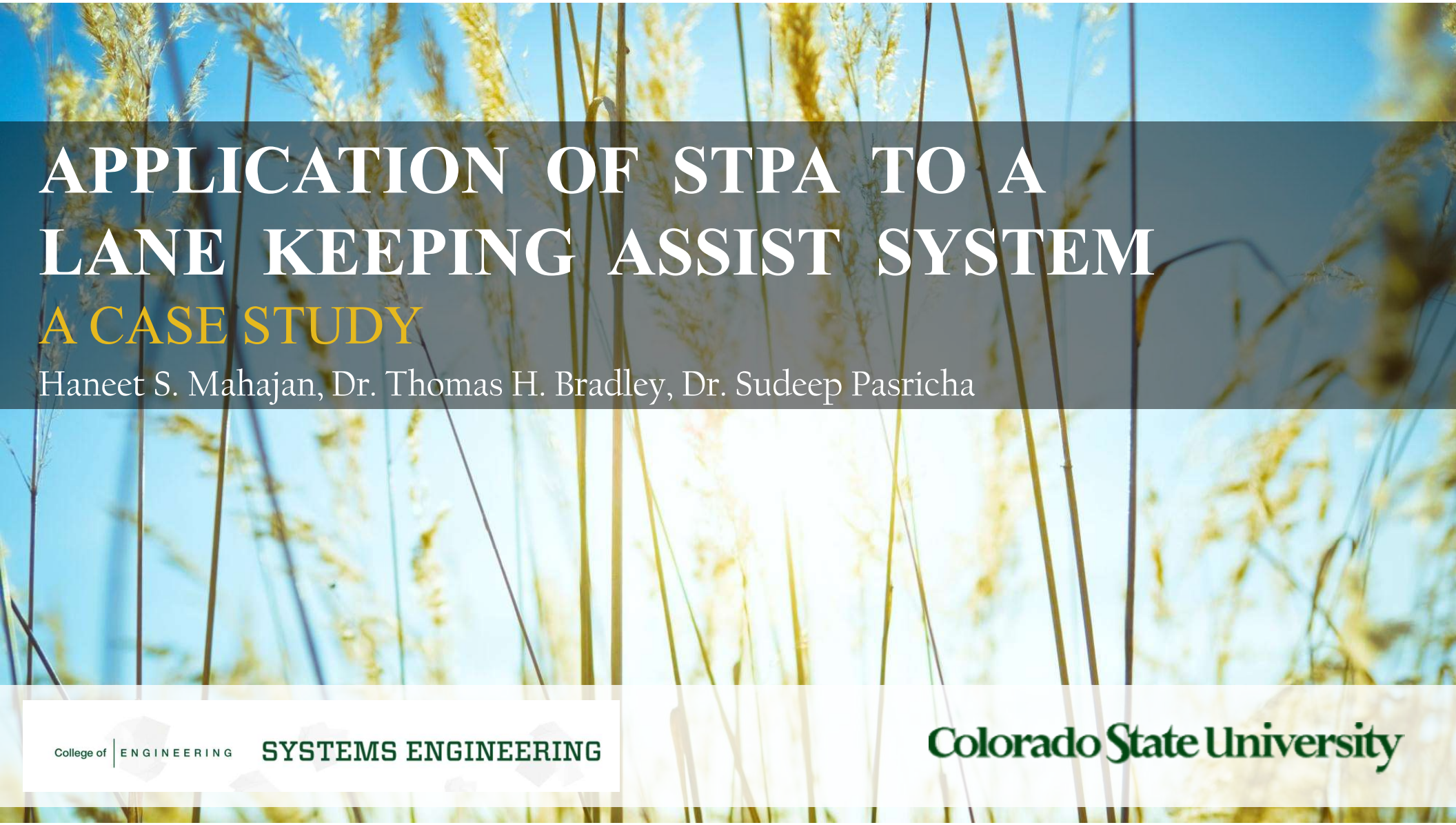


APPLICATION OF STPA TO A LANE KEEPING ASSIST SYSTEM

A CASE STUDY

Haneet S. Mahajan, Dr. Thomas H. Bradley, Dr. Sudeep Pasricha

College of ENGINEERING SYSTEMS ENGINEERING

Colorado State University

ABOUT ME

EcoCAR3
Advanced Vehicle Technology Competition

Colorado State University

IAV - More than 6000 engineers worldwide…




What we develop moves you.


- Development solutions automotive
- In 11 countries, at 27 locations
- Full vehicle development to components (e.g. E-mobility, autonomous driving, connectivity, HMI)
- From system simulation to software development
- Car makers and suppliers
- Reinvestment of earnings for new solutions

OUTLINE

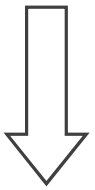
- Introduction
- Steps for the analysis
- Definitions for the analysis
- Application of STPA
- Results
- Discussion
- Future Scope

INTRODUCTION

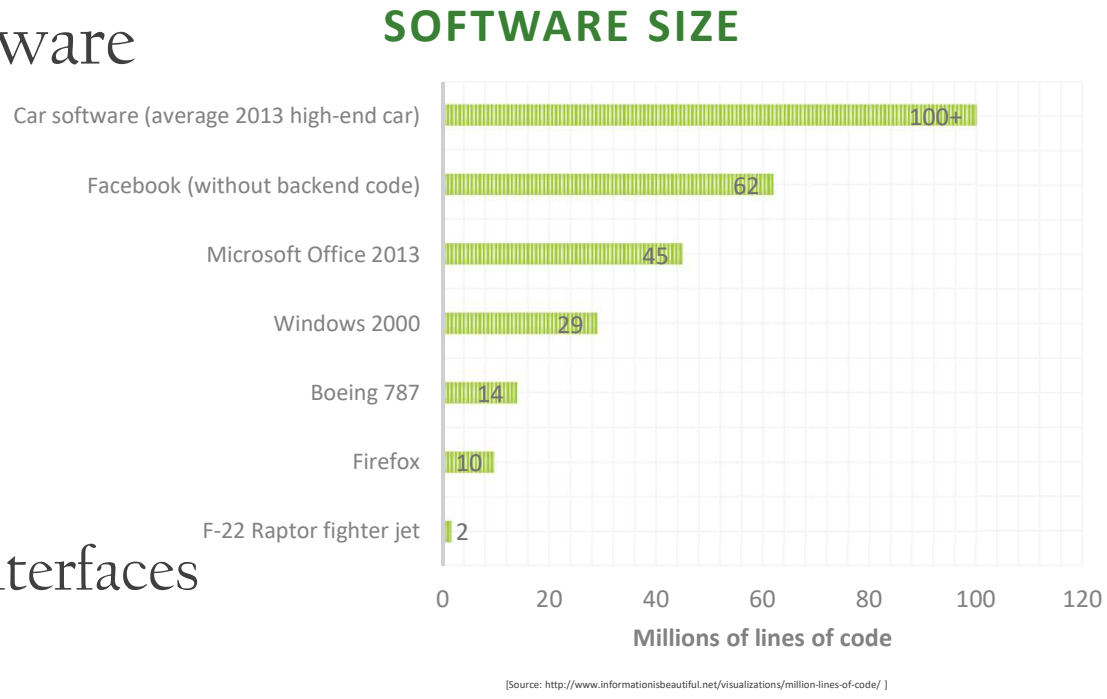
- Autonomous cars on the road by 2020
- Complex hardware and software:
  - RADARs, LIDARs, sensors, data fusion...
  - Machine learning algorithms
  - Neural networks
- Specially tailored software for each vehicle
- Rush to market new technology

INTRODUCTION

- 100 ECUs, millions of lines of code
- More computers and software



  - Complicated interactions
  - Random accidents (without any component failure)
  - Complex human-machine interfaces



[Source: http://www.informationisbeautiful.net/visualizations/million-lines-of-code/]

THE RIGHT APPROACH?

Specific functional safety teams to perform the safety lifecycle from the beginning of system lifecycle.

+

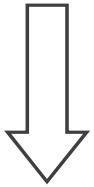
Initiating development of systems, with design constraints and requirements from safety analyses as the driving force

=

Safer system design processes

STPA

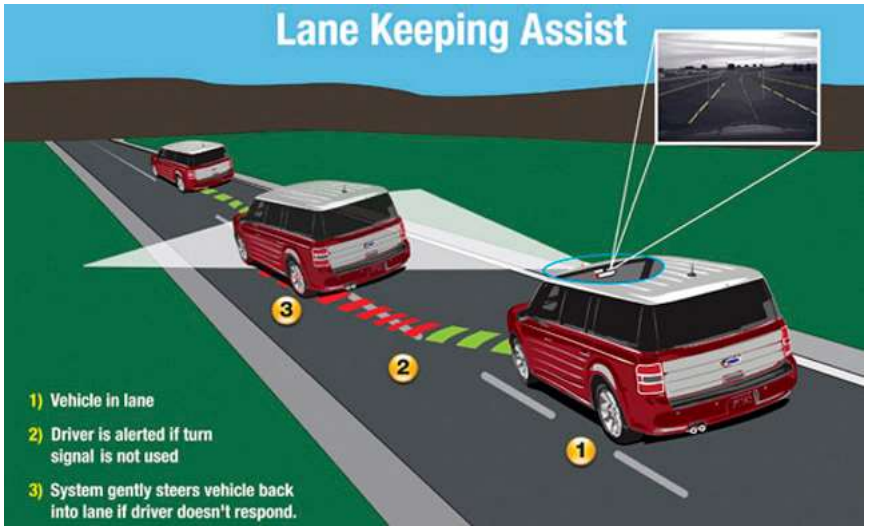
- Can be applied during any stage of development
- Focus on loss of control
- Not losing sanity with numbers, when you don't have data



Great technique for complex systems implemented in autonomous vehicles

LANE KEEPING ASSIST (LKA)

- Detects lane departure
- Warns driver if lane is changed without turn-signal
- Steers car back into lane, if no action is taken by driver



[Source: https://forums.nasioc.com/forums/showthread.php?t=2727899]

STEPS IN THE ANALYSIS

1. Define hazards, requirements and constraints based on system-level functionality
2. Develop high-level functional control structure
3. Identify hazardous states (Unsafe Control Actions)
4. Determine causal factors
5. Develop additional constraints and requirements

DEFINITIONS

High-level Hazards

- Absence of warning when vehicle moves out of lane, resulting in a collision
- No corrective action provided by the system when the car moves out of lane, leading to a collision
- Corrective action provided when it isn't required, resulting in a collision
- Corrective action (torque to the steering) provided in the wrong direction, causing a collision

High-level Requirements

- The LKA system shall warn the driver when the vehicle is switching lanes without a *turn-indicator*
- The LKA system shall provide corrective action if the driver doesn't respond to the warning signs and the vehicle continues to move out of lane

High-level Constraints

- The LKA system must not allow the vehicle switch to lanes without the correct *turn-indicator* being actuated
- The LKA system must not perform corrective action if the correct *turn-indicator* is actuated (if the direction of deviation is the same as the *turn-indicator*)
- The LKA system must verify that corrective action has been performed either from its inputs or feedback from the electrical steering system

PROPOSED CONTROL STRUCTURE

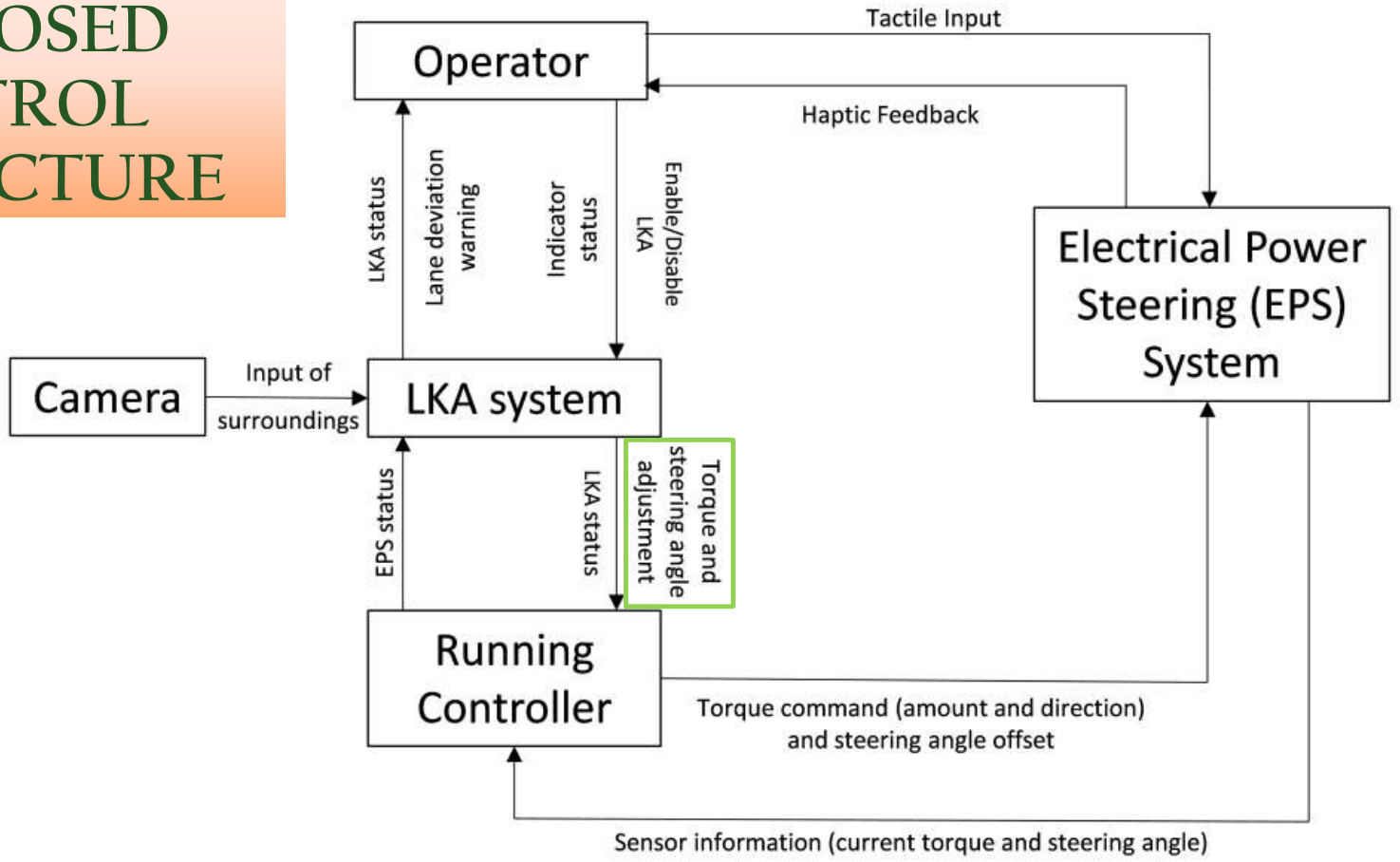


Fig: Initial control structure showing high-level system interactions

APPLICATION OF STPA

Control Function	Unsafe Control Actions (UCAs)			
	Constraint(s)			
	Required but not provided	*Provided but not required*	*Provided but wrong timing*	*Provided but incorrect duration*
Torque and steering angle calculations (from LKA to running controller)	Camera check; accurate detection and processing of lane markings H1: Torque request isn't transferred, while vehicle continues to drive out of lane	Camera check; continuous communication of EPS status H2: Unexpected torque to the steering to LKA; LKA refresh rate	LKA processing time; incorrect refresh rate; camera cycle rate H3: Controller sends torque request at the wrong time	LKA processing time; camera cycle rate; continuous EPS status communication H4: Controller continues to send torque request
	Requirement(s)			
	Causal Factor(s)			
	1. Incorrect input from camera to LKA. 2. Misinterpreted lane markings by LKA (system thinks vehicle is in lane) 3. Incorrect turn-indicator status transmitted to LKA 4. LKA is disabled	R1: The running controller shall send the current EPS status signal to the LKA once the LKA is enabled and has been initialized R2: The running controller shall update the LKA system if there is a mismatch between the sensor information from EPS and the EPS status stored in LKA	R3: The LKA system shall continuously monitor and verify the camera input with the current processing of deviation by LKA 1. Incorrect input from camera 2. LKA is frozen 3. Turn-indicator malfunction 4. EPS status communication is delayed	R4: The running controller shall refresh the LKA system if the LKA status is frozen 1. Incorrect input from camera 2. LKA is frozen 3. EPS status not communicated to LKA

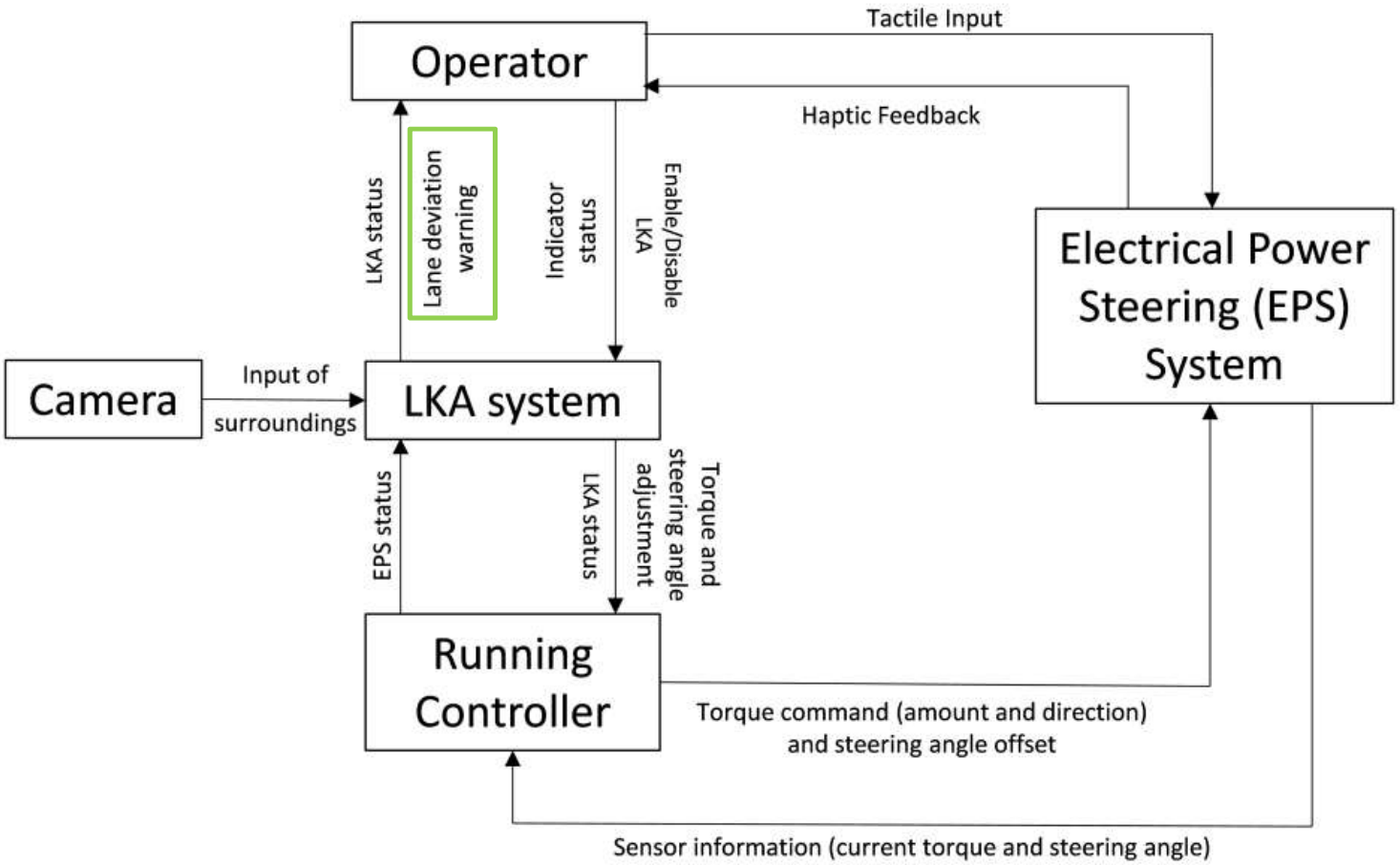


Fig: Initial control structure showing high-level system interactions

Control Function	Unsafe Control Actions (UCAs)			
	Required but not provided	*Provided but not required*	*Provided but wrong timing*	*Provided but incorrect duration*
Lane deviation warning to operator	H5: Operator does not provide corrective action	H6: Wrong warning misdirecting driver, possibly leading to incorrect torque request to running controller	H6	H6
	Causal Factor(s)			
	1. Incorrect input from camera 2. LKA is disabled when the operator thinks it is enabled 3. Incorrect turn-indicator status	1. Incorrect input from camera 2. LKA is enabled when it shouldn't be 3. Incorrect indicator status		
	Constraint(s)			
	Initial camera check; camera fidelity; initial relay check	Initial camera check; camera fidelity; relay check		
	Requirement(s)			
	R5: The running controller shall confirm that the LKA is functional with the operator when the system is enabled	R6: The LKA shall verify driver responsiveness before providing warnings and/or corrective action		

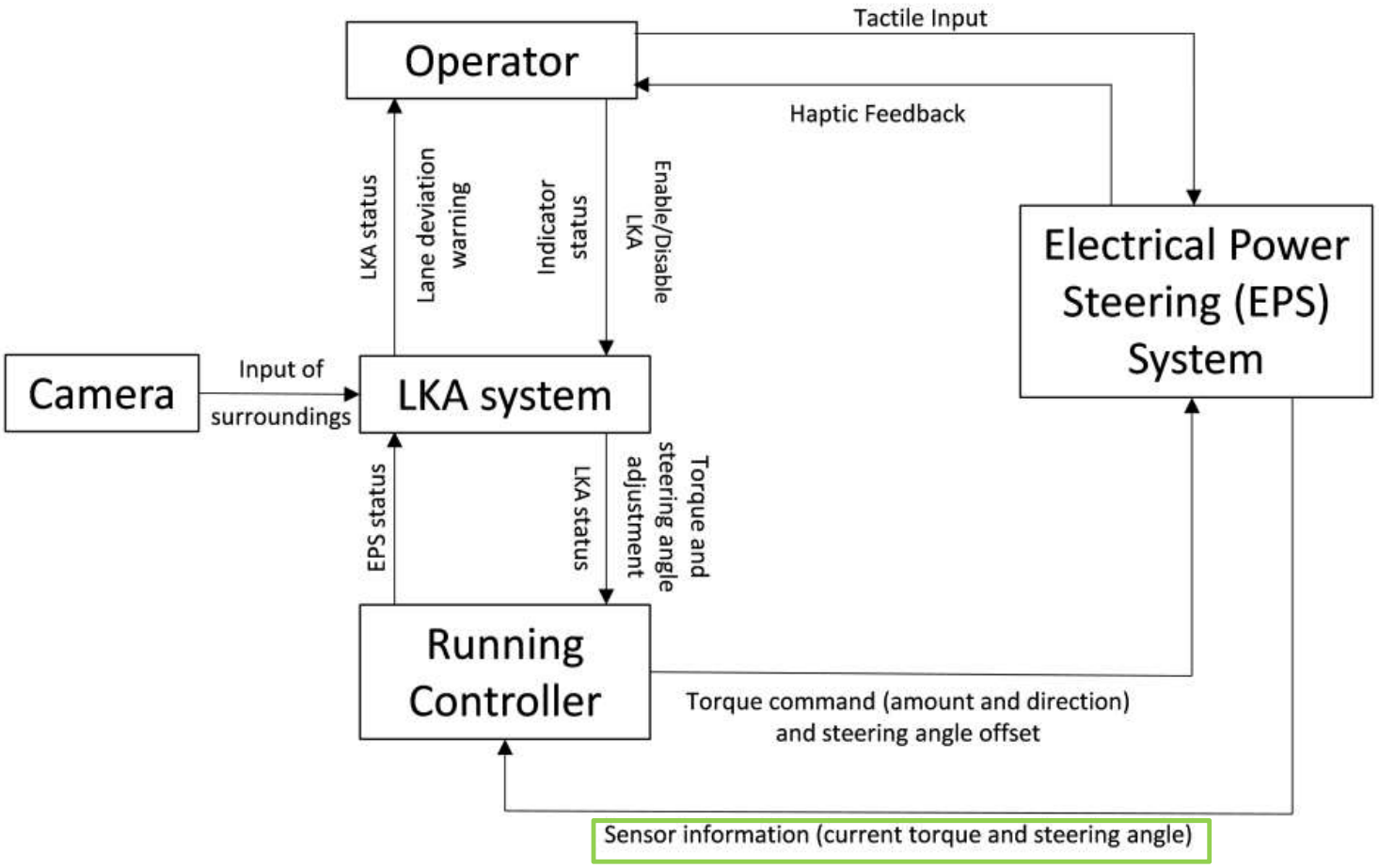


Fig: Initial control structure showing high-level system interactions

Control Function	Unsafe Control Actions (UCAs)			
	Required but not provided	*Provided but not required*	*Provided but wrong timing*	*Provided but incorrect duration*
Sensor information to running controller	H7: Controller is unaware of any changes implemented by the EPS	N/A	H7	N/A
	Causal Factor(s)			
	Sensor malfunction			
	Constraint(s)			
	Sensor diagnostics			
	Requirement(s)			
	R7: The running controller shall transfer torque requests to EPS only if sensor information is received			

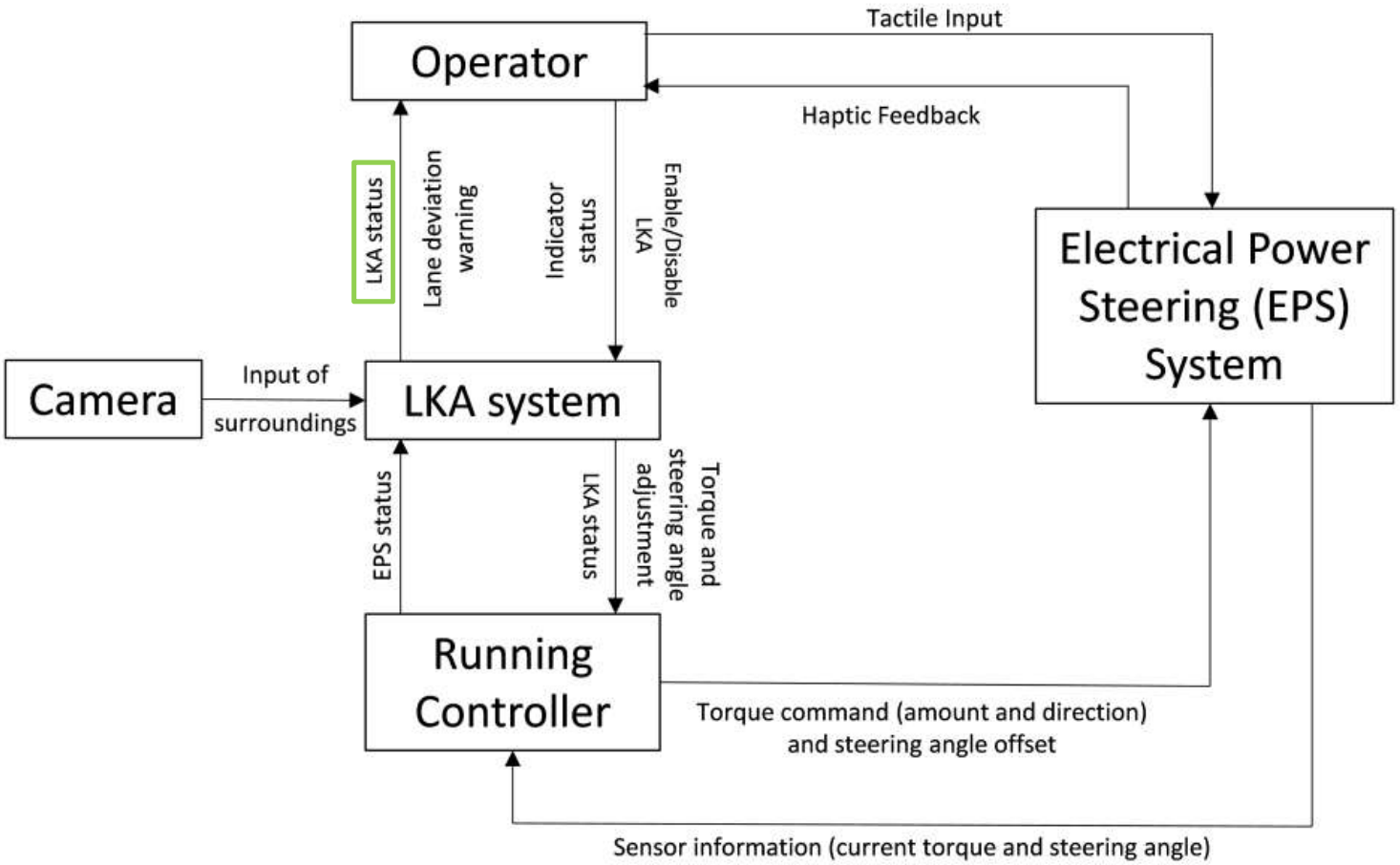


Fig: Initial control structure showing high-level system interactions

Control Function	Unsafe Control Actions (UCAs)			
	Required but not provided	*Provided but not required*	*Provided but wrong timing*	*Provided but incorrect duration*
LKA status to operator	H8: Operator is unsure if LKA is on or not	H9: LKA is on when not needed	H8	H8
	Causal Factor(s)			
	1. Communication breakdown between LKA and operator 2. LKA malfunction	LKA malfunction		
	Constraint(s)			
	LKA startup functionality test	Incorrect enable signal		
	Requirement(s)			
		R8: The running controller shall verify operator intention to enable LKA		

Hazard Number	Hazard
H1	Torque request isn't transferred, while vehicle continues to drive out of lane
H2	Unexpected torque to the steering
H3	Controller sends torque request at the wrong time
H4	Controller continues to send torque request
H5	Operator does not provide corrective action
H6	Wrong warning misdirecting driver, possibly leading to incorrect torque request to running controller
H7	Controller is unaware of any changes implemented by the EPS
H8	Operator is unsure if LKA is on or not
H9	LKA is on when not needed

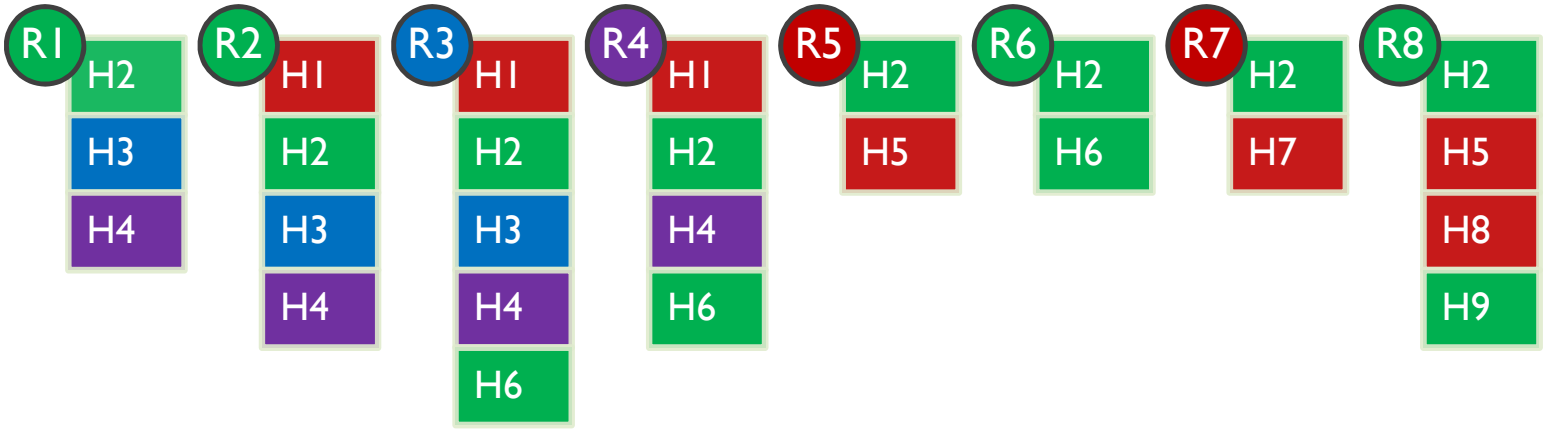
Requirement Number	Requirement
R1	The running controller shall send the current EPS status signal to the LKA once the torque command has been implemented
R2	The running controller shall update the LKA system if there is a mismatch between the sensor information from EPS and the EPS status stored in LKA
R3	The LKA system shall continuously monitor and verify the camera input with the current EPS status
R4	The running controller shall refresh the LKA system if the LKA status is frozen
R5	The running controller shall confirm the LKA is functional with the operator when the system is enabled
R6	The LKA shall verify driver responsiveness before providing warnings and/or corrective action
R7	The running controller shall transfer torque requests to EPS only if sensor information is received
R8	The running controller shall verify operator intention to enable LKA

- Required but not provided
- Provided but not required
- Provided but wrong timing (too early/too late)
- Provided but wrong duration (too long/ too short)

RESULTS

- STPA allows for development of requirements, even at the initial stages of the system lifecycle
- Clear understanding of systems and their intended functions, allowing better design processes
- Requirements developed from STPA lead to the realization of new signals and systems
- Analysis inspires safety-driven design decisions

TRACEABILITY



- Required but not provided
- Provided but not required
- Provided but wrong timing (too early/too late)
- Provided but wrong duration (too long/ too short)

Colorado State University

UPDATED CONTROL STRUCTURE

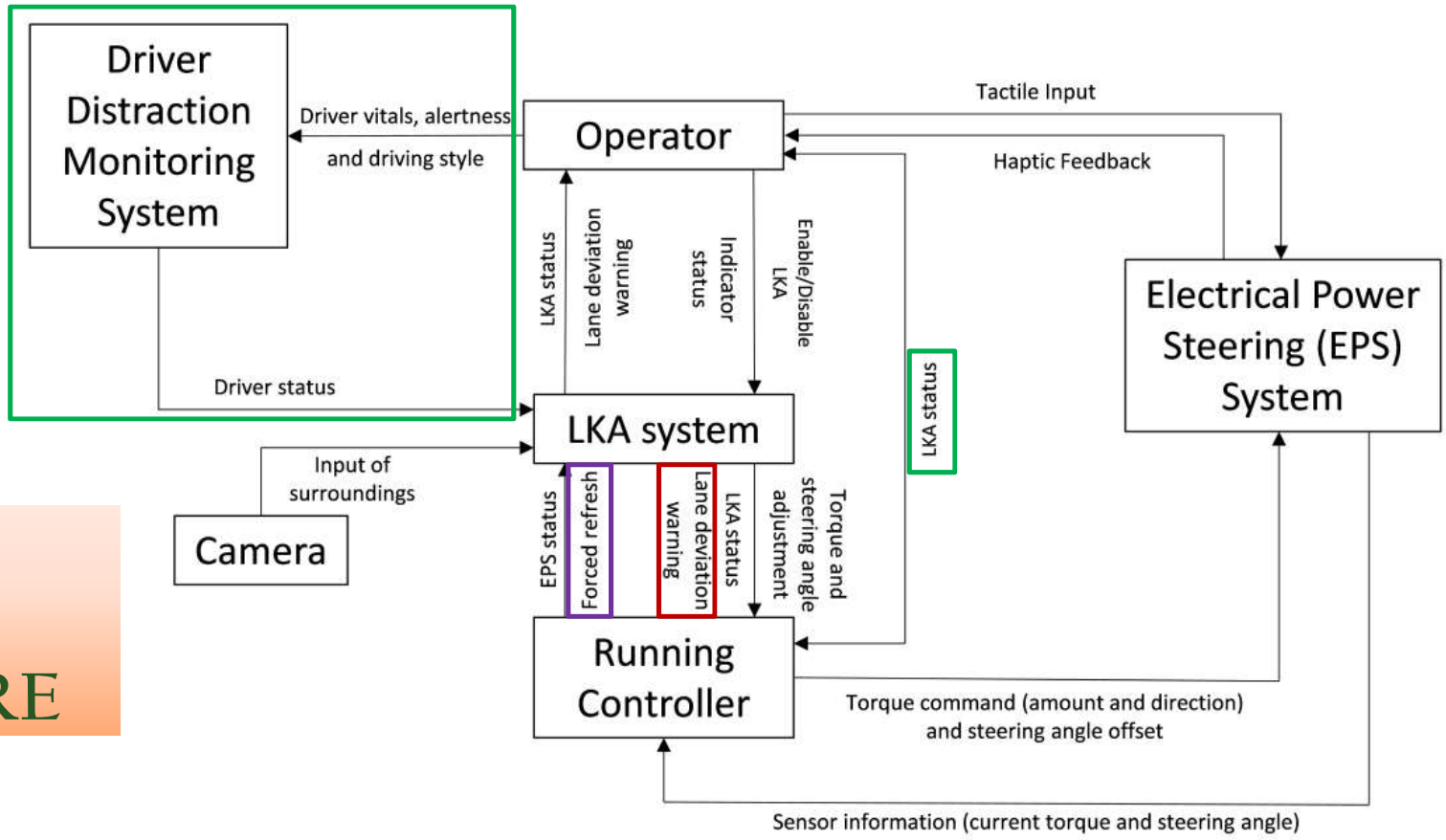


Fig: Updated control structure including changes derived from various requirements

DISCUSSION

- Including human error

  The operator was involved in the control loops that were analyzed for different UCAs. The Driver Distraction Monitoring System is intended to ensure that the driver is performing the necessary actuation, sensing and feedback control actions

- Requirements Engineering

  As the design process evolves, the requirements will be refined and new ones can be developed by repeating this process (with either new information or a modified control structure)

FUTURE SCOPE

- Continue analysis through engineering development process
- Perform analysis with a more comprehensive control structure (interactions with other systems such as Adaptive Cruise Control)
- Further innovation in systems, based on requirements

Colorado State University

REFERENCES

1. http://www.informationisbeautiful.net/visualizations/million-lines-of-code/
2. https://forums.nasioc.com/forums/showthread.php?t=2727899
3. Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety. Mit Press.
4. Leveson, N., & Thomas, J. (2013). An STPA Primer. Cambridge, MA.

Colorado State University