Automating Time Series Safety Analysis for Automotive Control Systems using Weighted Partial Max-SMT

Shuichi Sato[1,2], Shogo Hattori[2], Hiroyuki Seki[2], Yutaka Inamori[1], Shoji Yuen[2]

[1] Toyota Central R&D Labs.,Inc. [2] Nagoya University

Appeared FTSCS 2016

Contents

- Background
- Motivation
- Approach and method
- Case Study
- Concluding remarks

Background

- Applying STAMP*1/STPA*2 to automotive safety analysis.

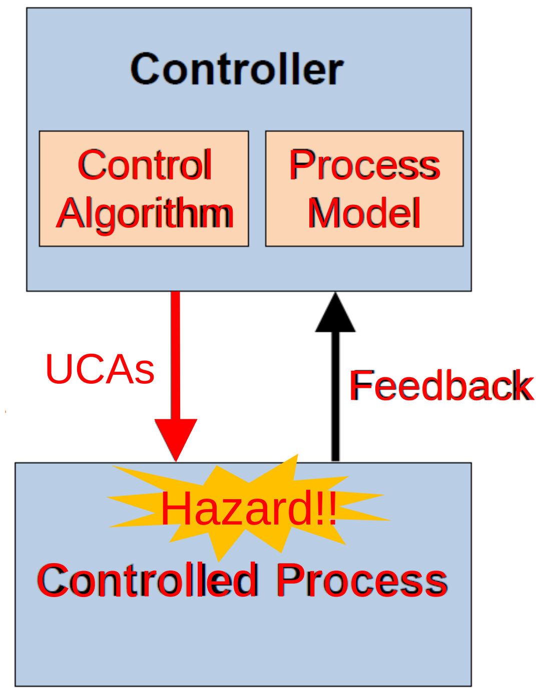
Preparation (Step 0)

- Identify Accidents and Hazards
- Construct a Control Structure

Step 1: Identify Unsafe Control Actions(UCAs)

Ex. System outputs a steering command while a driver doesn't do steering actions.

Step 2: Identify Causes of UCAs



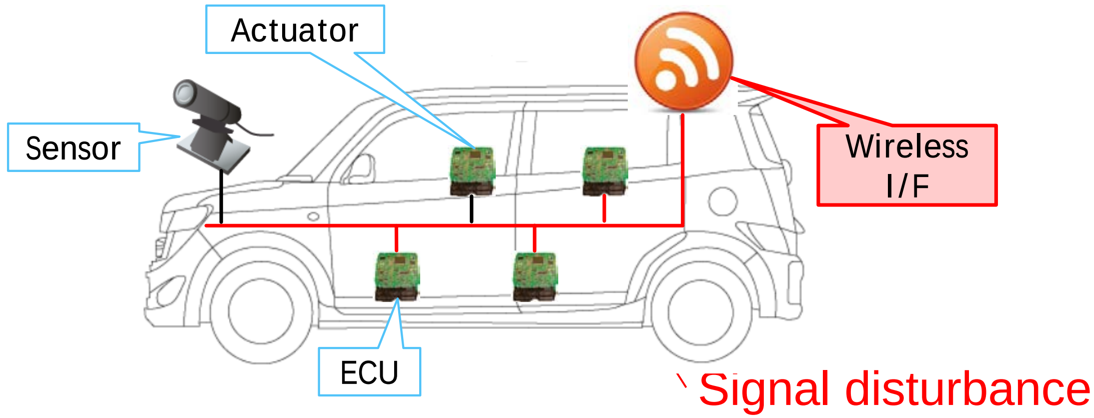
*1 System-Theoretic Accident Model and Process

*2 Systems-Theoretic Process Analysis

Motivation

(Intermittent) multi-signal disturbance that causes UCAs

Ex.

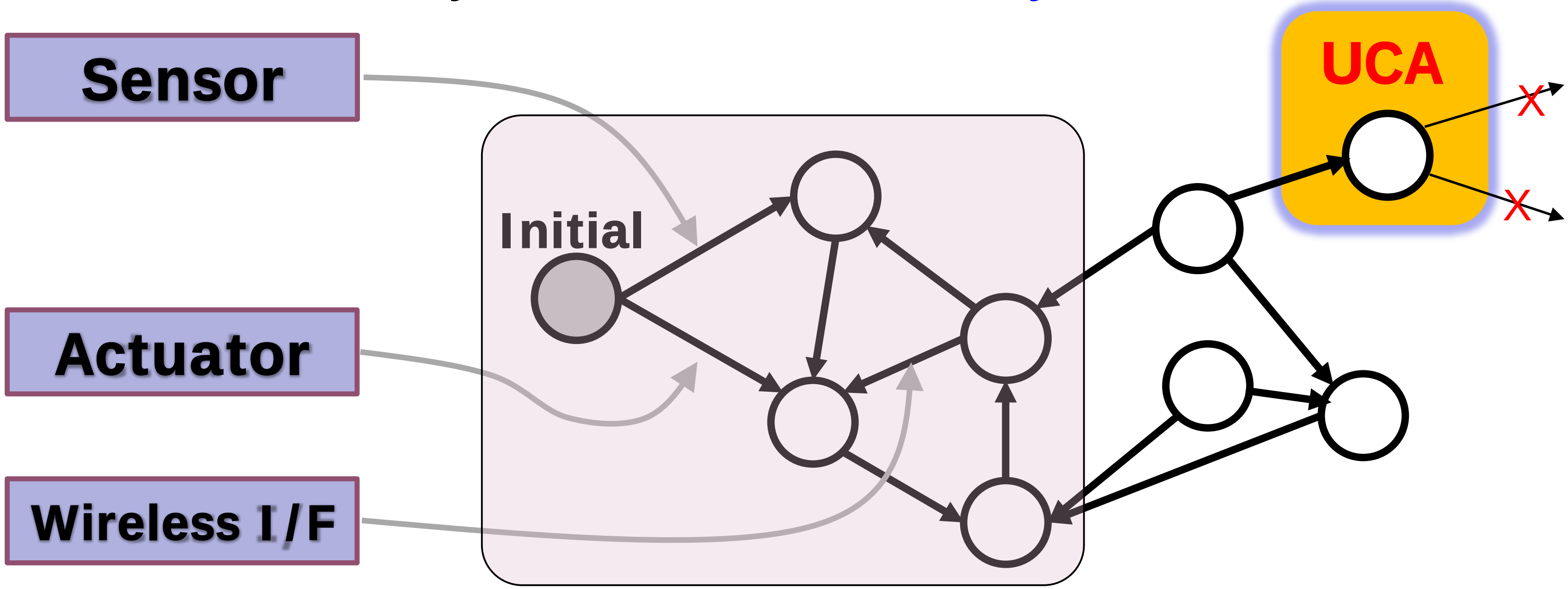


- Challenge:
  Too many signal combinations and time series patterns in designing error/attack-proof systems

To detections of intermittent multi-signal disturbances.

Behavioral Model

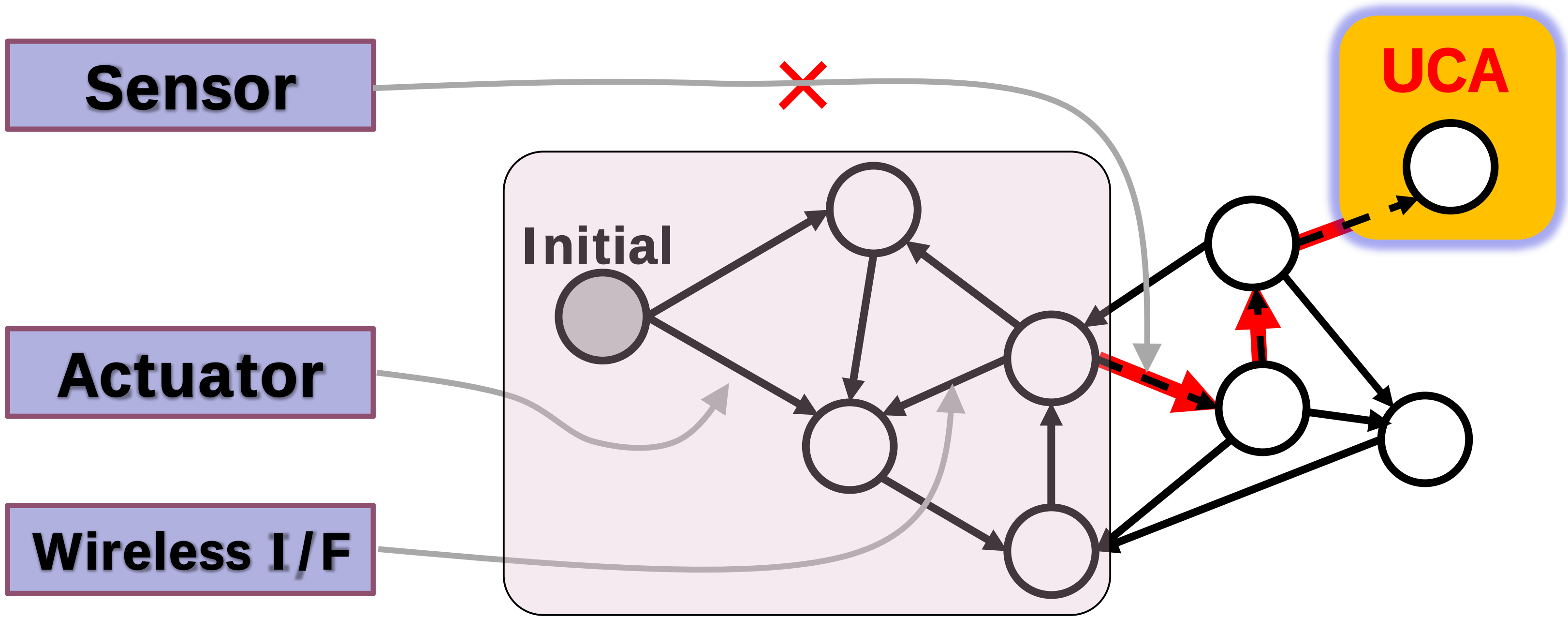
- Synchronous transition system with Boolean guard conditions.
  - Complete graph: Potentially ill transitions possible
- UCA states: states with transitions of UCAs unreachable by normal transition only.



Behaviour with Disturbance

If signals should be disturbed,

unexpected transitions should occur leading to an UCA.



Analysis overview

Input:

- Transition system
- UCAs
- Possible disturbed signals

→

Output:

- Disturbed signal patterns

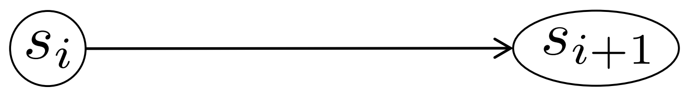
Approach

Transition System

- Transition system $M = (S, X, s_0, W)$

S : Control state X : State variable $s_0 \in S$: Initial control state

$W = \{ (s_i, \rho, s_{i+1}) \mid s_i, s_{i+1} \in S$, ρ : Constraints over $X \}$: Transitions



$\nu_i : u_{j,i} \mapsto v_{j,i}$ $\nu_{i+1} : u_{j,i+1} \mapsto v_{j,i+1}$

$\nu_i, \nu_{i+1} \models \rho$

$\nu_{i+1} : u_{j,i+1} \mapsto v_{j,i+1}$

Deterministic transition system: s_{i+1} is unique to s_i $\nu_{i+1}(u_{j,i+1}) = f_{j,i}(\nu_i(u_{j,i}))$

- A trace of M : $\alpha = (s_0, \nu_0)(s_1, \nu_1) \cdots (s_n, \nu_n)$

$s_i \in S$, $(s_i, \rho_i, s_{i+1}) \in W$

where ν_i : Value assignment for X_i, $\nu_i, \nu_{i+1} \models \rho_i(X_i, X_{i+1})$

Bounded Trace Formula

- A trace formula $\mathrm{TF}^{\leq K}$ of M (length: K) is a logical formula.

$$\rho_{s_0,s_1}(\vec{u}_0,\vec{u}_1) \wedge \rho_{s_1,s_2}(\vec{u}_1,\vec{u}_2) \wedge \cdots \wedge \rho_{s_{K-1},s_K}(\vec{u}_{K-1},\vec{u}_K)$$

$$\vec{u}_1 = f_0(\vec{u}_0) \wedge \vec{u}_2 = f_1(\vec{u}_1) \wedge \cdots \wedge \vec{u}_K = f_{K-1}(\vec{u}_{K-1})$$

$\mathrm{TF}^{\leq K}$ is satisfied by value assignments $\nu_0, \nu_1, \ldots, \nu_K$
iff $\alpha = \nu_0, \nu_1, \cdots, \nu_i, \cdots$ is a trace M

Straightforwardly constructed from M

Trace Formula of Transition System

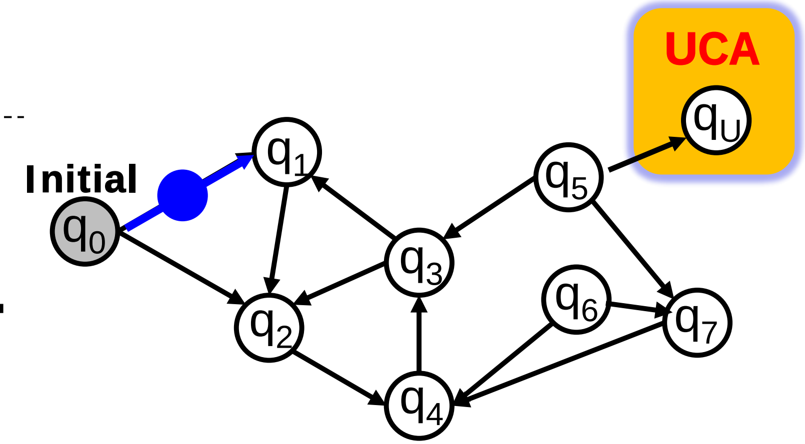
Trace (length K)

q_0 q_1 … q_K

$u_{1,0} = v_{1,init}$
$u_{2,0} = v_{2,init}$

$u_{1,1} = f_{0,1}(u_{1,0})$ $u_{1,2} = f_{1,1}(u_{1,1})$
$u_{2,1} = f_{0,2}(u_{2,0})$ $u_{2,2} = f_{2,1}(u_{2,1})$ …

Trace Formula: $\mathrm{TF}^{\leq K}$



satisfied by the values along the trace

Trace Formula of Transition System

Trace (length K)

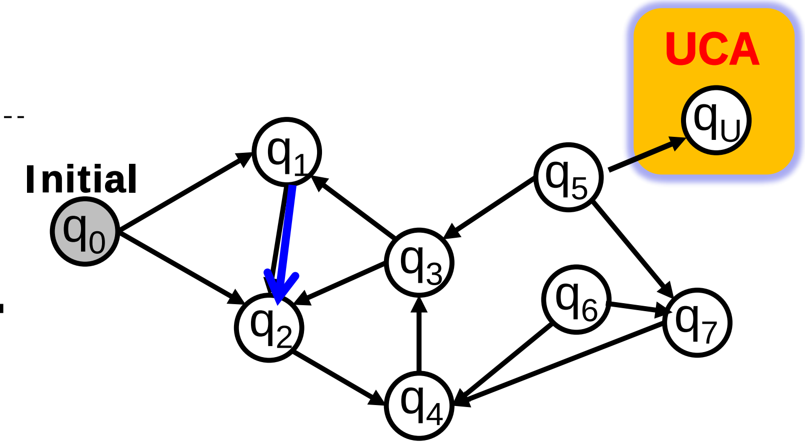
q_0 q_1 … q_K

$$u_{1,0} = v_{1,init} \qquad u_{1,1} = f_{0,1}(u_{1,0}) \qquad u_{1,2} = f_{1,1}(u_{1,1})$$

$$u_{2,0} = v_{2,init} \qquad u_{2,1} = f_{0,2}(u_{2,0}) \qquad u_{2,2} = f_{2,1}(u_{2,1}) \cdots$$

Trace Formula: $\mathrm{TF}^{\leq K}$

satisfied by the values along the trace

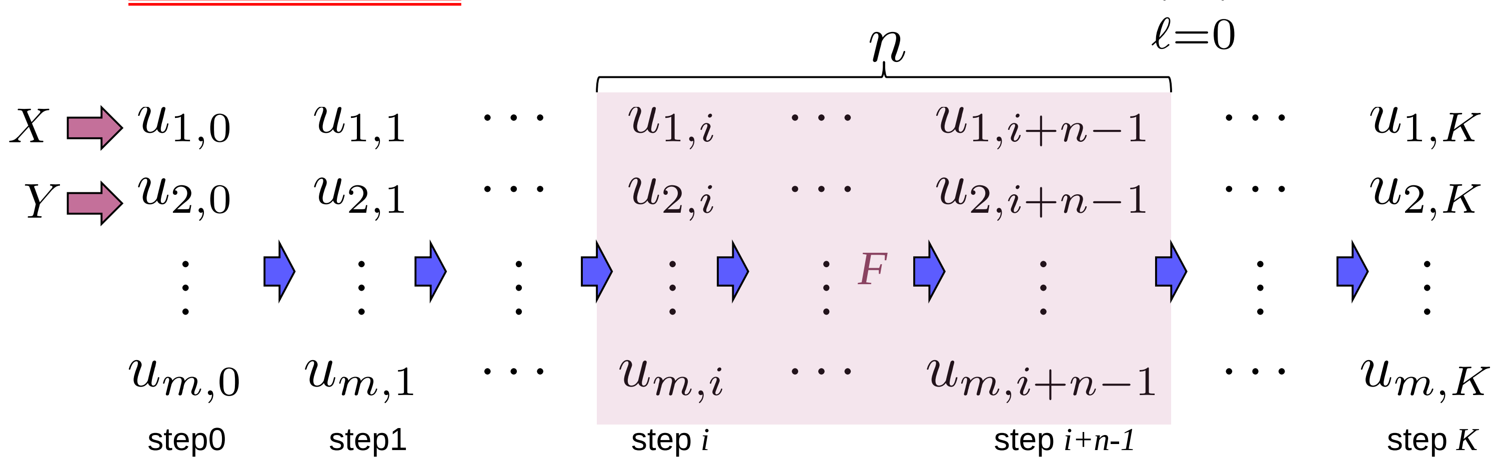


Unsafe Control Actions (UCAs)

- Reachability to hazardous states with unexpected values for a consecutive period of time (not expected in the design).

UCAs as constraint:

$$\underline{\underline{n - UCA_F^{\leq K}}} \equiv \exists i. i \leq K - n + 1 \wedge \left(\bigwedge_{\ell=0}^{n-1} f_{i+\ell-1}(\vec{u}_{i+\ell}) \right)$$



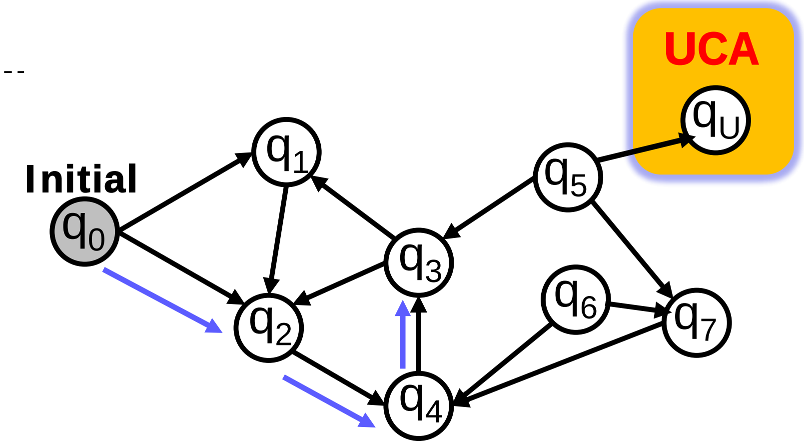
Signal Disturbance

$$q_0 q_2 q_4 q_3$$

$$(u_{1,3}, u_{2,3}) \not\models g_{36}$$

$$u_{1,0} = v_{1,init} \qquad u_{1,3} = f_{4,1}(\vec{u_2})$$

$$u_{2,0} = v_{2,init} \quad \cdots \quad u_{2,3} = f_{4,2}(\vec{u_2})$$



Signal Disturbance

$$q_0 q_2 q_4 q_3 q_6$$

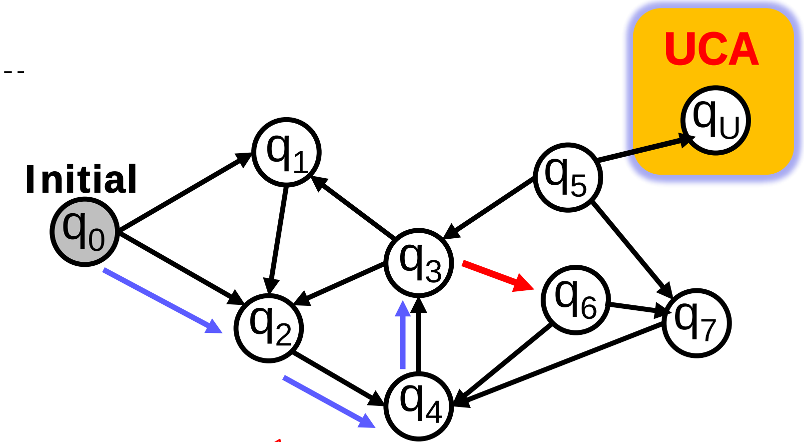
$(u_{1,3}, v_{bad}) \models g_{36}$

$u_{1,0} = v_{1,init}$
$u_{2,0} = v_{2,init}$ …

$u_{1,3} = f_{4,1}(\vec{u_2})$
$u_{2,3} = v_{bad}$

$u_{1,4} = f_{3,1}(u_{1,3}, v_{bad})$
$u_{2,4} = f_{3,2}(u_{1,3}, v_{bad})$

$(u_{1,4}, u_{2,4}) \not\models g_{65}$



$u_{2,3} = v_{bad}$

Accidentally altered

Signal Disturbance

$$q_0 q_2 q_4 q_3 \color{red}{q_6 q_5}$$

$\color{red}{(u_{1,3}, v_{bad}) \models g_{36}}$

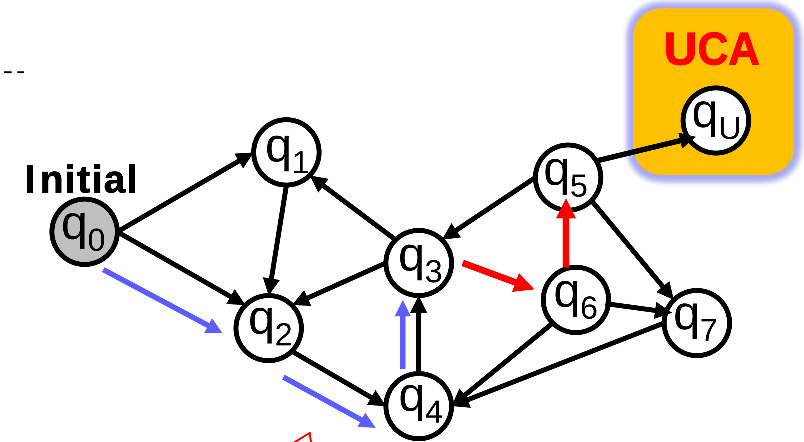
$u_{1,0} = v_{1,init}$ … $u_{1,3} = f_{4,1}(\vec{u_2})$ $\color{red}{u'_{1,4} = v'_{bad}}$

$u_{2,0} = v_{2,init}$ $u_{2,3} = \color{red}{v_{bad}}$ $u_{2,4} = f_{3,2}(u_{1,3}, \color{red}{v_{bad}})$

$\color{red}{(v'_{bad}, u_{2,4}) \models g_{65}}$

$u_{1,5} = f_{6,1}(\color{red}{v'_{bad}}, u_{2,4})$

$u_{2,5} = f_{6,2}(\color{red}{v'_{bad}}, u_{2,4})$



$u_{1,4} = v'_{bad}$

Accidentally altered

Signal Disturbance

$$q_0 q_2 q_4 q_3 q_6 q_5 q_u$$

$(u_{1,3}, v_{bad}) \models g_{36}$

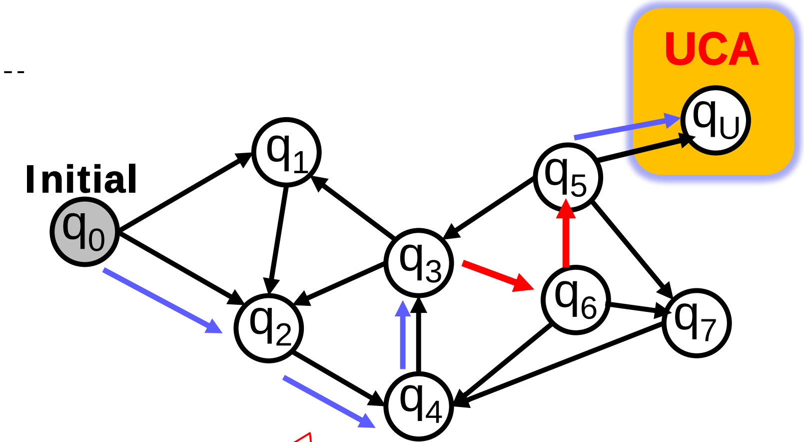
$u_{1,0} = v_{1,init}$ ... $u_{1,3} = f_{4,1}(\vec{u_2})$ $u'_{1,4} = v'_{bad}$

$u_{2,0} = v_{2,init}$ $u_{2,3} = v_{bad}$ $u_{2,4} = f_{3,2}(u_{1,3}, v_{bad})$

$(v'_{bad}, u_{2,4}) \models g_{65}$ $(u_{1,5}, u_{2,5}) \models g_{5u}$

$u_{1,5} = f_{6,1}(v'_{bad}, u_{2,4})$

$u_{2,5} = f_{6,2}(v'_{bad}, u_{2,4})$



$u_{1,4} = v'_{bad}$

Accidentally altered

Disturbed Signal Pattern

Definition of disturbed signal pattern

$$DSP_U(\sigma) = \{u_{i,j} = u'_{i,j} | \sigma(u_{i,j}) \neq \sigma(u'_{i,j}), i \in I, j \leq K\}$$

where

$U = \{u_{i_1}, \cdots, u_{i_m}\}$: Set of variables

σ : Value assignment to variables

I : Time series of variables

K: Trace bound length

$u_{i,j}$: Original variables

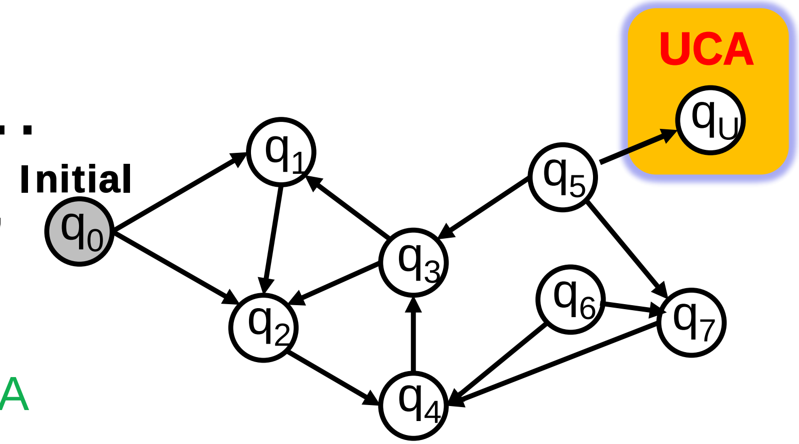
$u'_{i,j}$: Cushion variables

Modified Trace Formula with Cushion Variables

q_0 q_1 … q_K

$$u_{1,0} = v_{1,init} \quad u_{1,1} = f_{0,1}(u_{1,0}) \quad u_{1,2} = f_{1,1}(u_{1,1}) \ldots$$
$$u_{2,0} = v_{2,init} \quad u_{2,1} = f_{0,2}(u_{2,0}) \quad u_{2,2} = f_{2,1}(u_{2,1})$$

$\mathrm{TF}^{\leq K}$



Errors assign deferent values leading to UCA

Introduce "cushion variables $\vec{u}_i'$ ".

Replace variables on RHS with cushion variables.

$$u_{1,0} = v_{1,init} \quad u_{1,1} = f_{1,0}(u'_{1,0}, u'_{2,0}) \quad u_{1,2} = f_{1,1}(u'_{1,1}, u'_{2,1})$$
$$u_{2,0} = v_{2,init} \quad u_{2,1} = f_{2,0}(u'_{1,0}, u'_{2,0}) \quad u_{2,2} = f_{2,1}(u'_{1,1}, u'_{2,1}) \ldots$$

Modified Trace Formula: $\mathrm{TF}'^{\leq K}_{U}$

U: Set of variables disturbed

Disturbed Signal Detection

$\mathrm{TF}'^{\leq K}_{U} \wedge \Omega^{K}_{U} \wedge n\text{-}UCA^{\leq K}_{F}$ is not satisfiable,

where $\Omega^{K}_{U} \equiv \bigwedge_{u_i \in U} \bigwedge_{j \leq K} u_{i,j} = u'_{i,j}$,

($u_{i,j}$: Original variables $u'_{i,j}$: Cushion variables)

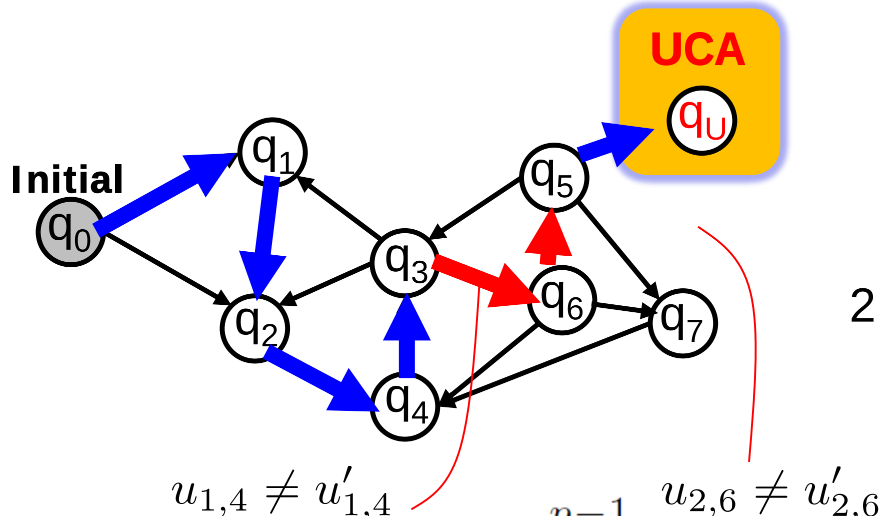
because $\mathrm{TF}'^{\leq K}_{U} \wedge \Omega^{K}_{U} \Leftrightarrow \mathrm{TF}^{\leq K}$.

$\mathrm{TF}'^{\leq K}_{U} \wedge (\Omega^{K}_{U} - DSP_U(\sigma)) \wedge n\text{-}UCA^{\leq K}_{F}$ is satisfiable.

Find a subset of Ω^{K}_{U} to make ϕ satisfiable

Intermittent Signal Disturbance

Signal disturbances occur no more than L times in p execution steps.



$$\Psi \equiv \forall i, j,\ i \in I,\ 1 \leq j \leq K - p + 1.\ \sum_{r=0}^{p-1} R(u_{i,j+r}, u'_{i,j+r}) \leq L$$

where

$$R(u_{i,j}, u'_{i,j}) = \begin{cases} 0 & \text{if } u_{i,j} = u'_{i,j} \\ 1 & \text{if } u_{i,j} \neq u'_{i,j} \end{cases}$$

I : Set of variable indexes of U

U : Set of variables

Constaints with signal disturbance

Trace formula with Cushions

Intermittent constraint

Equality between original and cushion variables

$$\Phi \equiv \mathrm{TF}'^{\leq K}_{U} \wedge n\text{-}UCA^{\leq K}_{F} \wedge \Psi \wedge \Omega^{K}_{U}.$$

Hard [*1] Soft [*2]

*1 : Must be satisfied
*2 : Can be falsified

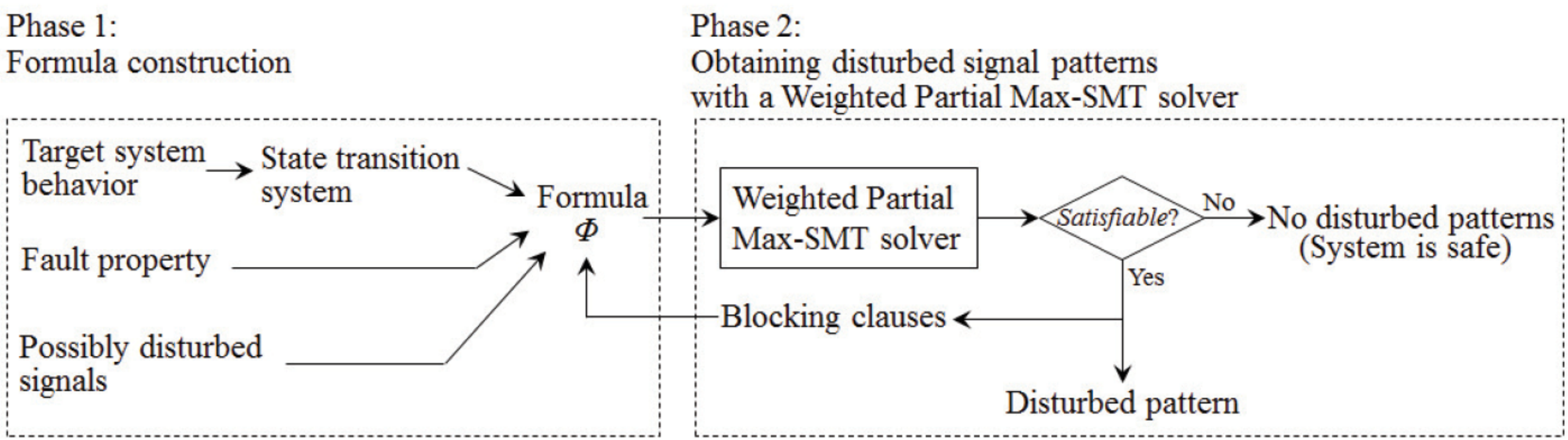
Apply Φ to pMax-SMT solver

Weighted Partial Max-SMT solver finds $\Omega^{K}_{U} - DSP_{U}(\sigma)$ with minimum cost

Cost is heuristically assigned to Ω^{K}_{U}

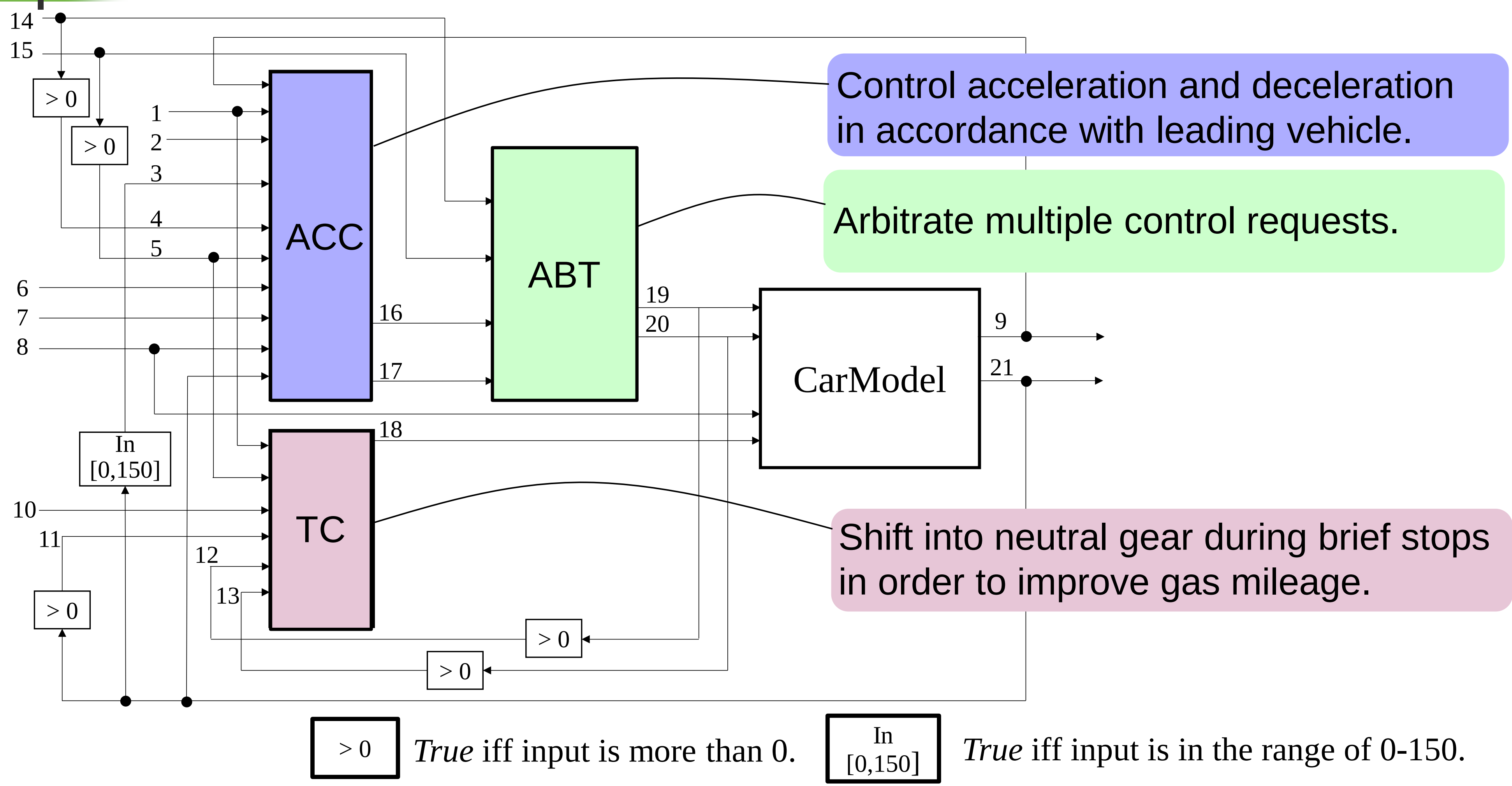
- Uniform
- As soon as possible: bigger costs for bigger step index

Design process overview



Case Study

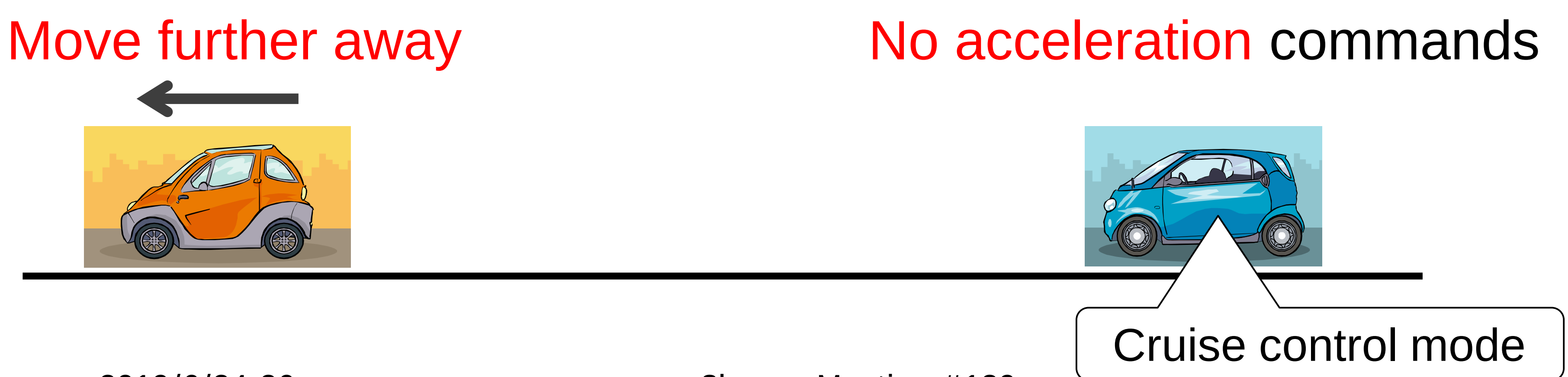
Overview of Simplified Automotive Control System



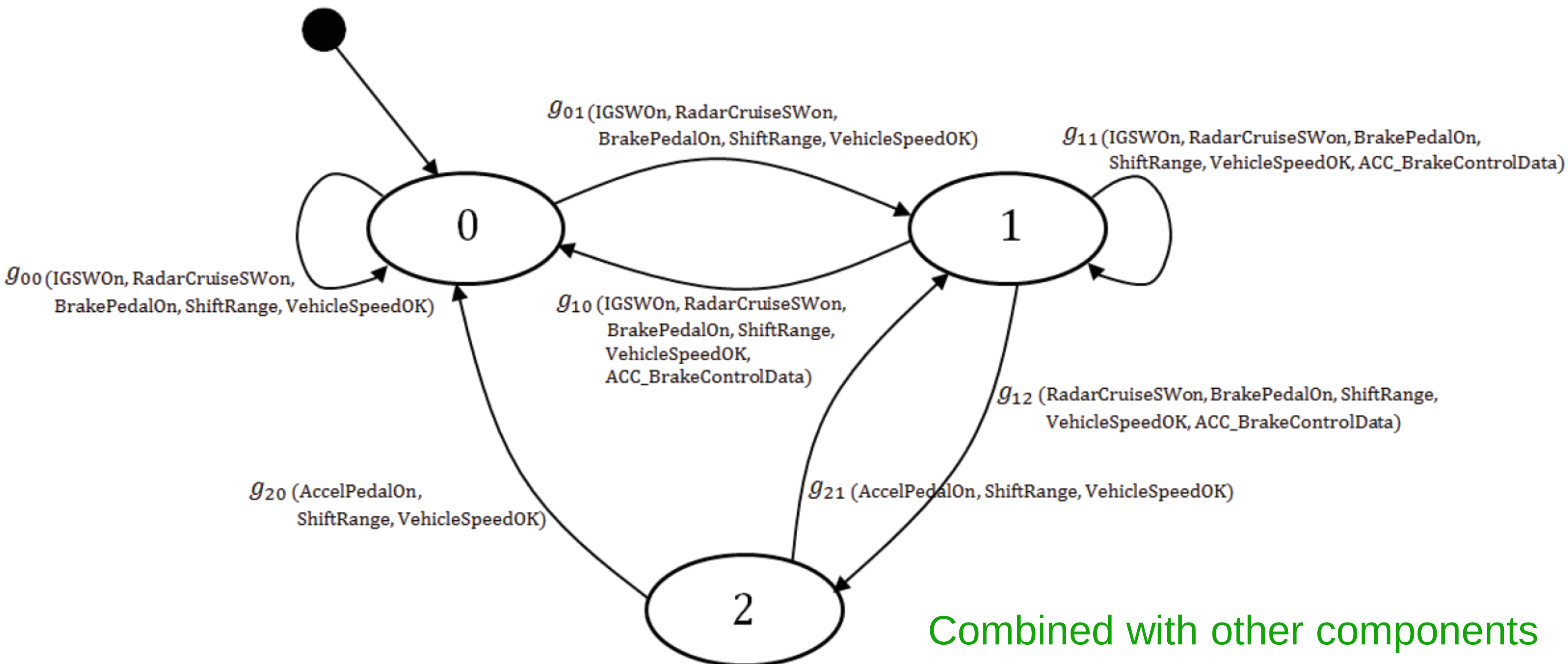
UCA Example

UCA:

Acceleration command is not provided for five consecutive clock cycles in the cruise control mode, even though the leading vehicle moves further away.



LTS (ACC-ECU component)



Combined with other components by shared variables

Derivation of failures

Following STAMP/STPA …

Step 1: Identify Unsafe Control Actions
Step 2: Identify Causes of Unsafe Control Actions

apply our method in Step 2

UCA definition

$$
\begin{aligned}
\text{LeadingVehicleSpeed} &> 0 \wedge \text{Distance} > C_d \\
\wedge \quad & \text{BrakePedal} = 0 \wedge \text{AccelPedal} = 0 \\
\wedge \quad & \text{RadarCruiseSWOn} = \mathit{true} \\
\wedge \quad & \text{ABT\_AccelControlData} = 0.
\end{aligned}
$$

lasts for n-units of time in a row:

$$
\begin{aligned}
n\text{-}UDC_F^{\leq K} \equiv\ & \exists i.1 \leq i \leq K - n + 1 \wedge \\
\textstyle\bigwedge_{r=0}^{n-1} \quad & (LeadingVehicleSpeed^{(i+r)} > 0 \wedge Distance^{(i+r)} > C_d \\
\wedge \quad & BrakePedal^{(i+r)} = 0 \wedge AccelPedal^{(i+r)} = 0 \\
\wedge \quad & RadarCruiseSWOn^{(i+r)} = true \\
\wedge \quad & ABT\_AccelControlData^{(i+r)} = 0).
\end{aligned}
$$

Result (1/2)

Signal names in each pattern

Signal Names	
ShiftRange	*VehicleSpeed*
RadarCruiseSW	*VehicleSpeed*
VehicleSpeedOK	*VehicleSpeed*
BrakePedalOn	*VehicleSpeed*

Example of obtained pattern

t	*VehicleSpeed*		*ShiftRange*	
	Normal Value	Disturbed Result	Normal Value	Disturbed Result
1	0	0	4	4
2	0	151	4	4
3	0	0	4	4
4	0	0	4	3
5	0	0	4	4

disturbed

Result (2/2)

Disturbed patterns under the condition *VehicleSpeed* is not disturbed. (Number of disturbed signals = 3)

Signal names in each pattern

RadarCruiseSW	*LeadingVehicleSpeed*	*ACC_AccelControlData*
RadarCruiseSW	*ShiftRange*	*LeadingVehicleSpeed*
ShiftRange	*LeadingVehicleSpeed*	*ACC_AccelControlData*
RadarCruiseSW	*VehicleSpeedOK*	*LeadingVehicleSpeed*
VehicleSpeedOK	*LeadingVehicleSpeed*	*ACC_AccelControlData*
RadarCruiseSW	*BrakePedalOn*	*LeadingVehicleSpeed*
VehicleSpeedOK	*ShiftRange*	*LeadingVehicleSpeed*
VehicleSpeedOK	*BrakePedalOn*	*LeadingVehicleSpeed*
BrakePedalOn	*LeadingVehicleSpeed*	*ACC_AccelControlData*
BrakePedalOn	*ShiftRange*	*LeadingVehicleSpeed*

Example of obtained pattern

t	*RadarCruiseSW*		*LeadingVehicleSpeed*		*ACC_AccelControlData*	
	Normal Value	Disturbed Result	Normal Value	Disturbed Result	Normal Value	Disturbed Result
1	on	on	30	30	0	0
2	on	on	60	−21	0	0
3	on	off	90	90	0	0
4	on	on	90	90	0	0
5	on	on	120	120	280	−1

disturbed

Result (2/2)

Disturbed patterns under the condition *VehicleSpeed* is not disturbed. (Number of disturbed signals = 3)

Signal names in each pattern

RadarCruiseSW	*LeadingVehicleSpeed*	*ACC_AccelControlData*
RadarCruiseSW	*ShiftRange*	*LeadingVehicleSpeed*
ShiftRange	*LeadingVehicleSpeed*	*ACC_AccelControlData*
RadarCruiseSW	*VehicleSpeedOK*	*LeadingVehicleSpeed*
VehicleSpeedOK	*LeadingVehicleSpeed*	*ACC_AccelControlData*
RadarCruiseSW	*BrakePedalOn*	*LeadingVehicleSpeed*
VehicleSpeedOK	*ShiftRange*	*LeadingVehicleSpeed*
VehicleSpeedOK	*BrakePedalOn*	*LeadingVehicleSpeed*
BrakePedalOn	*LeadingVehicleSpeed*	*ACC_AccelControlData*
BrakePedalOn	*ShiftRange*	*LeadingVehicleSpeed*

Example of obtained pattern

t	*RadarCruiseSW*		*LeadingVehicleSpeed*		*ACC_AccelControlData*	
	Normal Value	Disturbed Result	Normal Value	Disturbed Result	Normal Value	Disturbed Result
1	on	on	30	30	0	0
2	on	on	60	−21	0	0
3	on	off	90	90	0	0
4	on	on	90	90	0	0
5	on	on	120	120	280	−1

disturbed

Concluding remarks

- Faulty behavior caused by (intermittent) signal disturbance, in an automotive control system using Weighted Partial Max-SMT solvers.
  - Trace formulae with cushion variables.
  - Constraints for intermittent disturbance .
- Case study on a simplifed automotive control system
- Finding clues to point out which signals are essential to avoid failures.