Fault Analysis and Design Trade-Offs in Networked Cyber Physical Systems: A Formal Methods-Based Approach

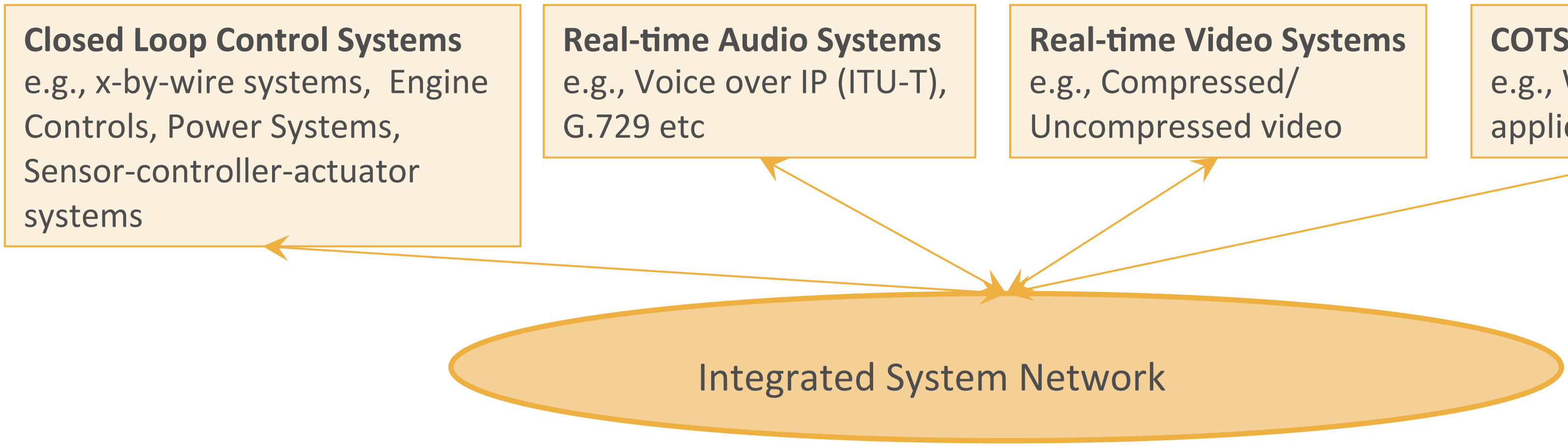
1st International Workshop on Reliable Cyber Physical Systems
Irvine, October 8th, 2012

Grit Denker, Daniel Elenius, Carolyn Talcott
SRI International
Gene Zhijing Qin, Nalini Venkatasubramanian
University of California Irvine

Overview

- Objective of Formal-Method Based Analysis
- Analyzed Network Types
  - Multinetworks
  - Time-Triggered Ethernet
- Summary

Objective: Integrated Fault and Performance Analysis



Integrating CPS subsystems with varying criticality levels and varying fault-tolerance and performance requirements over a common network

Design and Verification Objectives:

- Performance (latency, jitter, bandwidth) requirements of each application are met
- Fault tolerance requirements for each subsystem are met in presence of failure of network/ host components
- Expose emergent behavior that may invalidate system assumptions and requirements

"Co-optimization" with verification proofs over general space of architecture is intractable

Our approach: Analysis for selected points in architecture space or selected network configurations to gain insights into tradeoffs

Multinetworks

Objective:
Use up-to-date network state info to model and analyze network configurations

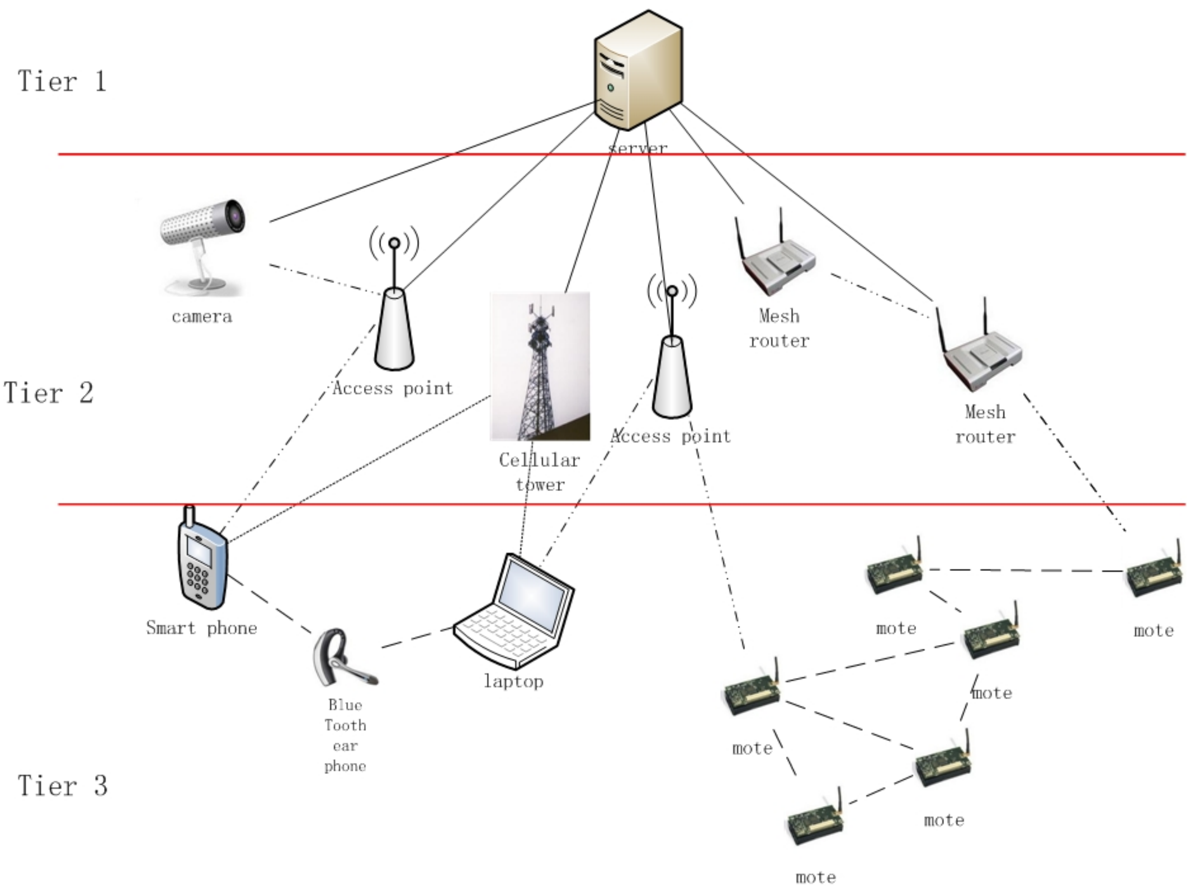
Approach:
Perform formal “What If?” analysis on network model

Benefits:
Insights from analysis provides guidance for network administrator

Multinetwork Information Architecture (MINA)

Centralized DB holds the network state information collected from devices and links

(Luca Iannario, Gene Qin et al, UC Irvine)



What If Analysis

- Which flow will be affected if node is down? **(Node Criticality Index)**
- What happens if load of selected flows is changed?
- What happens if link quality changes (e.g., congestion, interference)?

Node Criticality Index

For each network node

- Assume node goes down
- Reroute all flows
- Analyze QoS parameters of affected flows

Use node criticality index to decide use of network resources in reconfigurations so that likelihood of application requirement satisfaction will increase

Compare with conventional approaches

Conventional Approaches

Node Centrality
- Node degree
- Closeness-based (find center)
- Betweenness (check shortest path/flow load passed through)

Hypothesis: Centrality-Based Techniques not suitable for dynamic and heterogenous networks

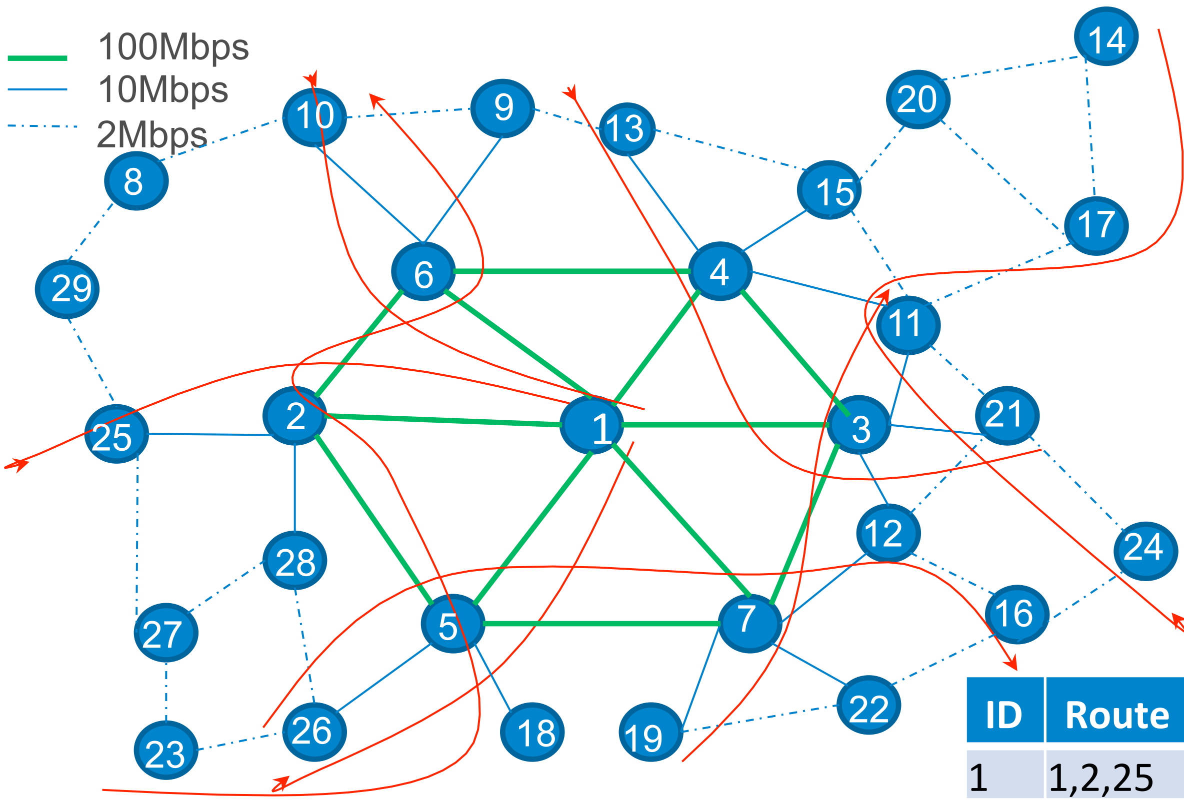
Backup and Reconfiguration Planning
- Work-load based backup
- Load balanced-based reconfiguration

Hypothesis: These approaches do not exploit impacts across redistributed flows

Network Planning and Simulator-Based Approaches

Hypothesis: More time consuming than high-level formal model

Experiment – Backup Nodes: Setup



- Constant bit rate applications to describe flows
- Analyze end-to-end QoS parameter for each flow, assuming one node down
- Do analysis for every node

- Reroute affected nodes using Dijkstra algorithm
- Compute impact of failing node on delay of flows
- Compare critical node index with centrality index

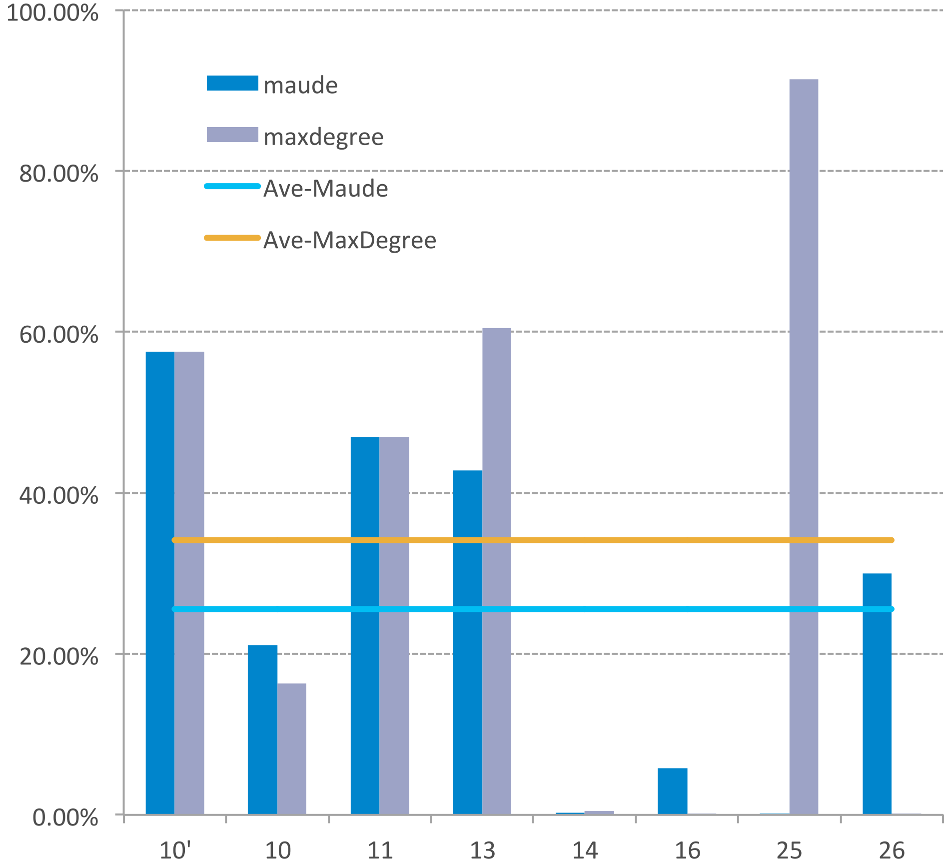
ID	Route	Type	TP	Length	Num
1	1,2,25	1	0.8	0.0016	500
2	1,5,26	1	0.8	0.002	400
3	19,7,3,11	1	0.8	0.0016	500
4	21,3,4,13	1	0.48	0.0016	300
5	1,6,10	2	0.48	0.0016	300
6	24,21,11,17,14	2	0.4	0.002	200
7	23,26,5,2,6,10	2	0.4	0.002	200
8	26,5,7,12,16	2	0.24	0.0008	300

Experiment I – Backup Nodes: Results

Importance Ranking

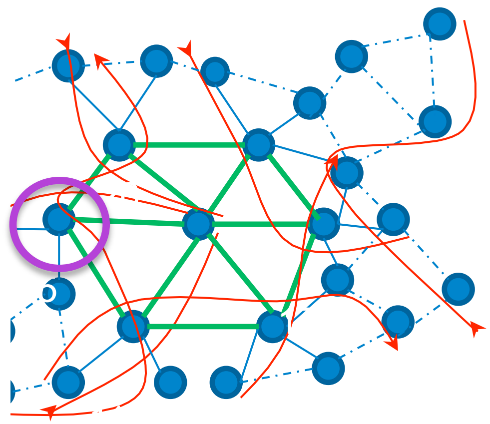
Criticality	Degree & Load
3	5
2	3
7	7
4	4
6	2
5	6

Assume limited backup resources
Choose backup node using criticality or centrality
-> backed up nodes won't fail
Let other nodes (not src/dest of flows) fail for 300ms, and determine overall impact on delay of all flows

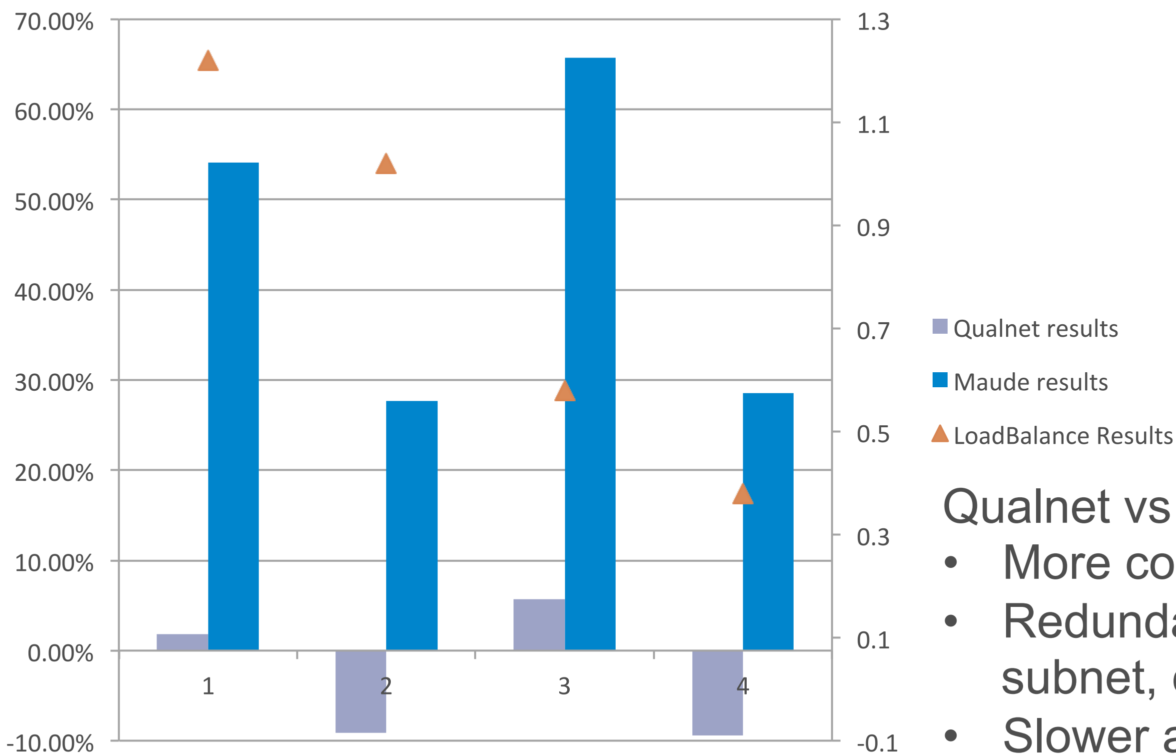


Experiment II – NW Reconfiguration

- Node 2 is down
- Nodes 25 & 26 can re-associate to either node 5 or 6
- Simulate four possible new configurations to rank them
- Compare rankings with Qualnet ranking



NW Config	Avg Delay Increase	Rank
NW1	54.0502%	3
NW2	27.6939%	1
NW3	65.6767%	4
NW4	28.5294%	2



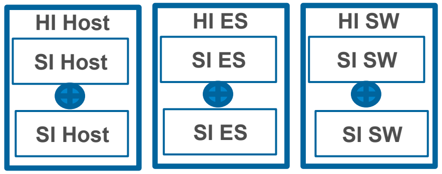
NW Config.	Load Difference	Rank
NW1	1.22	4
NW2	1.02	3
NW3	0.58	2
NW4	0.38	1

Qualnet vs Formal Method

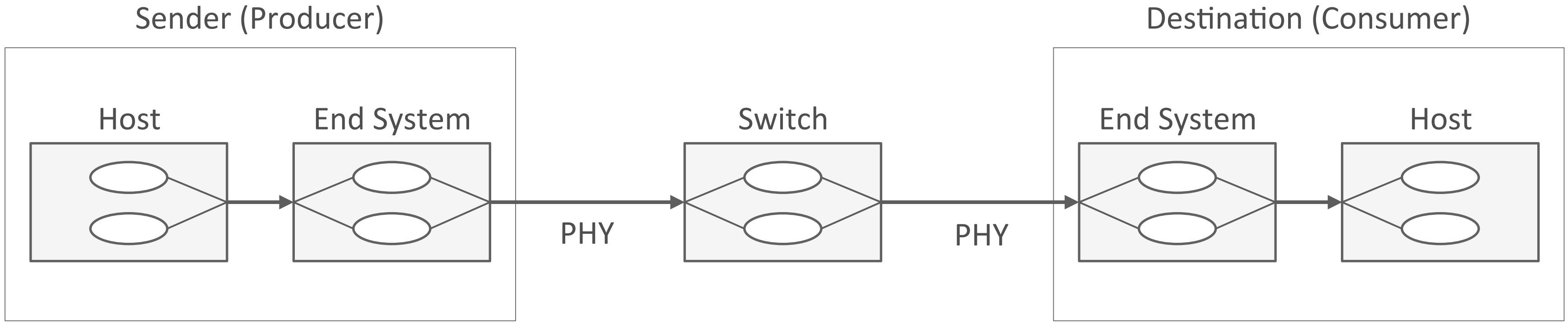
- More complex configuration, less reuse
- Redundant operations: e.g. setup subnet, configure ip, etc.
- Slower at runtime

Time Triggered Ethernet (TTEthernet)

- Used in safety-critical, real-time CPS such as aircrafts and automobiles
- Has three message types: Time-triggered, rate-constrained and best-effort
- Three types of components: Host, End System (ES), Switch (SW)
  - Each has Tx (transmit) and Rx (Receive) functionality
  - Each as standard (SI) and high (HI) integrity
    - HI with duplicated processing between Rx and Tx
- Achieves fault tolerance via high integrity and path and system redundancy: But how much is sufficient and necessary?



Legend:
SI: Standard Integrity
HI: High Integrity
SW: Switch
ES: End System
: High Integrity Check



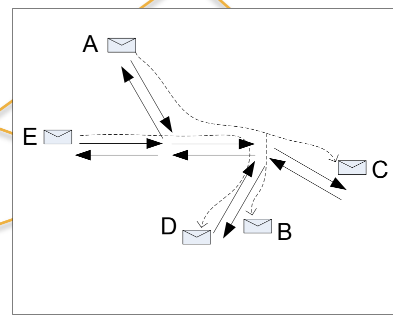
If **path redundancy**, every **dataflow** is broken into 2 or 3 **channels** with disjoint **physical links**

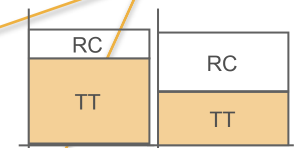
Network Architecture Tradeoff Analysis Tool Chain

System and Traffic Inputs
- **Applications**
- **Traffic Profiles**
- **System Level Requirements**

Network Architectural Choices
- **Topology**
- **Integrity**
- **Availability**

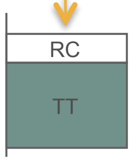
Architecture Specific Choices
- **Synchronization**
- **Mixed Mode Traffic Classes**





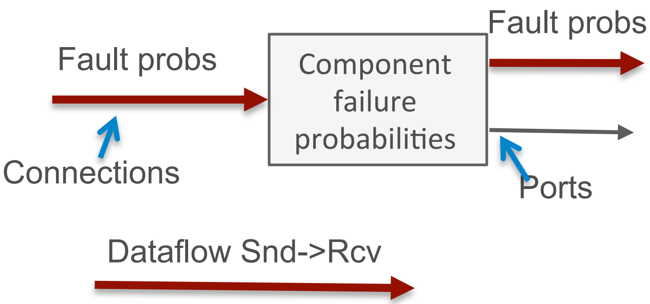
Performance Fault Free Analysis Tools
- RC: Check feasibility
  - end-to-end latency/utilization/ buffer size
- TT: Check schedulability

Probabilistic Fault Analysis Tool
- Check Fault Tolerance Properties

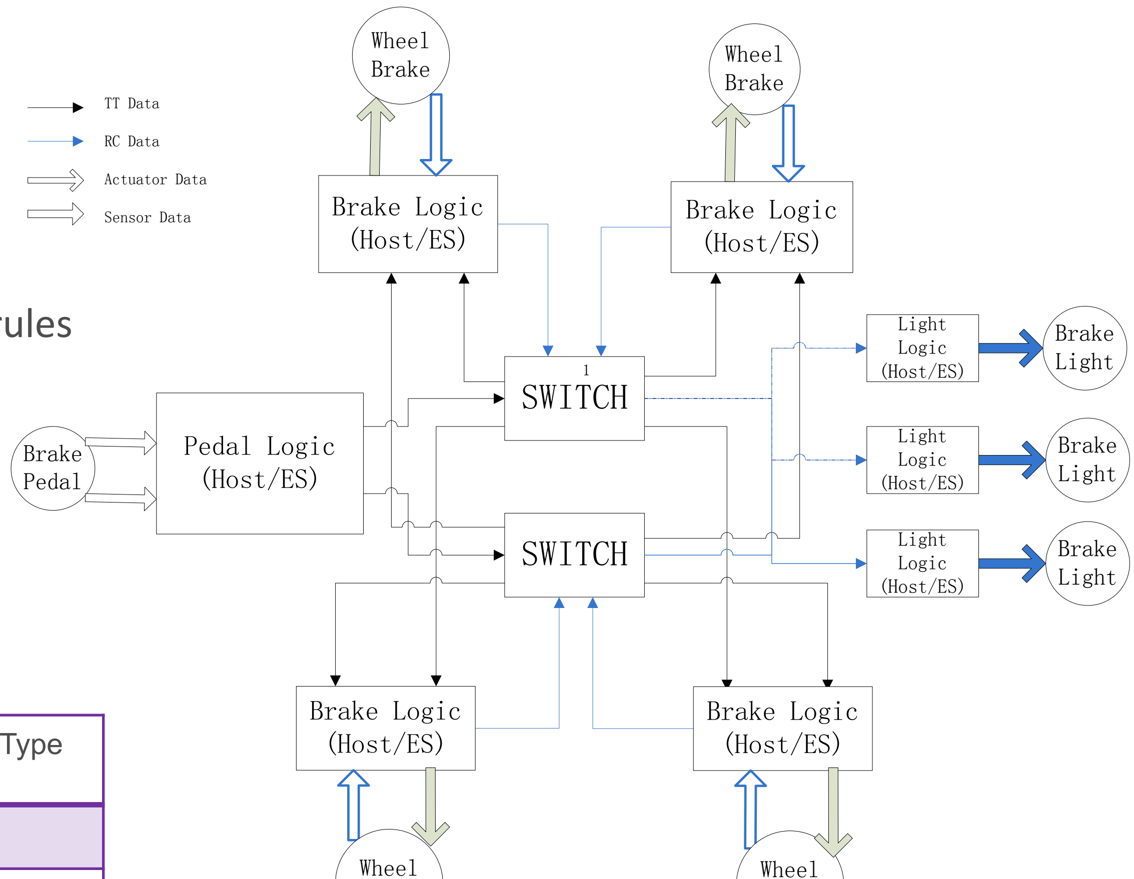


Architecture	Fault Probabilities	TT Schedule	RC Latency
HI, TT only, 75% load on nw	(1e-4,0,…,1e-18)	Yes	n/a
HI, TT only, 90% load on nw	(1e-4,0,…,1e-18)	No	n/a
HI/SI, TT/RC, 90% load on nw	(1e-4,0,…,1e-18)	Yes	VL1<x, VL2<y
SI, TT only, 50% load on nw	(1e-2,1e-3, …)	…	…

Brake-by-Wire Fault Analysis and Performance Checks



Analyzed Faults: silent, omission, commission, invalid fields, untimely



Generic fault propagation/introduction rules

OMout := OMin or ESFail
COMout := COMin or ESFail
VSAout := VSAin or ESFail
…
VFCSout := ESFail
TEout := TEin or ESFail
TLout := TEout or ESFail

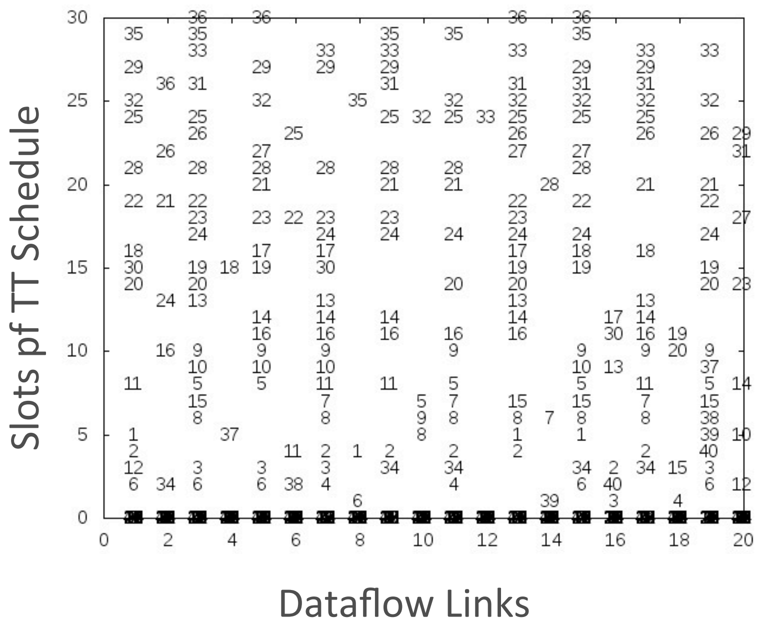
VL	Sender	Receiver	Traffic Type
1	Pedal Logic	Brake Logic 1,2,3,4	TT
2	Brake Logic 1	Motor Logic	TT
6	Brake Logic 1	Light Logic 1,2,3,4	RC
10	Light Logic 1	Display Logic	BE

Safety Requirements

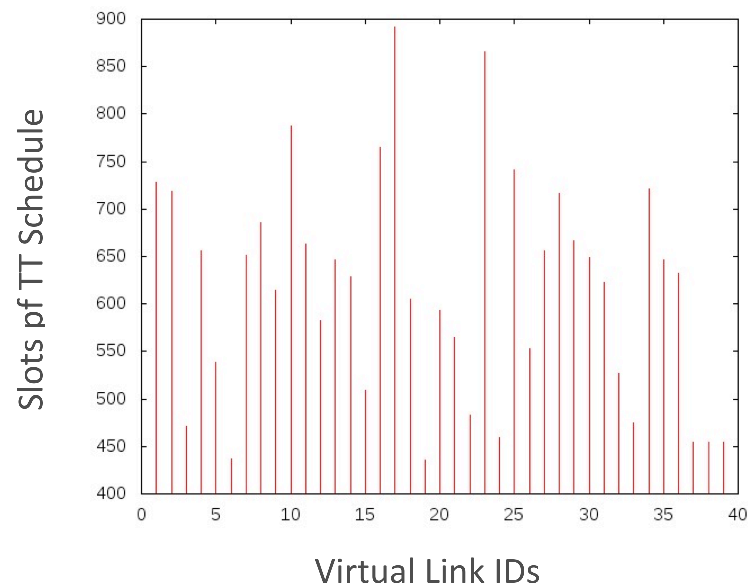
- If the brake pedal is engaged, brake at each wheel
- If wheel brake is engaged, illuminate brake lights
- If wheel brake is engaged, close throttle at motor
- If brake light doesn't work, show warning in driver display

BBW Schedulability, Utility and Fault Results

TT Schedule with 35 additional Frames



Approximate the end-to-end latency for given topology



Arch	VL ID	Fault Probabilities
All HI	1	OM: 1.3e-4, COM: 0, VSA: 0, VDA: 0, VSN: 0, VLEN: 0, VDATA: 1.0e-8, VFCS: 1.0E-10, TE: 0, TL: 0
All SI	1	OM: 1.3e-4, COM: 1.0e-5, VDA: 1.0e-5, VSN: 0, VLEN1.0e-5, VDATA: 2.001E-5, VFCS 1.0e-5, TE: 1.0e-5, TL:1.0e-5

Summary

- Formal what-if analysis
  - Is suitable for analyzing faults in heterogeneous networks
  - Can account for impact across flows
- Co-optimization of fault tolerance and performance with verification proofs over general space of architecture is intractable
- Tradeoff analysis for selected points in design space is feasible
- Integration of latency, utilization, buffer size and fault tolerance analysis is scalable to vehicle-sized network architectures

Support architecture design or network configuration choices through formal methods-based analysis