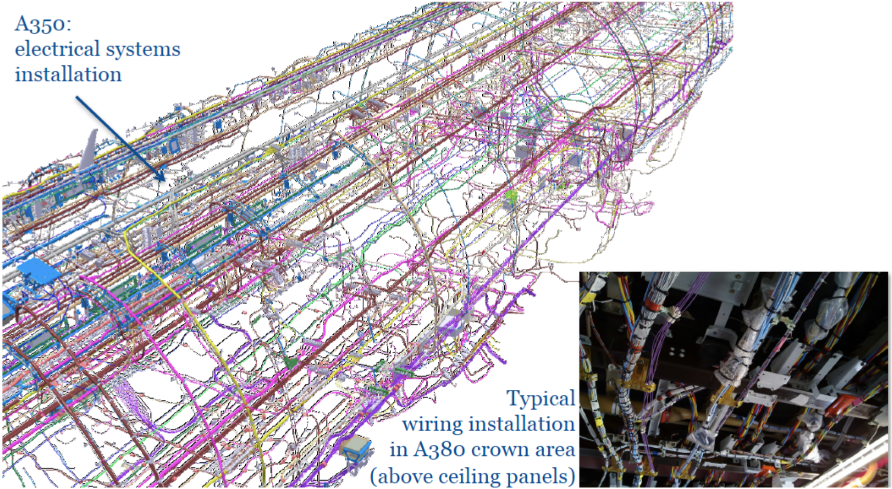
A Case Study in Safety, Security, and Availability of Wireless-Enabled Aircraft Communication Networks

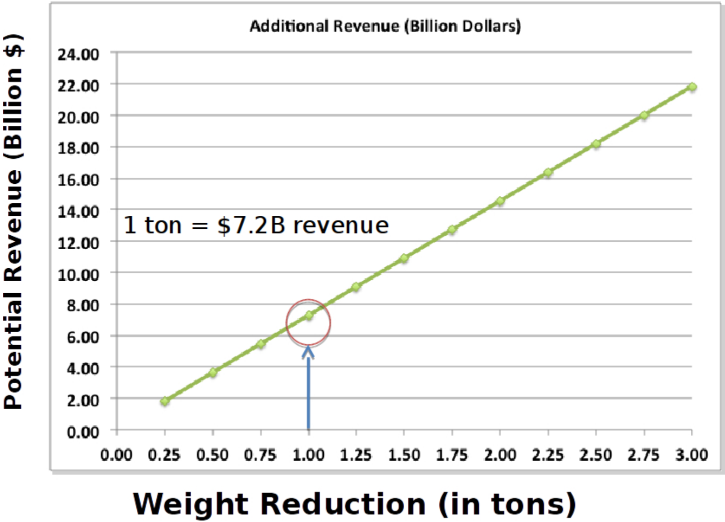
Rohit Dureja, Eric W.D. Rozier, and **Kristin Yvonne Rozier**
Iowa State University

http://laboratory.temporallogic.org
June 5, 2017



A380-800 has about 100,000 wires, 470 km long, 5700kg of weight
+ additional 30% weight for wiring harnesses

Cost of Aircraft Weight



The War on Wiring!

- 1984 Boeing 767: 140km wiring → Boeing 787: 500km wiring
- Prediction: shed 1,800kg wiring:
  1. non-avionics controls & health management
  2. safety systems, sensors, avionics
  3. communications, commands for fly-by-wire
- WAIC: Wireless Avionics Intra-Communications

Wired → Wireless

Wireless Network Trade-offs

- Scale
- Cost
- Setup
- Maintenance
- Weight
- Reconfigurability

- Security
- Complexity

Bottom Line: Wired-Wireless Hybrid Networks are the Future

Wired → Wireless

Wireless Network Trade-offs

- Scale
- Cost
- Setup
- Maintenance
- Weight
- Reconfigurability

- Security
- Complexity

Bottom Line: Wired-Wireless Hybrid Networks are the Future

...So how do we do that?

Hybrid Networks That Can Be Flight-Certified

Need:

- Comparative analysis of network configurations:
    - with respect to requirements
    - with respect to fault tolerance
- Validation across system models
- Analysis of different network protocols
- Reliability and trustworthiness of wireless communication

Requirements:

"The new wireless networks needs to be at least as safe, and secure, as the existing wired network."

Hybrid Networks That Can Be Flight-Certified

Need:

- Comparative analysis of network configurations:
  - with respect to requirements
  - with respect to fault tolerance
- Validation across system models
- Analysis of different network protocols starting with ZigBee
- Reliability and trustworthiness of wireless communication

Requirements:

"The new wireless networks needs to be at least as safe, and secure, as the existing wired network."

Hybrid Networks That Can Be Flight-Certified

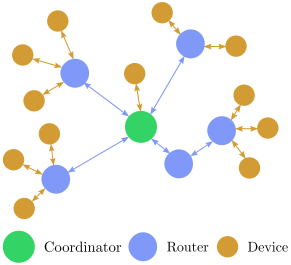
Need:

- Comparative analysis of network configurations:
  - with respect to requirements
  - with respect to fault tolerance
- Validation across system models
- Analysis of different network protocols starting with ZigBee
- Reliability and trustworthiness of wireless communication by extension to ZigBee

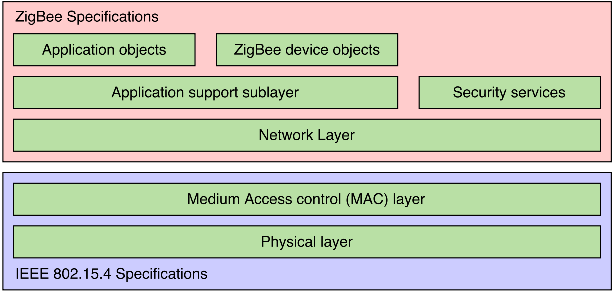
Requirements:

"The new wireless networks needs to be at least as safe, and secure, as the existing wired network."

System Model: ZigBee Wireless Communication Protocol



(a)

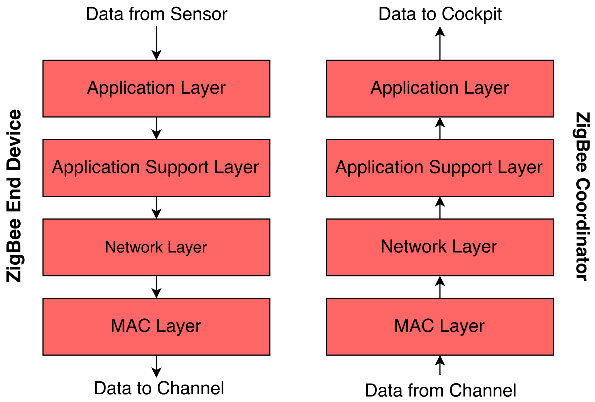


(b)

(a) Mesh topology of ZigBee networks
(b) Layered architecture of the ZigBee 802.15.4 protocol stack

Requirements for Analysis

Abstracted, layered ZigBee communication network model:
data flows across layers



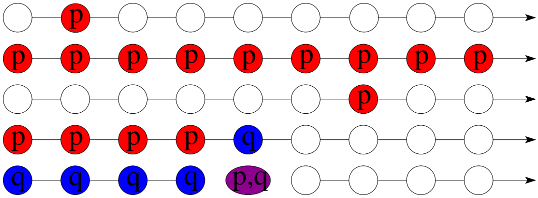
Sending data now → data reaches target within time-bound, uncorrupted

A Natural Logic for Operational Timelines: Linear Temporal Logic

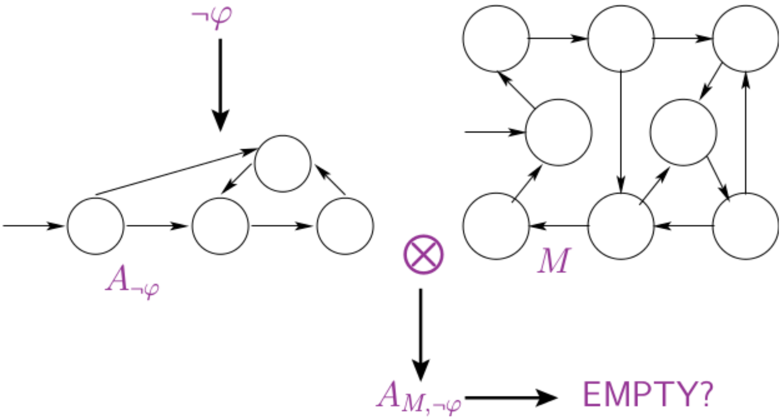
Linear Temporal Logic (LTL) formulas reason about linear timelines:

- finite set of atomic propositions $\{p\ q\}$
- Boolean connectives: $\neg$, $\wedge$, $\vee$, and $\rightarrow$
- temporal connectives:

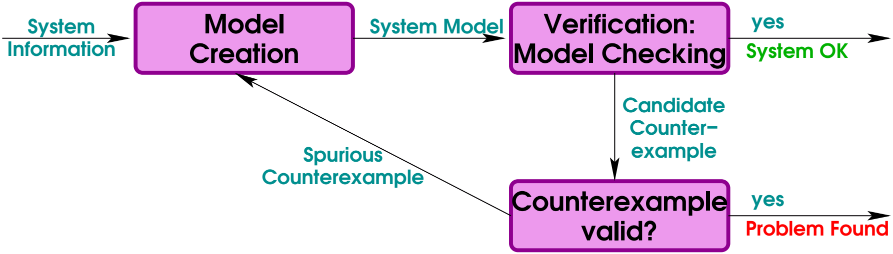
$\mathcal{X}p$	NEXT TIME
$\Box p$	ALWAYS
$\Diamond p$	EVENTUALLY
$p\mathcal{U}q$	UNTIL
$p\mathcal{R}q$	RELEASE



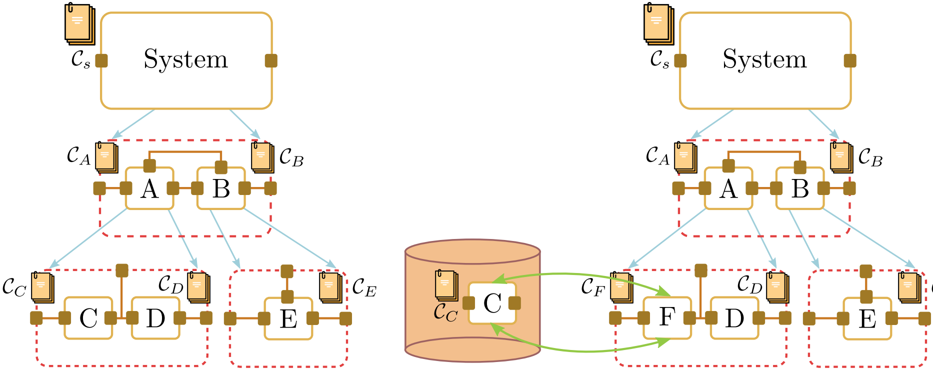
Automata-Theoretic Approach to Model Checking



Model Checking Process: Nominal Case Analysis

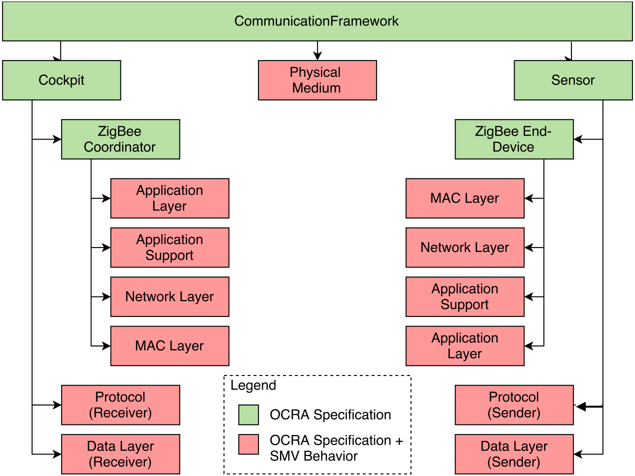


Compositional, Contract-Based Models



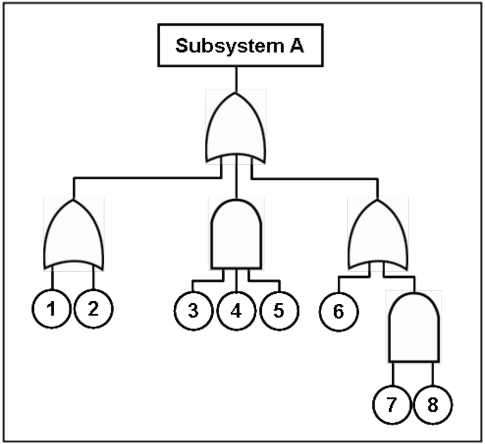
Contract based design allows easy re-use of components from a library provided the contracts of the swapped components are the same.

Extensible System Model: Wired/Wireless



Nominal framework model for the ZigBee wireless communication system

Differentiating Passing Models with Fault Trees



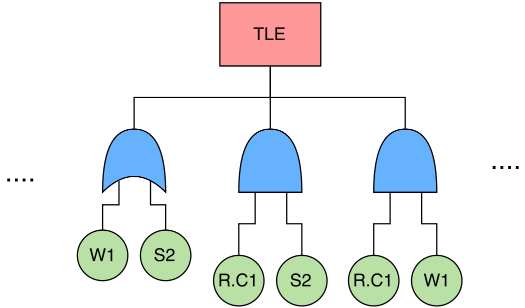
Model Checking Pass → Fault Annotations → Fault Tree Analysis

Adding Faults: Wired Network Components

Faults associated with wired network analyzed (S: sensor, R: cockpit)

Fault	Description	Mode	Authority
W1	Physical medium breaks	Permanent	Physical Medium
C1	Error recovery mechanism fails	Transient	Protocol (S/R)
S2	Sensor fails	Permanent	Data Layer (S)

Fault Tree/Minimal Cut Sets: Extended Wired System



CutSets = ({W1, S2, R.C1, S2, R.C1, W1}, {W1, R.C1, S2, R.C1, W1}, {S2, R.C1, S2, R.C1, W1}, W1, S2, {R.C1, S2}, {R.C1, W1} . . .)

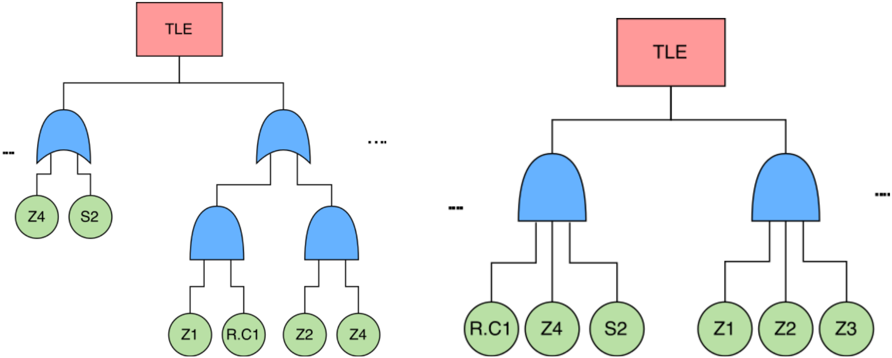
Min Cut Set = (W1, S2, {R.C1, S2}, {R.C1, W1})

Adding Faults: Wireless Network Components

Faults associated with wired network analyzed (S: sensor, R: cockpit)

Fault	Description	Mode	Authority
Z1	Signal interference	Transient	Physical Medium
Z2	End-Device not discoverable	Transient	Network Layer (S)
Z3	Coordinator cannot accept new connections	Transient	Network Layer (R)
Z4	Coordinator fails to set up network	Permanent	Application Layer (R)
C1	Error recovery mechanism fails	Transient	Protocol (S/R)
S2	Sensor fails	Permanent	Data Layer (S)

Fault Trees/Minimal Cut Sets: Extended Hybrid Network

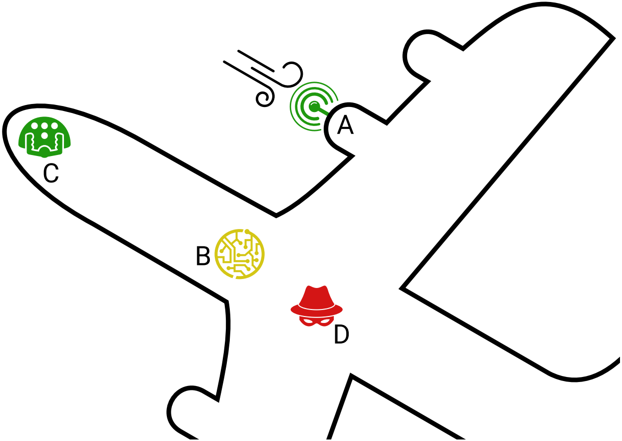


(a) Sample fault tree 1

(b) Sample fault tree 2

Fault trees using minimal cut sets for the extended wired system.

Need to Avoid Accidental & Intentional Interference

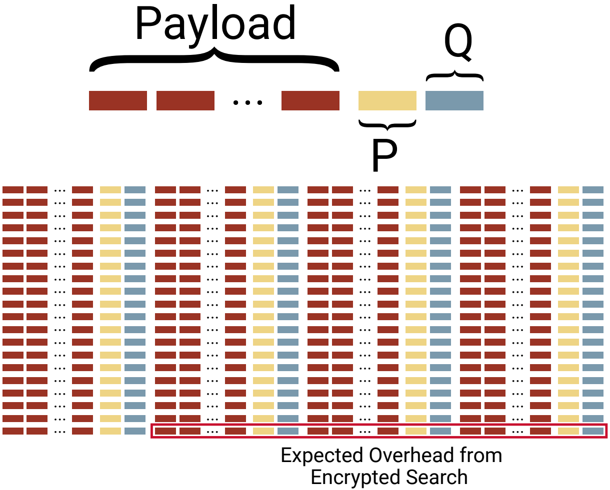


Pitot Tube (A) transmitting to Cockpit (C) by relay through (B), avoiding spoofing (D)

Octets	1	0/1	0/2	0/2	0/2	0/1	1	Variable
	Frame Control	Destination Endpoint	Group Address	Cluster Identifier	Profile Identifier	Source Endpoint	APS Counter	Frame Payload

Octets	1	0/1	Variable
	Payload Index	Payload Size	Frame Payload

Modified format of ZigBee packet as part of a burst.



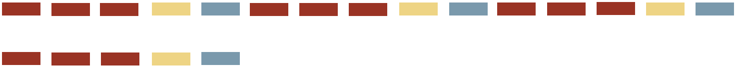
Anatomy of a file transmitted using secure, and reliable, packet bursts

Original Data

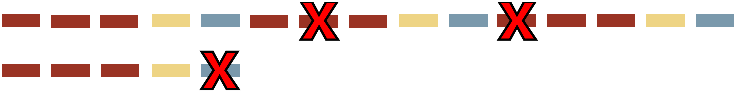
Data Chunked into Zigbee Packets

Packets Divided into Bursts of Size 3

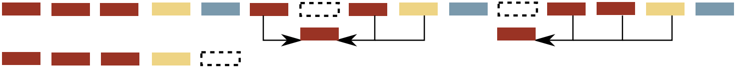
XOR Syndromes Computed for Bursts



Galois Field Syndromes Computed for Bursts

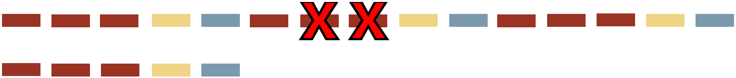


Block Losses During Transmission

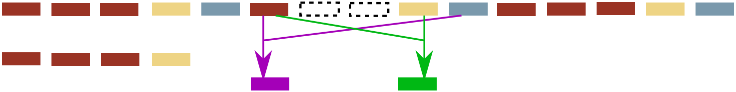


XOR Recomputation

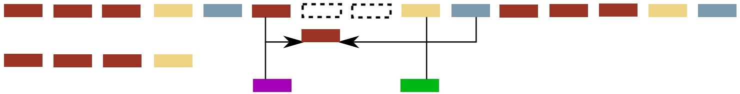
Galois Field Recomputation



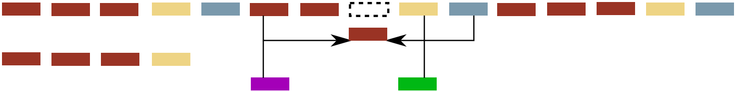
Double Packet Loss from a Single Burst



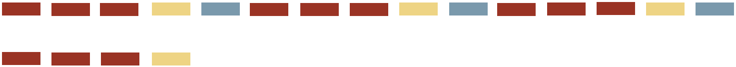
Galois Field Recomputation



Galois Field Recomputation

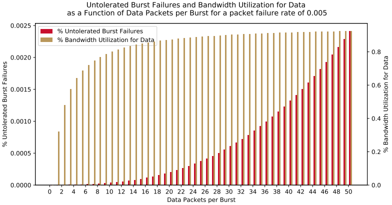


Galois Field Recomputation

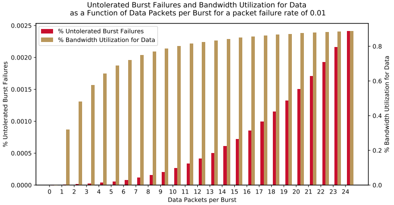


Restored Original Dataset

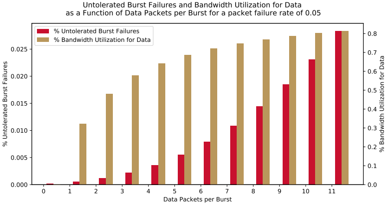
Impact of Burst Size on Failures & Bandwidth Utilization



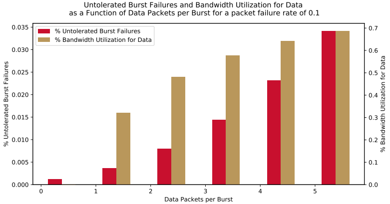
(a) Per Packet Failure Rate $\mu = 0.005$



(b) Per Packet Failure Rate $\mu = 0.01$



(c) Per Packet Failure Rate $\mu = 0.05$



(d) Per Packet Failure Rate $\mu = 0.1$

Summary[1]

Contributions:

- Proof of concept
  - Comparative analysis of multiple hybrid network models
  - Nominal and fault analysis
  - Extensible framework: plug-and-play, COTS-compatible
- ZigBee security extension
- Trade-off exploration
  - Adaptive burst configuration

Future Work:

- Quantitative failure probability assessment
- Common Cause Analysis (CCA)
- Adding more wireless communication protocols

[1] Thanks to NASA's Efficient Reconfigurable Cockpit Design and Fleet Operations using Software Intensive, Networked and Wireless Enabled Architecture (ECON) Grant NNX15AQ84G for supporting this work.