

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



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

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

イロト 不得 トイヨト イヨト



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

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

Motivation	Safety	Security	Availability
000000			

Cost of Aircraft Weight



IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

æ

IOWA STATE

Laboratory for UNIVERSITY Temporal Logic Safety

GAIAA.

Security

The War on Wiring!

Ballder a better microscope kill, induity work the diameter AEROSPA War on wiring smart TV doesn't need data so why do airliners need tons of them? Meet the researchers who don't think they do. -

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

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

< ロ > < 回 > < 回 > < 回 > < 回 >

Motivation	Safety	Security	Availability
0000000			

Wired \rightarrow Wireless

Wireless Network Trade-offs

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

- Security
- Complexity

Bottom Line: Wired-Wireless Hybrid Networks are the Future

イロト 不得下 イヨト イヨト

э

Motivation	Safety	Security	Availability
0000000			

Wired \rightarrow 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?

イロト イポト イヨト イヨト

Wireless-Enabled Aircraft Communication Networks

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:

aboratory for

IOWA STAT

UNIVERSITY Temporal Logic

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

イロト イポト イヨト イヨト

э

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:

aboratory for

IOWA STAT

UNIVERSITY Temporal Logic

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

イロト 不得 トイヨト イヨト

3

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:

Laboratory for

IOWA STAT

UNIVERSITY Temporal Logic

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

イロト イヨト イヨト イヨト

э.

Motivation	Safety	Security	Availability
0000000			

System Model: ZigBee Wireless Communication Protocol



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

IOWA STATE Laboratory for UNIVERSITY Temporal Logic イロン イヨン イヨン -

Motivation	Safety	Security	Availability
000000			

Requirements for Analysis

Abstracted, layered ZigBee communication network model:

data flows across layers



Sending data now \rightarrow data reaches target within time-bound, uncorrupted

IOWA STATE Laboratory for UNIVERSITY Temporal Logic ・ 同 ト ・ ヨ ト ・ ヨ ト

Motivation	Safety ●००००००००	Security 0000	Availability
A Natural Log	ic for Operational	Timelines:	
		Linear Tem	noral Logic

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

- finite set of atomic propositions $\{p \ q\}$
- \bullet Boolean connectives: $\neg,$ $\wedge,$ $\lor,$ 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



Wireless-Enabled Aircraft Communication Networks

イロト イポト イヨト イヨト

Motivation	Safety	Security	Availability
	00000000		

Automata-Theoretic Approach to Model Checking



IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

Motivation	Safety	Security	Availability
	00000000		

Model Checking Process: Nominal Case Analysis





Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

イロト イポト イヨト イヨト

э

Motivation	Safety	Security	Availability
000000	00000000	0000	

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.

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

イロト イポト イヨト イヨト

Motivation	Safety	Security	Availability
	00000000		

Extensible System Model: Wired/Wireless



Nominal framework model for the ZigBee wireless communication system

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Motivation	Safety	Security	Availability
	000000000		

Differentiating Passing Models with Fault Trees



Model Checking Pass \rightarrow Fault Annotations \rightarrow Fault Tree Analysis

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

イロト イポト イヨト イヨト

Motivation	Safety	Security	Availability
	0000000000		

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)

イロト イヨト イヨト イヨト

э

Motivation	Safety	Security	Availability
0000000	0000000000	0000	

Fault Tree/Minimal Cut Sets: Extended Wired System



 $\begin{aligned} \mathsf{CutSets} &= (\{\mathsf{W1}, \mathsf{S2}, \mathsf{R.C1}, \mathsf{S2}, \mathsf{R.C1}, \mathsf{W1}\}, \{\mathsf{W1}, \mathsf{R.C1}, \mathsf{S2}, \mathsf{R.C1}, \mathsf{W1}\}, \\ &\{\mathsf{S2}, \mathsf{R.C1}, \mathsf{S2}, \mathsf{R.C1}, \mathsf{W1}\}, \mathsf{W1}, \mathsf{S2}, \{\mathsf{R.C1}, \mathsf{S2}\}, \{\mathsf{R.C1}, \mathsf{W1}\} \ldots) \end{aligned}$

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

< ロ > < 同 > < 回 > < 回 > .

Motivation	Safety	Security	Availability
	000000000		

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)
73	Coordinator cannot accept new	not accept new Transient	Network Layer
25	connections		(R)
74	Coordinator fails to set up network	Permanent	Application Layer
24			(R)
C1	Error recovery mechanism fails	Transient	Protocol
			(S/R)
s a	Sensor fails	Pormanant	Data Layer
52		remanent	(S)
			INVENJEN E DOG

Motivation	Safety	Security	Availability
0000000	00000000	0000	

Fault Trees/Minimal Cut Sets: Extended Hybrid Network



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

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

イロト イヨト イヨト イヨト

э

Motivation 0000000	Safety 0000000000	Security ●000	Availability
Need to Avoid	Accidental &	Intentional Interferen	ice
C			

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

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks



Modified format of ZigBee packet as part of a burst.

イロト イポト イヨト イヨト

0000000	Safety	oo€o	00
	Payload 	Q	
	Expected	Overhead from	
Anator	Encryp my of a file transmitted using s	ecure, and reliable,	packet bursts
		< D > < B > <	ミト・ミト ヨー わへで

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Motivation	Safety	Security	Availability
		0000	

Original Data

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

メロト メタトメモトメモト

= 990

Motivation	Safety 000000000	Security 000●	Availability



Data Chunked into Zigbee Packets

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

メロト メタト メヨト メヨト

Ξ.

Motivation	Safety 000000000	Security ○○○●	Availability

Packets Divided into Bursts of Size 3

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

メロト メロト メヨト メヨト

Motivation	Safety 000000000	Security ○○○●	Availability





XOR Syndromes Computed for Bursts

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

< ロ > < 回 > < 回 > < 回 > < 回 >

Ξ.

Motivation 0000000	Safety 000000000	Security ○○○●	Availability

Galois Field Syndromes Computed for Bursts

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

イロト イポト イヨト イヨト

Ξ.

Motivation 0000000	Safety 000000000	Security ○○○●	Availability



IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

イロト イヨト イヨト イヨト

Motivation	Safety 000000000	Security ○○○●	Availability



XOR Recomputation



Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

メロト スポト メヨト メヨト

Ξ.

Motivation	Safety	Security	Availability
		0000	



IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

メロト メタト メヨト メヨト

æ

Motivation	Safety 000000000	Security ○○○●	Availability



Double Packet Loss from a Single Burst

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

・ロ・・ (日・・ (日・・)

Motivation	Safety 000000000	Security ○○○●	Availability



IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

イロト イヨト イヨト イ

Motivation	Safety 000000000	Security ○○○●	Availability
<u> </u>			





Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

イロト イヨト イヨト イ

Motivation	Safety 000000000	Security ○○○●	Availability





Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

メロト メロト メヨトメ

Motivation 0000000	Safety 000000000	Security ○○○●	Availability

Restored Original Dataset

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier Wireless-Enabled Aircraft Communication Networks

メロト メロト メヨト メヨト

= 990

Motivation	Safety	Security	Availability	
			•0	

Impact of Burst Size on Failures & Bandwidth Utilization



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



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

Untolerated Burst Failures and Bandwidth Utilization for Data as a Function of Data Packets per Burst for a packet failure rate of 0.01



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



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

イロト イポト イヨト イヨト

IOWA STATE Laboratory for UNIVERSITY Temporal Logic

Kristin Yvonne Rozier

Wireless-Enabled Aircraft Communication Networks

Motivation	Safety	Security	Availability
			00

Summary¹

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

¹Thanks 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. $\langle \mathcal{O} \rangle \rightarrow \langle 0 \rangle \rightarrow$