Air Force Institute of Technology

MIL-STD-1553 Characterization using Existing Interface Functionality

John M. Willis
Robert F. Mills
Logan O. Mailloux
Scott R. Graham

Outline

- Purpose of research
- Motivation
- Methodology
- Results
- Conclusions
- Future research
- Questions

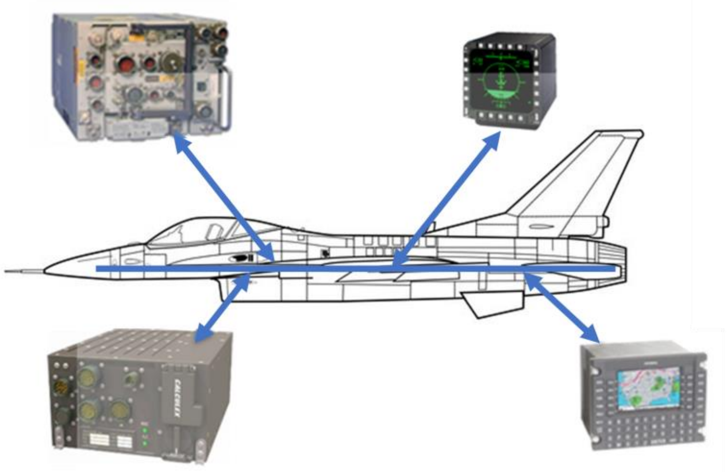
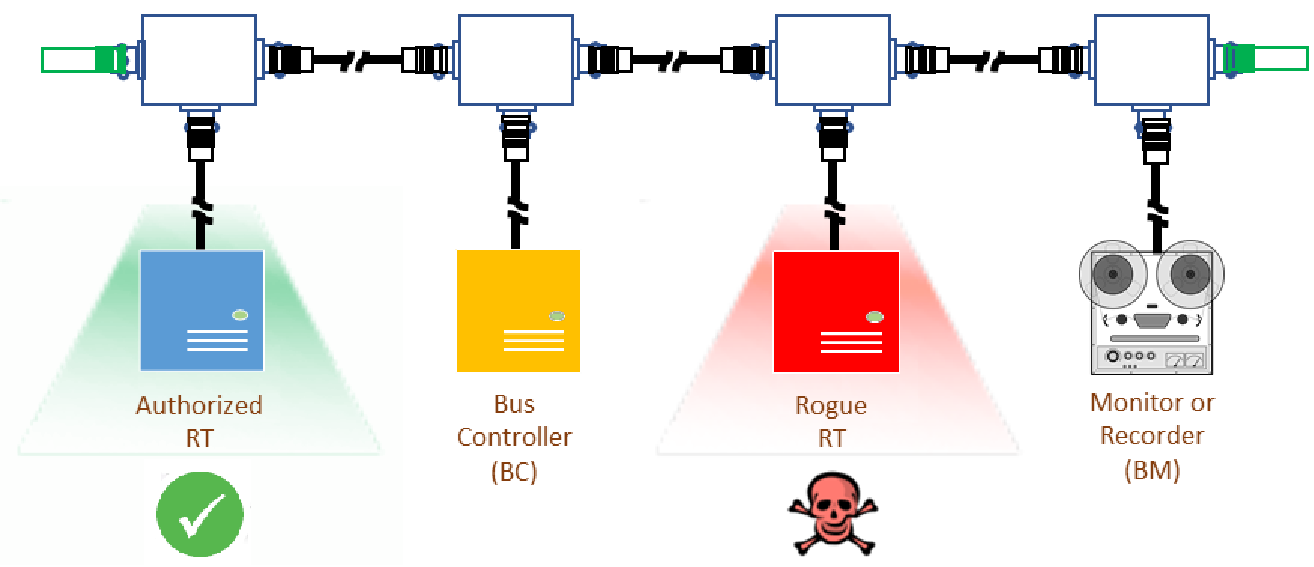


Image Modified from SudsySutherland under Creative Commons: https://sudsysutherland.deviantart.com/art/F-16-Fighting-Falcon-124505343

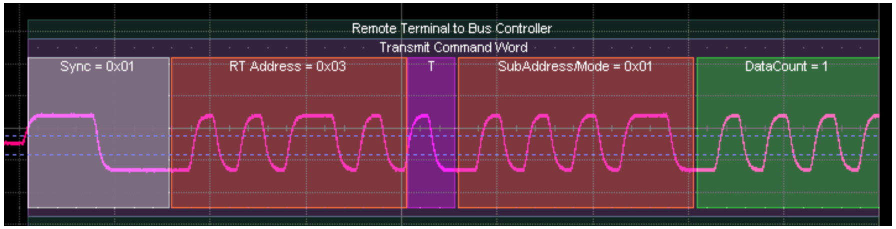
Purpose

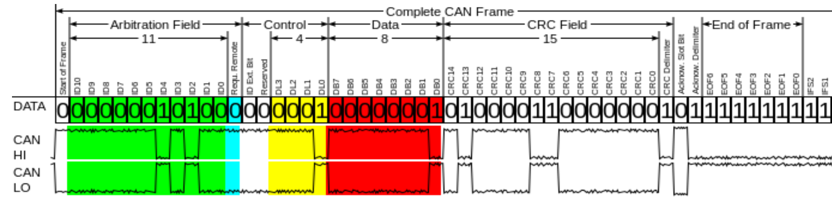
- **Objective: Detect rogue devices without additional size, weight and power (SWAP) requirements**

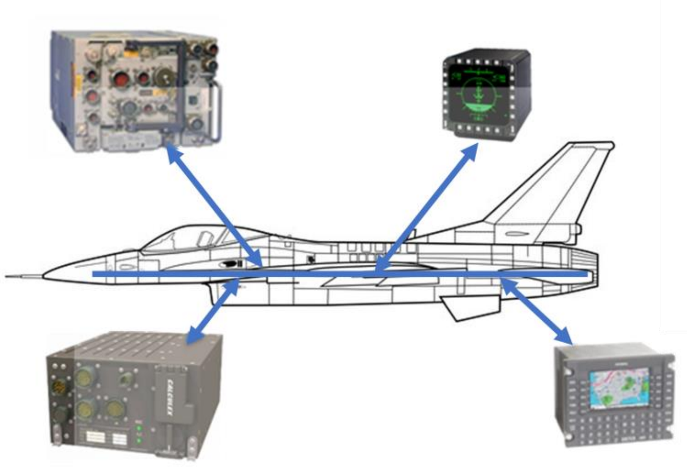
- **Research Questions:**
  - What capability exists on current 1553 devices for characterization?
  - Can they be used for device characterization & discrimination?
  - What limitations exist with using the built-in technology?

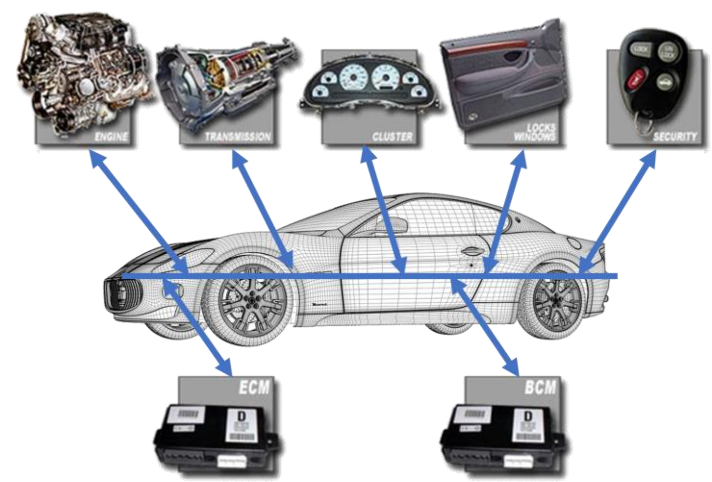


Motivation









MIL-STD-1553 avionics data bus

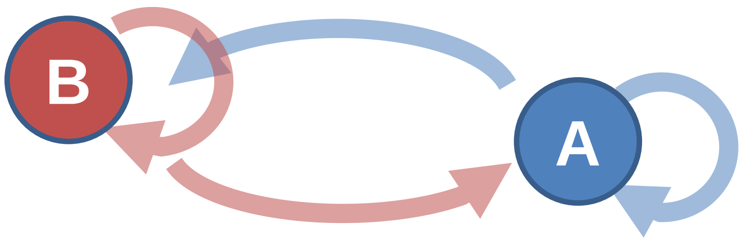
- Ubiquitous military standard
- Developed 1973 SAE
- Broadcast capable, bit stuffing, TDMA
- Equivalent technologies

Controller Area Network (CAN) bus

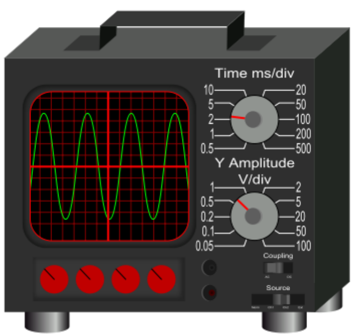
- Ubiquitous Industry Standard
- Developed 1983 SAE
- Broadcast capable, bit stuffing, TDMA
- Proven / demonstrated vulnerabilities

Current Research/Limitations

- **Markov chains to create an IDS based on periodicity**
  - Good for picking up anomalous sequences but not for detecting a rogue.



- **Wired Signal Distinct Native Attributes (WS-DNA) fingerprinting**
  - Fingerprinting the sync portion of 1553 messages to discriminate between multiple devices
  - Sophisticated equipment required – no clear path for transition and implementation
  - Difficulty in updating for new devices



[Lop1] Lopez, Temple, Mullins "Exploitation of HART Wired Signal Distinct Native Attribute (WS-DNA) Features to Verify Field Device Identity and Infer Operating State, C.G. Panayiotou et al. (Eds.): CRITIS 2014, LNCS 8985, pp. 24–30, 2016.

Oscilloscope Image Courtesy of Wikimedia Commons.

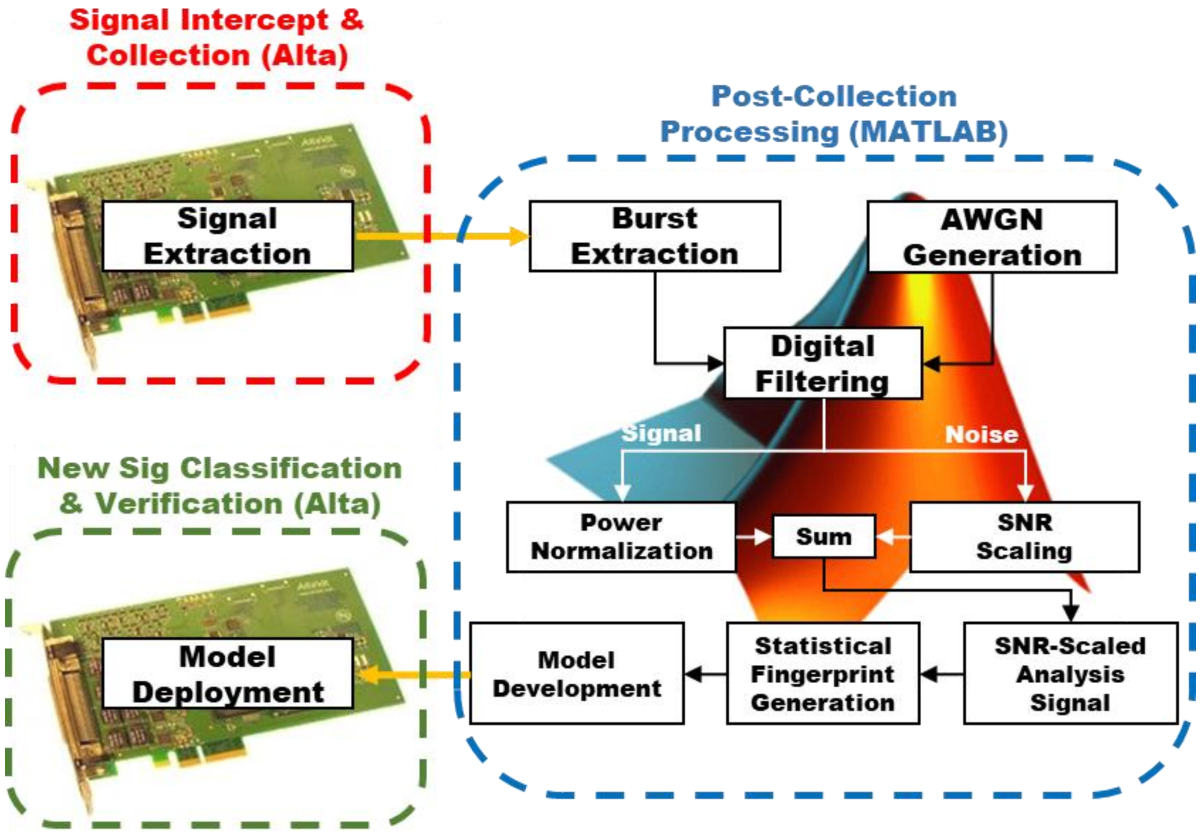
Methodology

WS-DNA = Wired Signal Distinct Native Attribute Fingerprinting

- Well-established method for device discrimination at the physical layer

Leverage native capability in commercial 1553 devices

- Signal collection/extraction
- Device classification and verification
- Updatability
- Equipment Agnostic



[Lop2] Lopez, Liefer, Busho, Temple, “Enhancing CIKR Level-0 PHY Process Security Using Field Device DNA Features,” IEEE Trans on Info Forensics & Security, Vol. 13, No. 5, pp. 1215-1229, May 2018.

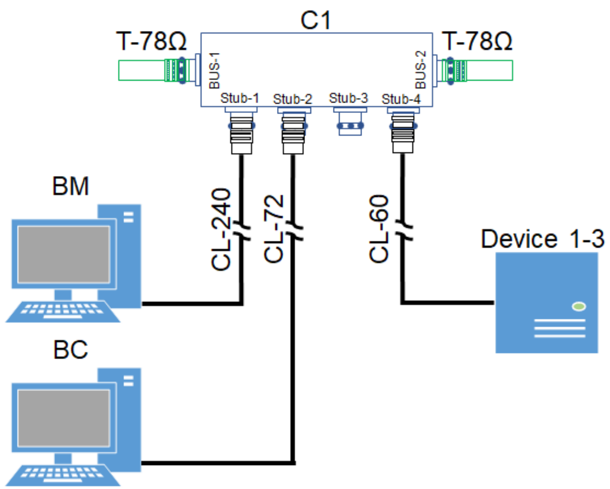
Methodology

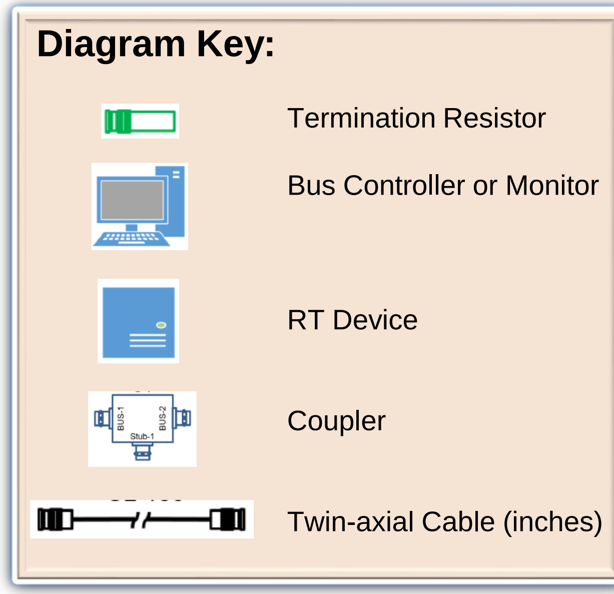
- **Two baseline configurations used:**
  - Simple bus with no cabling and only one coupler connecting the bus controller, bus monitor, and a remote terminal
  - 150 foot bus more representative of what would be found on an aircraft or ship

- **In each configuration, three LRUs (line replaceable units) were used**
  - Train classifier using data collects using LRUs in a variety of bus locations
  - After model has been developed, assess ability to accurately classify signals as coming from a specific LRU
  - Assess ability to recognize if a device is not one that is expected

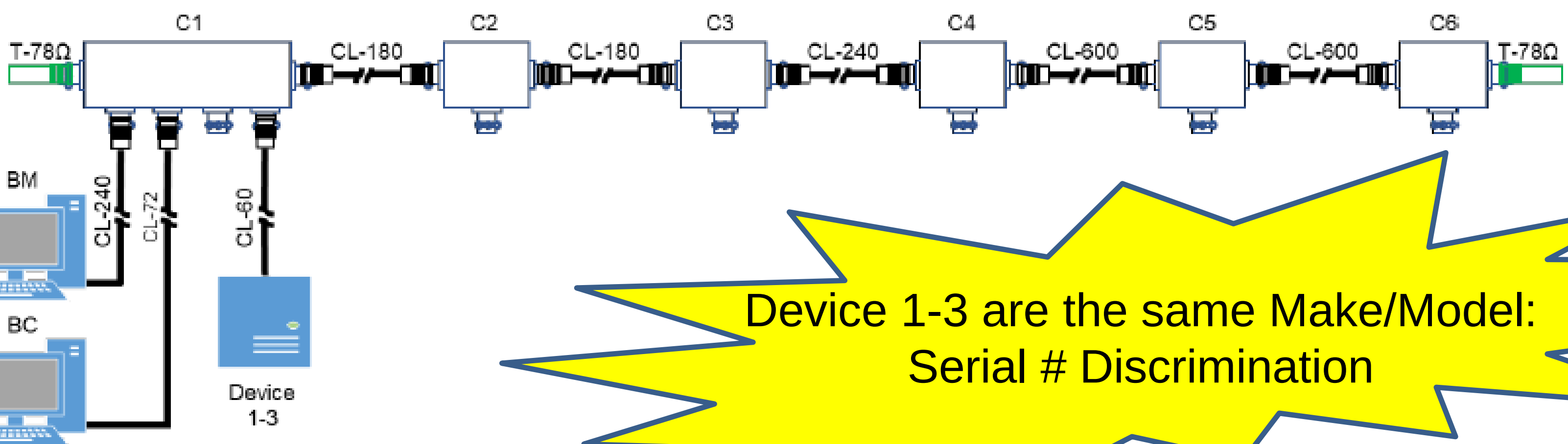
Baseline Configurations

Configuration 1: Proof of Concept





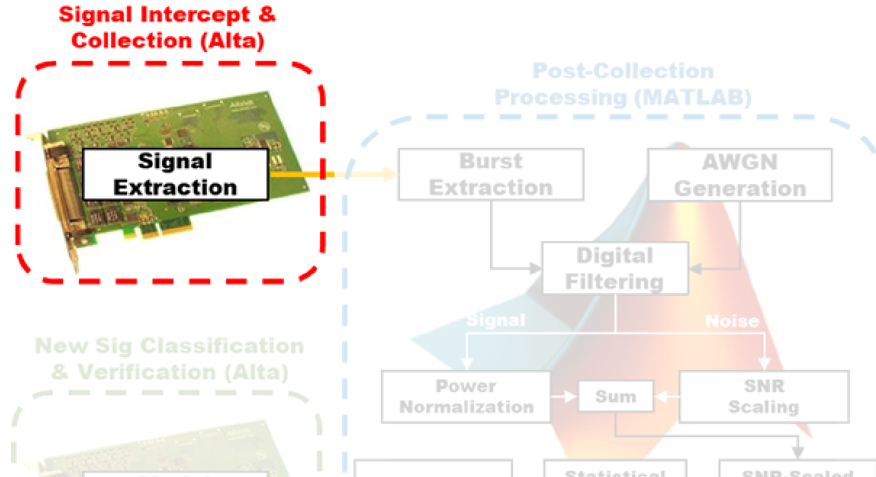
Configuration 2: Operational Simulation

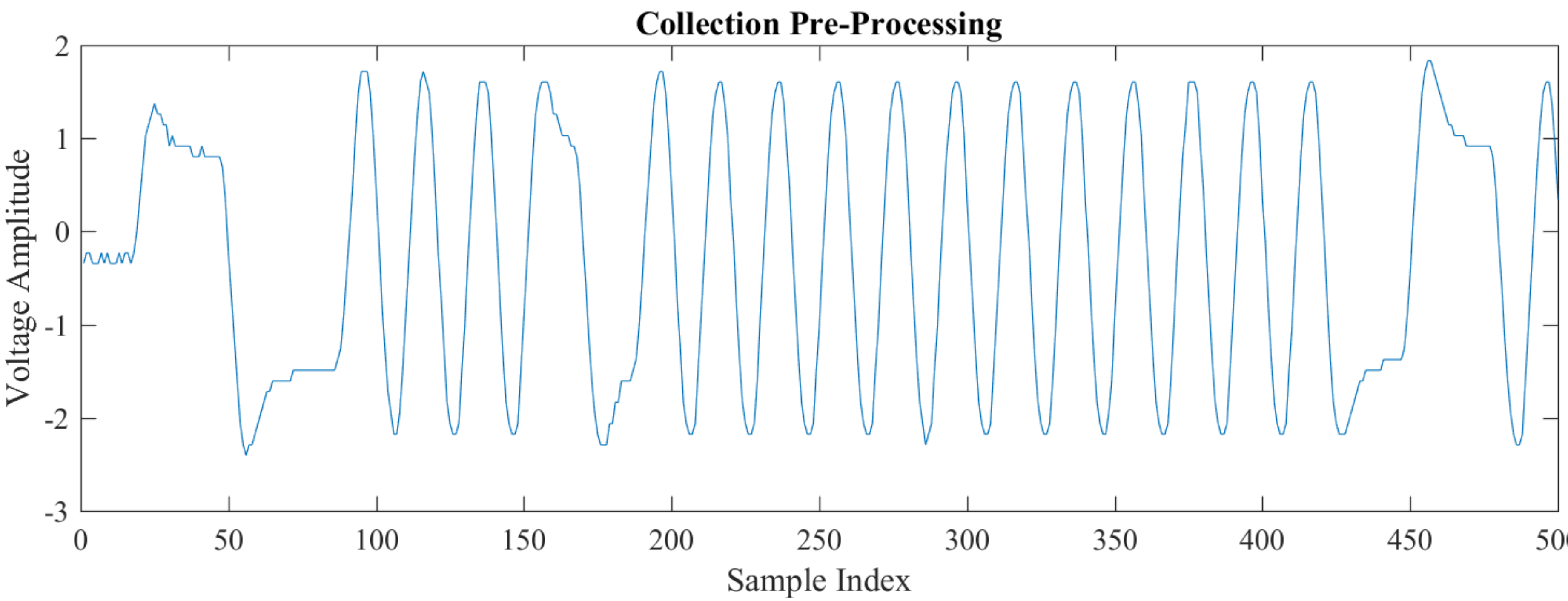


Device 1-3 are the same Make/Model:
Serial # Discrimination

WS-DNA – Signal Collection

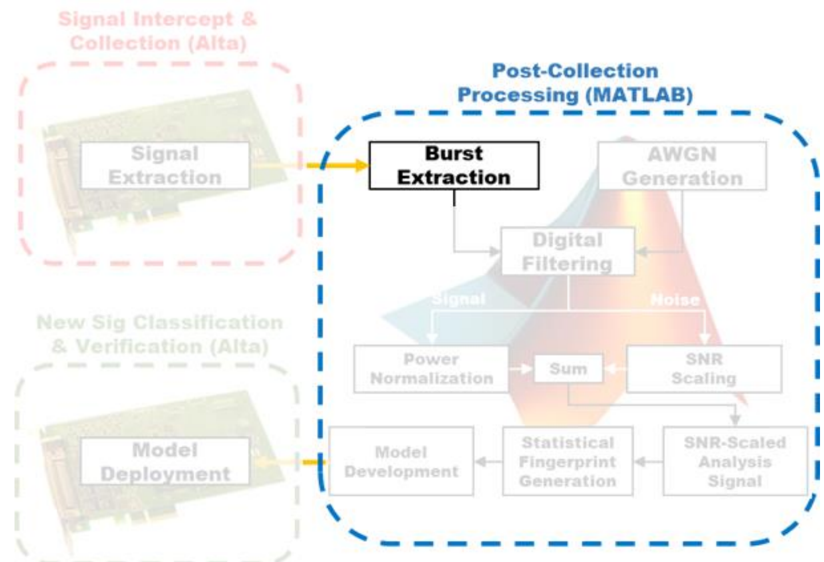
- Alta Signal Capture
- Collection Triggered on Status Word
- 20 Lead Samples for Alignment/Spacing
- Collects up to 2048 Samples (420 used)
- 20nS and 8-bit resolution



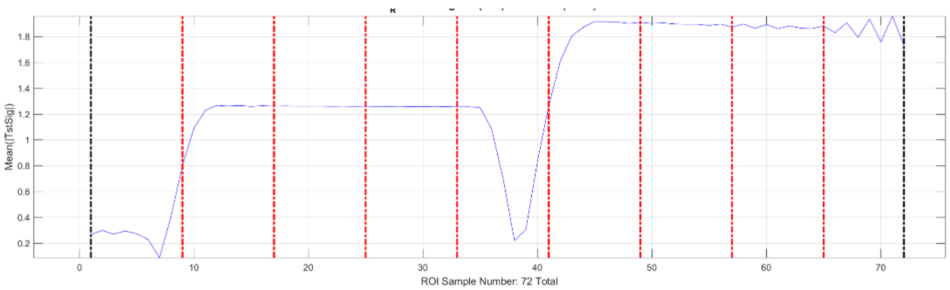


WS-DNA – Burst Extraction

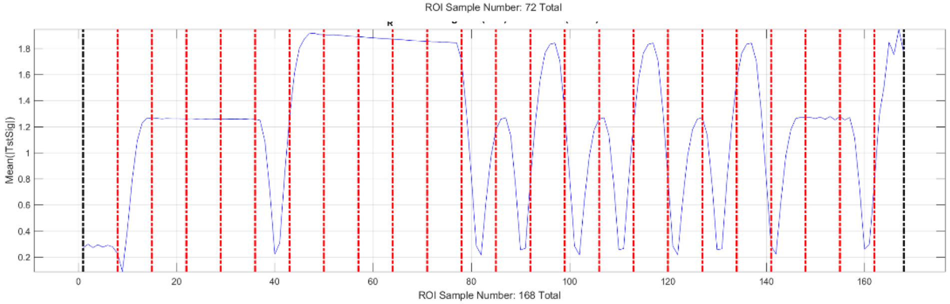
- Alignment / centered
- Absolute value
- Regions and sub-regions of interest



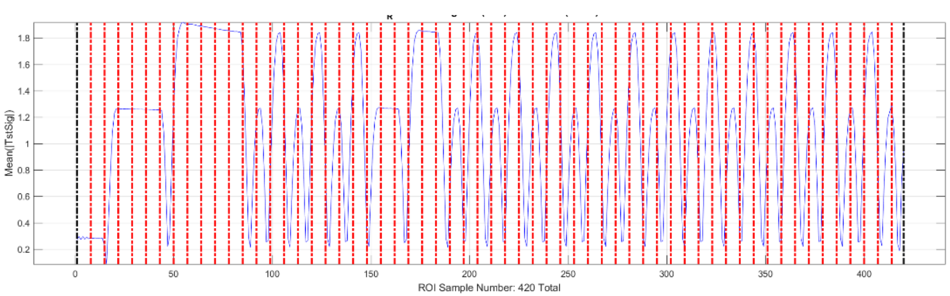
SYNC



RT



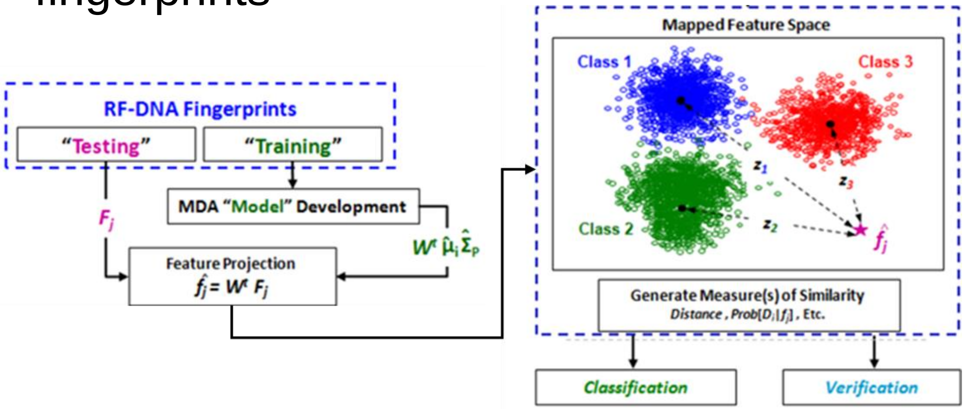
STATUS

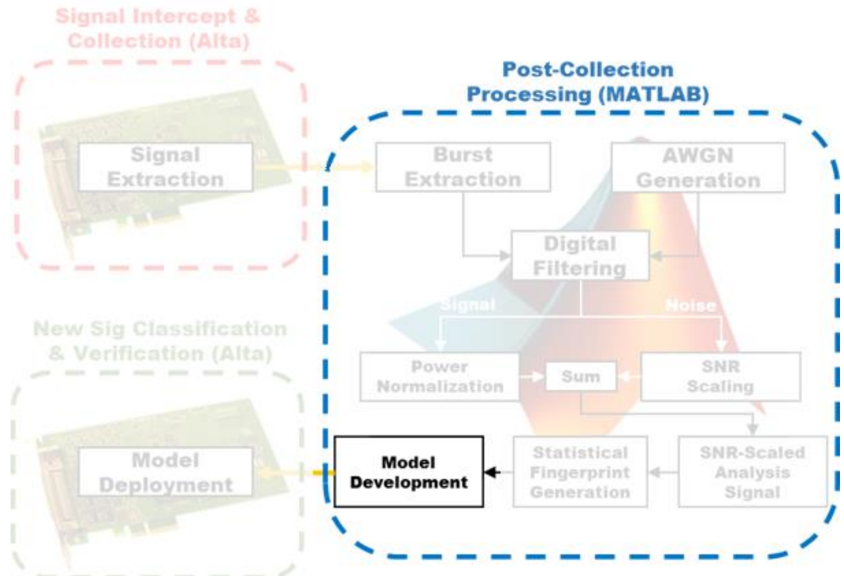


	Start Index	Stop Index	Subregions	Samples/ Subregion
Sync	10	81	9	8
RT	8	175	24	7
Status	1	420	60	7

WS-DNA – Classifier Model

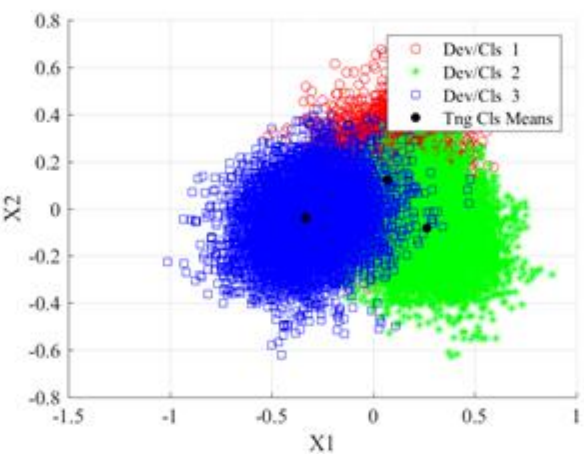
Multidimensional discriminant analysis (MDA) model developed using statistical fingerprints



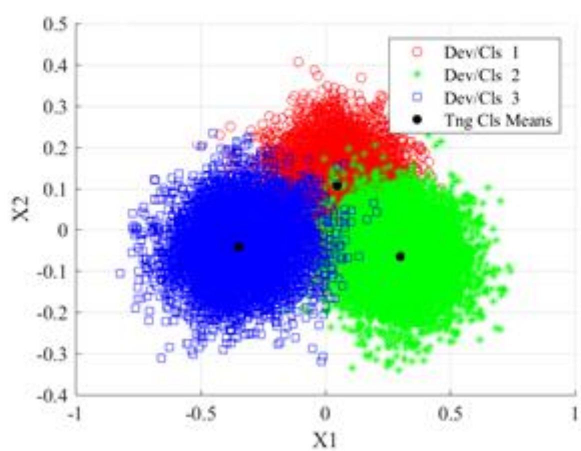


Fisher Space Plots with 7500 testing waveforms (SNR 50 dB Model):

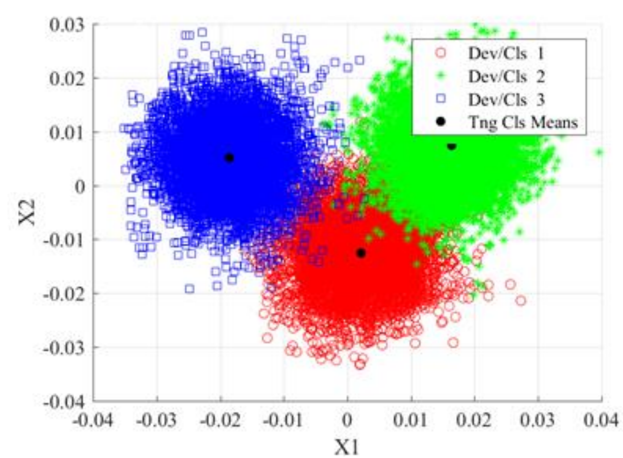
Sync



RT

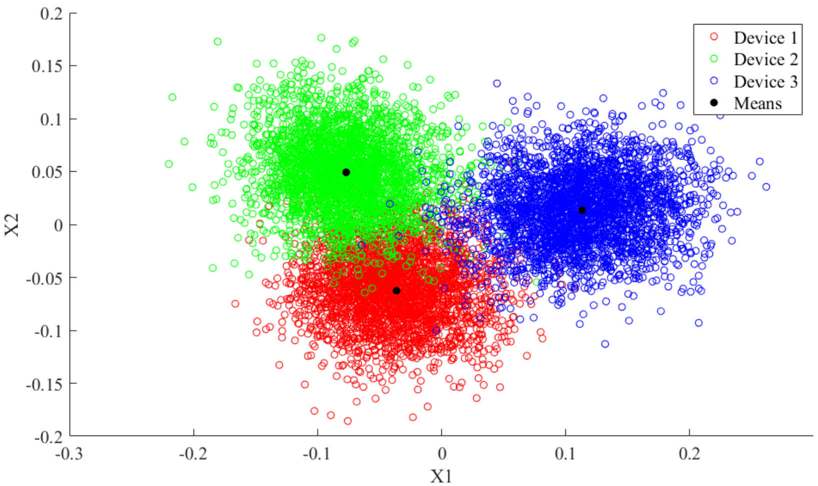


Status



Classification & Verification

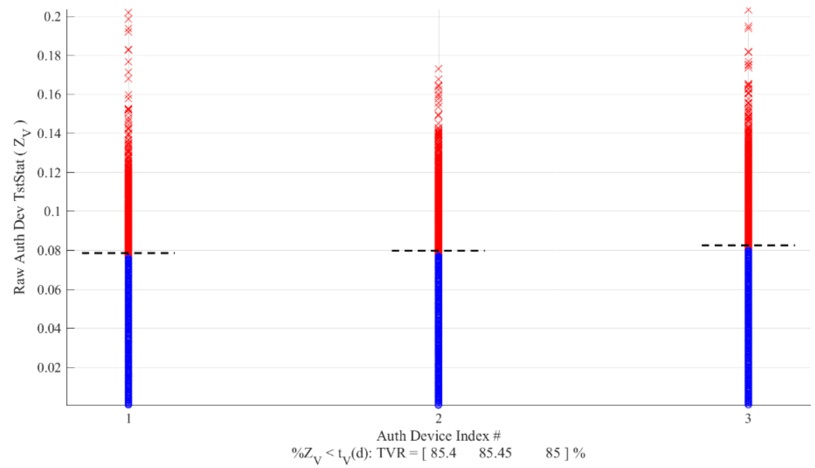
"Looks Most Like"



True-Positive - Cases where we predicted a certain LRU, and it is that LRU

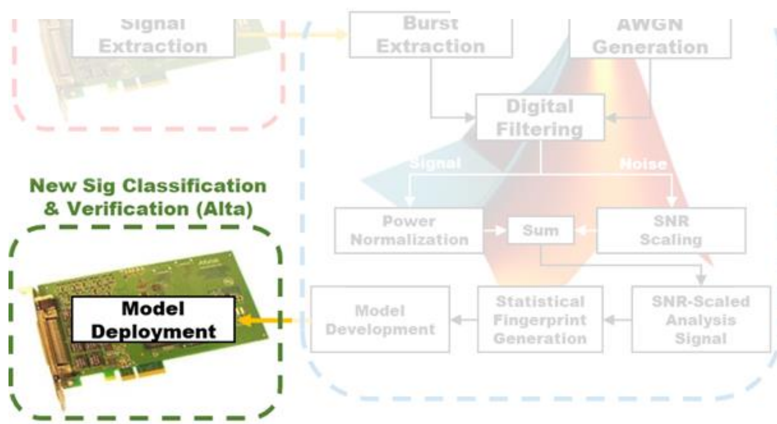
False-Positive - Cases where we predicted a certain LRU, and it is a *different* LRU

"Looks How Much Like"

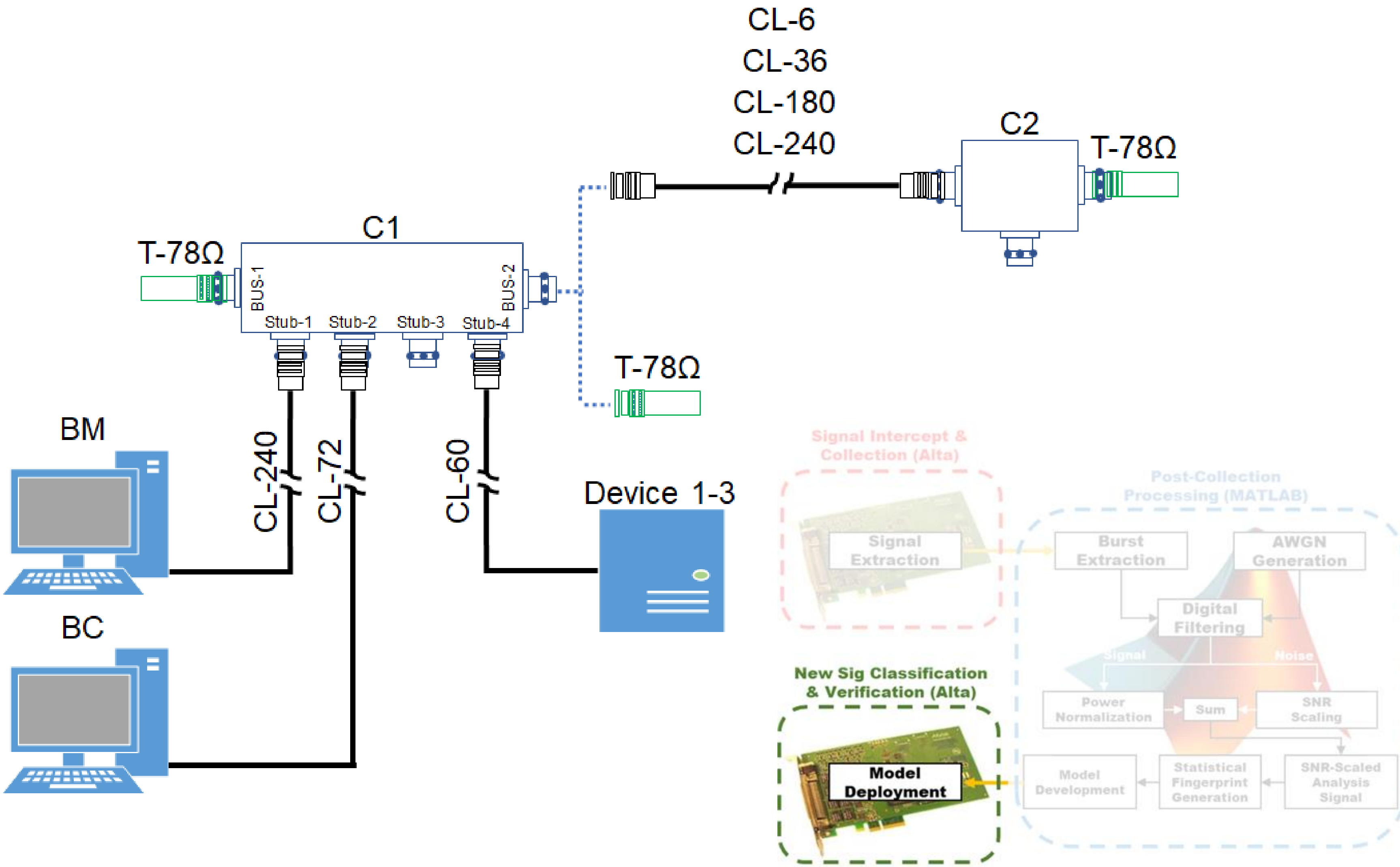


True Verification Rate (TVR) - Cases where an LRU authentic threshold is met, and it is that LRU

False Verification Rate (FVR) - Cases where LRU authentic threshold is met, but it is *not* that LRU



Configuration 1 Test



Configuration 1 Test Results

			Classified As														
			C1 - No Coupler			6 in Cable & C2			36 in Cable & C2			180 in Cable & C2			240 in Cable & C2		
			Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3
Actual Device	Dev 1	Sync	74.3	19.9	5.81	69.6	25.1	5.31	70.9	23.3	5.86	79.2	16	4.76	82.8	7.56	9.64
		RT	84	13.6	2.42	79.4	16.3	4.3	77.3	16.5	6.28	73.1	9.62	17.3	53	3.82	43.2
		Status	92	7.27	0.71	89.5	9.69	0.84	88.9	10	1.06	89.1	6.66	4.28	70.8	2.55	26.7
	Dev 2	Sync	24.5	70.2	5.34	18.8	73.5	7.69	20.4	71.1	8.5	39	52.8	8.23	44.7	46.3	9.01
		RT	10.8	87.9	1.23	8.62	87.8	3.54	9.47	86.2	4.34	19.7	73.1	7.2	22.7	65.5	11.9
		Status	6.42	93.3	0.33	5.57	93.5	0.92	6.23	92.6	1.13	15.7	81.2	3.16	19.1	74.8	6.12
	Dev 3	Sync	28.8	12.2	59	46	13	41	44.8	10.2	45	36	5	59	35.3	5.09	59.6
		RT	13.8	4.12	82.1	12.5	4.18	83.3	9.55	3.15	87.3	3.62	0.99	95.4	3.56	1.03	95.4
		Status	8.42	2.64	88.9	9.07	3.49	87.4	5.98	2.59	91.4	1.57	0.58	97.9	1.28	0.64	98.1

Classification Trends:

- Longer ROI increases true-positive classification accuracy
  - 17.09% gain Sync->RT
  - 7.90% gain RT->Status
- Only one scenario incorrect
- Shifting Effects

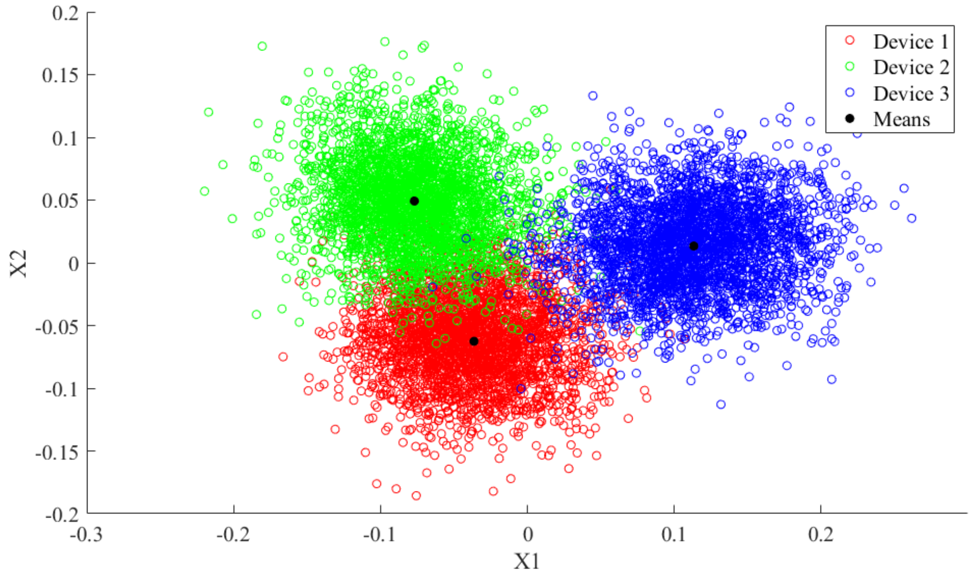
			Acceptance Rate														
			C1 - No Coupler			6 in Cable & C2			36 in Cable & C2			180 in Cable & C2			240 in Cable & C2		
			Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3
Actual Device	Dev 1	Sync	89.6	64	50.2	84.4	61.8	39.5	84.3	61.3	41.5	82.7	48.8	38.7	80.6	36.9	43.9
		RT	89.6	31.4	7	89.1	36.5	11.3	87.3	35.6	14.6	80.2	22.8	30.5	56	10.1	52.9
		Status	83.1	10.2	0.32	85.8	14.1	0.47	84.3	14.8	0.67	82	10.5	2.61	53.7	3.69	17.3
	Dev 2	Sync	57.9	88.1	44.4	47.6	82.3	35.2	49.5	83.2	37.6	71.2	83.8	51	76.3	81.2	55.2
		RT	30.1	88.9	2.56	25	85.2	5.25	26.6	84.9	6.2	42.8	81.7	12.9	46.1	75.3	20.1
		Status	10.4	86	0.18	9.09	85.3	0.42	10.3	85.7	0.52	21.2	78.4	1.43	23.6	70.5	3.18
	Dev 3	Sync	60.3	52.2	90.3	76.4	54.9	83.2	73.2	48.9	83.3	56.8	30.4	80.1	52.9	27.7	76.7
		RT	20.8	6.42	87.1	18.9	6.37	87.5	14.7	4.34	87.8	5.53	1.31	73.4	5.08	1.3	66.2
		Status	4.97	1.22	80.8	5.65	1.72	79.1	3.51	1.13	82.2	0.91	0.2	75.1	0.66	0.22	67.8

Verification Trends:

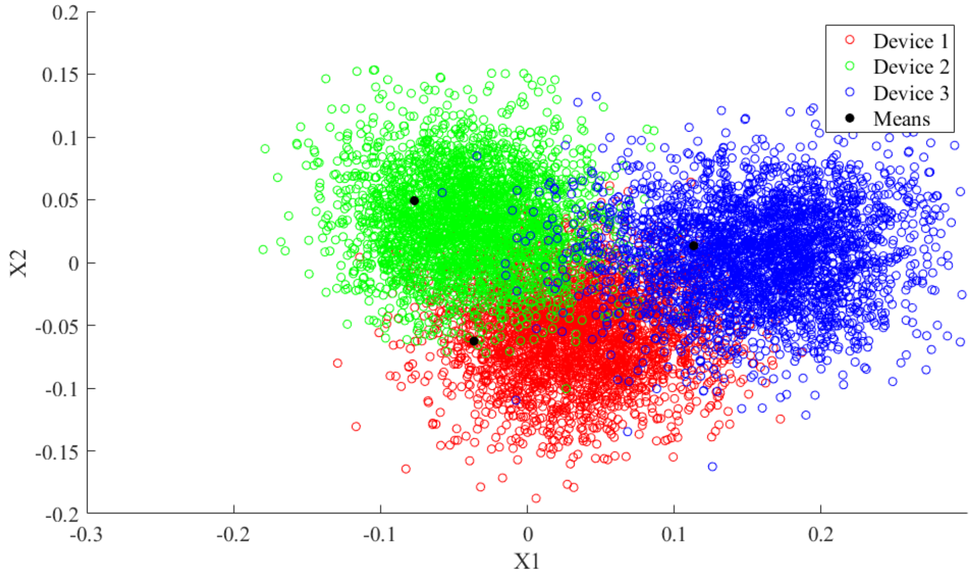
- Generally more cabling leads to lower TVR
- Longer ROI reduces FVR
  - Sync - 51.53%
  - RT -18.50%
  - Status - 5.84%
- Shifting Effects

Configuration 1 Test 1 Shift

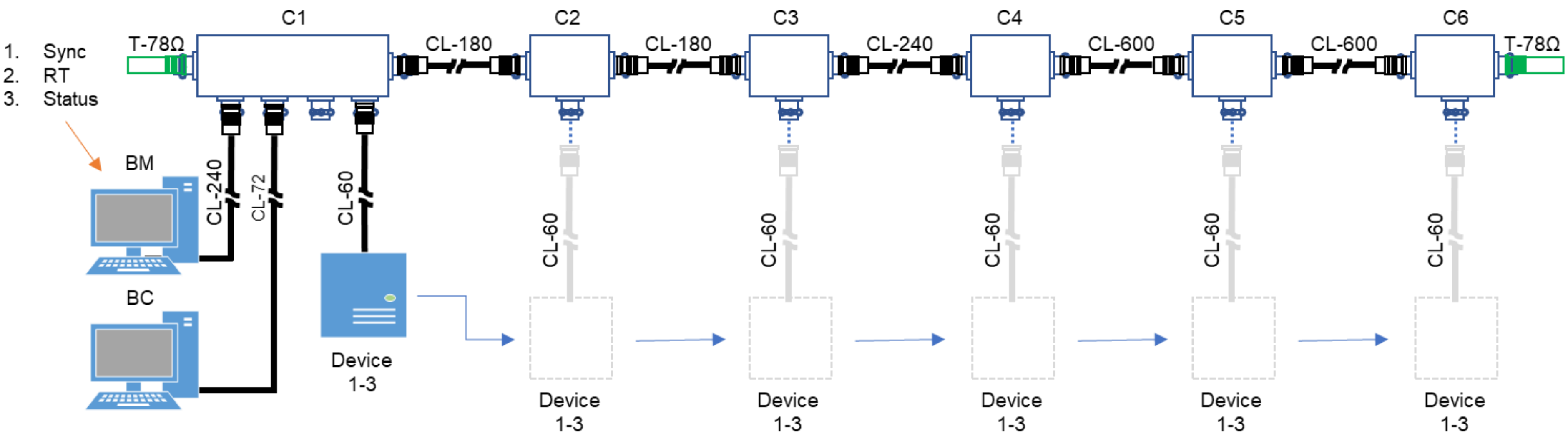
No Coupler
(*Baseline*)

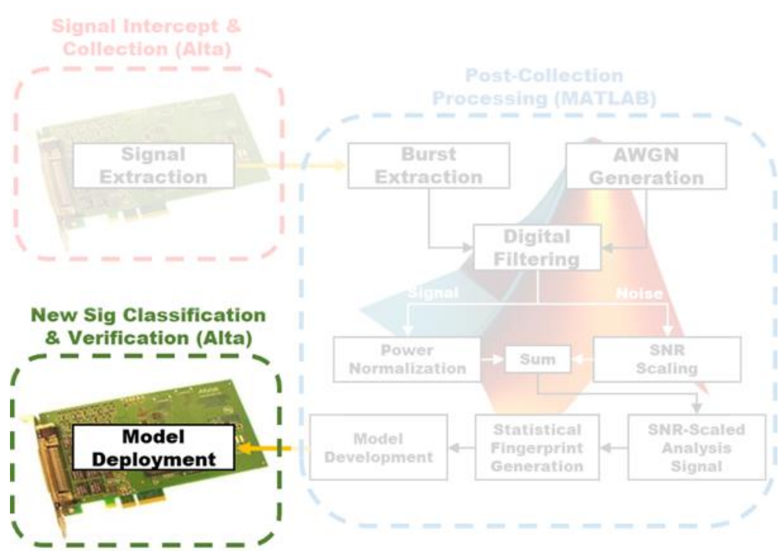


Coupler
+ 240 inch cable



Configuration 2 Test 1





Configuration 2 Test 1 Results

		Classified As																	
		C1			C2			C3			C4			C5			C6		
Actual Device		Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3
Dev 1	Sync	63.	13.9	23.1	58.4	23.1	18.5	44.6	55.4	0.	5.7	94.1	0.1	0.	91.6	8.4	0.	68.8	31.2
	RT	78.9	7.	14.1	0.6	99.4	0.	0.	100.	0.	0.	100.	0.	0.	100.	0.	0.	100.	0.
	Status	90.3	2.1	7.6	0.	100.	0.	0.	100.	0.	0.	100.	0.	0.	88.5	11.5	0.	90.1	9.9
Dev 2	Sync	21.7	66.7	11.6	34.1	47.	18.9	16.8	83.2	0.	1.9	97.9	0.3	0.	93.2	6.8	0.	78.5	21.5
	RT	16.1	82.6	1.3	0.	100.	0.	0.	100.	0.	0.	100.	0.	0.	100.	0.	0.	100.	0.
	Status	8.1	91.6	0.3	0.	100.	0.	0.	100.	0.	0.	100.	0.	0.	95.8	4.3	0.	94.	6.
Dev 3	Sync	11.8	3.6	84.6	34.5	34.	31.5	43.1	56.8	0.1	1.5	98.5	0.	0.	82.5	17.5	0.	38.4	61.6
	RT	5.7	0.2	94.1	3.1	96.4	0.5	0.	100.	0.	0.	100.	0.	0.	100.	0.	0.	100.	0.
	Status	1.3	0.	98.7	1.3	98.7	0.	0.	100.	0.	0.	100.	0.	0.	61.7	38.3	0.	84.1	15.9

		Acceptance Rate																	
		C1			C2			C3			C4			C5			C6		
Actual Device		Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3
Dev 1	Sync	87.1	52.7	56.7	70.4	48.2	37.2	2.1	2.3	0.1	1.4	5.5	0.3	0.	0.	0.	0.	0.	0.
	RT	87.8	16.8	23.6	1.5	30.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
	Status	80.5	1.6	4.2	0.	1.8	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
Dev 2	Sync	60.9	88.4	31.4	63.5	71.6	36.8	1.9	5.3	0.1	1.3	7.7	0.3	0.	0.	0.	0.	0.	0.
	RT	33.	86.8	1.6	0.	5.9	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
	Status	5.8	79.7	0.	0.	0.1	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
Dev 3	Sync	41.3	18.5	87.8	61.	56.4	47.6	11.	12.9	0.8	0.6	4.8	0.1	0.	0.	0.	0.	0.	0.
	RT	13.	0.3	87.6	7.5	65.9	0.3	0.	0.1	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
	Status	0.6	0.	82.7	0.9	53.3	0.	0.	0.2	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.

Classification Trends:

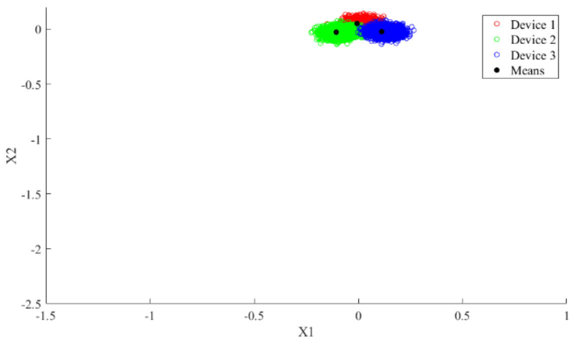
- Very degraded results after C1
- Strong favoring of Device 2

Verification Trends:

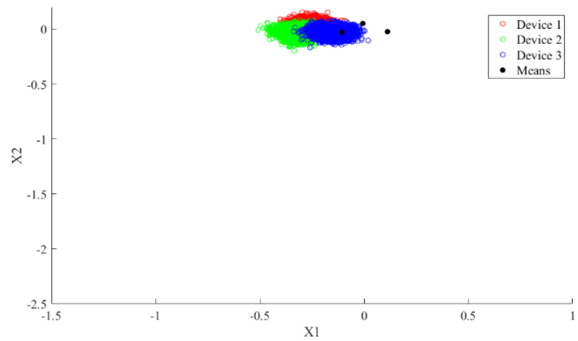
- Results not reliable after C1…especially for longer ROIs

Configuration 2 Test 1 Shift

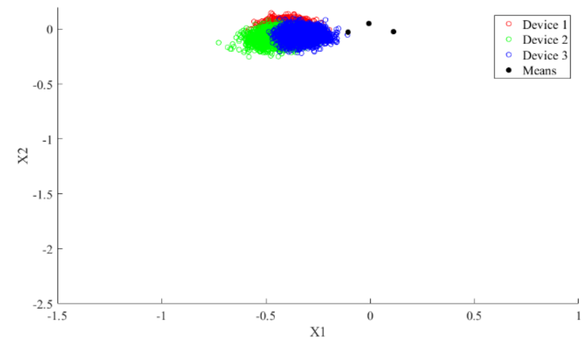
Off C1



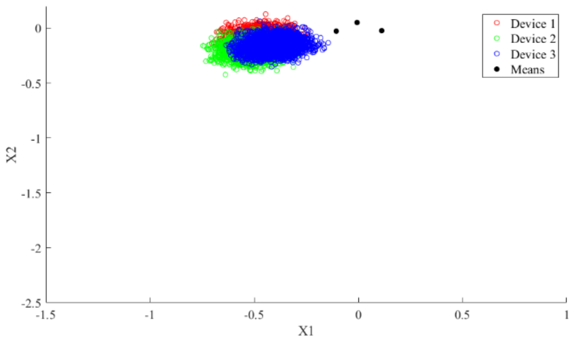
Off C2



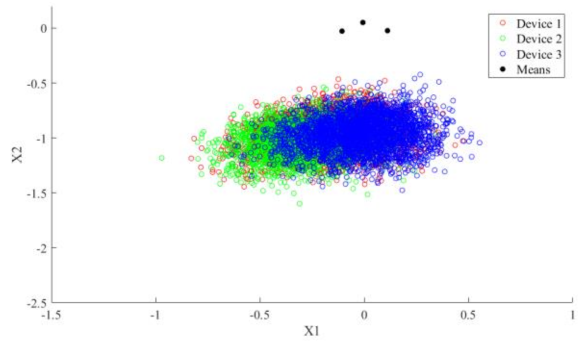
Off C3



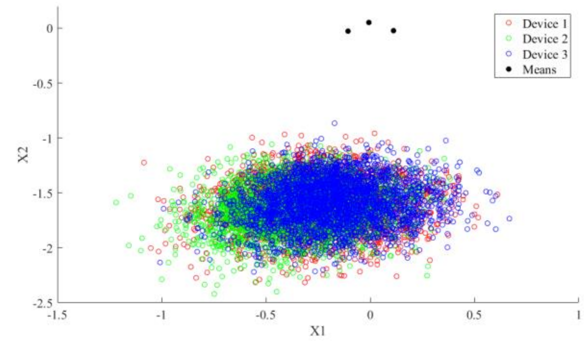
Off C4



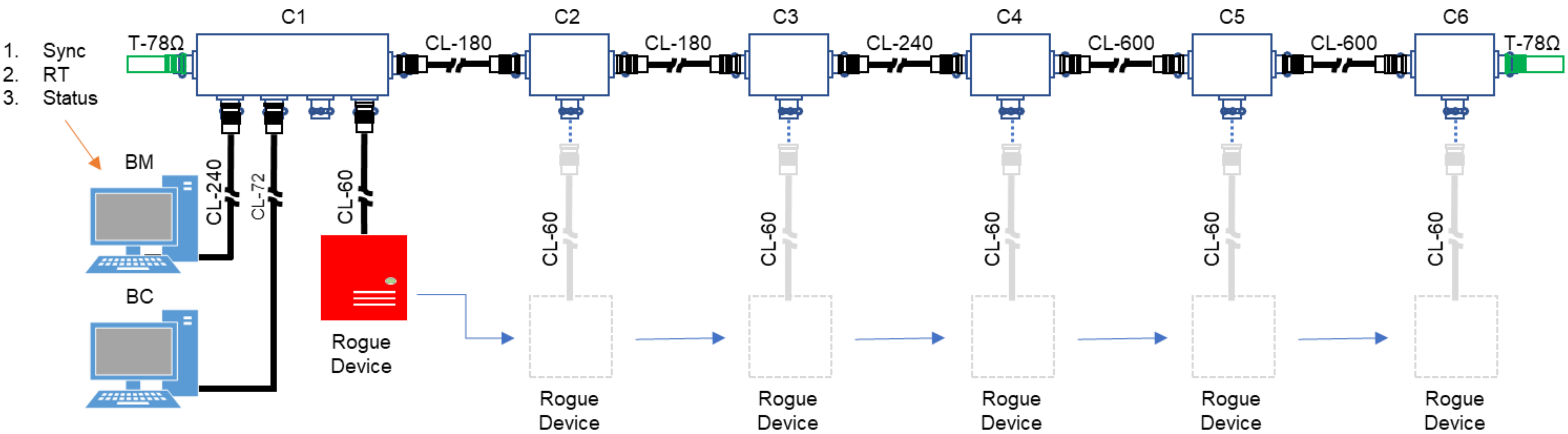
Off C5

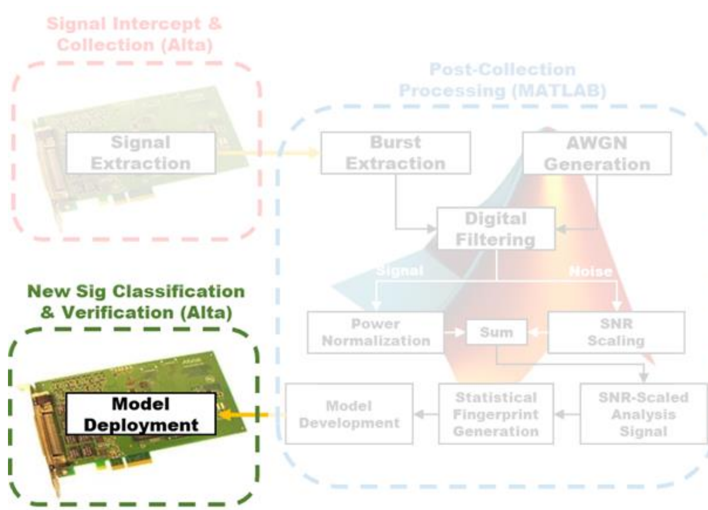


Off C6



Configuration 2 Test 2





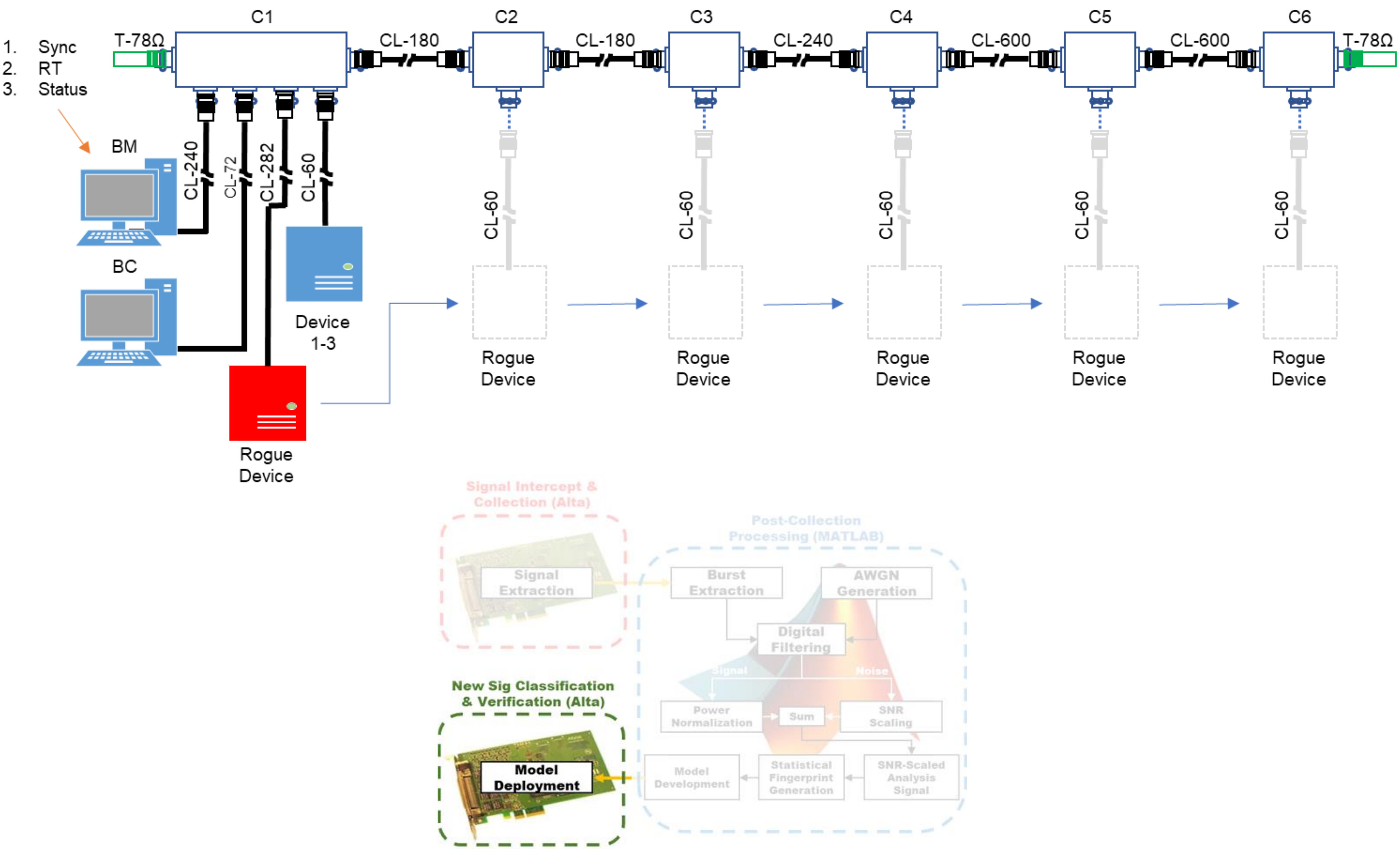
Configuration 2 Test 2 Results

			Acceptance Rate																	
			C1 Rogue			C2 Rogue			C3 Rogue			C4 Rogue			C5 Rogue			C6 Rogue		
			Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3
Act Dev	Dev 4	Sync	34.5	83.	26.9	48.3	44.8	12.5	1.3	10.	0.5	1.5	9.6	2.8	0.	0.	0.	0.	0.	0.
		RT	37.1	63.	12.3	0.2	9.9	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
		Status	31.7	22.2	8.4	0.	6.4	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.

Verification Trends:

- High FVR for Dev 2 with Sync and RT ROIs off C1.
- FVR better on average for C1:
  - Sync – 48.13% RT - 37.37% Status - 20.77%

Configuration 2 Test 3



Configuration 2 Test 3 Results

AIR FORCE INSTITUTE OF TECHNOLOGY

		Classified As																				
		C1 - No Listener			C1 - Listener			C2 - Listener			C3-Listener			C4 - Listener			C5 - Listener			C6 - Listener		
		Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3
Actual Device Dev 1	Sync		63.6	18.1	18.3	26.7	4.8	68.5	0.	2.7	97.3	0.	15.6	84.5	0.3	43.	56.7	71.8	25.6	2.6	61.1	36.7	2.2
Dev 1	RT		78.9	8.	13.1	0.8	0.	99.2	0.	0.	100.	0.	0.	100.	0.3	0.5	99.2	67.7	32.1	0.2	59.9	39.7	0.4
Dev 1	Status		84.9	1.6	13.5	3.2	0.	96.8	0.	0.	100.	1.3	0.2	98.5	26.9	16.7	56.4	91.5	8.5	0.1	87.	8.5	4.6
Dev 2	Sync		23.3	68.	8.7	9.6	39.2	51.3	0.	16.8	83.2	0.	49.4	50.6	0.	78.2	21.9	11.6	86.9	1.5	14.4	84.	1.5
Dev 2	RT		16.3	82.5	1.3	4.7	4.5	90.9	0.	0.	100.	0.	0.6	99.4	0.2	10.8	89.1	1.4	98.6	0.	2.2	97.8	0.
Dev 2	Status		12.3	85.6	2.1	5.8	4.3	89.9	0.	0.1	99.9	0.6	10.2	89.2	3.5	64.2	32.3	0.7	99.3	0.	11.7	86.8	1.5
Dev 3	Sync		17.9	3.5	78.6	2.3	0.6	97.1	0.	0.8	99.2	0.	2.8	97.2	0.	15.	85.1	30.	18.7	51.2	40.	30.7	29.3
Dev 3	RT		6.3	0.3	93.4	0.	0.	100.	0.	0.	100.	0.	0.	100.	0.	0.	100.	38.5	10.	51.5	54.	15.8	30.2
Dev 3	Status		0.9	0.	99.1	0.	0.	100.	0.	0.	100.	0.	0.	100.	0.	0.7	99.3	30.4	8.8	60.7	16.9	2.7	80.4

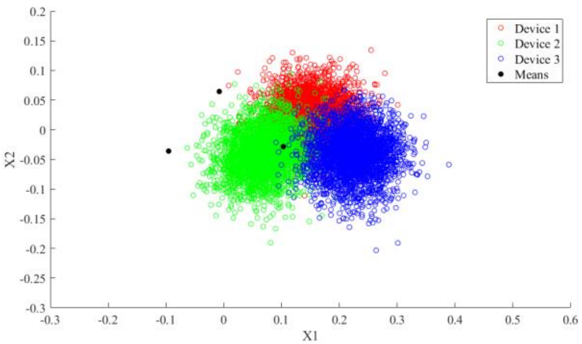
		Acceptance Rate																				
		C1 - No Listener			C1 - Listener			C2 - Listener			C3-Listener			C4 - Listener			C5 - Listener			C6 - Listener		
		Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3	Dev 1	Dev 2	Dev 3
Actual Device Dev 1	Sync	87.4	53.4	58.	54.1	21.3	87.7	0.2	0.3	18.8	0.2	1.1	11.4	3.8	20.7	32.1	81.9	55.7	22.5	76.4	63.1	19.7
Dev 1	RT	87.	15.6	23.3	1.7	0.	53.7	0.	0.	0.	0.	0.	3.9	0.9	0.1	56.8	64.5	32.4	0.9	58.7	36.4	1.3
Dev 1	Status	70.2	0.7	6.4	0.5	0.	30.4	0.	0.	0.6	0.4	0.	41.9	15.3	4.9	33.	61.2	3.4	0.	70.7	4.5	2.
Dev 2	Sync	59.1	88.7	38.1	38.5	58.9	74.7	0.	0.3	4.8	0.	0.2	1.3	0.1	4.9	3.2	32.1	83.7	9.9	32.2	79.2	10.5
Dev 2	RT	29.5	85.	1.7	8.7	1.4	81.1	0.	0.	0.7	0.	0.	5.8	0.4	0.4	30.8	3.8	68.8	0.	5.1	66.8	0.
Dev 2	Status	7.1	66.5	0.2	2.	0.4	65.	0.	0.	12.8	0.2	0.3	33.8	1.1	8.8	8.5	0.4	71.	0.	7.5	63.3	0.2
Dev 3	Sync	42.2	18.2	89.3	10.4	3.5	69.9	0.	0.	2.7	0.	0.	1.4	0.1	1.7	7.7	63.7	50.7	82.1	74.6	66.2	68.5
Dev 3	RT	12.1	0.3	87.4	0.	0.	6.	0.	0.	0.	0.	0.	0.	0.	0.	2.2	50.7	11.9	59.7	67.8	20.7	40.2
Dev 3	Status	0.3	0.	79.6	0.	0.	5.5	0.	0.	0.	0.	0.	2.6	0.	0.	28.8	16.5	1.9	37.	8.6	0.6	59.8

Classification & Verification:

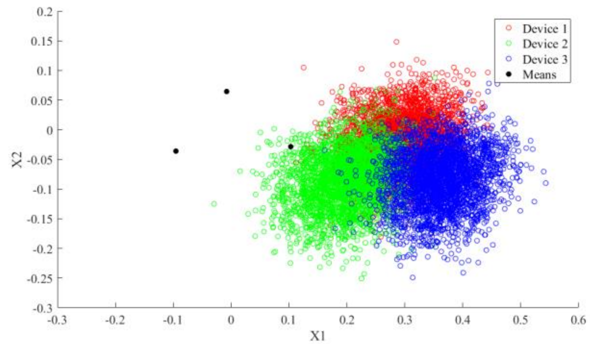
- Results worsen C1 → C2
- Improves C2 → C5
- Slightly degrades at C6

Configuration 2 Test 3 Shift

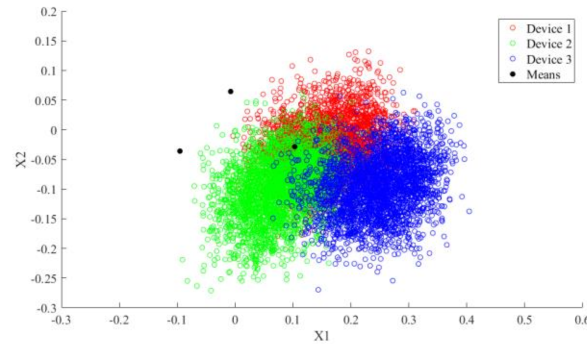
Off C1



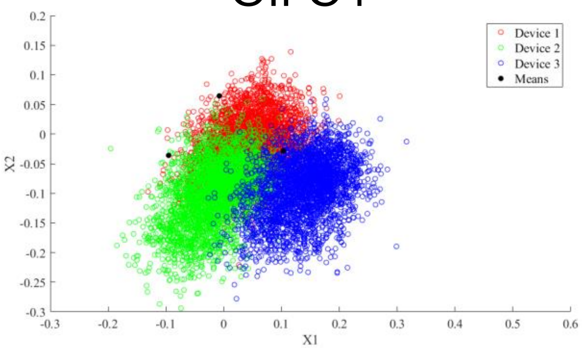
Off C2



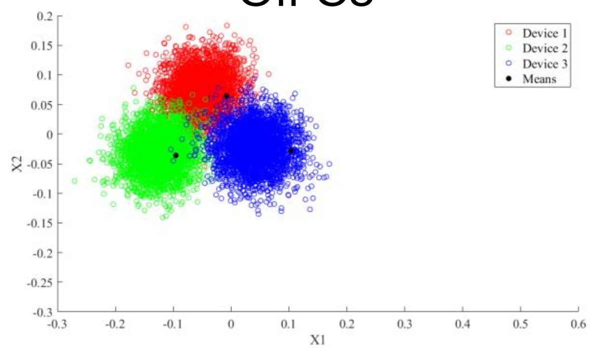
Off C3



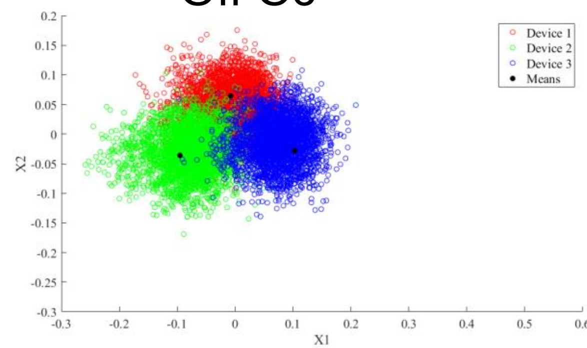
Off C4



Off C5



Off C6



Conclusions

- **MDA models work well for baseline configuration**
  - 90+% for most status classification and 80+% verification
- **Approach breaks down for configuration changes, swapped positions, or added devices**
  - Avionics buses are fairly stable and don't (shouldn't) change much
  - Implication → perfectly suited to detect jamming, masquerading, and eavesdropping
- **WS-DNA and Alta approach could be easily & quickly transitioned to real world operations**
  - Little or no cost
  - Minimal equipment required
  - Real time
  - Provides capability that does not currently exist

Future Work

- Migrating the work to an operational 1553 bus could prove its viability to a program office
- Expanding program to auto-update MDA model over time – implement entire WS-DNA process in the Alta card
- Additional exploration and analysis of the Fisher shifting … i.e., can it be predicted?

Questions?

References

[1] Condor Engineering Inc, “MIL-STD-1553 Tutorial,” 2000.

[2] A. Nourian and S. Madnick, “A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet Arash,” *IEEE Trans. Dependable Secure. Computer*, 2015.

[3] D. Kushner, “The Real Story of Stuxnet,” *IEEE Spectrum*, 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. [Accessed: 13-Jun-2017].

[4] S. Checkoway *et al.*, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” *USENIX Secure.*, 2011.

[5] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, “Review on cyber-physical systems,” *IEEE/CAA J. Autom. Sin.*, vol. 4, no. 1, pp. 27–40, 2017.

[6] Department of Defensce, “MIL-STD-1553B 22Jan79.pdf.” 1979.

[7] K.-T. Cho and K. G. Shin, “Fingerprinting Electronic Control Units for Vehicle Intrusion Detection Fingerprinting Electronic Control Units for Vehicle Intrusion Detection,” *25th USENIX Secure. Symp. is*, 2016.

[8] M. Enev, A. Takakuwa, K. Koscher, and T. Kohno, “Automobile Driver Fingerprinting,” *Proc. Priv. Enhancing Technol.*, vol. 2016, no. 1, pp. 34–51.

[9] A. Taylor, S. Leblanc, and N. Japkowicz, “Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks.”

[10] A. Taylor, N. Japkowicz, and S. Leblanc, “Frequency-based anomaly detection for the automotive CAN bus,” in *2015 World Congress on Industrial Control Systems Security, WCICSS 2015*, 2016.

[11] O. Stan, Y. Elovici, A. Shabtai, G. Shugol, R. Tikochinski, and S. Kur, “Protecting Military Avionics Platforms from Attacks on MIL-STD-1553 Communication Bus.”

[12] C. M. Talbot, M. A. Temple, T. J. Carbino, and J. A. Betances, “Detecting rogue attacks on commercial wireless insteon home automation systems,” no. 17, 2017.

[13] T. J. Bihl, K. W. Bauer, and M. A. Temple, “Feature Selection for RF Fingerprinting with Multiple Discriminant Analysis and Using ZigBee Device Emissions,” *IEEE Trans. Inf. Forensics Secure.*, 2016.

[14] Alta Data Technologies LLC, “MIL-STD-1553 Tutorial and Reference,” 2014.

[15] Department of Defense, “MIL-STD-1553B: Interface Std for Digital Time Division Command/Response Multiplex Data Bus,” 1996.

[16] D. K. (David K. Cheng, *Field and wave electromagnetics*. Addison-Wesley, 1989.

[17] N. H. Modi, J. R. Armstrong, J. G. Tront, and M. Z. Khan, “Modeling and simulation of 1553 bus for upset tolerance experiments,” in *Seventh Annual International Phoenix Conference on Computers an Communications. 1988 Conference Proceedings*, 1998, pp. 131–135.

[18] Department of Defense, “MIL-HDBK-1553A Multiplex Applications Handbook,” 1988.

[19] Alta Data Technologies LLC, “AltaAPI Software User’s Manual,” 2016.

[20] B. Sklar, *Digital Communications: Fundamentals and Applications*. Prentice-Hall PTR, 2001.

[21] J. Lopez, N. C. Liefer, R. Busho, Colin, and M. A. Temple, “Enhancing Critical Infrastructure and Key Resources (CIKR) Level-0 Physical Process Security Using Field Device Distinct Native Attribute Features,” *IEEE Trans. Inf. FORENSICS Secure.*

[22] J. Lopez, M. A. Temple, and B. E. Mullins, “Exploitation of HART Wired Signal Distinct Native Attribute (WS-DNA) Features to Verify Field Device Identity and Infer Operating State .,” *9th Int. Conf. Crit. Inf. Infrastructures Secure.*, 2014.