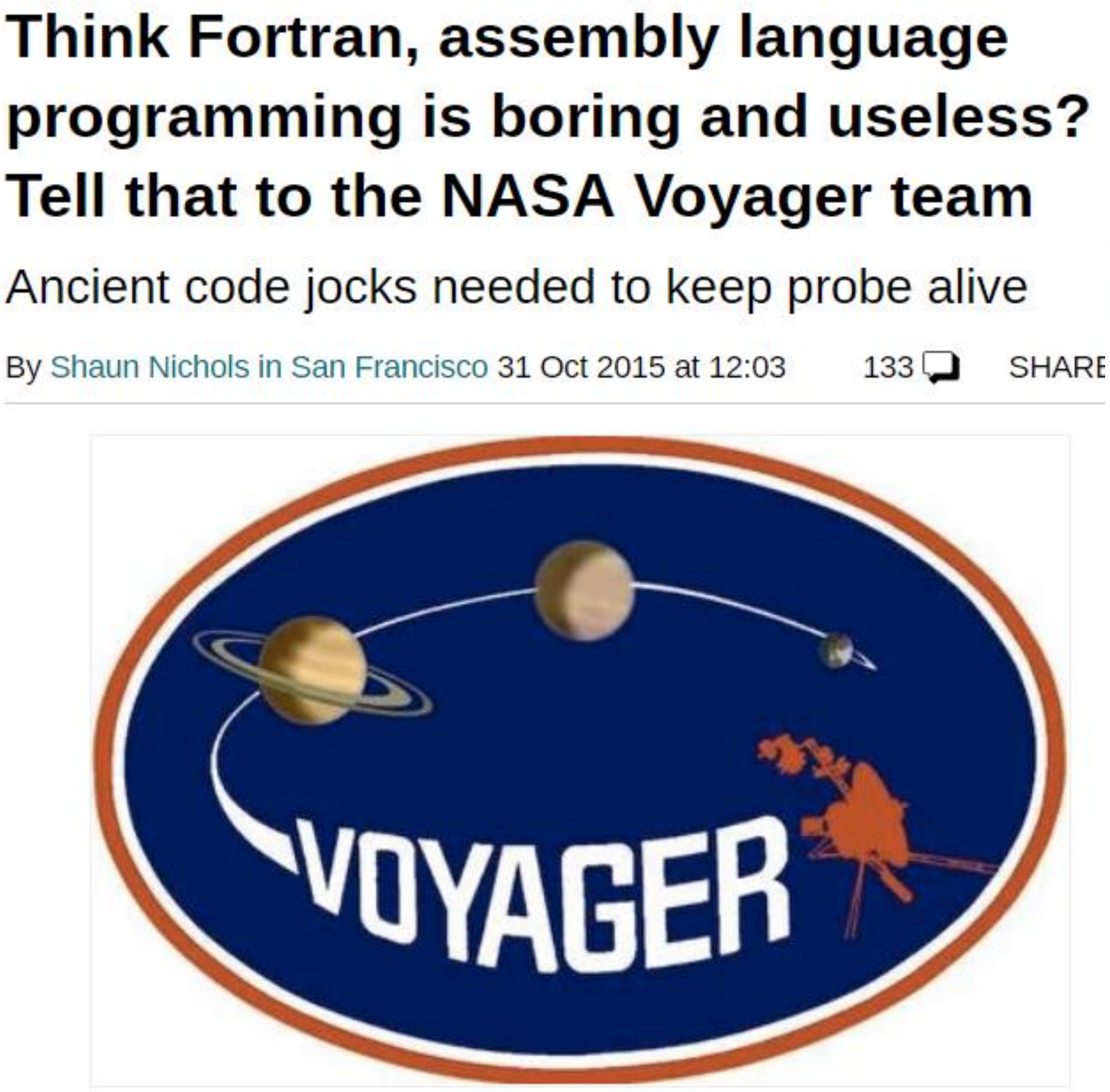
CAERUS:
Chronoscopic Assessment Engine for Recovering Undocumented Specifications

Adam Seitz,[1] Adam Satar, [1] Brian Burke, [1] Lok Yan,[2] **Zachary Estrada**[1]

[1] Rose-Hulman Institute of Technology, Terre Haute, IN USA

[2]Air Force Research Laboratory, Rome, NY USA



Think Fortran, assembly language programming is boring and useless? Tell that to the NASA Voyager team

Ancient code jocks needed to keep probe alive

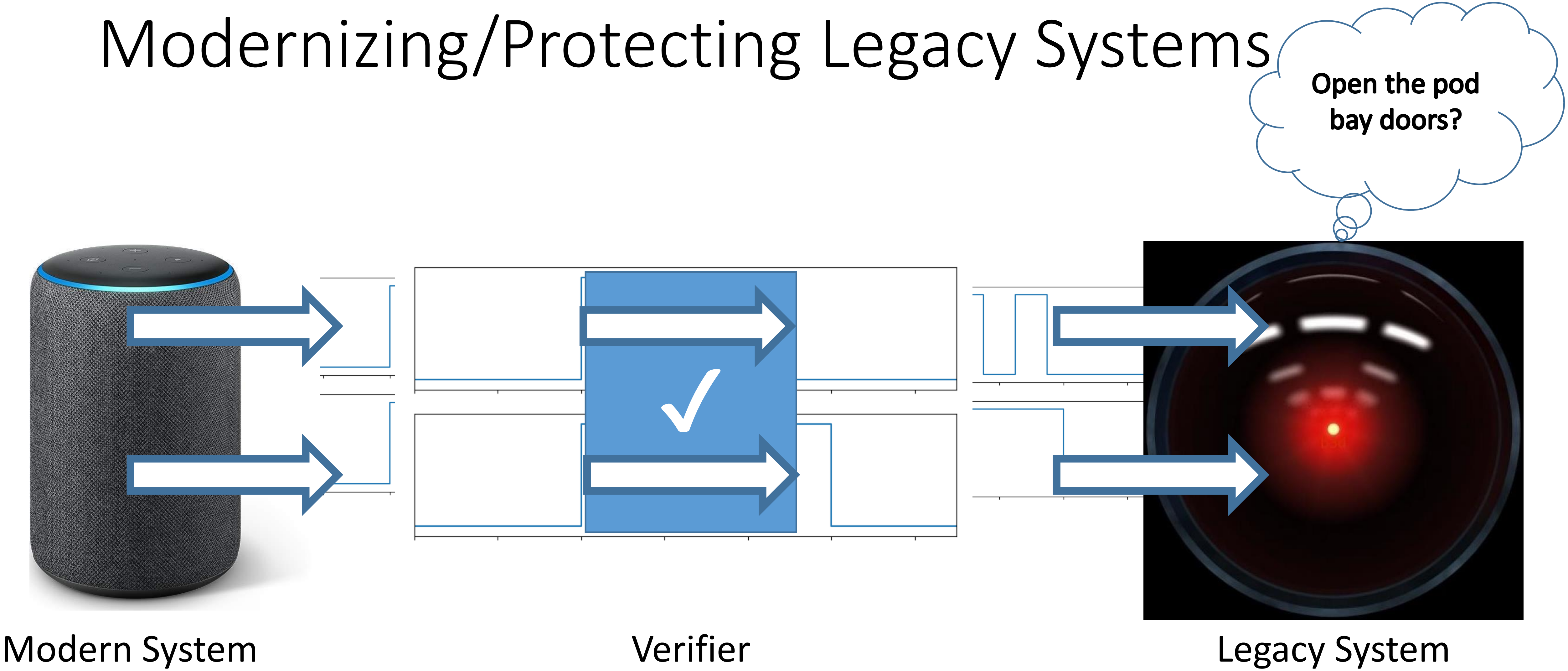
By Shaun Nichols in San Francisco 31 Oct 2015 at 12:03 133 SHARE

Legacy IT Systems Pose an Obstacle to Cybersecurity Best Practices, GAO Head Says

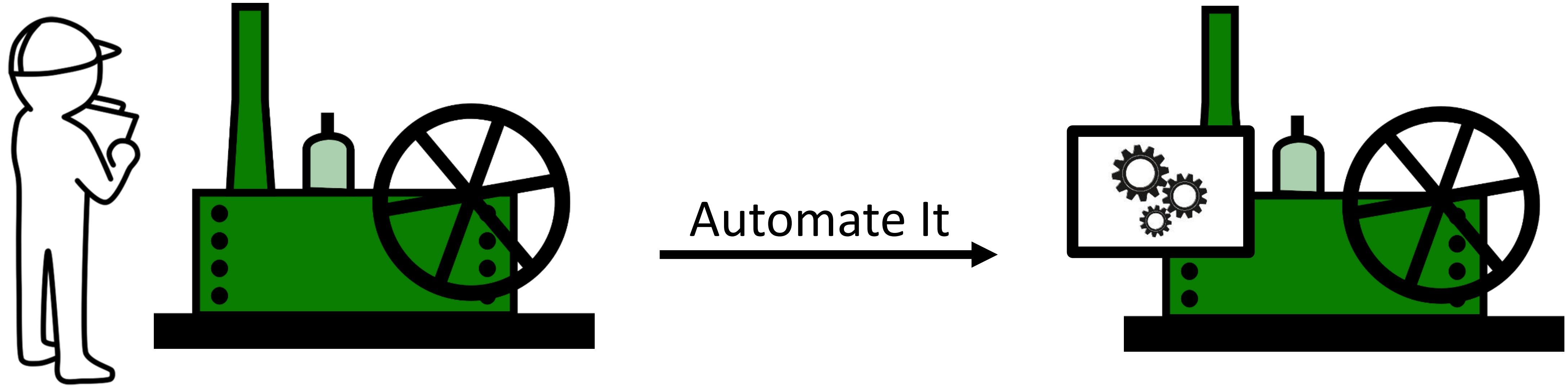
NEWS EMERGING TECH CYBERSECURITY Feb 15, 2017 | 2:48 pm

SHARE THIS STORY

Modernizing/Protecting Legacy Systems

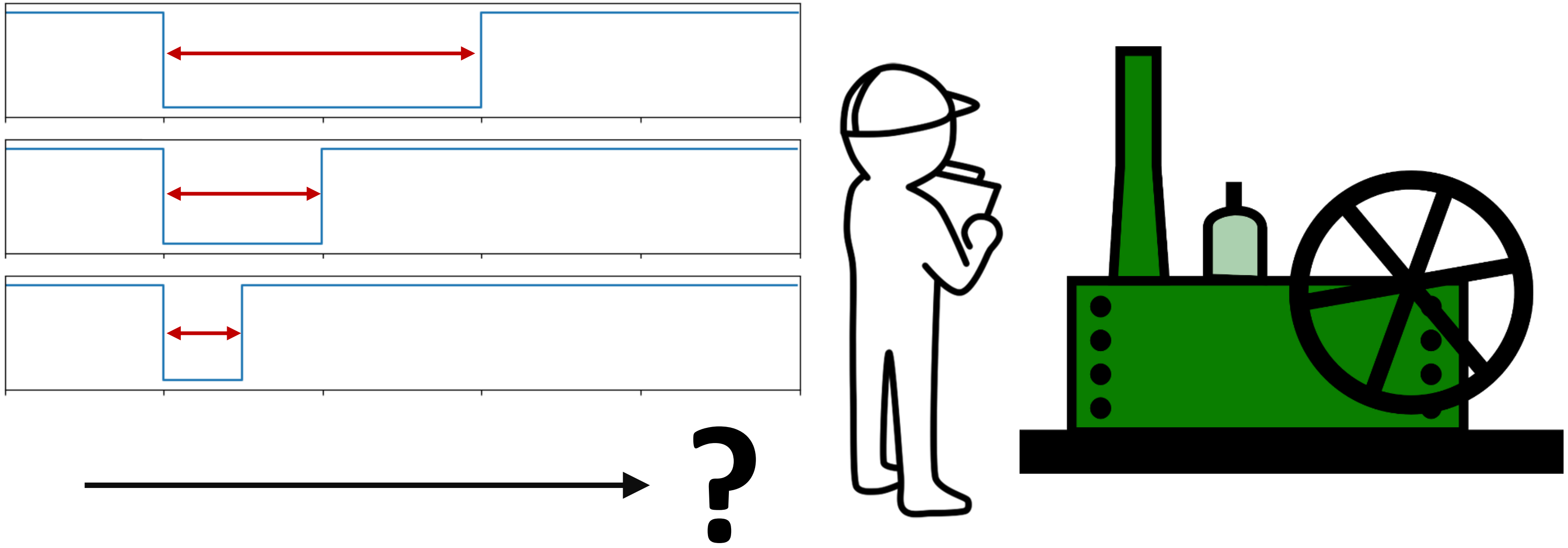


Undocumented Specification: Toy Example



Automate It

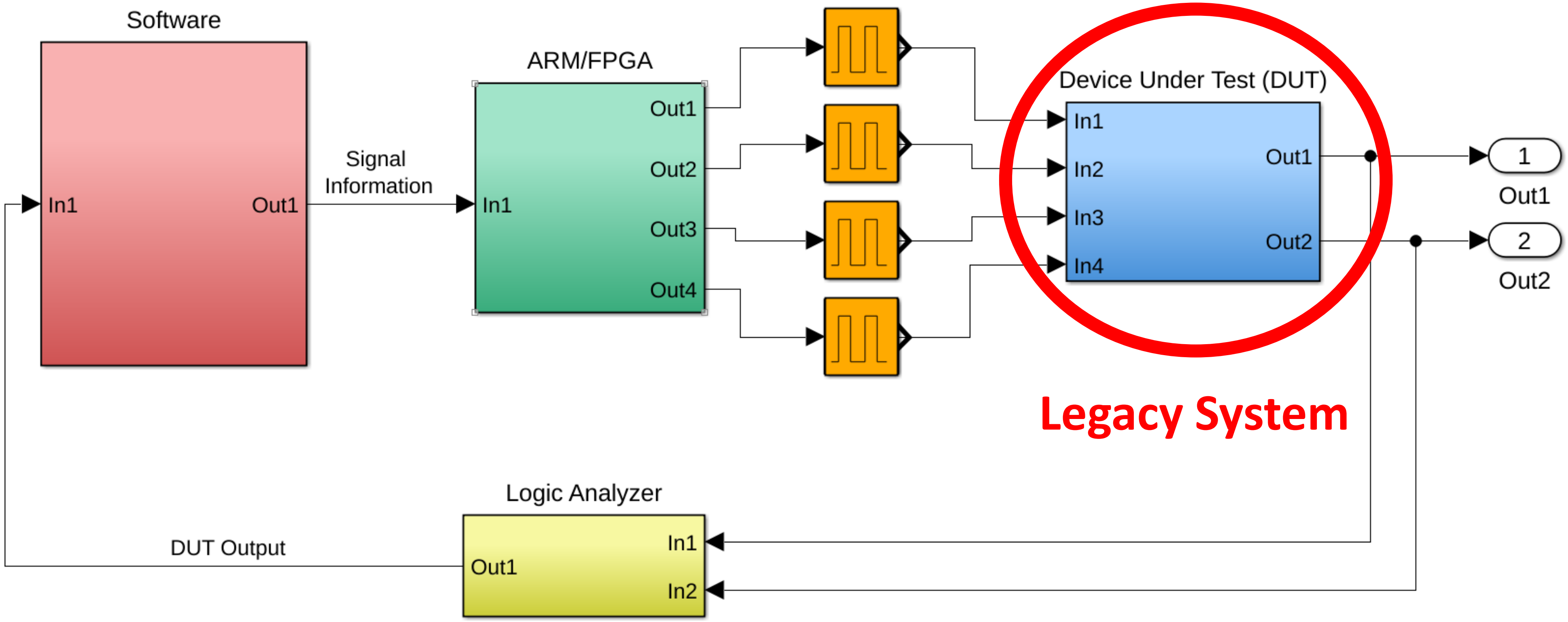
We want to automate the task of finding timing sensitivities



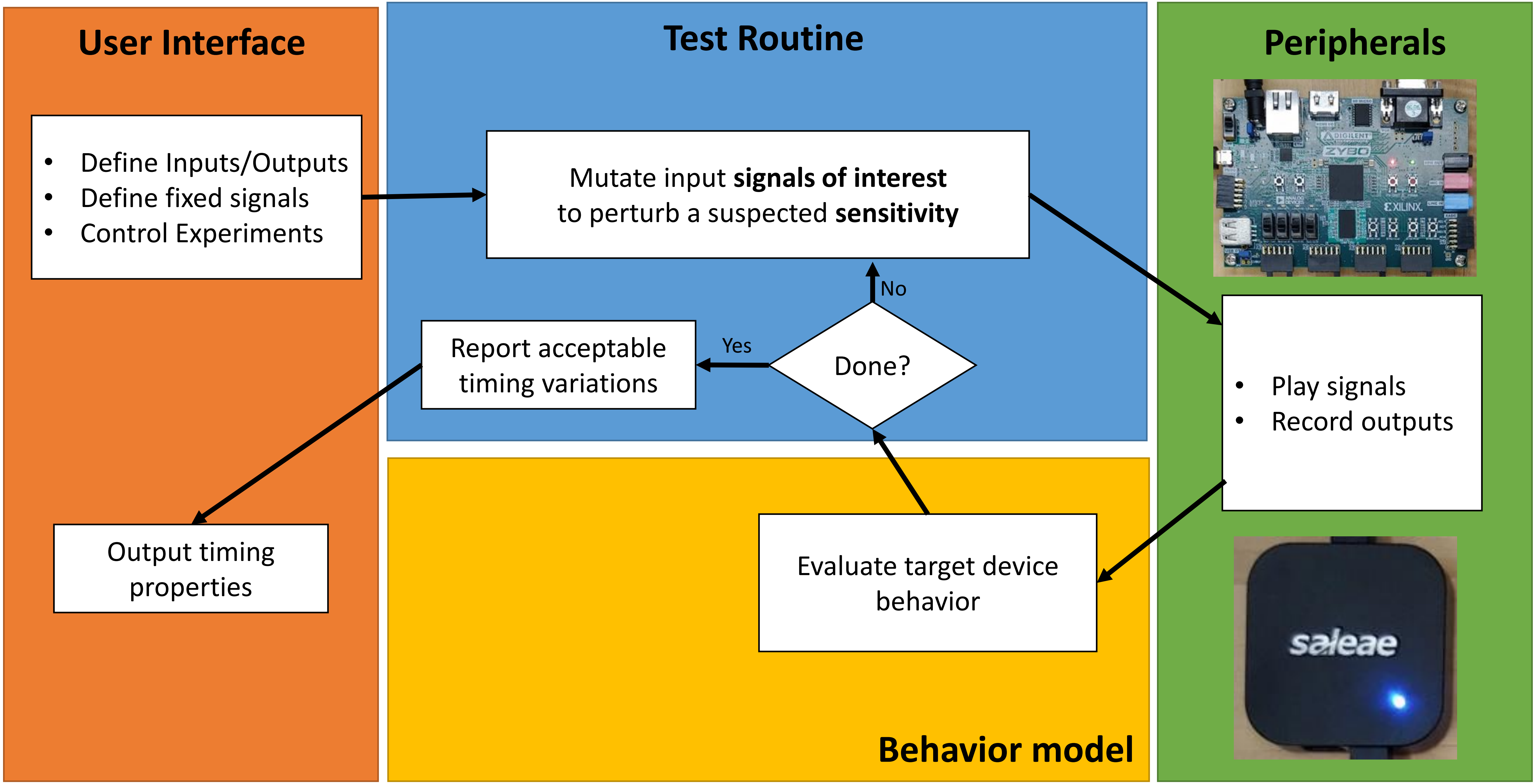
Goal: a tool for uncovering timing sensitivities

- Automated: run with minimal user interaction
- Versatile: applicable to different target devices
- Extensible: system capabilities can be augmented

Chronoscopic Assessment Engine for Recovering Undocumented Specifications



Legacy System



User Interface

- Define Inputs/Outputs
- Define fixed signals
- Control Experiments

Output timing properties

Test Routine

Mutate input **signals of interest** to perturb a suspected **sensitivity**

Done?

No

Yes

Report acceptable timing variations

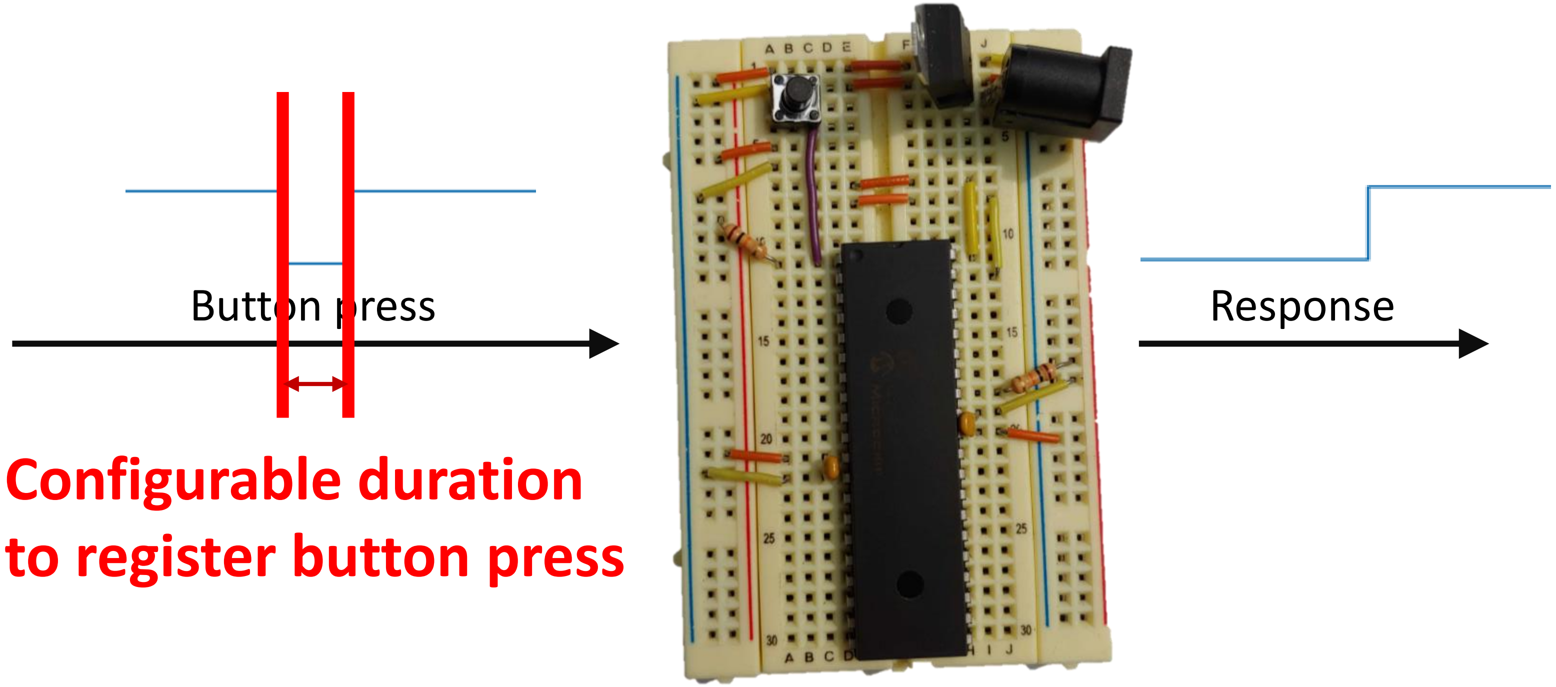
Behavior model

Evaluate target device behavior

Peripherals

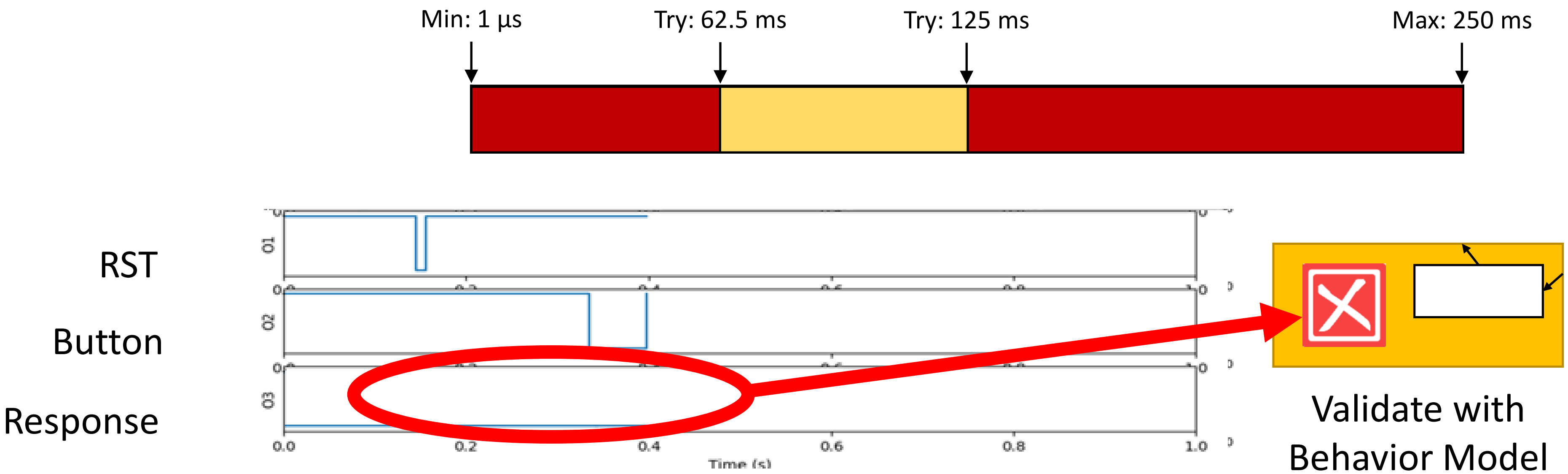
- Play signals
- Record outputs

Example Test Routine: Button Duration



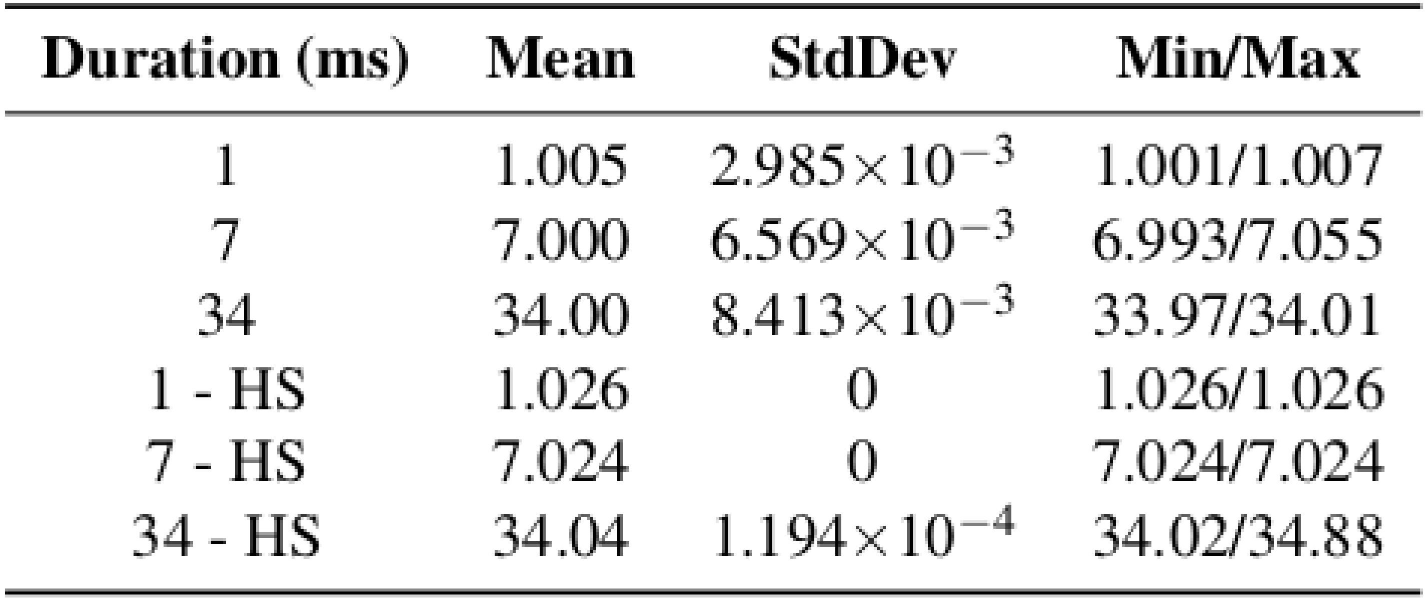
Configurable duration to register button press

Example Test Routine: Button Duration



Validate with Behavior Model

Example Test Routine: Button Duration



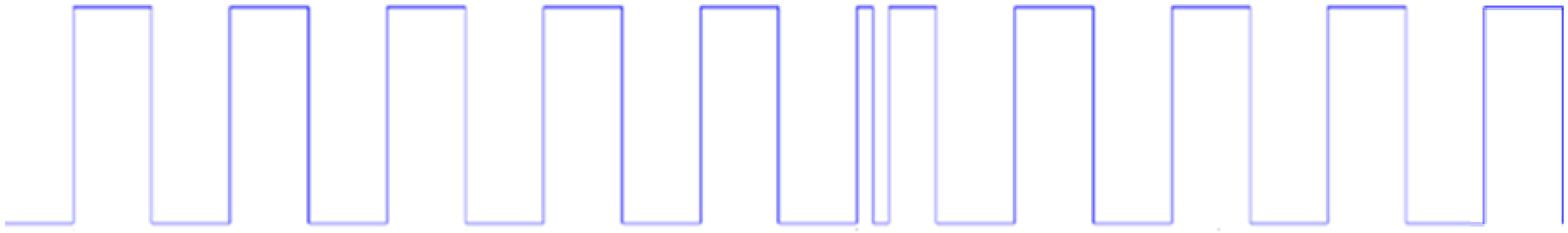
Duration (ms)	Mean	StdDev	Min/Max
1	1.005	2.985×10^{-3}	1.001/1.007
7	7.000	6.569×10^{-3}	6.993/7.055
34	34.00	8.413×10^{-3}	33.97/34.01
1 - HS	1.026	0	1.026/1.026
7 - HS	7.024	0	7.024/7.024
34 - HS	34.04	1.194×10^{-4}	34.02/34.88

- HS = High Speed crystal oscillator (precise)

Current & Future Work

Security Applications: Fault Injection Attacks

- CAERUS as an embedded device fuzzer
- Clock glitching (e.g., instruction skipping)
- CAERUS is useful for tasks such as finding the right clock cycle, etc…



Going Forward

- Released as open-source under Mozilla Public License
- Stream-lining installation, set-up
- Currently have library support for RS232, looking to add CAN, J1939
- Analog to test other attacks (e.g., brownout, reset)
- Combine peripheral devices

Summary

- Legacy systems & timing sensitivity
- CAERUS architecture
- Minimum button duration example
- Security applications
- Source available on github: https://github.com/caerus-timing