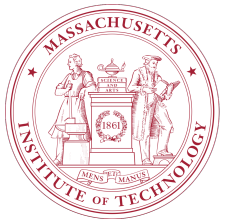


STORMBREAKER

AI-Enhanced
Industrial Control Systems Security

LT Joseph Post, USN

LT Sean Fitzgerald, USN

Garry Rosene

Olasunkanmi Kupoluyi

Problem Statement

Industrial Control Systems pose a significant vulnerability in today's society.

"…weapons of mass destruction…billions of dollars of damage…innocent lives lost…"

–Michael

Problem Statement

- ICS equipment, devices, applications, and protocols were not designed with security in mind.
- Vulnerabilities will always exist in legacy and new ICS networks (including air-gapped systems).
- ICS networks are susceptible to inadvertent user compromise of cybersecurity measures ("What's on this thumb drive?").
- Attackers are constantly utilizing sophisticated techniques (e.g., supply chain infiltration) to gain access to networks to potentially impose harm and disorder (e.g., equipment damage).

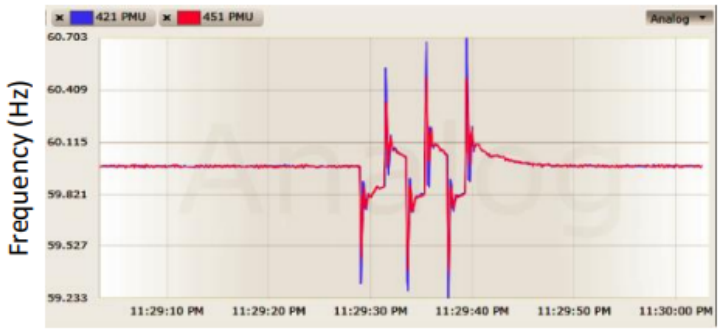
Case Study: HARVEY(1)

http://dx.doi.org/10.14722/ndss.2017.23313

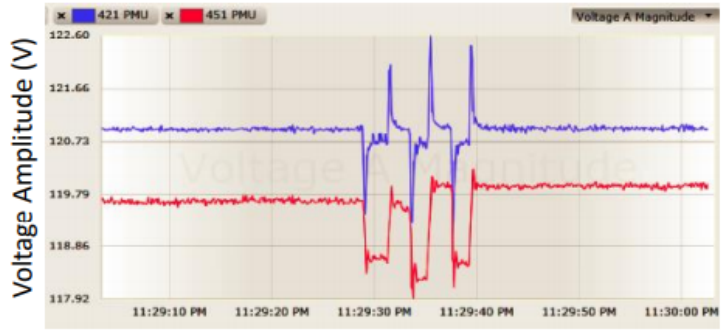
Case Study: HARVEY

- Researchers have created rootkit for Allen Bradley PLCs that can overwrite "good" logic commands with malicious commands
- Rootkit ("HARVEY") examines signal space of PLC and determines the optimal malicious modification to output commands
- HARVEY also generates fake data displayed to operators

Case Study: HARVEY

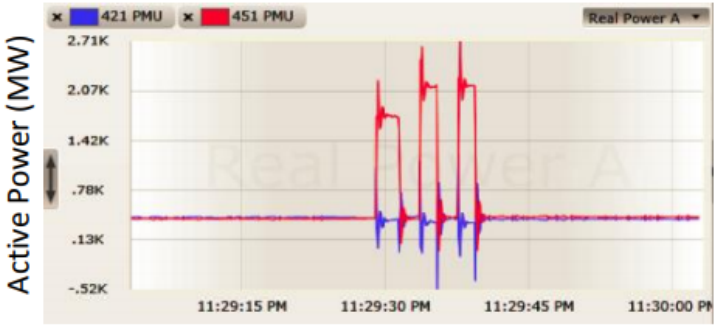


(a) Frequency



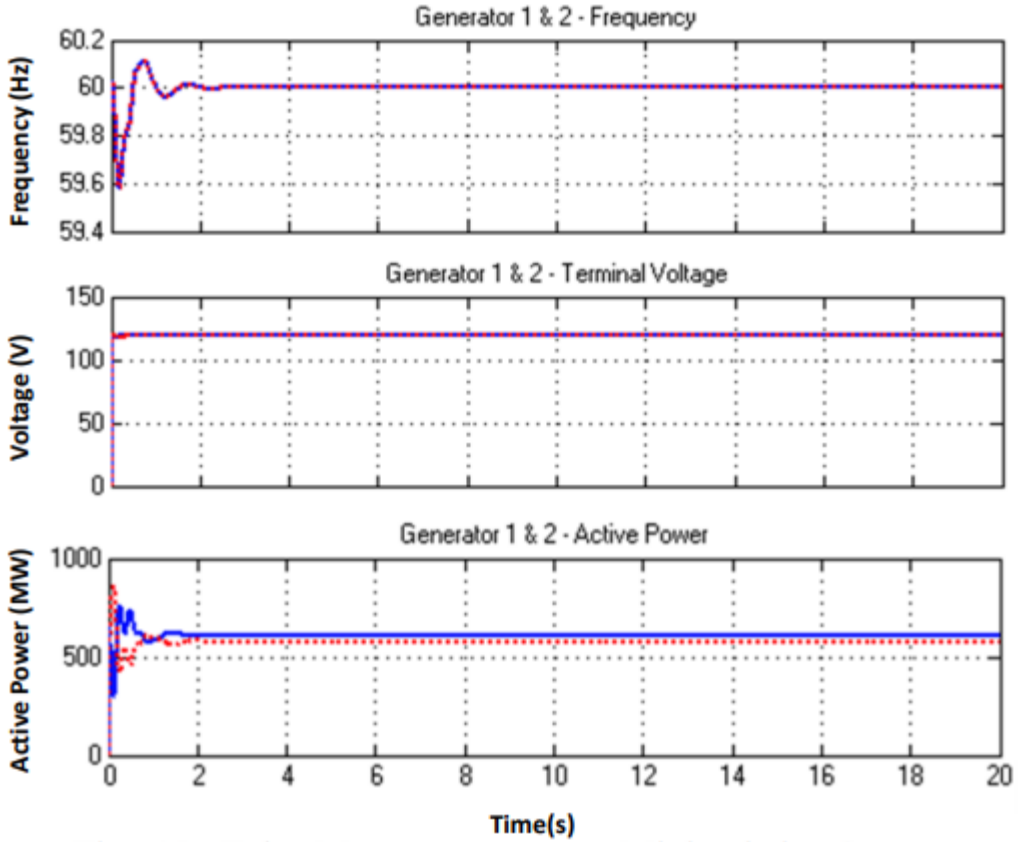
(b) Voltage Magnitude

(c) AC Voltage Phase Angle



(d) Power

Case Study: HARVEY



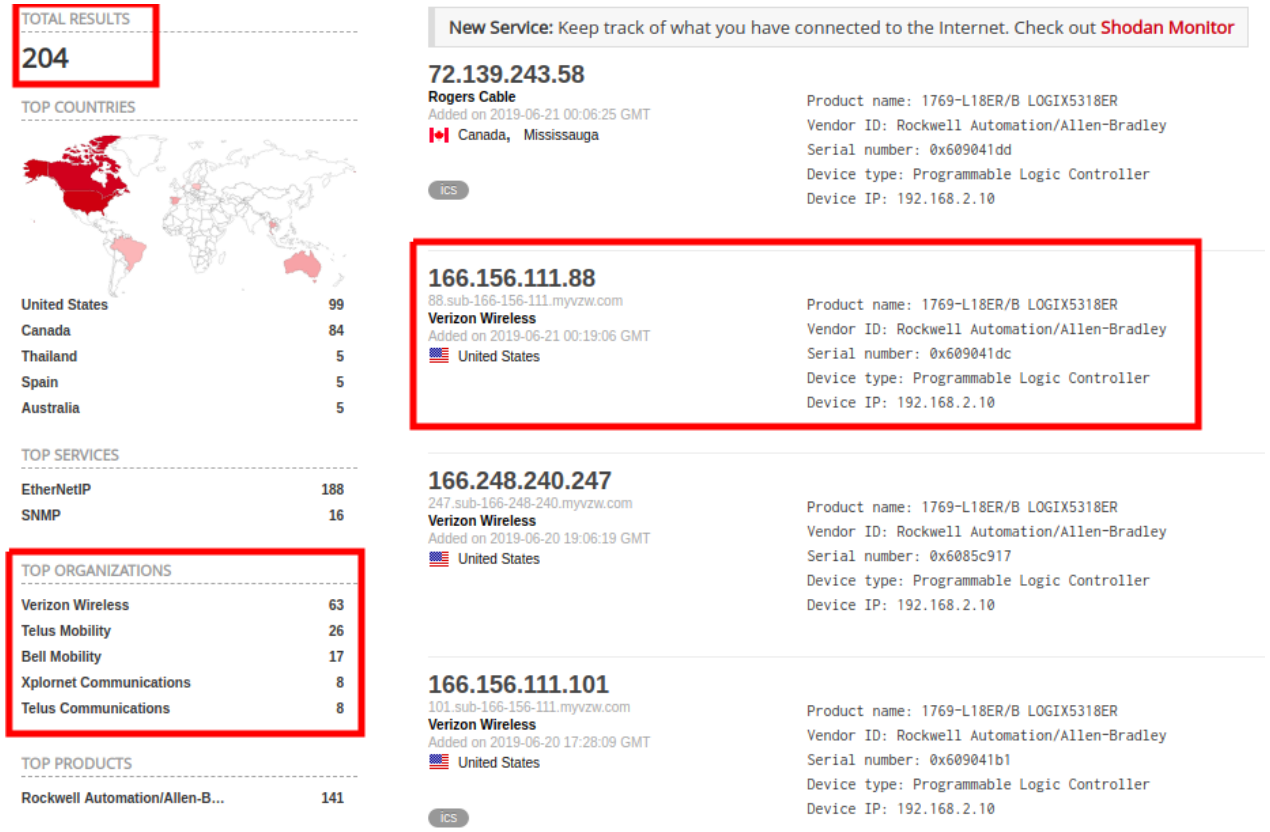
Case Study: HARVEY

Per the researchers: “HARVEY can be protected against using three major mitigation solutions: i) remote attestation allows a verifier to check the software integrity of a system... ii) with secure boot [which] ensures that only a known and trustworthy software can be loaded on a device...and”

Case Study: HARVEY

"iii) an external bump-in-the-wire device between the PLC controller and the physical plant could be monitoring the two-way sensor-to-PLC and PLC-to-actuator data streams. **The solution could possibly check whether the control commands issued by the PLC satisfy the plant's essential safety requirements** that must be defined by the operators. Additionally, the solution could implement coarse-grained control consistency checks **to validate whether sensor measurements and actuation commands are consistent in terms of how the plant should be controlled.**"

Case Study: HARVEY



TOTAL RESULTS

204

TOP COUNTRIES

United States	99
Canada	84
Thailand	5
Spain	5
Australia	5

TOP SERVICES

EtherNetIP	188
SNMP	16

TOP ORGANIZATIONS

Verizon Wireless	63
Telus Mobility	26
Bell Mobility	17
Xplornet Communications	8
Telus Communications	8

TOP PRODUCTS

Rockwell Automation/Allen-B...	141

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

72.139.243.58
Rogers Cable
Added on 2019-06-21 00:06:25 GMT
Canada, Mississauga

ICS

Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x609041dd
Device type: Programmable Logic Controller
Device IP: 192.168.2.10

166.156.111.88
88.sub-166-156-111.myvzw.com
Verizon Wireless
Added on 2019-06-21 00:19:06 GMT
United States

Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x609041dc
Device type: Programmable Logic Controller
Device IP: 192.168.2.10

166.248.240.247
247.sub-166-248-240.myvzw.com
Verizon Wireless
Added on 2019-06-20 19:06:19 GMT
United States

Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x6085c917
Device type: Programmable Logic Controller
Device IP: 192.168.2.10

166.156.111.101
101.sub-166-156-111.myvzw.com
Verizon Wireless
Added on 2019-06-20 17:28:09 GMT
United States

ICS

Product name: 1769-L18ER/B LOGIX5318ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x609041b1
Device type: Programmable Logic Controller
Device IP: 192.168.2.10

Our Solution: STORMBREAKER

Our Solution: STORMBREAKER

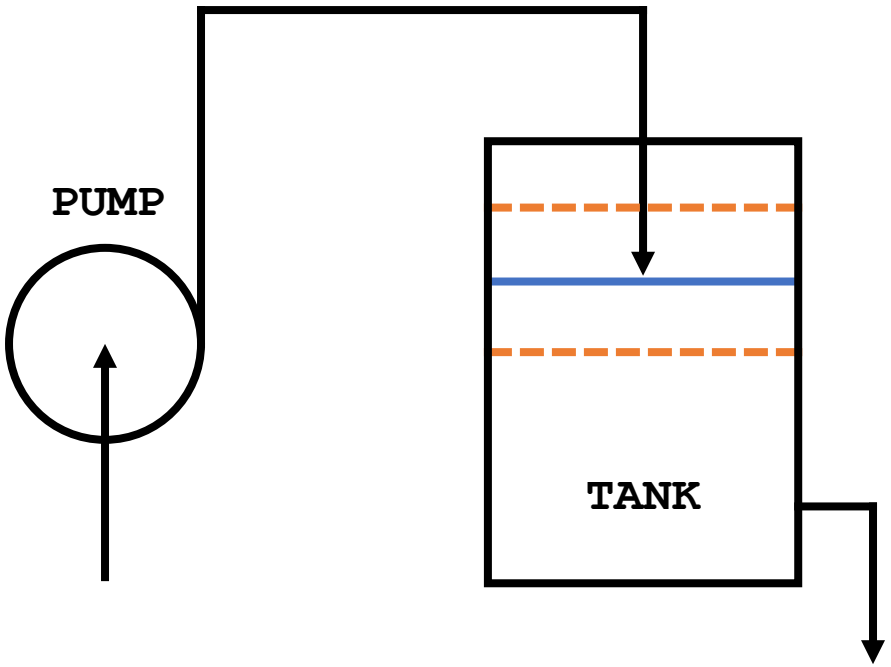
- An artificial intelligence (AI) algorithm implemented via Generative Adversarial Network (GAN)
- GANs are composed of two competing neural networks which attempt to fool each other
- The STORMBREAKER GAN is comprised of two, one-dimensional convolutional neural networks with a total of over 1 million parameters

STORMBREAKER

- Operator aid to mitigate safety issues such as equipment malfunction, environmental issues associated with critical systems.
- Can also be used as an electrical interlock to prevent inadvertent field device actuation of safety-critical systems
- Used in conjunction with existing ICS cybersecurity measures, not replace ICS-specific measures, policies, and procedures such as network blacklists, for example
- Comparable to existing AI-based tools used to process corporate (enterprise) network traffic (e.g., Amazon Web Services (AWS) GuardDuty™)

Feasibility Assessment

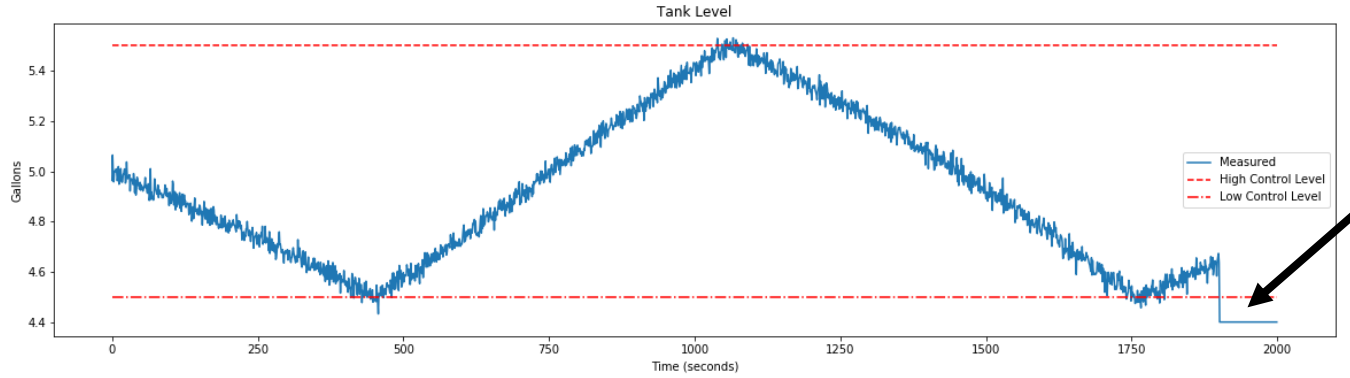
Feasibility Assessment

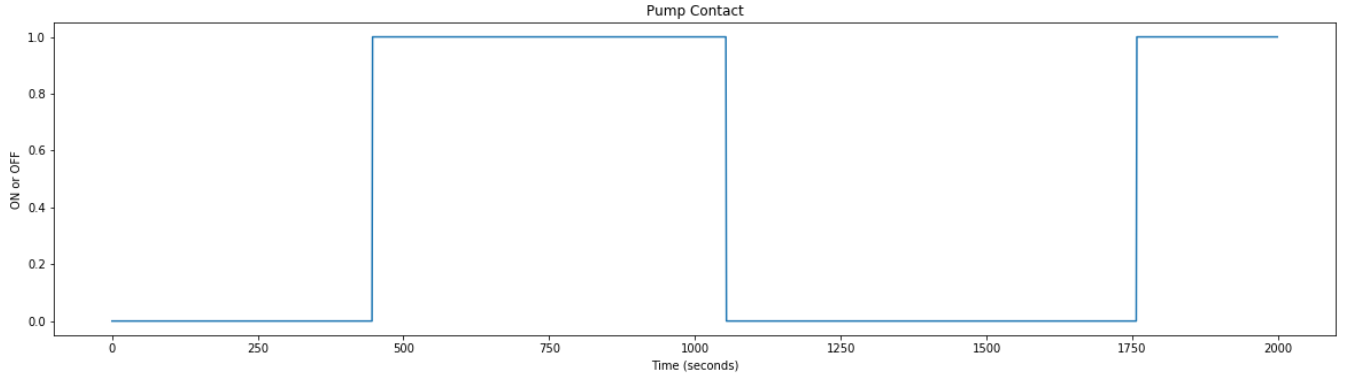


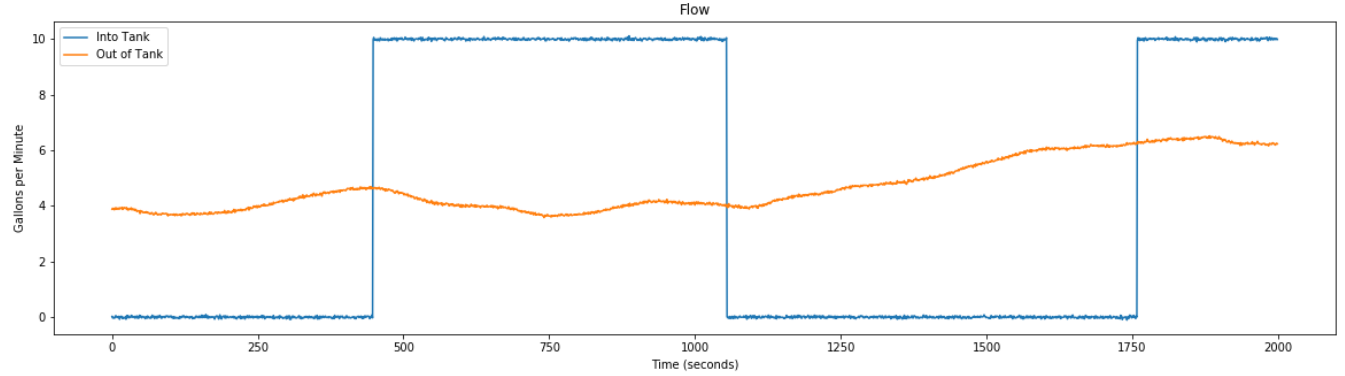
Measured Parameters:

- Pump ON / OFF
- Tank Level
- IN Flow
- OUT Flow

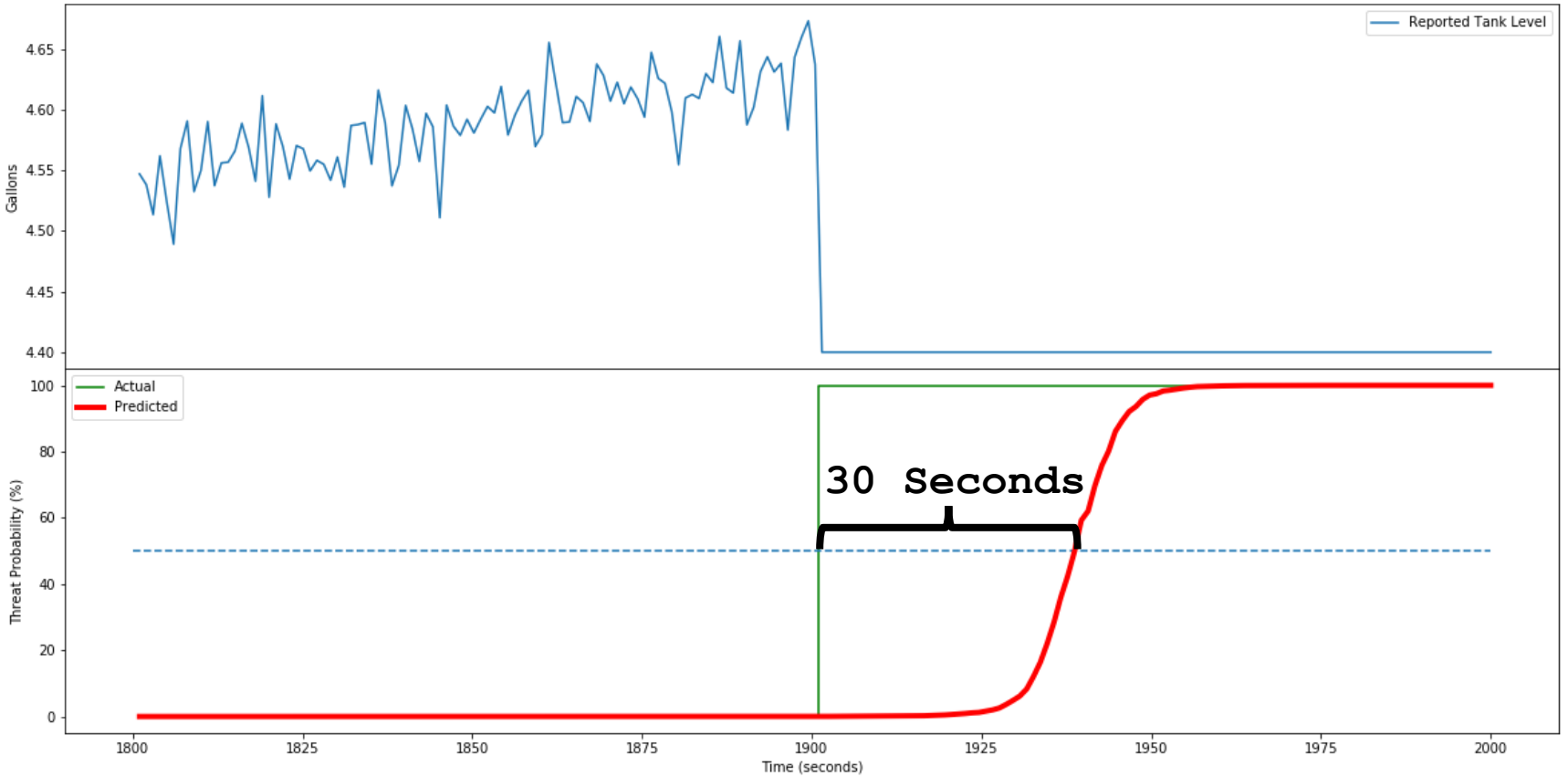
ICS Attack


Tank Level
Gallons
Time (seconds)
Measured
High Control Level
Low Control Level


Pump Contact
ON or OFF
Time (seconds)


Flow
Into Tank
Out of Tank
Gallons per Minute
Time (seconds)

Feasibility Assessment



Safety Critical ICS

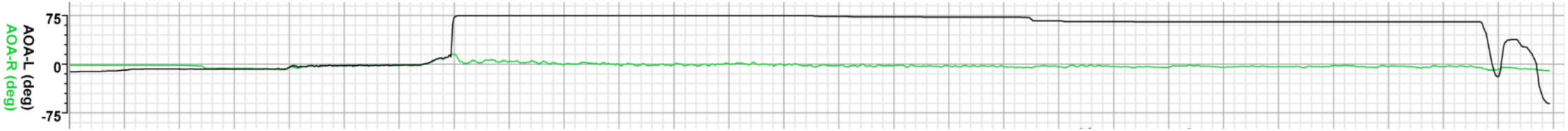
Lion Air flight 610

178 Perished

30 Minutes

Ethiopian Airlines flight 302

150 Perished

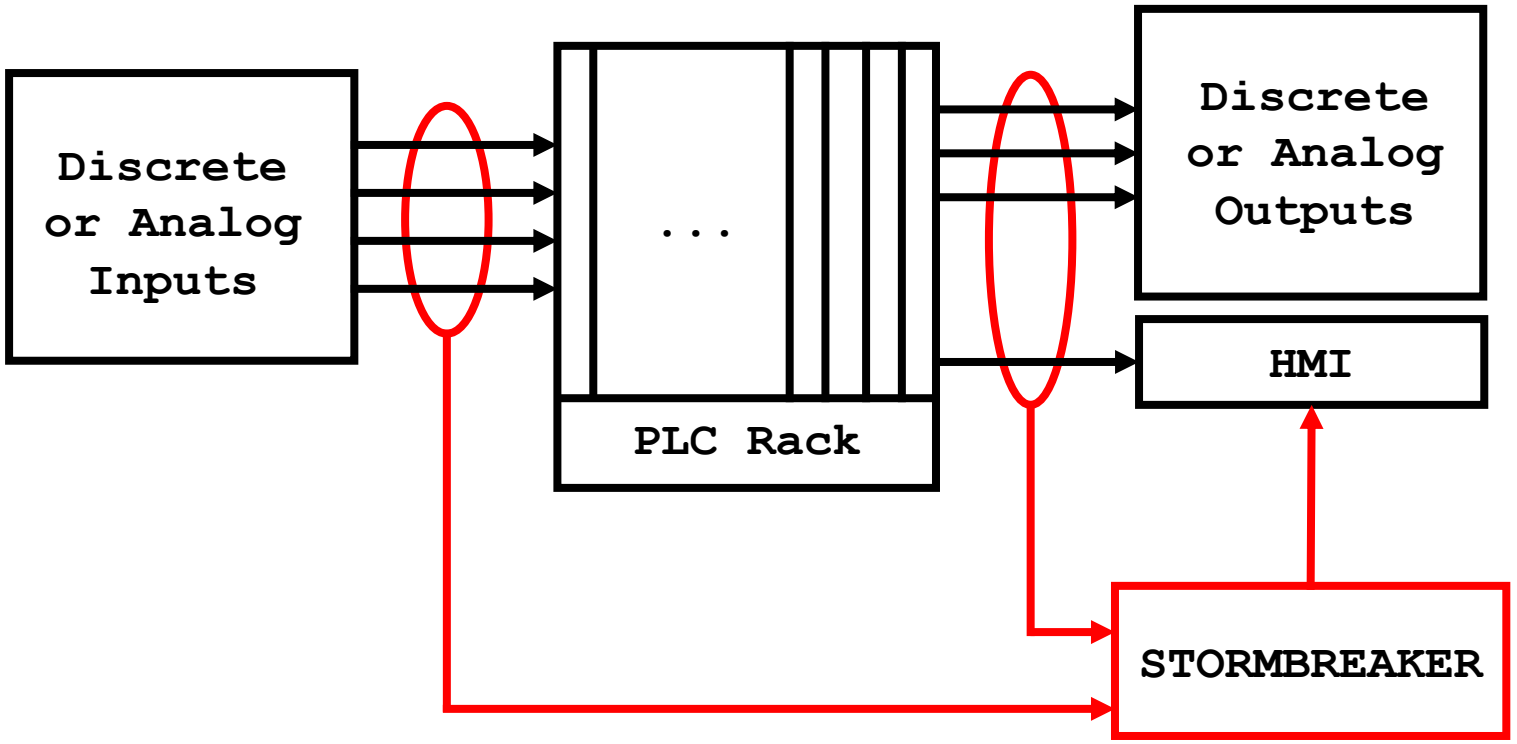


5 Minutes

Implementation

Implementation

We install STORMBREAKER in parallel with your current ICS.



Implementation

- Can be installed without downtime.
- Independent of current ICS
- Mitigates supply chain compromise
- Provides defense in depth

Implementation

Once installed, STORMBREAKER will alert when it detects abnormal parameters.

Potential Alarm Responses:

- Graceful degradation
- Switch to backup control
- Operator intervention (Safety Critical Systems)

GAN Pitfalls

- The “typical” GAN is notoriously susceptible to “mode collapse”(2)
- Mode collapse is when a GAN generator begins sending the discriminator data near a highly probabilistic mode in a multi-modal system
- This causes the discriminator to truly guess whether the generator data is real or not instead of optimally using the predictive algorithm
- This can lead to a “cat-and-mouse” scenario if the generator begins sending data near another highly-probabilistic mode in that system
- This can also lead to the discriminator completely forgetting large parts of the training dataset

GAN Pitfall Mitigations

- There are some solutions to mode collapse, such as Generative Latent Optimization (GLO)
- GLO is when the discriminator is essentially excluded from the generator training – this prevents mode collapse
- A discriminator would then be trained using the GLO generator
- Another alternative is using multiple GANs, although this is a potentially unwieldy solution – especially for large ICS networks

References

1. L. Garcia, F.Brasser, M. Cintuglu, A.R. Sadeghi, O. Mohammed, S. Zonouz, "Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit" https://www.ndss-symposium.org/wp-content/uploads/2017/09/ndss2017_08-1_Garcia_paper.pdf

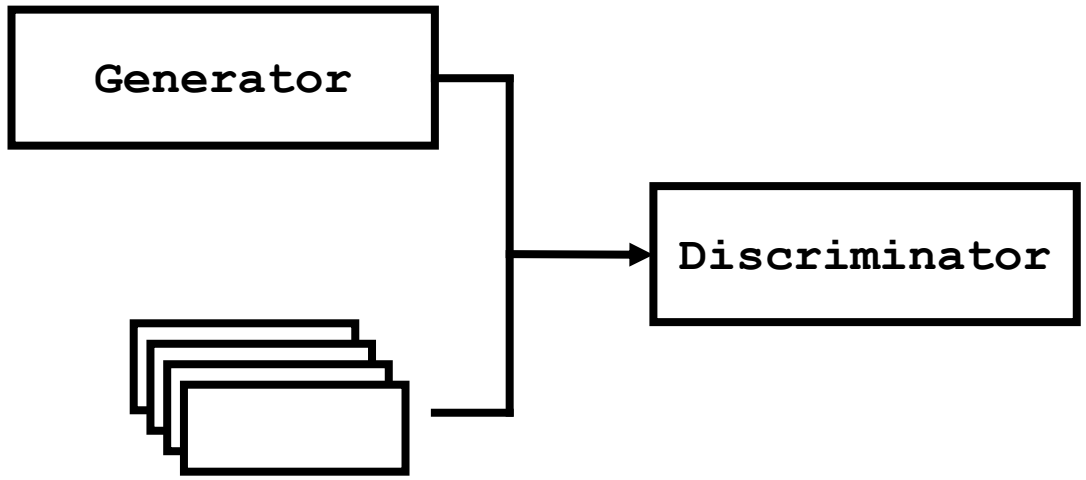
2. A. Nibali, "Mode collapse in GANs", 18 Jan 2017 https://aiden.nibali.org/blog/2017-01-18-mode-collapse-gans/

3. P. Bojanowski, A. Joulin, D. Paz, A. Szlam, "Optimizing the Latent Space of Generative Networks" https://arxiv.org/pdf/1707.05776.pdf


I WENT FOR THE HEAD

Backup Slides

Generative Adversarial Network



Generator: Neural Network for generating artificial data

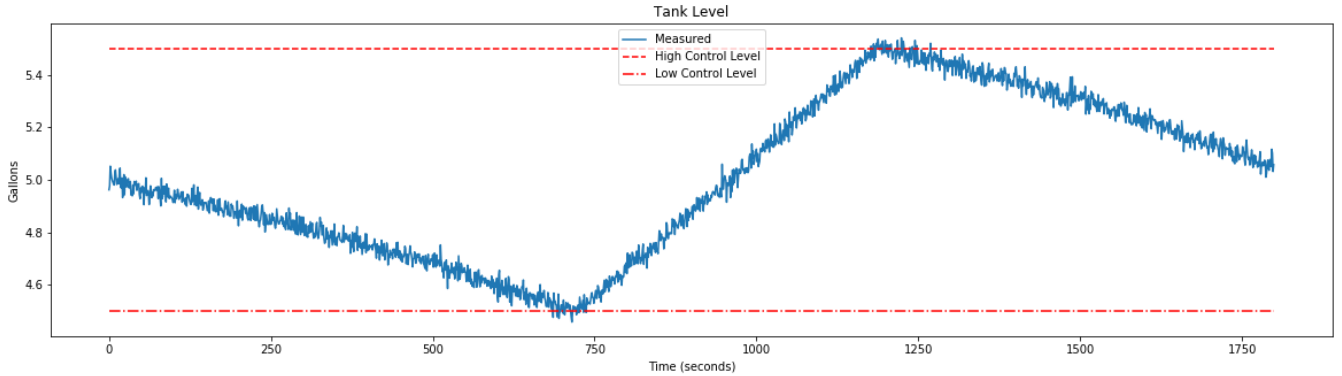
1. Input Layer (Latent space in R^{100})
2. Fully Connected(1800 neurons)
3. 1D Convolution* (128 length kernel)
4. 1D Convolution* (64 length kernel)
5. 1D Convolution* (32 length kernel)
6. 1D Convolution* (1 length kernel)

Discriminator: Neural Network for recognizing artificial data

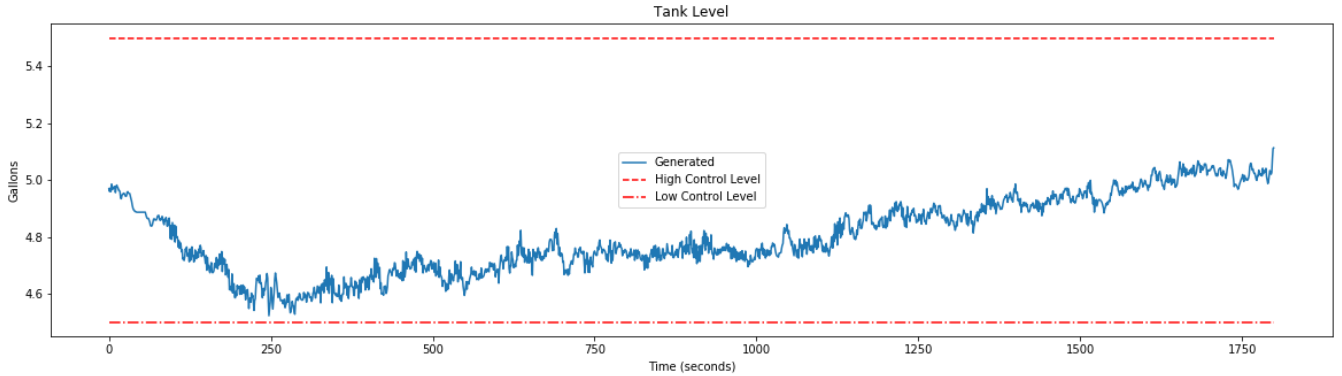
1. Input Layer (Tank level curve)
2. Fully Connected(128 neurons)
3. 1D Convolution** (128 length kernel)
4. 1D Convolution** (64 length kernel)
5. 1D Convolution** (1 length kernel, sigmoid activation)

* Length = 15, same padding
** Length = 7, valid padding

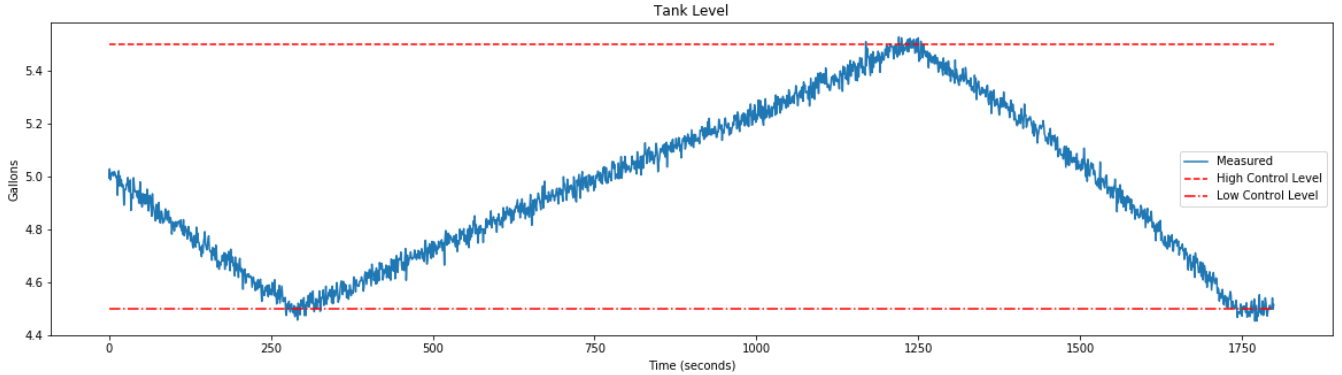
Generated Data

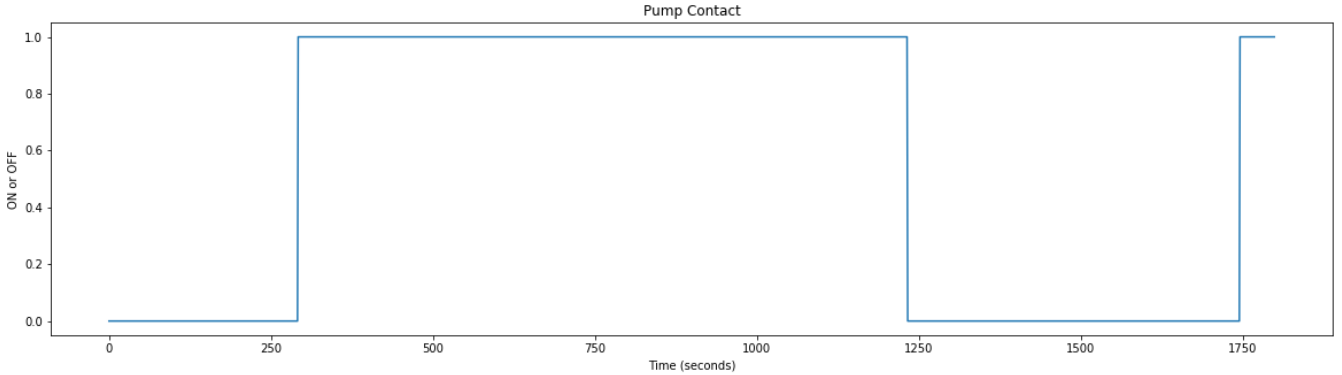


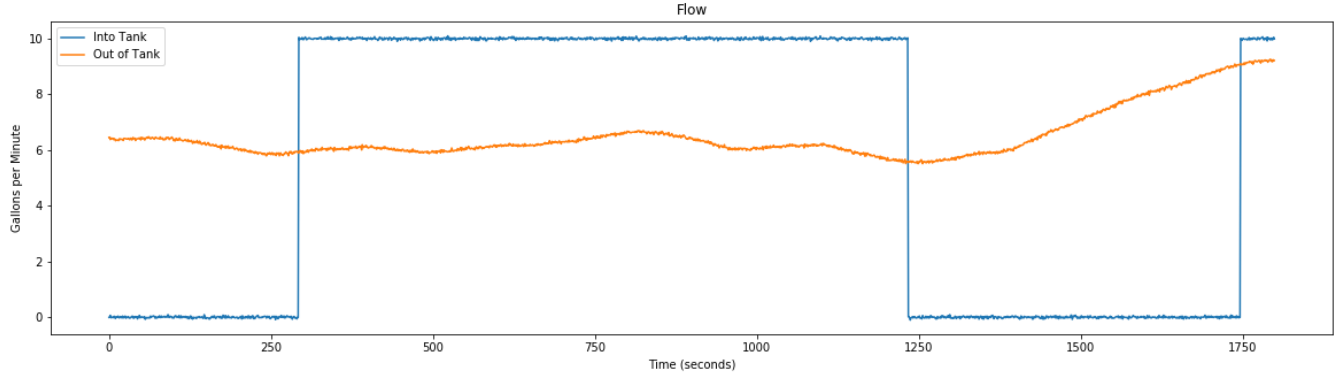
VS



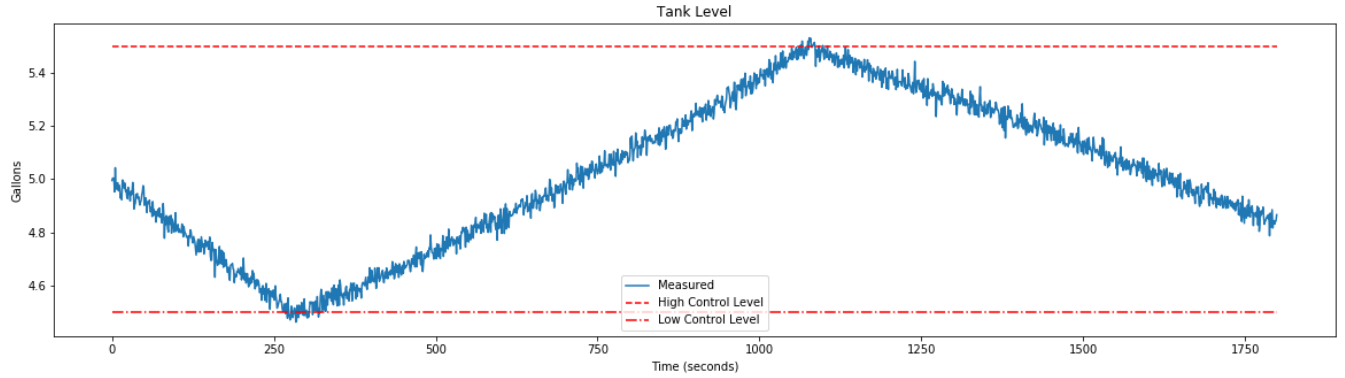
Sample Data 1

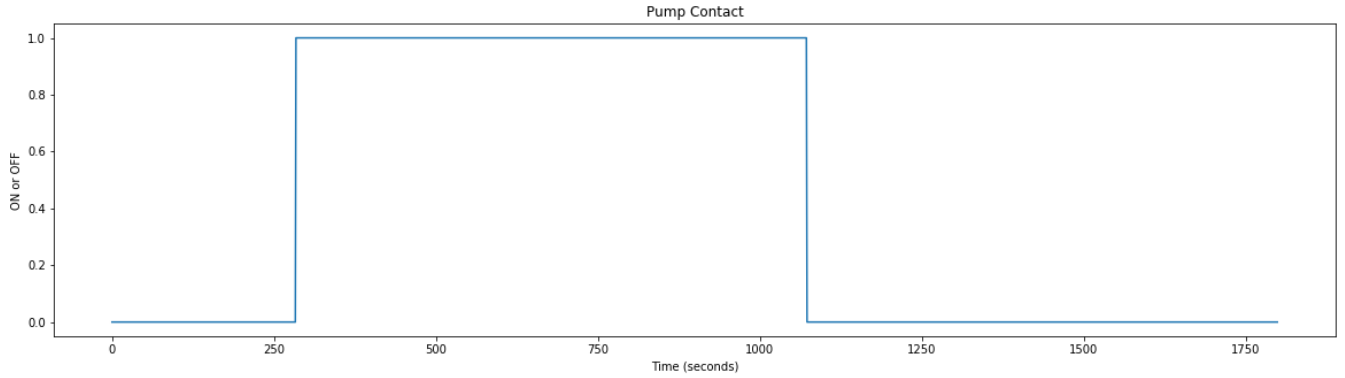


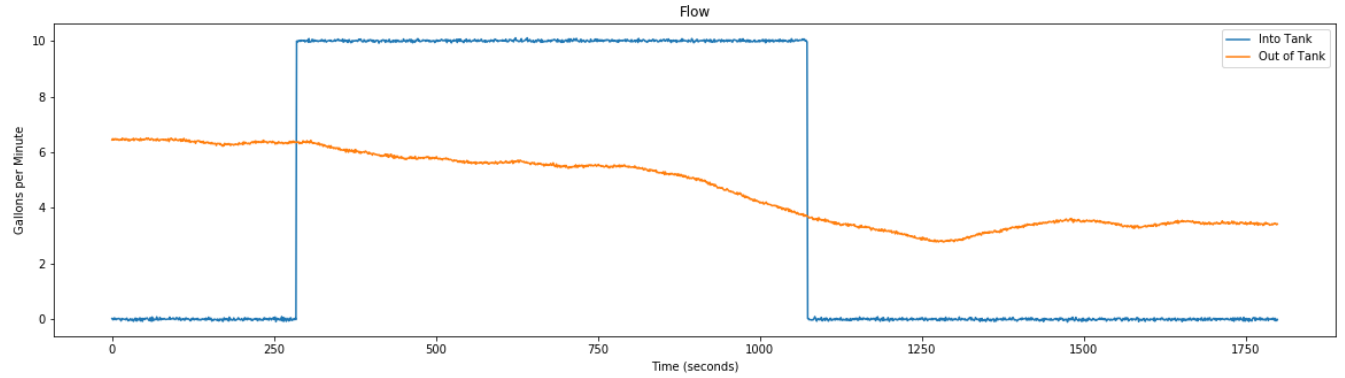




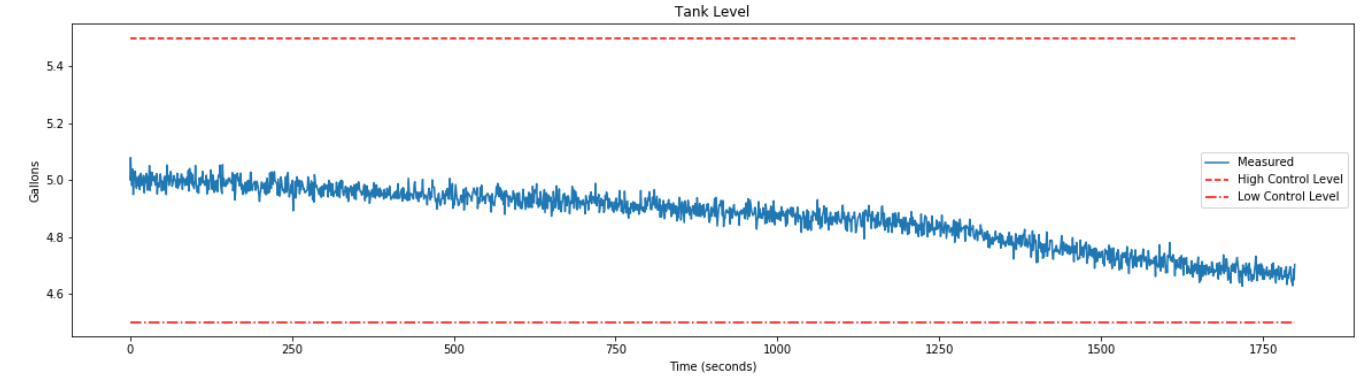
Sample Data 2

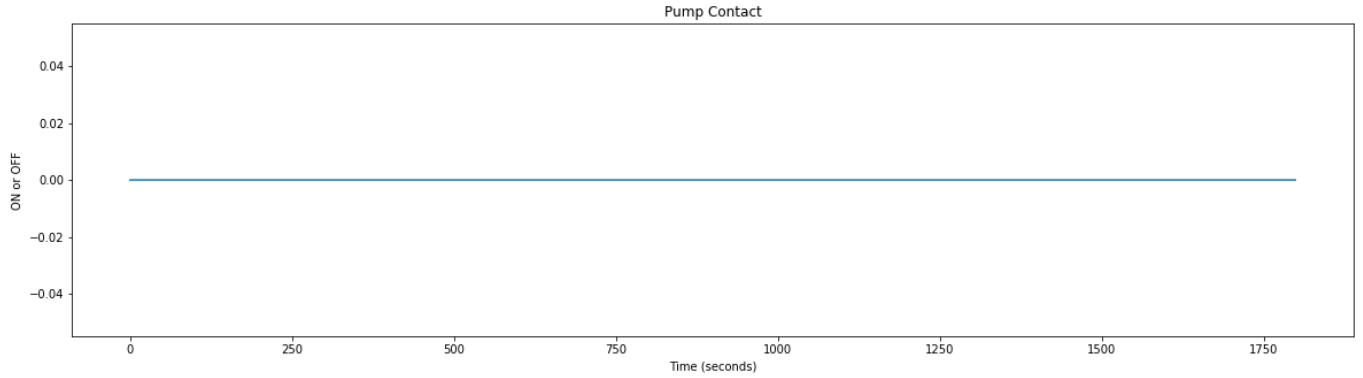


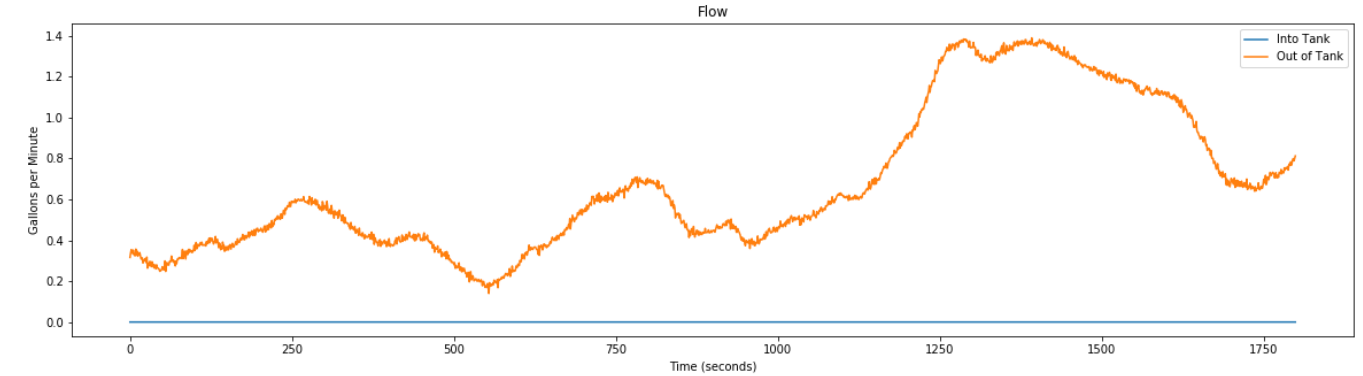




Sample Data 3







Sample Data 4