ADVANCECRT

Centre for Research Training

Science Foundation Ireland sfi For what's next

Collins Aerospace | APPLIED RESEARCH & TECHNOLOGY

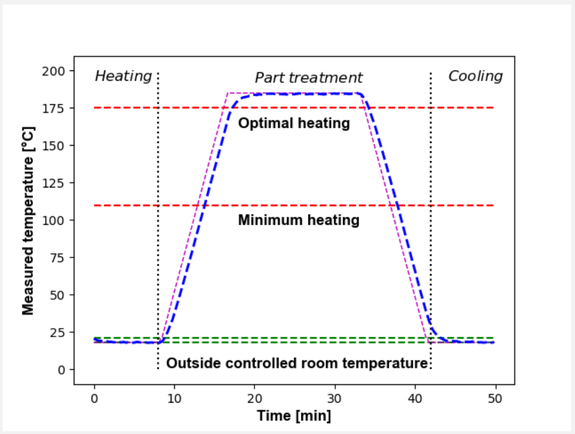
Challenges of Real-World CPS Anomaly Detection

Piotr Sobonski <120225685@umail.ucc.ie>, Utz Roedig <u.roedig@ucc.ie>

Introduction

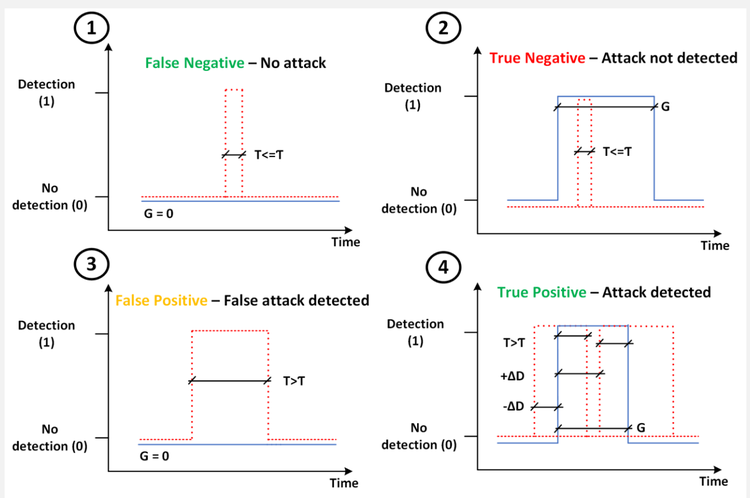
Cyber Physical System (CPS) are used to monitor and control large-scale industrial production processes. These installations can be subject to cyber attacks and appropriate attack detection methods are necessary. In this work we consider a facility producing medical implants. The implants require complex heat treatment and it is essential to detect potential tampering with this process. We describe potential attacks on this production process and show how a Machine Learning (ML) based Intrusion Detection System (IDS) can be constructed. We evaluate the effectiveness of different ML techniques used for intrusion detection. Then we describe and analyse challenges with such an IDS in a real-world setting; specifically we analyse the impact of limited training data and the drift of environmental conditions over time. Our work shows that sophisticated attacks on production environments can be detected but that constraints in real-world settings must be considered carefully.

Industrial process



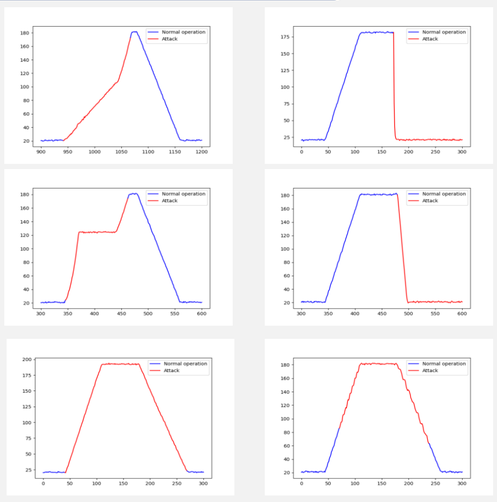
The graph represents reconstructed thermal process used in coating of medical implants in production line. The process ensures high quality of the implant by coating special material that ensures biological bonding inside the body. It is important to keep thermal profile stable during whole heat treatment process. The alternative leads to incorrect physical properties of the implant resulting in lower lifespan (replacement surgery) and patient discomfort. Anomaly detection process in this case is critical to maintain implant high quality, minimise production material loss and resources used.

Detection system design



To perform per cycle detection a cycle detector (CD) have been designed. The CD operates using depicted confusion matrix to detect anomalies based on number of detected faults coming from ML anomaly detection algorithm. Then depending on the CD configuration the number of anomalies are compared with desired attack detection length (system sensitivity).

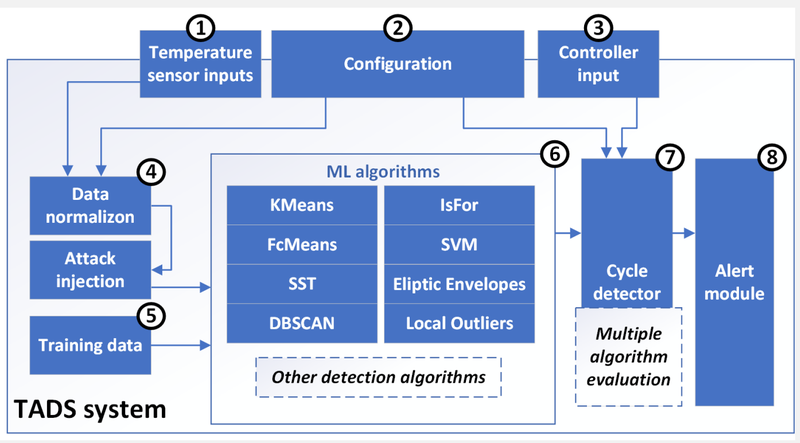
Attack modeling



Attacks were modelled based on the physical phenomena observed in the thermal chamber (industrial control system manipulation and accidental door opening). Both attacks have been modelled with two different variants. They belong to simple attacks category where even simple detection system can observe sudden thermal profile changes. Those attacks in our experimental effort were used as baseline.

The other two attacks listed on the bottom represents complex class of attacks, where shape of attack thermal profile is very similar and simile system will not be able to distinguish difference between benign and anomalous trace.

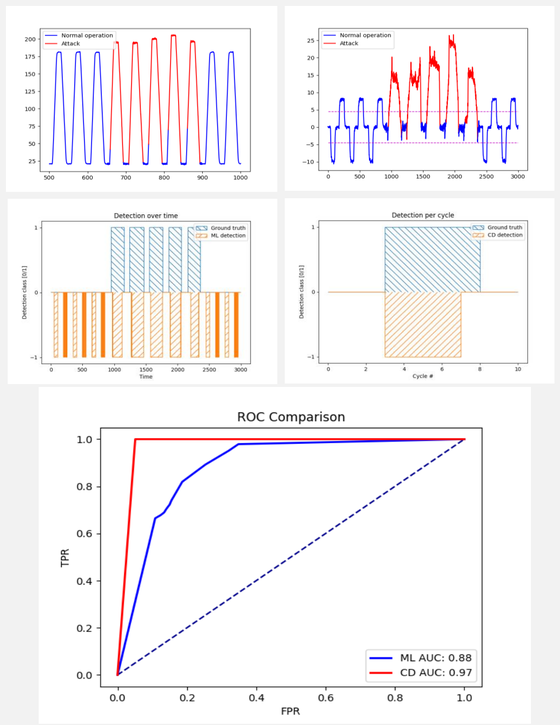
Experiment design



To perform designed experiment a Thermal Anomaly Detection System (**TADS**) has been designed to run experimentation and evaluation to asses detection capacity vs. simple and complex attacks. The picture depicts high level system architecture.

In step **1** all thermal sensor inputs are recorded and together with TADS configuration are sent data normalization process (**4**) where also attack injection is performed and this data set as part of training data(**5**) is sent to ML part of TADS system to create detection models (**6**). In step **7** all detection are received by cycle detector (**CD**) and evaluated from thermal perspective. Additional input is taken from thermal controller system (**3**) and configuration regarding CD sensitivity settings (**2**). Lastly depending on the CD output an alter system generates alters based on classification performed by CD component. With this system configuration we have performed simulated simple and complex attacks to evaluate designed system performance.

Results



Example shown here provides a sample generated based on complex attack called constant offset (marked red). Frist two graphs represents original attack trace and it differential input that was fed to ML detection and CD detector.

Middle graphs represents detection performed by ML and CD part of the experimental TADS system, where blue represents ground truth and orange detection. We can observe a higher fidelity performed by CD where only longer duration anomalies where classified as attack. In return this approach brings higher level of confidence in detection and reduce number of fake alerts that would result in fault production and reduced production rate.

Last graph represents generated ROC (Receiver Operating Characteristics) detection performance comparison between ML and CD part of TADS system.

Conclusions

The experimentation results provided insight that confirms following findings:

- **Attack duration** – longer attack lasts there is higher likelihood to detect it,
- **Attack complexity** – the more complex (high similarity) attack is the less chance detection system have to correctly classify it,
- **ML detection algorithm** – various detection algorithms are useful in detection different type of attacks,
- **IDS complexity** – system complexity incurs higher detection rate at a higher cost.

Future work

Next stage of research work will look into employment of deep learning algorithms and more complex and subtle attacks (more difficult to detect) and evaluate results with same design of experiment. Further stage will include development of **CP (Constraint Programming) based optimization** detection engine to improve anomaly detection across all type of industrial process attacks. Lastly the **multi-dimensional CPS systems** will be taken into consideration to applied techniques with more complex and dynamic environments of **aero-space domain**.

Host Institution

University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University

Maynooth University National University of Ireland Maynooth

TU DUBLIN Ollscoil Teicneolaíochta Bhaile Átha Cliath Technological University Dublin

Trinity College Dublin Coláiste na Tríonóide, Baile Átha Cliath The University of Dublin