Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1403

사이버 공격 대비 가동 물리장치에 대한 실시간 간접 상태감시시스템 설계 및 구현*

김 홍 준†‡
대전대학교 컴퓨터공학과

Design and Implementation of Real-Time Indirect Health Monitoring System for the Availability of Physical Systems and Minimizing Cyber Attack Damage*

Hongjun Kim†‡
Dept. of Computer Engineering, Daejeon University

요 약

터빈, 배관 및 저장탱크와 같은 물리장치들의 경우 노후화뿐만 아니라 제어장치에 대한 사이버공격으로 인해 PLC (Programmable Logic Controller)와 같은 제어시스템의 보호 및 상태감시기능이 동작하지 않는 경우, 피해파급력이 크고, 가동 중지 시 그 비용 손실 또한 매우 크다. 가동 중인 물리장치의 작동을 중지하지 않고 간접적으로 상태감시를 함으로써 가용성을 유지하기 위한 방안으로써 온도, 가속도, 전류 등을 간접적으로 감지하고, 데이터들을 Influx DB에 저장하여 실시간으로 감시하는 시스템을 설계 및 구현한다. 실제 구현된 시스템으로부터 데이터를 얻고 이를 이용하여 이상상태를 감지할 수 있음을 검증하였다. 간접적 실시간 감시시스템의 범용화를 통해 데이터를 축적해 활용하면, 추가비용 없이 가동을 중지하지 않고 사용할 수 있을 뿐만 아니라 미리 고장을 예측하고 필요한 경우에만 조치를 취하는 고장예지기술, 이상상태를 이중으로 감시하는 신뢰도 높은 건전성 관리 기술을 통해 유지보수비용과 위험도를 대폭적으로 감소시키고, 보안위협에 대한 대비가 가능하다.

ABSTRACT

Effect of damage and loss cost for downtime is huge, if physical devices such as turbines, pipe, and storage tanks are in the abnormal state originated from not only aging, but also cyber attacks on the control and monitoring system like PLC (Programmable Logic Controller). To improve availability and dependability of the physical devices, we design and implement an indirect health monitoring system which sense temperature, acceleration, current, etc. indirectly, and put sensor data into Influx DB in real-time. Then, the actual performance of detecting abnormal state is shown using the indirect health monitoring system. Analyzing data are acquired using the real-time indirect health monitoring system, abnormal state and security threats can be double-monitored and lower maintenance cost utilizing prognostics and health management.

Keywords: PHM (Prognostics and Health Management), failure prediction, indirect sensing, real-time surveillance

Received(09. 04. 2019), Modified(12. 03. 2019), Accepted(12. 03. 2019)

* 이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2019S1A5C2A03082827)

† 주저자, hjkim99@dju.kr
‡ 교신저자, hjkim99@dju.kr(Corresponding author)

I. 서 론

터빈, 배관, 그리고 저장탱크와 같은 물리장치의 경우, 노후화 및 사이버 공격으로 인한 손상이나 완벽하지 않은 모델링으로 인한 오작동 및 오류 발생 시, 그리고 유지관리 및 정비를 위해 가동을 중지하는 경우 막대한 손실을 입기에 고장예지기술 및 간접적 건전성 관리시스템의 연구가 필요하다. 고장예지 및 건전성 관리(PHM, Prognostics and Health Management)기술은 운용 중인 시스템이나 장치에 대해 결함이나 성능저하를 지속적으로 관찰하고, 이상 징후를 진단하며, 이상상태에 도달할지 미리 예측, 필요한 경우에만 정비조치를 하는 기술을 의미한다. 최근 수명주기 동안 안전을 보장하는 신뢰성기반 설계기술이 활발하게 연구[1]되고 있지만 물리장치들과 제어시스템들의 가동 중 발생하는 모든 상황과 조건들을 고려하는 것이 불가능하기 때문에 실제 적용에는 한계가 있다.

한편, 국내의 한국 수력원자력 해킹사례를 비롯하여 최근 우리나라뿐만 아니라 전 세계적으로 산업제어시스템에 대한 보안위협이 증가하고 있고, 관련된 사고도 늘어나는 추세를 보이고 있다.

본 논문에서는 사이버공격이나 고장으로 인한 피해파급력이 큰 터빈, 배관, 그리고 저장탱크를 선정한 후 간접적 센싱 기반의 모니터링을 통해 해당 물리장치들이 가동 중에서도 실시간 모니터링이 가능한 간접적 센싱 기반 실시간 상태감시 시스템을 제안하고 구현한다. 이를 통해 해당 물리장치들의 상태확인 및 정비를 위해 필연적이었던 가동 중단을 막음으로써 가용성을 확보하여 신뢰성 확보와 유지보수 비용을 최소화 하는 것과 더불어 보안성을 향상시킨다.

본 논문은 다음과 같이 구성된다. 2장에서는 각 물리장치의 사고와 고장요인을 분석하고, 3장에서는 이를 바탕으로 각 물리장치의 간접적 상태감시 방안을 제시한다. 4장에서는 공격 시나리오를 제시하고, 5장에서 간접적 건전성 관리시스템을 구현, 이상상태를 감지할 수 있음을 검증한다. 마지막으로 5장에서는 논문의 내용 및 결과를 요약하여 끝맺는다.

II. 물리장치 사고원인 및 주요고장요인 분석

2.1 터빈

터빈은 높은 온도와 압력, 그리고 원심력 등 악조건 하에서 운영되므로 강인하게 설계되지만 사고의 위험 및 그 피해 정도가 심각하며 어떤 문제가 발생하였을 경우에는 짧은 시간이 아닌 장시간의 소음과 과열, 진동 증상이 발생한다[2].

증기터빈의 경우 러빙, 피로와 크립 파손, 베어링 손상, 열응력 균열 순으로 나타나는 고장의 형태가 전체 고장의 60% 이상을 차지하고, 가스터빈의 경우는 상당수의 고장이 터빈의 블레이드와 로터, 노즐, 베어링 부분에서 발생하므로, 터빈 블레이드와 로터를 우선적으로 상태 감시하여 이상상태를 판별할 필요가 있다.

2.2 배관

배관은 내부 물질의 종류에 따라 누출된 경우의 피해 차이가 크고 노후화 및 부식, 균열로 인한 사고가 꾸준히 발생하고 있다[3]. 가스배관은 도심의 지하를 관통하고, 원자력 발전소의 배관은 파손 시 원전의 안전성에 직접적이고 심대한 영향을 미치기 때문에 수명기간 동안 배관 자체의 건전성이 보장되어야 하며, 배관파손의 경우에도 주변 기기 및 구조물의 건전성이 유지되어야 한다.

배관의 결함은 대표적으로 부식 결함과 기계적 결함으로 나눌 수 있다. 부식 결함은 단일 부식, 다중 부식으로 나뉠 수 있으며, 기계적 결함의 경우 가우지 결함, 덴트 결함으로 나뉠 수 있다[4]. 노후화에 따른 부식도 매년 크게 늘고 있다[5].

2.3 저장탱크

저장탱크 또한 배관과 마찬가지로 저장탱크 내부 물질의 종류에 따라 누출된 경우 피해 차이가 크고, 과압 및 부압, 균열에 의한 누출사고 빈도가 높다. 저장탱크 과충전에 의한 넘침, 고압에 의한 손상, 진공에 의한 손상, 기계적 건전성 상실 등 탱크 자체의 고장에 의한 파손뿐만 아니라 전원 상실, 계기용공기 상실 등을 초기사건으로 하는 탱크파손사고도 발생한다[6]. 그 밖의 요인으로는 관련배관이 파손되는 경우로 유입배관 파열, 송출배관 파열 등이 있다.

2.4 제어시스템

터빈, 배관, 그리고 저장 탱크와 같은 물리장치에 대한 제어시스템(PLC, Programmable Logic

Controller)의 보안은 상대적으로 취약하여 지난 10년간 많은 사이버공격이 성공한 바 있다[7]. 이와 같은 사이버공격을 감지하여 안정성을 확보하는 것은 해당 물리장치들의 피해파급력을 생각할 때 매우 중요한 일이다. 최근 높은 복잡도를 갖는 제어시스템을 선형 모델로 근사화하고, 이 모델을 기반으로 제어시스템의 다음 상태를 칼만필터를 이용, 예측하여 오차가 일정이상 큰 경우를 이상이라고 판단하는 알고리즘들이 있다[8][9]. 그러나 사이버공격자들도 제어시스템의 운영 상태를 통해 선형 모델을 유추하고, 이 모델을 이용하여 오차범위 내에 있도록 하는 공격을 하고 있고[10][11], 기계학습을 이용한 제어시스템 이상 징후 탐지시스템들도 공격자가 탐지를 우회할 수 있다는 한계점들을 가지고 있다.

III. 물리장치 간접적 상태감시 방안

3.1 터빈

터빈이 이상상태에서 동작하는 경우 증상으로 나타나는 것은 장시간의 과열 및 진동이므로 터빈의 구성요소 외부에 온도 및 가속도계를 밀착하여 장착한 후 감지한다. 측정된 온도가 내부 온도와 차이를 보이는 문제는 동일 환경에서의 실험결과 및 모델기반 캘리브레이션을 통해 보정이 가능하고, 진동의 경우도 마찬가지로 데이터를 축적한 후 모델링을 통해 높은 확률로 이상상태 감지가 가능하다. 풍력터빈의 경우는 경사계와 가속도를 융합하여 변위를 추정함으로써 풍력 터빈의 변위를 상시 계측하여 안정성관리를 하는 연구가 수행된 바 있다[12].

3.2 배관과 저장탱크

배관이나 저장탱크가 이상상태에서 동작하는 경우 증상으로 나타나는 것은 각종 결함이나 균열에 의한 파손이므로 물리장치에 초음파두께측정기를 부착하여 이를 감지할 수 있다. 초음파두께측정기는 단 방향으로 측정이 가능하기 때문에 운용 중인 배관을 분해하거나 미리 설치 할 필요가 없다. 하지만 의미 있는 데이터를 얻기 위해서는 배관의 부식 및 침전물 누적 등 이상상태에 도달시켜야 하는 현실적 어려움이 있고, 배관 겉면에 윤활제, 물, 커플런트 등의 도포가 필수적이며, 이러한 물질은 짧게는 몇 초 길게는 수 시간의 측정만이 가능하므로 수 일, 수년과 같이 긴 시간 동안의 모니터링 작업을 수행하기 위해서는 주기적인 도포작업 후 재설치가 필요하다.

그 밖의 방법으로는 초음파 음향 센서를 활용하여 누출 유무를 간접적으로 모니터링하는 방법이 있다. 4개의 초민감 음향 센서가 장착되어 가압 가스 방출 시 생성되는 다양한 초음파 영역을 모니터링 하는 'Incus 초음파 가스 누출 감지기'를 통해 가스 누출을 간접적으로 감지할 수 있다. 후각센서를 활용하는 방법에 비해 반응속도가 빠르지만 매우 고가이고, 배관의 미세한 균열로 인한 음향 감지를 위한 배관 재현 및 복원이 현실적으로 매우 어렵다.

3.3 제어시스템

각 물리장치로 입력되는 제어신호 및 모터 구동 신호의 전류를 간접 모니터링하여 이상상태 유무를 판별가능하다. 전류를 간접적으로 센싱할 수 있는 센서로는 클램프식 전류계가 있다. 분할변류계에 전류가 흐르면 철심에 감긴 2차 코일에 전자유도작용으로 기전력이 발생하고 이 코일을 폐회로로 구성하여 전류를 측정한다. 하지만 실드처리된 전선은 측정 오차가 커지고 클램프의 중심에 전선에 위치하지 않거나 측정기기의 각도가 달라지면 그 값이 달라지며 근접한 위치에 전선이 존재하는 경우 쉽게 간섭을 받는 등 여러 가지 문제가 있다.

3.4 사이버 공격

여러 센서들을 이중화하여서 이들 센서로부터 다양한 특징적인 패턴을 공통적으로 추출하여 비교하는 방법으로 사이버 공격을 감시하는 것이 효과적이다. 온도센서를 통한 온도감지, 가속도센서를 통한 진동 이상 감지, 클램프미터를 사용하여 간접적 전류측정을 통해서 단순히 하나의 센서 값을 확인하는 것이 아니라 여러 센서 데이터의 융합을 통해 공통적인 또는 중요하다고 판단되는 물리 값을 추출 후 비교하여 이상상태를 감지해 파악한다면 사이버공격에 대한 가동중지 상태를 확인할 수 있을 뿐만 아니라 보안위협 상황에서 물리장치의 상태를 파악하여 사이버공격에 의한 안정성을 확보할 수 있다.

IV. 공격 시나리오

'사이버 공격'이란 통신 네트워크를 통해 가동기기

제어 시스템의 상태를 교란하는 시도를 뜻한다[13]. 이를 감지하기 위해 제어 시스템(PLC)의 코드 비교를 통해 이를 감지하는 연구[14]가 있지만 코드 비교 후 정상 및 비정상을 판별하고 이를 승인하는 과정으로 이루어져 판별 알고리즘에 의존적이며 실시간 대처가 힘들다. 하지만 과거 양질의 데이터들을 이용, 기계 학습을 통해 판별 알고리즘 및 모델이 완벽해진다면 성능향상을 기대할 수 있다[15].

4.1 사이버 공격의 분류

공격은 터빈, 배관 및 저장탱크, 제어 시스템 등과 같은 공격 대상에 따라, 혹은 데이터의 조작 형태에 따라 분류가능하다. 조작 형태는 고정 바이어스(FB, Fixed Bias), 변동 바이어스(VB, Variable Bias), 간헐적 고장 바이어스(FBI, Fixed Bias Intermittent), 간헐적 변동 바이어스(VBI, Variable Bias Intermittent)로 나누어지며, 그밖에 제어 시스템의 펌웨어에 구현되어 있는 제어 로직을 변경하는 공격, 서비스 거부 공격(DoS, Denial of Service attack) 등이 있다.

4.2 대상 공격 시나리오

본 연구에서 제안한 시스템은 간접적으로 '사이버 공격'을 인지하고 실시간으로 대응하고자 하는 데 그 목적이 있다. 다음 2가지 형태 모두 별도의 독립된 간접적 물리장치 감시 시스템(IHMS, Indirect Health Monitoring System)를 통해 간접적으로 실시간 감시하여 공격으로 인한 피해를 방지한다.

1) 정상상태 → 비정상상태

터빈의 경우는 온도와 압력, 배관 및 저장탱크의 경우는 두께와 균열감지여부, 제어 시스템의 경우는 액추에이터로 출력되는 제어신호출력 값 조작을 통해 비정상상태를 감지하고, 가동을 중지하여 비용 손실을 초래한다.

2) 비정상상태 → 정상상태

지속적으로 높은 열과 압력 상태를 정상 수준 상태로 인지함으로써 생기는 터빈의 과부하, 배관 및 저장탱크의 균열, 비정상적인 제어 시스템의 제어 출력 등을 감지하지 못함으로 인해 가동기기의 폭발 및 큰 물리적 피해를 야기한다.

V. 실 험

5.1 하드웨어

5.1.1 하드웨어구조

터빈, 배관, 저장탱크와 같은 물리장치들은 실제로 시험으로 검증하기가 현실적으로 힘들기 때문에 Festo 수처리시스템에서의 검증을 목표로 건전성 관리시스템을 개발한다. 테스트베드와 비슷한 사양의 소형 물 펌프와 제어기를 대상으로 전류, 온도, 진동을 측정하기 위하여 DC 전류 클램프 센서와 비접촉식 적외선 온도 센서, 3축 가속도 센서를 활용한다. 센서에서 측정된 값들은 필터 회로가 꾸며져 있는 Interface Board를 통해 Waspmote의 ATmega1281 MCU로 데이터를 전달하게 되고 이는 다시 Host PC와 연결된 4214A-Xbee 보드로 Bluetooth를 통하여 전송된다. 센서 값들로 이루어진 파일을 구성하고, Host PC는 쿼리를 통해 Influx DB로 데이터를 전송한다.

5.1.2 센서노드

센서노드 중 leaf node의 역할을 하게 될 IHMS는 Waspmote를 선정하여 활용한다. 물리장치 주변 부에 장착하여 간접적으로 각종 파라미터들을 센싱하여 전달하는 역할을 하는 IHMS는 성능적인 측면에서 Arduino Uno정도면 충분하나 유지보수성 및 안정성이 고려되어야 한다. ZigBee, Wifi, Bluetooth는 물론이고 LoRa와 같은 최신 장거리 무선 통신 기술 등 다양한 통신 프로토콜을 지원한다는 점, 동작시간 및 확장성 등을 고려하여 선정한다.

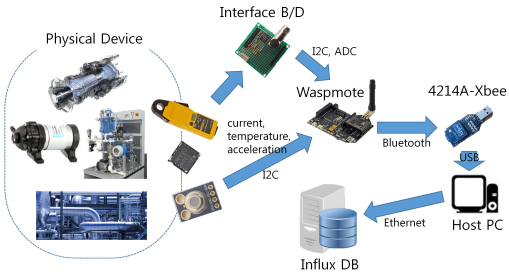


Fig. 1. Hardware Structure Block Diagram

5.1.3 전류모니터링모듈

클램프 미터 전류 측정계들은 대체로 산업용 높은 전류를 감지하기 위한 기기들로 분해능이 100mA이상이므로 테스트베드에서 PWM 신호에 흐르는 전류 값을 고정밀도로 측정하기에는 적절하지 않다. 즉각적인 검증이 가능하면서도 일반적으로 수 kHz로 생성하는 PWM 신호에 의한 전류 값들을 읽는 시험을 위한 전류 센서로 Hall effect 효과를 활용하고, 내부적으로 offset조정 및 증폭기능이 있는 고사양의 current clamp들이 필요하다.

Fluke사, Chauvin Arnoux사의 여러 가지 제품들이 시험 사양을 만족하였지만, 데이터 전송이 불가능하거나 DC 전류가 아닌 AC전류만 측정이 가능하고 오실로스코프와 연동이 불가능한 경우 등 여러 가지 사유로 적합하지 않아 Fluke사의 I30S로 선정하여 IHMS 구현 시 활용한다. I30S의 경우, 5mA~30A의 측정범위, 100 kHz의 주파수 범위, 1mA의 분해능을 가지고 있고, 오실로스코프와 문제없이 연동되며 DC전류 측정값을 측정할 수 있다.

5.1.4 온도 및 가속도 센싱

GY-906은 MLX90614 비 접촉식 온도센서 칩에 10-bit ADC와 DSP가 내장되어 구성된 센서보드로 측정된 센서 값은 I2C를 통해 송신된다. 이를 Interface B/D를 통해 Waspmote에 전달하여 데이터를 획득한다. 한편 가속도 정보는 Waspmote에 내장된 LIS3LV02DL을 사용하며 마찬가지로 I2C 통신을 통해 데이터가 전달된다.

5.2 소프트웨어

온도 데이터는 raw data를 칩 제조사에서 제공하는 수식을 통해 가공하고, x, y, z축 가속도 값을 요청하여 얻는다. 전류 센서인 Fluke사의 I30S의 아날로그 출력은 ADC 포트를 통해 값을 입력 받는다. 각 센서의 데이터들은 Waspmote에서 1ms 주기로 읽게 되므로 우선 RAM에 공간을 할당하여 데이터를 전송한다. 일정 크기의 데이터가 쌓이게 되면 4214A-Xbee를 통하여 Host PC에 데이터를 전달하게 되고, Host PC는 수신된 데이터들을 파일로 저장한다. Waspmote에서 send error가 발생한 경우는 SD 카드에 저장하여 다시 전송한다.

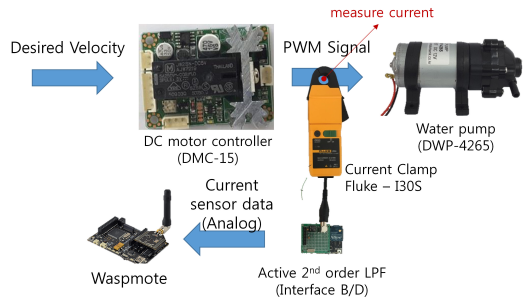


Fig. 2. Current Monitoring Hardware Structure Block Diagram

5.3 실험결과

5.3.1 전류

일반적으로 수 kHz 주파수를 사용하는 PWM 신호에 대한 전류 리플을 필터링하기 위해 Sallen-key 2차 능동 LPF (Low Pass Filter) 적용한다. LT1490 칩을 사용, Cut off 주파수, 1.2 kHz, Damping ratio, 1로 설계하였다.

모터 제어기(DMC-15)를 통해 duty ratio가 0%, 50%, 100%인 PWM 신호를 인가하고 모터에 흐르는 전류를 측정하는 시험을 수행하여 전류를 모니터링한다. 각각의 경우, 전원공급기에서 보이는 전류 값은 0.07, 0.33, 0.44A이다. Duty ratio가 0%인 PWM 신호가 인가된 경우에도 나타나는 전류가 0이 아닌 이유는 모터 드라이버가 아닌 제어기의 MCU를 비롯한 여러 소자에서 소모되는 전류 때문으로 이 크기가 약 0.07A이다. 즉, 모터에서 소모

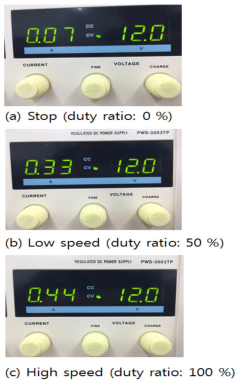


Fig. 3. Current values shown in the power supply

하는 전류는 0.07, 0.33, 0.44A보다 약간 낮다.

Fig. 4는 전류 값들이 ADC 포트를 통해 들어온 값을 나타낸 그림으로, Duty ratio가 0%인 PWM 신호가 인가되는 경우, 전류 센서인 I30S에서 측정된 값 및 이 신호의 ADC 값들이 정상적으로 0을 연속으로 출력한다. Duty ratio가 50% 인 PWM 신호가 인가되는 경우, 전원공급기에서 표시되는 전류 값은 0.33A로 I30S에서 출력되는 신호가 0.33A를 가리키는 33mV(I30S의 경우 100mV/A)에서 스윙하는 파형을 관찰할 수 있다. 또한 이를 읽어 들인 ADC 값은 0.25A 정도에서 스윙하는 파형이 읽혀졌는데 이는 ADC 포트의 boundary 값 오차로 추정된다. 또한, Duty ratio가 100% 인 PWM 신호가 인가되는 경우, 전원공급기에서 표시되는 전류 값은 0.44A이지만 I30S에서 출력되는 신호가 0.38A를 가리키는 38mV에서 스윙하는 파형을 관찰할 수 있다. 제어기에서 기본적으로 소모되는 전류 때문으로 추정되고 실제로 이를 읽어 들인 ADC 값은 0.38A가 아닌 0.28A 정도에서 스윙하는 파형이 읽혀졌는데 이는 Duty ratio가 50% PWM 신호가 인가될 때와 마찬가지로 ADC 포트의 boundary 값 오차로 추정된다. 또한, duty ratio가 50%안 PWM 신호를 인가하였을 때 보다 좀 더 스윙이 큰 전류 파형이 출력되는데 이는 추가적인 노이즈 필터의 필요성을 보여준다.

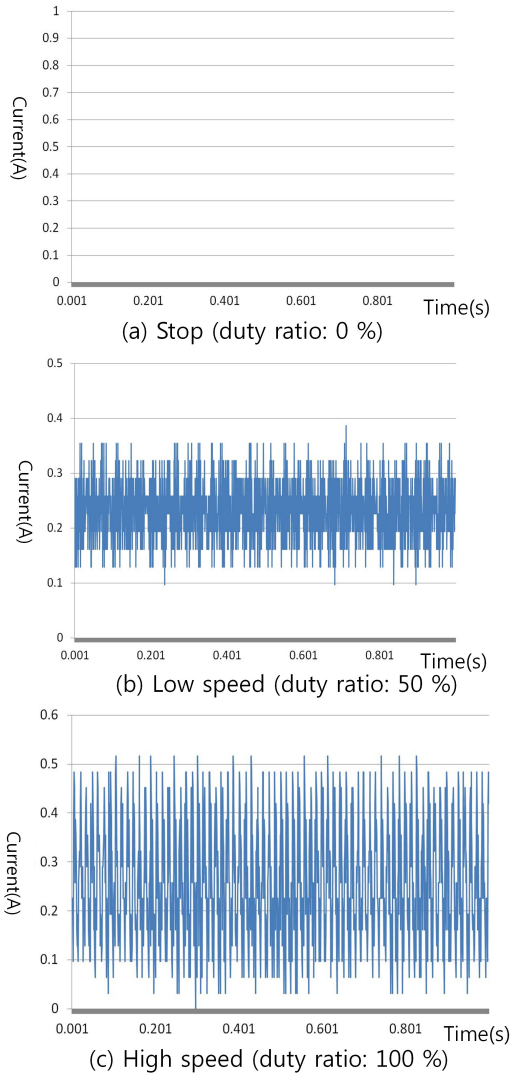


Fig. 4. ADC values for the current sensor data at various duty ratio

감지된 전류를 통해 제어 입력을 역으로 유추하여 제어입력 및 제어로직의 상태를 알 수 있다. 우선, 정규 제어 입력에 대한 모터 전기자에 흐르는 전류의 동역학 식을 살펴보면 다음과 같다.

$$L_a\frac{di_a}{dt}+R_a i_a = V_s u - K_b n\dot{\theta}. \tag{1}$$

여기서, L_a는 모터의 리액턴스(reactance), V_s는 공급 전압, u는 정규화된 제어 입력, i_a는 전기자에 흐르는 전류, R_a는 모터의 내부 저항, K_b는 모터의 역기전력, n은 기어비이다. 기계적 시정수(time constant)에 비해 모터의 전기적 시정수는 매우 작으므로, 모터의 리액턴스를 무시할 수 있다. 따라서 모터의 전류는 아래 식과 같이 정리할 수 있다.

$$i_a = \frac{V_s u - K_b n\dot{\theta}}{R_a}. \tag{2}$$

제어가 정상적으로 이루어지는 경우 모터는 주어진 목표 속력에 맞는 등각속력을 내게 되고 K_b, n, R_a와 같은 모터 파라미터와 V_s는 고정된 값이므로 거의 일정한 전류가 흐르게 된다는 것을 알 수 있다. 제어 알고리즘에서 외란에 의한 약간의 오차들을 보정하기 위해서 제어 입력 u가 약간씩 변화함에 따라 약간의 리플이 있을 수 있지만 평균값을 활용하여 전류를 측정한다면 역으로 해당 모터의 속력을 추정할 수 있다.

PWM duty ratio가 50%인 경우, 공급 전압

(V_s)이 12V이고 실제로 모터에 공급되는 입력은 6 V이며, 이 때 측정된 전류 값은 약 330mA이다. PWM duty ratio가 100%인 경우는 입력 전압이 12V이고 약 380mA가 흐르는 셈이다. 입력 전압이 2배로 증가했음에도 불구하고 늘어난 각속력 때문에 생기는 역기전력의 증가로 인해 전류의 변화는 크지 않다는 것을 알 수 있다. 역기전력으로 인해 비례적 관계를 이루지는 않지만 앞서 살펴본 모터의 전류에 관한 식에 따른 값들이 측정되었고 반대로 이 측정값들을 통해 모터의 구동 상태를 추정할 수 있다. 비정상적으로 로드가 커진 경우 주어진 제어 입력 대비 전류 소모가 커지게 되므로 이를 센싱 하여 기록하고 알림으로써 침입 혹은 사고에 대한 대비를 미리 할 수 있게 된다. 예를 들어 터빈에서 회전부(로터)와 정지부(케이싱)가 접촉할 때 발생하는 러빙의 경우 마찰력으로 인해 로드가 커지게 된다. 마찰이 커짐으로 인해 같은 속력으로 구동함에도 불구하고 힘이 더 필요하게 되고 이를 위해 전류가 더 많이 들게 되는 과정을 살펴보면 다음과 같다. 정확한 모델링을 위해서는 전체 질량과 각 부분별 질량, 이를 통한 관성력까지 계산이 되어야 하나, 단순히 점 질량을 구동하는 하나의 모터를 생각한다면 구동 시 드는 토크는 다음과 같다.

$$\tau = K_t n i_a = K_t n \frac{V_s u - K_b n \dot{\theta}}{R_a}. \quad (3)$$

또한, 로드에서의 동역학 식은 다음과 같이 정리할 수 있다.

$$J\ddot{\theta} + f_v \dot{\theta} = \tau_i - rf. \quad (4)$$

위 두 개의 식을 이용하면 해당 시스템의 동역학 모델을 다음과 같다.

$$J\ddot{\theta} + \left(f_v + \frac{K_t K_b n^2}{R_a} \right) \dot{\theta} = \frac{V_s K_t n}{R_a} u - rf. \quad (5)$$

등각속도 운동할 경우 마찰(f_v)이 커지면 더 큰 제어 입력(u)이 필요하게 되고 따라서 전류소모가 더 커지게 된다. 세부 파라미터들을 적용하여 시스템 모델링을 통한 전류 및 구동 속력 대비 마찰력 등을 정확히 추정하진 못하더라도 축적된 데이터를 바탕으로 세부 파라미터들의 항들 값을 추정할 수 있고 또한 비정상 구동인 경우 감지가 가능하다.

5.3.2 가속도

가속도 센서로부터 얻은 ADC 데이터 값을 그래프로 나타난 낸 결과를 보면 초기 센서 기울기에 따라 초기 값은 변경될 수 있지만 정지, 저속, 고속 구동 시 진동 진폭과 주파수가 다르게 나타남을 알 수 있다. 가속도계를 통해 얻은 진동 데이터를 기반으로 모터의 구동 상태를 추정가능하다.

5.3.3 온도

고온 및 저온의 액체를 넣어 외부에서 비접촉식 온도 센서를 통해 온도를 모니터링한 결과, 테스트베드의 배관 및 저장탱크, 소형 펌프에 캘리브레이션 후 적용 가능함을 알 수 있다. Fig. 5는 고온(case2) 및 저온(case1)의 액체를 외부에서 2시간 동안 측정한 결과이다. 두 가지 경우 모두 시간이 흐름에 따라 상온으로 수렴하는 것을 볼 수 있고, 온도계에서 측정된 내부 온도 값과 비접촉식 온도 센서에서 측정된 센서 값은 거의 동일한 패턴을 보이며 증감한다. 부착되는 물리장치의 재질에 따른 캘리브레이션만 적절히 이루어진다면 간접 온도 모니터링이 가능함을 알 수 있다.

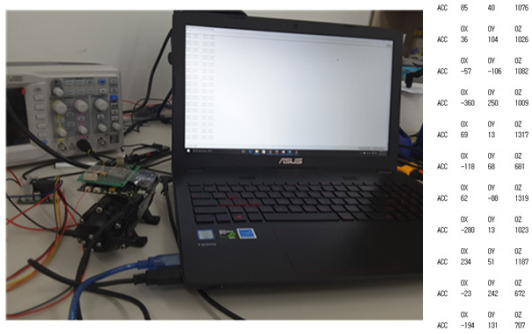
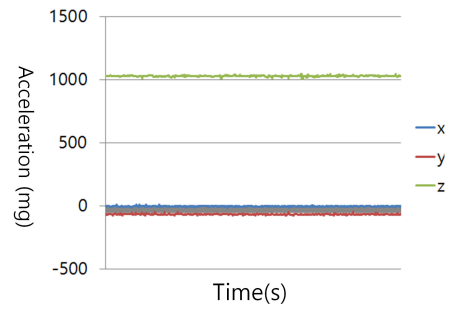


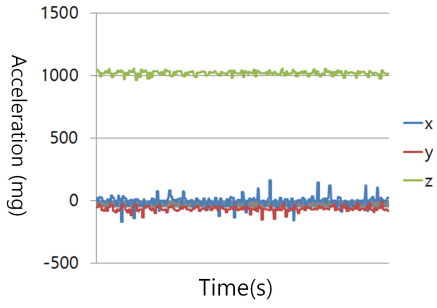
Fig. 5. Acceleration monitoring module test environment and the acquired accelerometer data at high speed

5.3.4 Influx DB연동

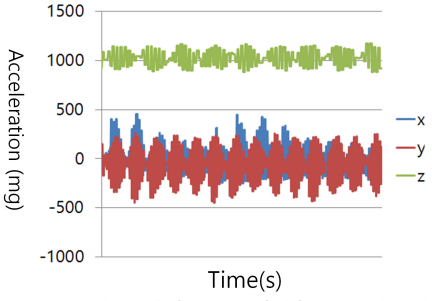
각각의 센서 출력과 시간은 환산되어 오픈소스DB 중 하나인 Influx DB에 저장한다. 이렇게 저장된



(a) Stop (duty ratio: 0 %)



(b) Low speed (duty ratio: 50 %)



(c) High speed (duty ratio: 100 %)

Fig. 6. ADC data for the accelerometer at various duty ratio

데이터는 향후 모델링을 위한 작업을 수행한다. Fig. 7은 여러 센서 데이터 중 DB 내 저장된 가속도 센서 데이터를 웹에서 확인한 모습이다. test은

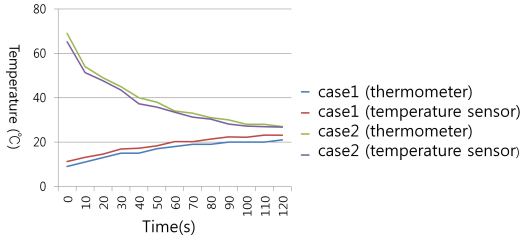


Fig. 7. Acquired temperature data

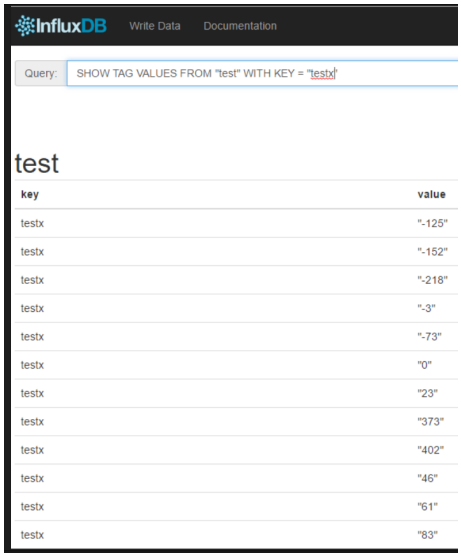


Fig. 8. X-Axis accelerometer data stored in Influx DB

가속도 센서의 데이터를 influx DB로 query 하여서 넣은 값이다. Influx DB는 시계열 데이터를 저장하고 활용하는데 특화된 형태의 데이터베이스로 설치가 간단하고, 캘리브레이션을 지원해주는 다양한 tool들과 grafana를 통한 시각화가 용이하다.

VI. 결 론

본 논문에서는 터빈, 배관, 저장탱크와 같이 피해 파급력이 큰 물리장치를 대상으로 사이버 공격을 받거나 수명이 다할 경우의 주요요인을 분석하고, 이를 간접적 센싱함으로써 가용성(availability)을 침해하지 않는 간접적 상태감시 시스템을 설계, 개발 후 간접적 상태감시를 통해 이상상태 감지가 가능함을 검증하였다.

가동을 중지하지 않는 범위 내에서 물리장치에 진동을 측정하기 위해 가속도센서를 부착하고, 과열감지를 위한 온도센서와 제어신호 및 모터 구동 신호의 전류 이상 유무를 판단하기 위한 전류센서를 부착하여 간접적으로 센싱한다. 실험을 통해 정상적인 데이터 값과 비정상적인 데이터 값을 확인할 수 있으며 터빈, 배관, 저장탱크에 대한 간접적 실시간 감시시스템의 범용화를 통해 데이터를 축적하여 활용하게 되면, 미리 고장이나 사이버공격을 예측하고 필요한 경우에만 조치를 취하는 고장예지기술 및 건전성 관

리 기술을 통해 유지보수비용과 위험도를 대폭적으로 감소시킬 수 있다. 또한 사이버공격이 들어왔을 경우 실시간 간접상태감시시스템과 기존 PLC에서 이중 감시를 통해 대응함으로써 보안성을 강화한다.

향후, 테스트베드에서 FB, VB, FBI, VBI의 형태로 신호를 조작, 이를 IHMS로 감지함으로써 검증할 뿐만 아니라 데이터를 축적하여 이를 학습시킴으로써 정상 신호의 패턴을 모델링하는 연구가 이루어질 예정이다.

References

[1] Choi Joo-ho, "Prognostics and Health Management," *Journal of the KSME*, 53(7), pp. 26-27, 2013.

[2] Ha-yong Kim, "Vibration diagnosis example of cogeneration power plant," *Journal of Gyejang-Gisul*, pp. 114-124, 2010.

[3] http://biz.chosun.com/site/data/html_dir/2014/03/20/2014032001538.html, March 2014.

[4] Woo-Sik Kim, "Energy piping technology development trend," *Journal of the KSME*, 54(1), 2014

[5] http://the300.mt.co.kr/newsView.html?no=2014080711487679758, Aug., 2014

[6] Hyo Kim, Jae-sun Koh, Youngsoo Kim, Theofanius G. Theofanous, "Risk assessment of membrane type LNG storage tanks in Korea-based on fault tree analysis," *Korean Journal of Chemical Engineering*, 22(1), pp. 1-8, Jan. 2015.

[7] Manuel Cheminod, Luca Durante, Adriano Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, Feb. 2013.

[8] Han Kun Yeun, Lee Jae Young, Son In Ho, "Real Time Forecasting of Inundation Risk by Kalman Filter Technique," *Journal of the Korean Society of Civil Engineers*, 2000(3), pp. 233-236, 2000.

[9] Beomki Woo, On Park, Seungkeun Kim, Jinyoung Suk, Youdan Kim, "Real-time Aircraft Upset Detection and Prevention Based On Extended Kalman Filter," *Journal of the Korean Society for Aeronautical & Space Sciences*, 45(9), pp. 724-733, 2017.

[10] Cheng-Zong Bai, Vijay Gupta, and Fabio Pasqualetti, "On Kalman Filtering with Compromised Sensors: Attack Stealthiness and Performance Bounds," *IEEE Transactions on Automatic Control*, vol. 62, no. 12, pp. 6641-6648, June 2017.

[11] Qingyu Yang, Liguo Chang and Wei Yu, "On false data injection attacks against Kalman filtering in power system dynamic state estimation," *Security and Communication Networks*, Aug. 2013.

[12] Jong-Woong Park, Sung-Han Sim, Byung-Jin Jung, Jin-Hak Yi, "Study on Combined Use of Inclination and Acceleration for Displacement Estimation of a Wind Turbine Structure," *Journal of the Korean Society of Civil Engineers*, 35(1), pp. 1-8, 2015.

[13] S. Adepu and A. Mathur, "Generalized attacker and attack models for cyber physical systems," *proceedings of the 2016 IEEE 40th Annual Computer Software and Application Conference (COMPSAC)*, Atlanta, GA, USA, 10-14 June 2016.

[14] J.-O. Malchow, D. Marzin, J. Klick, R. Kovacss, and V. Roth, "PLC Guard: A practical defense against attacks on cyber-physical systems," *proceedings of 2015 IEEE Conference on Communications and Network Security (CNS)*, Florence, Italy, 28-30 Sept. 2015.

[15] C.-T. Lin, S.-L. Wu, and M.-L. Lee,

"Cyber attack and defense on industry control systems," *proceedings of 2017 IEEE Conference on Dependable and Secure Computing*, Taipei, Taiwan, 7-10 Aug. 2017.

〈저자소개〉

김 홍 준 (Hongjun Kim) 정회원
2004년 2월: 한국과학기술원 전자전산학과 졸업
2007년 2월: 한국과학기술원 전자전산학과 석사
2014년 2월: 한국과학기술원 전기및전자공학과 박사
2014년 2월~2015년 4월: 삼성전자 S/W Lab. 책임연구원
2015년 5월~현재: 대전대학교 컴퓨터공학과 조교수
〈관심분야〉 이동로봇, 건전성관리시스템, 기계학습