NIST: Enhancing Resilience of Industrial Control Systems to Cyber Attacks Using Hybrid Processes

Fault Diagnosis and Mitigation for CPS

PROJECT OBJECTIVE

This project enhances capabilities of fault diagnosis and mitigation for Cyber-Physical Systems (CPS), which can be modeled as continuous systems and hybrid systems.

MOTIVATION AND CHALLENGE

CPS integrate computation, networking, and physical processes. Because of the integration of cyber systems and physical systems, CPS are vulnerable to attacks/faults from both cyber domain and physical domain. An attack/fault from the cyber domain can affect the cyber domain or the physical domain or both. An attack/fault from the physical domain can affect the cyber domain or the physical domain or both. We are motivated to enhance fault diagnosis and mitigation for CPS, covering physical-to-physical and cyber-to-physical attacks/faults.

Challenge: Traditional fault diagnosis was developed for physical-to-physical attacks/faults, and has limited application to cyber-to-physical cross domain attacks/faults. Besides, CPS are hybrid systems, including both continuous and discrete variables. This work will enhance capabilities of fault diagnosis and mitigation for continuous systems and hybrid systems.

BENEFITS

- ✓ Enhancing capabilities to detect, isolate and mitigate faults in observable continuous systems
- ✓ Enhancing capabilities to detect, isolate and mitigate faults in observable hybrid systems without reset maps (containing both continuous and discrete characteristics)
- ✓ Enhancing capabilities to detect, isolate and mitigate faults in observable hybrid systems with reset maps (discontinuities exist in continuous variables)

OVERVIEW OF THE WORK

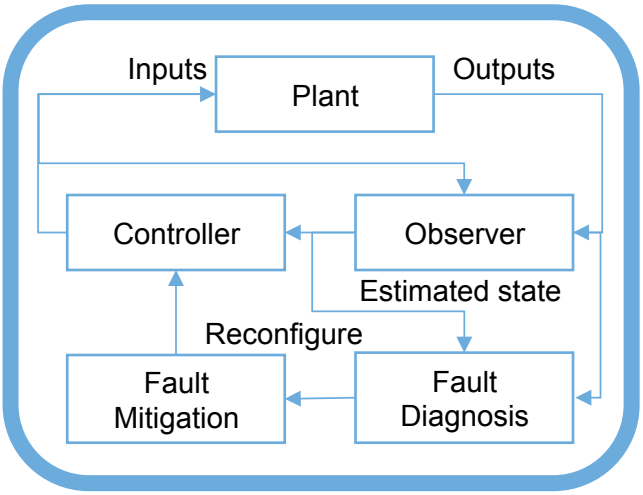
For continuous systems and hybrid systems, we develop observer-based methods for fault diagnosis and mitigation. Fault diagnosis involves both fault detection and fault isolation. After a fault is isolated, fault mitigation reconfigures the system controller to protect the system from unsafe behaviors.

- Fault detection makes a binary decision on whether a fault has occurred
- Fault isolation determines the location, and assesses the extent of the fault
- Fault mitigation reduces the effect of the fault

PROJECT DESCRIPTION

This project covers fault diagnosis and mitigation for continuous systems and hybrid systems. Hybrid systems can be additionally divided into hybrid systems without reset maps and with reset maps. Hybrid systems with reset maps contain discontinuities in continuous variables, making state estimation more challenging. For both continuous systems and hybrid systems, we develop observer-based fault diagnosis based on the assumption that the system is observable.

We start with sensor fault diagnosis for continuous systems. Dedicated Observer Scheme (DOS), which consists of multiple observers, is widely used for sensor fault diagnosis. We divide the sensors into critical sensors and non-critical sensors. Critical sensors are essential for system observability. We divide the observers' response into transient state and steady state. Existing observer-based sensor fault diagnosis focuses on non-critical sensor faults during observers' steady state. Two new methods are developed to address non-critical sensor faults during observers' transient state and critical sensor faults during observers' steady state. Additionally, one method is developed to potentially mitigate the impact of a sensor fault during fault diagnosis. We systematically integrate the three new methods with an existing method to improve the overall capability of sensor fault diagnosis and mitigation for observable continuous systems.

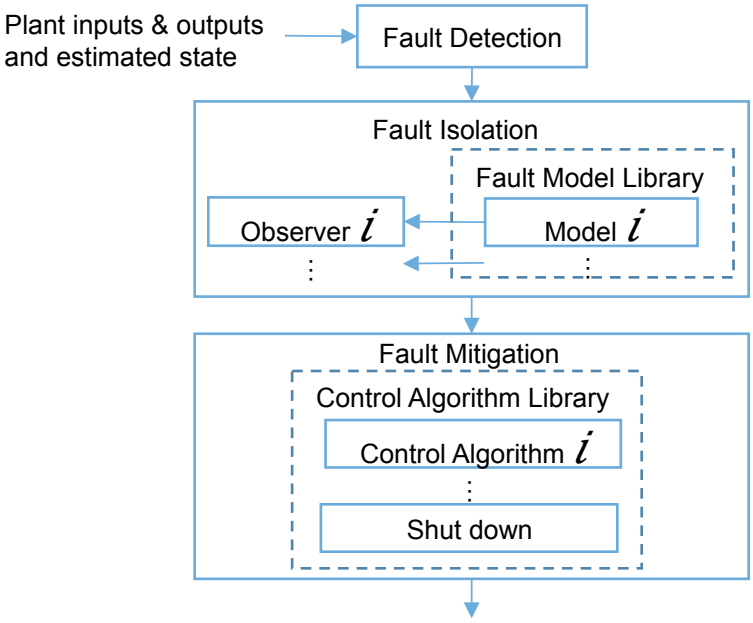


System connectivity between plant, controller, observer, fault diagnosis and mitigation

Fault Diagnosis and Mitigation for CPS

For hybrid systems without reset maps, we use a hybrid observer for fault diagnosis. A hybrid observer consists of a discrete state observer, which estimates the discrete state of the system, and a continuous state observer, which estimates the continuous state of the system. Based on the relation between the continuous and discrete variables, we define three conflict types which can occur under different types of faults. By checking the occurrence of the conflicts, we can detect the occurrence of faults. We call this method conflict-driven fault detection. In this method, we construct an initial set based on the estimated continuous state at each time step. If the volume of the initial set is larger than a certain bound (Conflict A), the system is faulty. With the estimated discrete state, we can get an invariant set, indicating the continuous state space the system can remain. A forward reachable set is calculated based on the continuous dynamics and the initial set. If either the initial set or the reachable set is not intersecting with the invariant (Conflict B or C), the system is faulty.

For hybrid systems with reset maps, we propose a new hybrid observer scheme for fault diagnosis. The old hybrid observer scheme can have a large estimation error right after each transition. The new hybrid observer consists of a discrete state observer and two continuous state observers. With two continuous state observers, we can calculate the estimation error for each continuous state observer. The estimated continuous state can be corrected based on the calculated estimation error to improve the accuracy of the state estimation. A more accurate state estimation can provide better fault diagnosis performance.



Observer-based fault diagnosis framework

DELIVERABLES

- ✓ New fault diagnosis and mitigation methods for continuous systems
- ✓ New fault diagnosis methods to utilize both the continuous part and the discrete part for hybrid systems without reset maps
- ✓ New hybrid observer design for hybrid systems with reset maps to detect faults

CONTACT INFORMATION

Zheng Wang
Ph.D. Candidate
E| zhengwa@umich.edu

Dr. James Moyne
Associate Research Scientist
E| moyne@umich.edu

Prof. Dawn Tilbury
Professor
E| tilbury@umich.edu

2350 Hayward Street
1100 HH Dow
Ann Arbor, Michigan 48109

CURRENT STATUS

- New fault diagnosis methods for continuous systems developed (2016).
- New fault detection method for hybrid systems without reset maps developed (09/2017).

FUTURE MILESTONES

- Design a new hybrid observer scheme for hybrid systems with reset maps (11/2017).
- Fault detection with the new hybrid observer scheme for hybrid systems with reset maps (12/2017).

REFERENCES

[1] Wang, Zheng, et al. "Improved sensor fault detection, isolation, and mitigation using multiple observers approach." *Systems Science & Control Engineering* 5.1 (2017): 70-96.
[2] Wang, Zheng, et al. “Conflict-driven Hybrid Observer-based Anomaly Detection.” ACC 2018, *submitted*