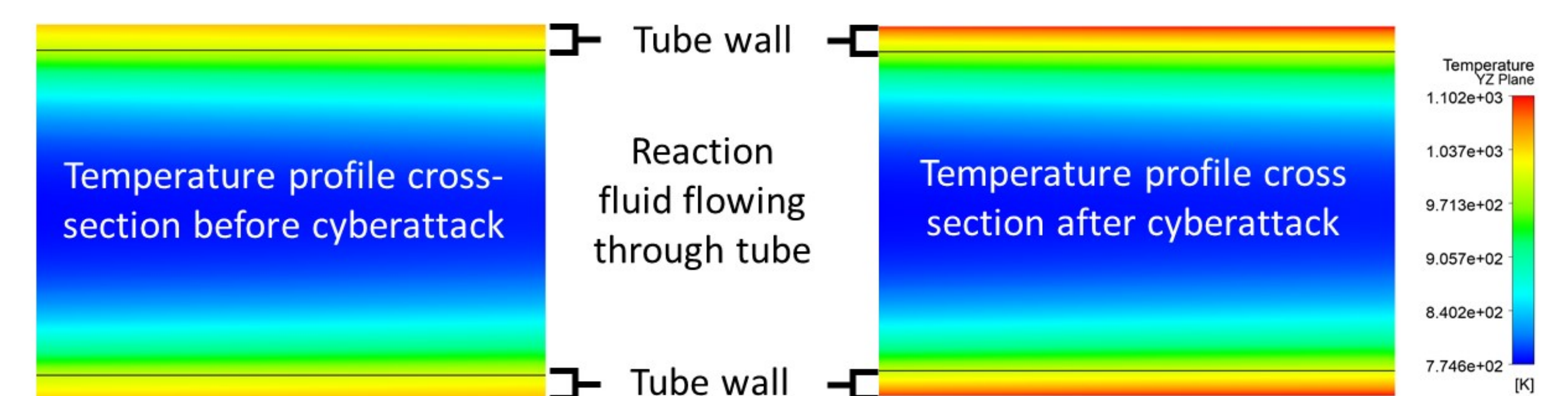# Enhancing Cybersecurity of Chemical Process Control Systems

Helen Durand, Wayne State University, Department of Chemical Engineering and Materials Science
PhD Students Involved in the Work: Henrique Oyama, Kip Nieman, Keshav Kasturi Rangan, Dominic Messina

The potential for cyberattacks on process control systems poses risks to safety, production volumes, and profits of US chemical manufacturing companies. We are working to develop control designs and theory for creating attack-resilient nonlinear systems which could protect manufacturing enterprises in a smart and connected Industry 4.0 environment.

- Cyberattacks are becoming an increasing threat to critical infrastructure
  - An attempt to manipulate the sodium hydroxide concentration in water in Oldsmar, Florida in February is one example of the looming threat of attacks against critical cyberphysical systems (F. Robles and N. Perlroth, *The New York Times*, 2021)

- Understanding how to make control systems verifiably resilient against attacks of different types is important for enabling flexibility and safety in implementing Industry 4.0

- Model predictive control (MPC) is an intelligent optimization-based framework for control action selection
  - Develop cyberattack detection strategies which, when integrated with an MPC, guarantee that safety is maintained for some time after an attack (H. Oyama and H. Durand, *AIChE J.*, 2020; K. K. Rangan, H. Oyama and H. Durand, *CHERD*, 2021)
  - Consider relationships between attacks and process or equipment design (H. Durand and M. Wegener, *Mathematics*, 2020; K. Nieman, H. Oyama, M. Wegener, and H. Durand, *Chemical Engineering Progress*, 2020)

Broader Impacts

- 2 undergraduates mentored via an REU supplement
- Presentation to high school students on cybersecurity of control systems
- Panel presenter for a cybersecurity panel geared toward Wayne State College of Engineering alumni
- Undergraduate involvement via Directed Study
- Aided in aspects of training for 4 PhD students

Closed-loop CFD and FEA simulations can be used to predict equipment material response to cyberattacks
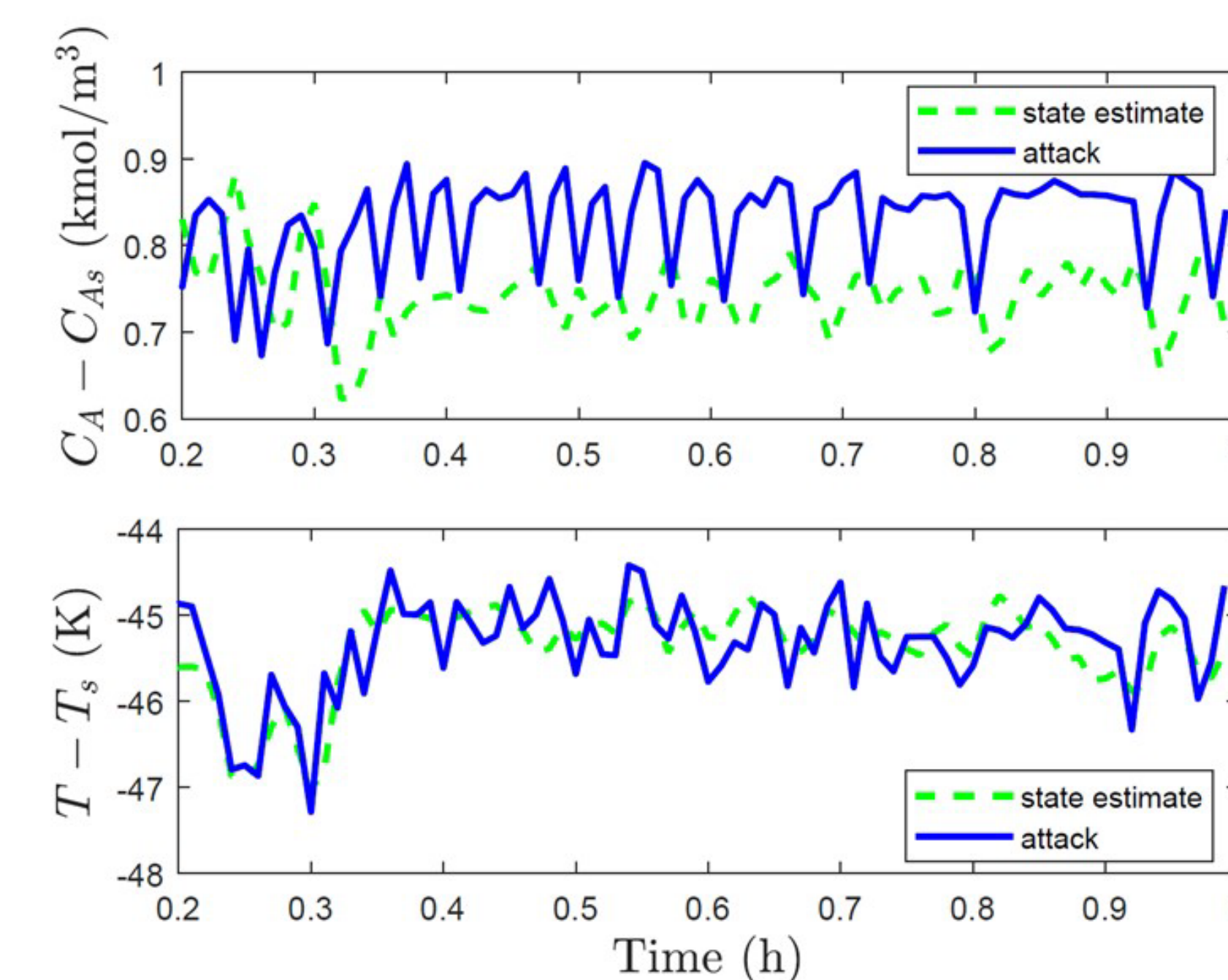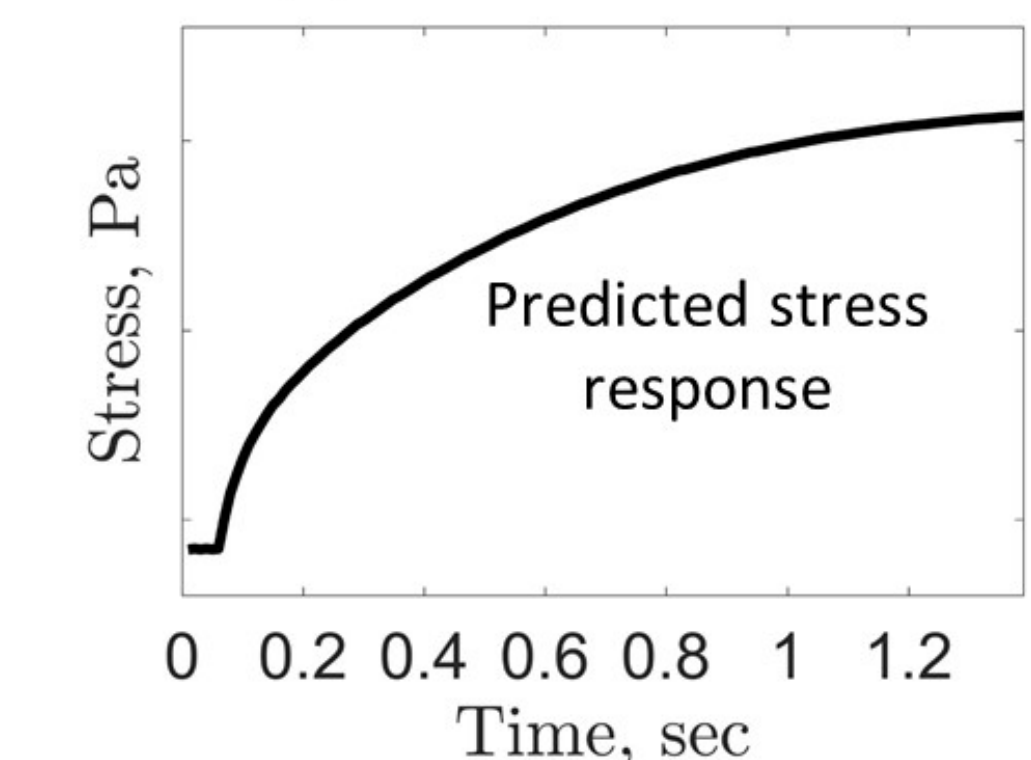
Attack on the sensor measurement causes state estimate to differ from falsified values

Controller can maintain closed-loop state in a safe region in the presence of sensor measurement attacks