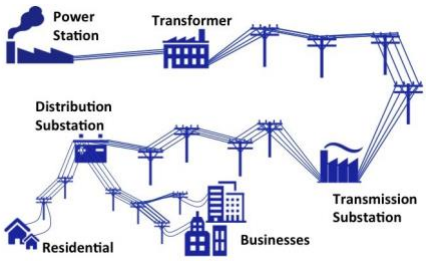
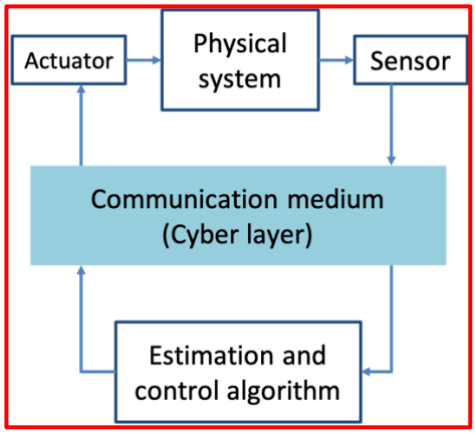
Securing Cyber-physical Systems

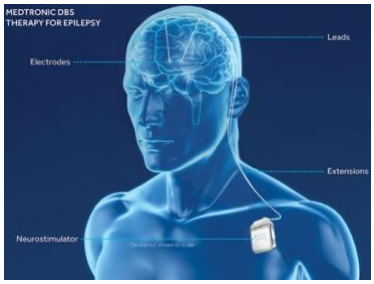
Cyber-physical systems (CPS) permeates all aspects of our lives, from critical infrastructures like power and water grids, traffic networks, to personal devices such as mobile phones and medical implants. CPS consists of a physical system equipped with sensors and actuators, which then communicates through a cyber layer with the estimation and control algorithm.



Power distribution system



Cyber-Physical System



Brain implant

Recent occurrences of cyber-attacks such as Stuxnet, Zero-day and many more highlight the importance of securing CPS against vulnerabilities to ensure its continuous safe operation in the presence of attacks. The attack types include the malicious manipulation of sensor and actuator data, the disruption of the communication medium, and the stealthy reconfiguration of the estimation and control algorithm. All of these attacks can lead to disastrous consequences. Hence, we need to safeguard CPS through intelligent estimation and controller designs.

Projects in this area include:

1. Observer design: prescribed performance; centralised; distributed; over-a-network.
2. Proactive design framework against algorithm corruption
3. Secure controller design with logic specifications
4. Applications in power distribution systems and brain implants.

Some related work can be found here:

1. M. Chong, H. Sandberg and J.P. Hespanha (2020)
   Paper available at https://arxiv.org/pdf/2008.12697.pdf
   Video presentation available at https://youtu.be/AgaJsFGmtCE

2. M. Chong, H. Sandberg and A. Texeira (2019) A tutorial introduction to security and privacy for CPS
   Paper available at https://ieeexplore.ieee.org/abstract/document/8795652

For more information, please contact:
Dr. Michelle S. Chong
Assistant Professor
Control Systems Technology (CST) section, Department of Mechanical Engineering, TU/e
Email: mstchong [at] tue [dot] nl