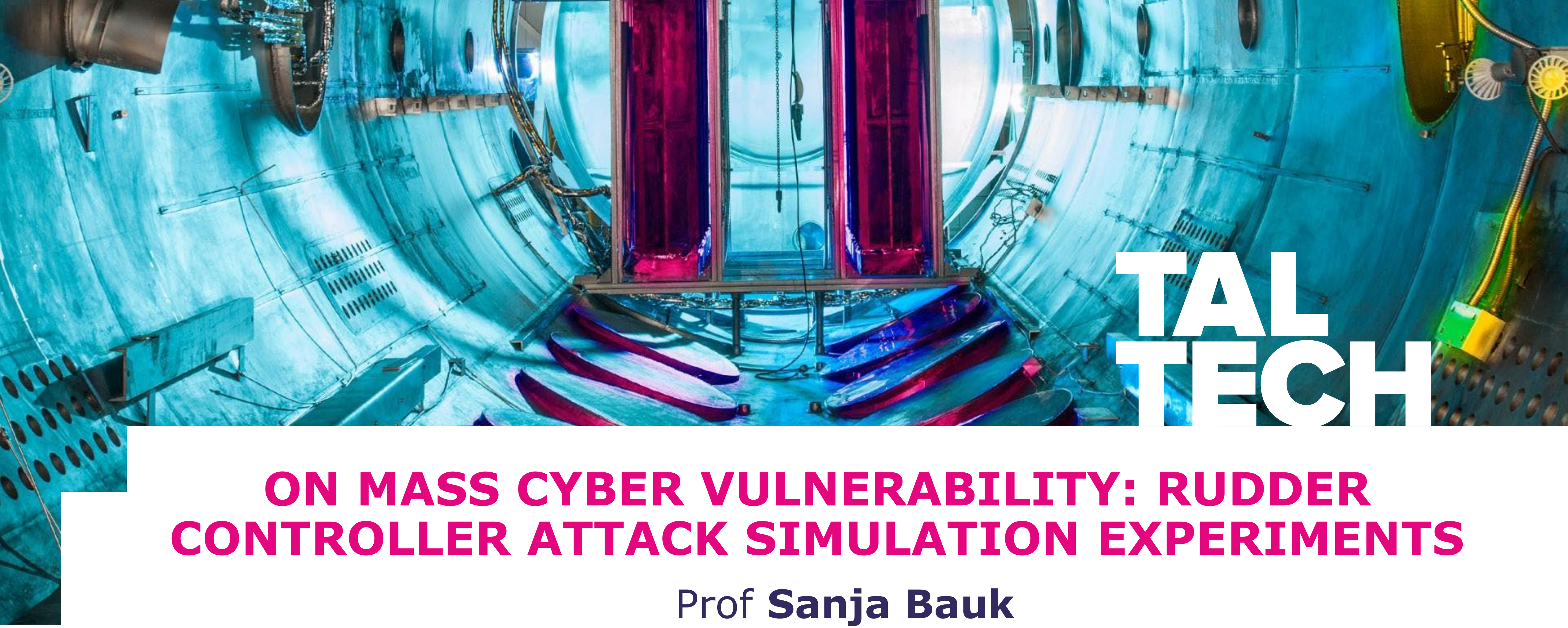


ON MASS CYBER VULNERABILITY: RUDDER CONTROLLER ATTACK SIMULATION EXPERIMENTS

Prof **Sanja Bauk**
Estonian Maritime Academy
Tallinn University of Technology, Estonia

Singapore Maritime Research Conference (SMRC) 2025
Powering Research in Digitalization and Decarbonisation
26 & 27 March 2025, Suntec Singapore Convention & Exhibition Centre

SCOPE

1. This presentation gives an overview of the research and achievements in the field of Maritime Autonomous Surface Ships (MASS).

2. The spotlight is on the cyber security of the MASS.

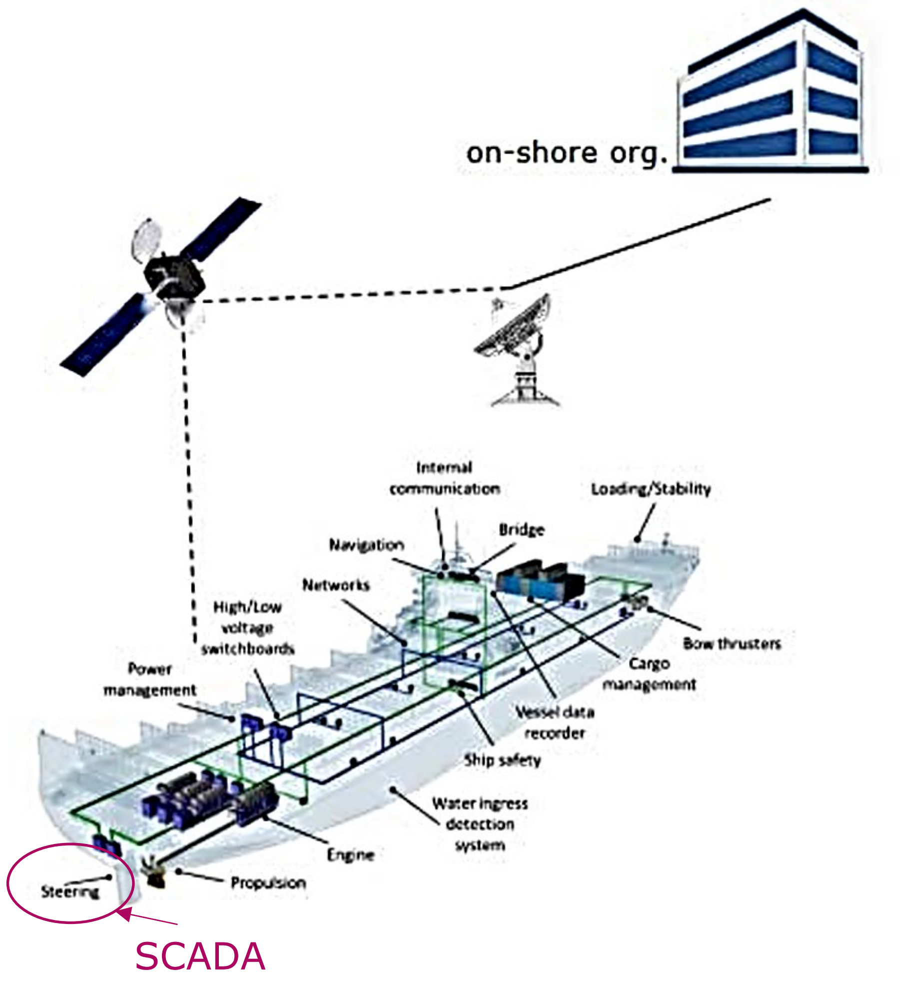
3. More precisely, the behavior of the MASS is simulated in the event of a Supervisory Control and Data Acquisition (SCADA) system hypothetical cyberattack on the MASS's rudder controller.

4. "Nymo" research autonomous vessel designed and built by Tallinn University of Technology and MindChip, Estonian start-up company was used as a testbed.

- Figure 1. "Nymo" MASS (https://mindchip.ee/nymo/)

PROBLEM

- The Proportional–Integral–Derivative (PID) controller and the Kalman filter are deployed as a SCADA cyber-attack mitigation tools.
- The simulation experiments gave insight into the system behavior without and with the Kalman filter, in the conditions of a cyber-intrusion on the input and output signals of the rudder controller.
- The effect of a cyber-attack has been modelled as an arbitrarily shaped periodic signal with a sawtooth waveform interposed to the rudder control system.



- Figure 2. Cyber-attack on a steering system (SAMK, IAMU Project, 2019)

STATE OF THE ART

- >1500 self-driving vehicles (the USA)
- >1.5 million registered drones in operation (the USA)

vs.

- 2 autonomous operational ferry boats: "Falco", built by Fineferries & Rolls-Royce, and another developed by Japanese Nippon Foundation within MEGURI 2040 project
- 2 operational container ships: "YARA Birkeland", built by Kongsberg and another developed by Japanese Nippon Foundation MEGURI 2040 project

- Figure 3. The first autonomous ferry boat "Falco", Finferries & Rolls-Royce, 220 cars, 3 decks, 2018 (*Source:* Baltic Transport Journal)

- Figure 4. The first autonomous container ship "Yara Birkeland", Kongsberg, 120 TEU, 2021 (*Source:* Yara)

STATE OF THE ART

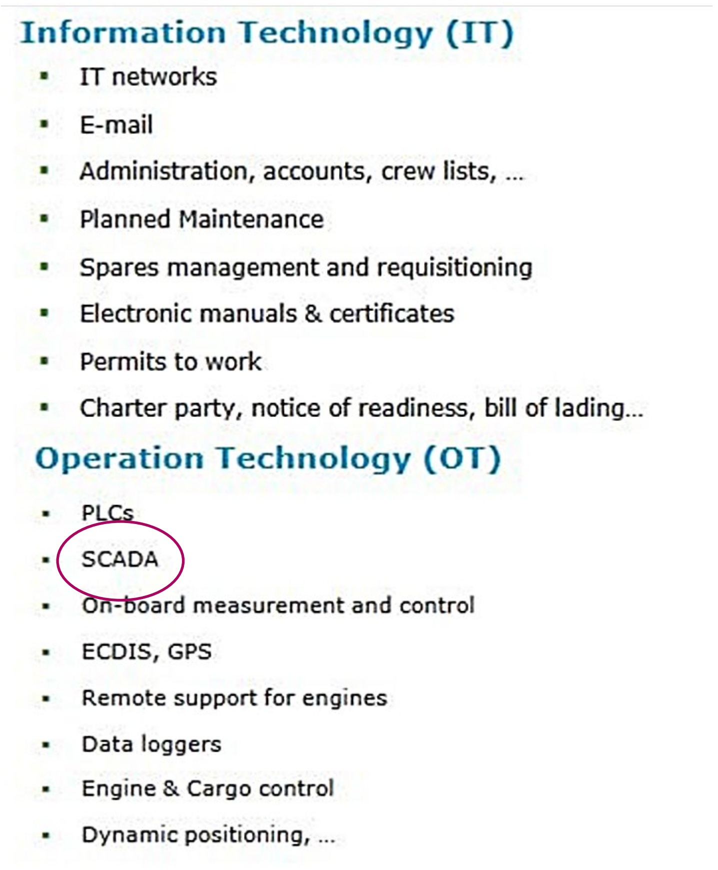
- SEA-KIT's USV **Maxlimer** is an autonomous vessel that successfully completed its first voyage between the UK and Belgium in 2019.
- The **US Navy** is creating **Extra Large Unmanned Undersea Vehicles** (XLUUVs) and **Large Unmanned Surface Vehicles** (LUSVs) to transport various kinds of military payloads.
- The Chinese autonomous mother ship **Zhu Hai Yun**, which can launch swarms of unmanned aerial, surface, and underwater vehicles for monitoring and research.
- Not to be overlooked is the **Mayflower** autonomous vessel, which was constructed by IBM and MarePro. This is a research vessel.
- In addition, until 2025, the autonomous surface ship **KASS**, being built in South Korea, is in the development process.
- The **Rolls-Royce AAWA** multipurpose ocean-going reduced crew ship. By 2035, it is anticipated that this vessel will be fully autonomous.

- Figure 5. “Mayflower”, IMB autonomous research vessel, 2022 (*Source:* Junior.scholastic.com)

- Figure 6. “Zhu Hai Yun”, intelligent unmanned scientific research vessel, 2023 (*Source:* Chinanews.com)

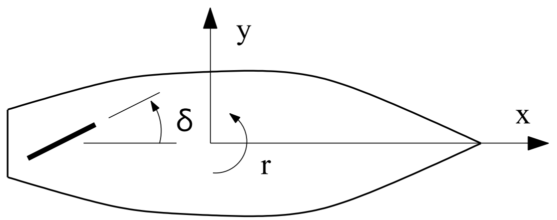
MASS VULNERABILITY TO CYBER-ATTACKS

- Malevolent actors may attack SCADA servers, which monitor, control, and analyze MASS devices and processes.
- The IoT- and Cloud-based SCADA may cause several security risks, including unwarranted data and information sharing via the Internet, increase in bandwidth overload, latency, etc.
- Cyber-attackers can use the technique known as a *privilege escalation* to breach SCADA system and obtain unauthorized access.



- Figure 7. Different cyber-attack vectors (SAMK, IAMU Project, 2019)

“NYMO” MASS MODEL



- Figure 8. The MASS reference system

- The model of MASS is turned into a control problem by using rudder angle δ as control input for controlling the heading angle ψ.

The transfer function from the input rudder angle δ to the output yaw rate r is obtained as [21]

$$W(s) = \frac{n_1 s^3 + n_2 s^2 + n_3 s + n_4}{d_1 s^4 + d_2 s^3 + d_3 s^2 + d_4 s + d_5} \qquad (1)$$

where

$n_1 = -0.0033; n_2 = -3.8015e-04; n_3 = -1.9583e-04; n_4 = -7.9273e-06; d_1 = 1; d_2 = 0.1913; d_3 = 0.0705; d_4 = 0.0069; d_5 = 1.2979e-04$

The heading angle ψ can be calculated so

$$\psi(\tau) = \psi(0) + \int_0^\tau r(t)\,dt. \qquad (2)$$

The reference for rudder angle $\delta_{ref} = 10\,deg$ for system (1) was applied during this maneuver.

PID controllers exist in many forms, one possible implementation is given by the next compensator formula

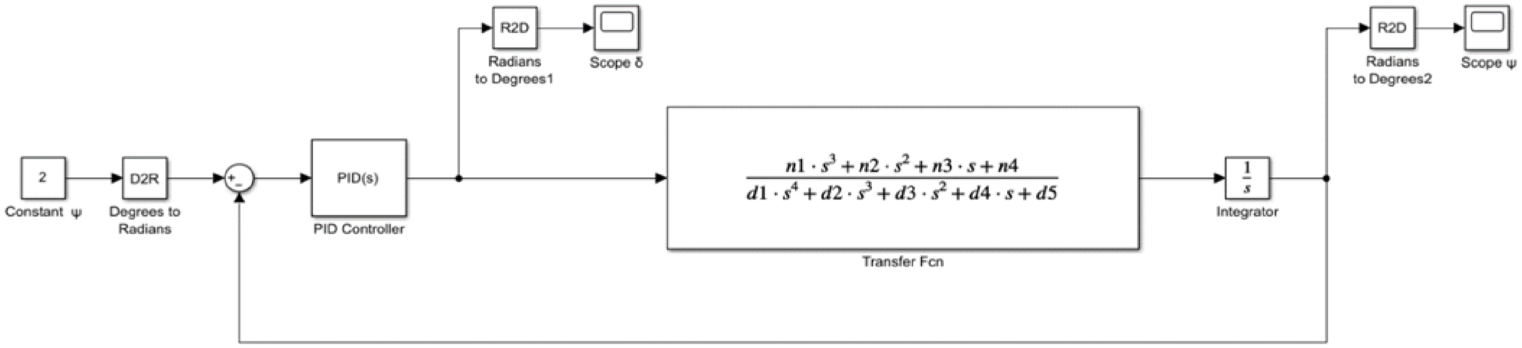
$$PID(s) = K_P + K_I\left(\frac{1}{s}\right) + K_D\left(\frac{K_N}{1+K_N\left(\frac{1}{s}\right)}\right) \qquad (3)$$

where $PID(s)$ is the transfer function, and K_P, K_I, K_D, K_N are proportional, integral and derivative filter coefficients of continuous-time parallel-form PID controller, respectively.

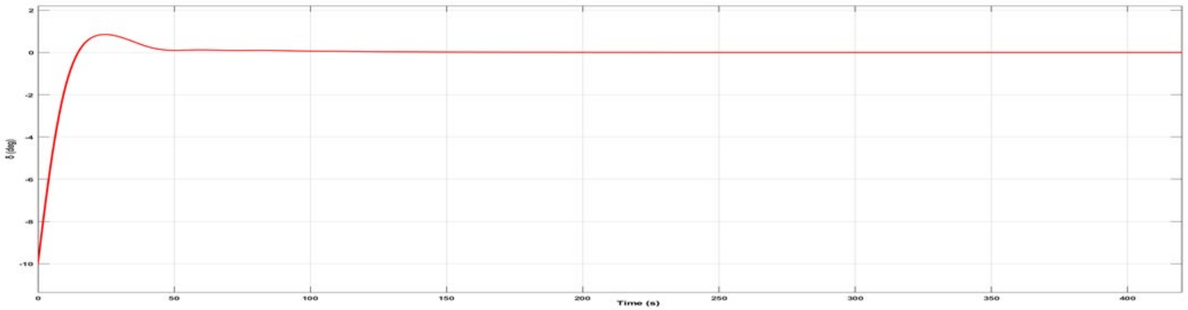
The fixed K_P, K_I, K_D, K_N parameters from (3), which used to tune the controller to a desired behavior, are obtained by using Simulink software for tuning as

$$K_P = -1.4251, K_I = -0.0136, K_D = -23.5407, K_N = 0.1519.$$

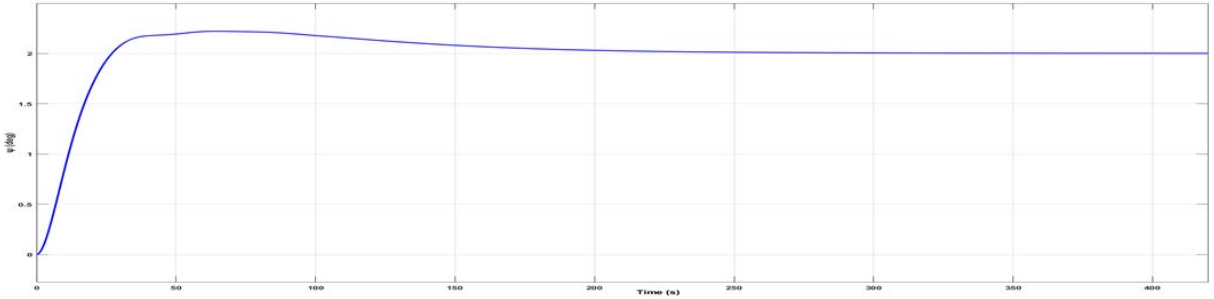
“NYMO” MASS MODEL – MATLAB/SIMULINK ENVIRONMENT



- Figure 9. Simulink-style block diagram of the MASS with PID controller without disturbances



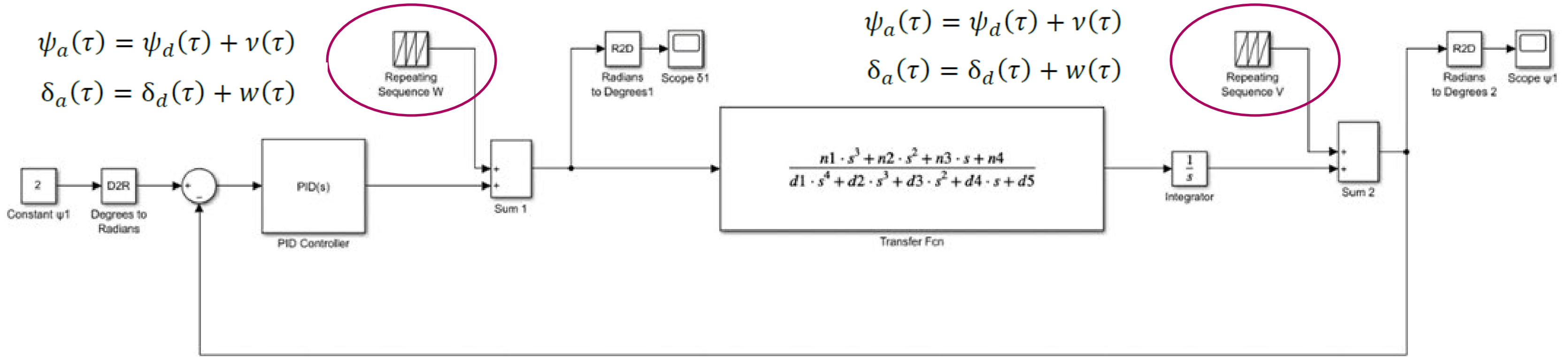
- Figure 10. Rudder angle of the MASS without disturbances



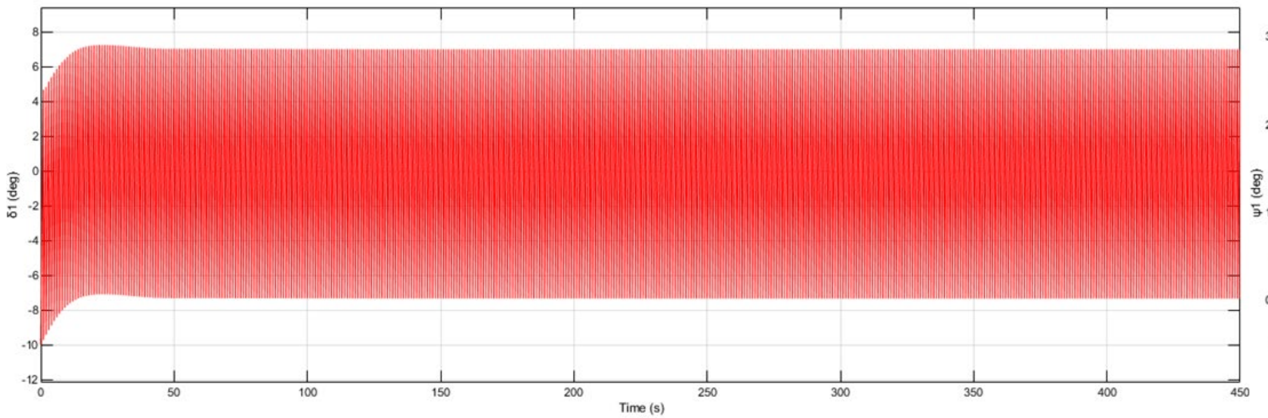
- Figure 11. Heading angle of the MASS without disturbances

"NYMO" MASS MODEL – MATLAB/SIMULINK ENVIRONMENT

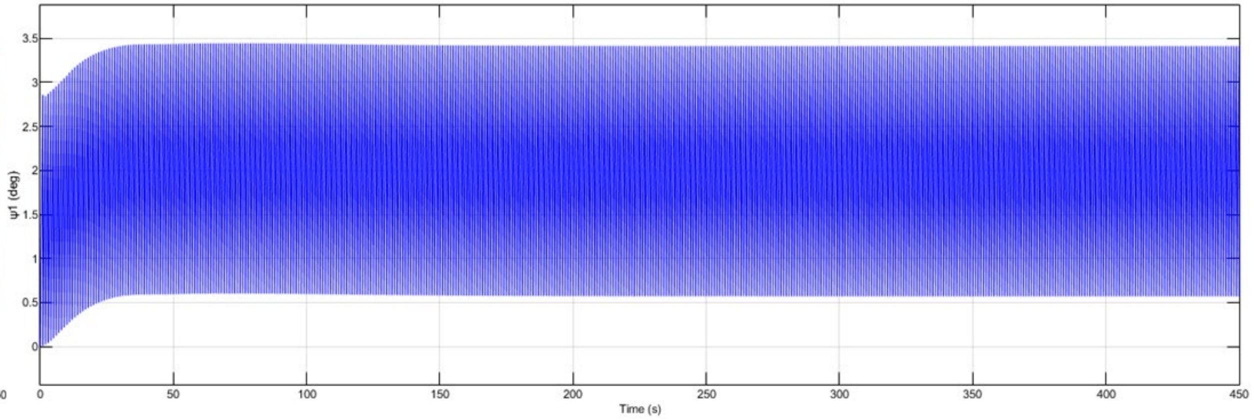
- The effect of a cyber-attack can be modeled as adding the arbitrarily shaped periodic signal having a sawtooth waveform to any control system component.



- Figure 12. Simulink-style block diagram of MASS with PID controller with disturbances



- Figure 13. Rudder angle of the MASS with disturbances



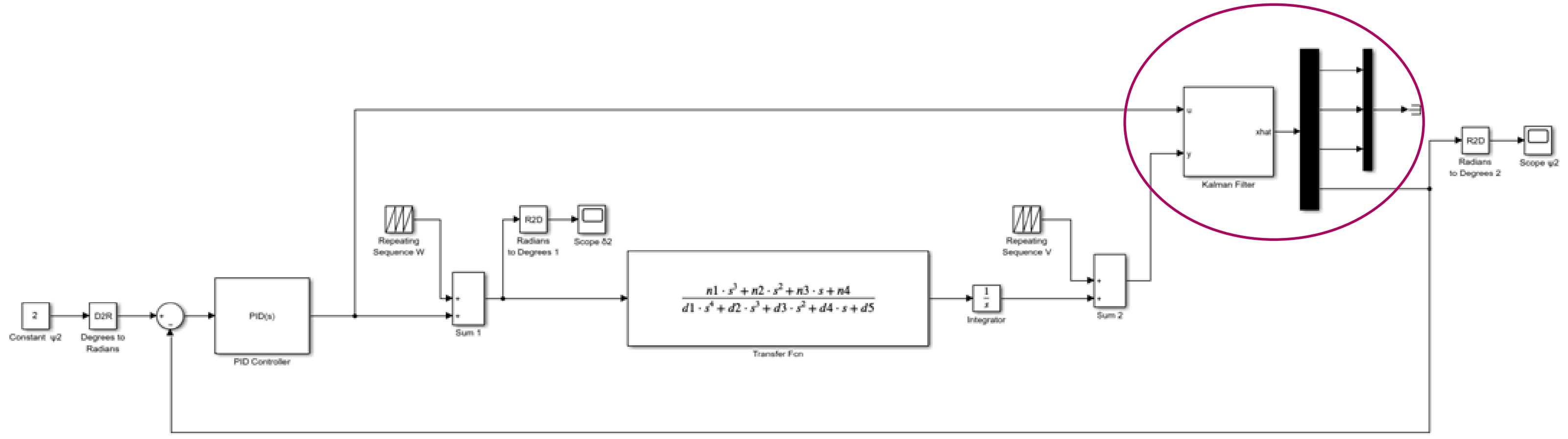
- Figure 14. Heading angle of the MASS with disturbances

- The reference for rudder angle *δ_ref=10 deg*, the waveform *w* repeats every 1 second from the start of the simulation and has a maximum amplitude of 0.002, and the waveform *v* repeats every 1 second from the start of the simulation and has a maximum amplitude of 0.05.

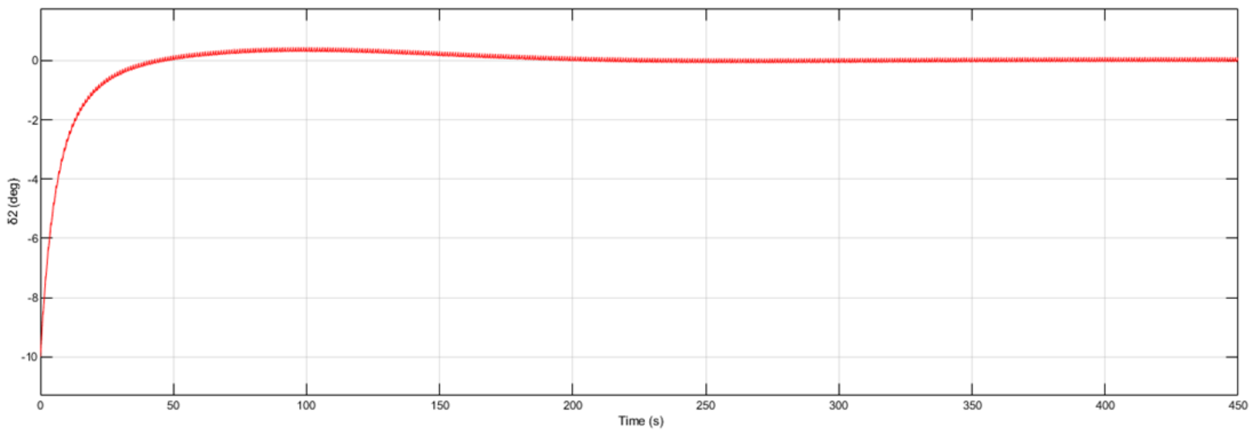
$$\psi_a(\tau) = \psi_d(\tau) + v(\tau)$$

$$\delta_a(\tau) = \delta_d(\tau) + w(\tau)$$

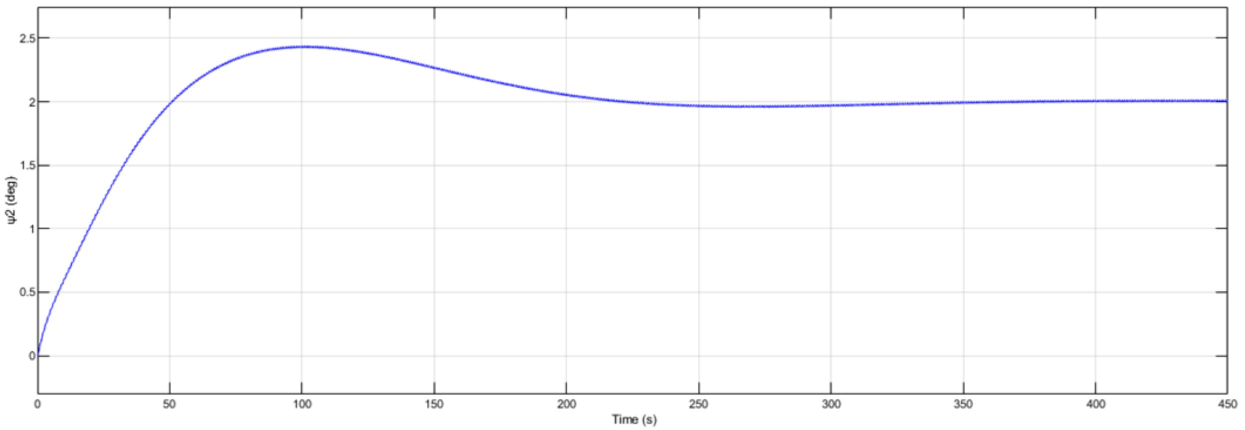
“NYMO” MASS MODEL – MATLAB/SIMULINK ENVIRONMENT



- Figure 15. Simulink-style block diagram of MASS with Kalman filtering

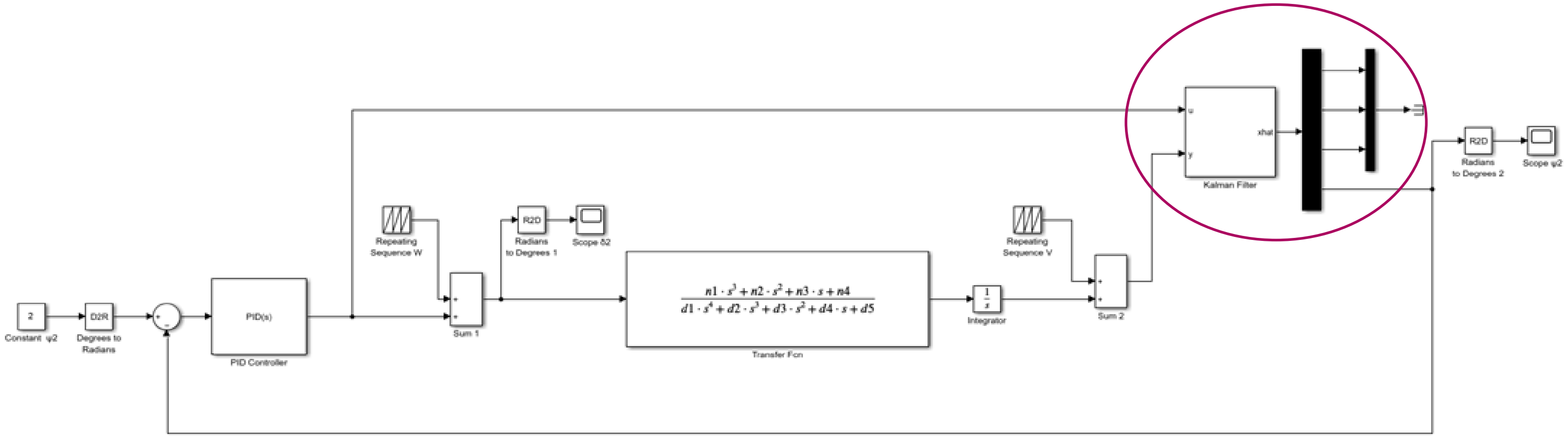


- Figure 16. Rudder angle of the MASS with Kalman filtering



- Figure 17. Heading angle of the MASS with Kalman filtering

"NYMO" MASS MODEL – MATLAB/SIMULINK ENVIRONMENT



- Figure 15. Simulink-style block diagram of MASS with Kalman filtering

The Kalman filter matrix gain L is designed so that the continuous, stationary Kalman filter:

$$\dot{X_e} = AX_e + BU + L(Y - CX_e - DU) \tag{6}$$

produces an optimal estimate X_e of vector X. The matrices A, B, C, D and vector L in (6) are calculated so

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -0.0590 & -0.0700 & -0.0059 & 0 \\ -0.0756 & 0 & -0.0400 & -1.9330 \\ 0.0011 & 0 & -0.0001 & -0.0813 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 \\ 0.0082 \\ 0.1559 \\ -0.0033 \end{bmatrix}, C = [0 \quad 0 \quad 0 \quad 1], D = [0],$$

$$L = \begin{bmatrix} 0.1386 \\ 0.0008 \\ -1.7568 \\ 0.9223 \end{bmatrix}.$$

TALTECH TALLINN UNIVERSITY OF TECHNOLOGY

CONCLUSION

- A cyber attack is simulated. This involved hypothetical breaking into the MASS SCADA system and inserting a malicious noise into the rudder control circuit.
- The control system for MASS is designed so that the MASS can remain close to the desired course when exposed to cyber-attacks simultaneously on the input and output of the system.
- This control system contains *PID controller* and *Kalman filter* as its main elements and demonstrates high efficiency for the selected maneuver.
- The simulated cyber-attack on a given model of MASS will present an important part of the development of an advanced ML/AI algorithm for the optimal control and exploitation of the actual MASS in the future.

AUTHORS’ CONTRIBUTION

- Dr Igor Astrov set up the simulation environment in MATLAB/Simulink and performed data analysis and optimizing techniques {igor.astrov@ieee.org; igor.astrov@taltech.ee}
- Prof Sanja Bauk carried out the environmental scan and proposed the research objective {sanja.bauk@taltech.ee}

AKNOWLEDGEMENT

- Research for this publication was funded by the EU Horizon 2020 project MariCybERA (Agreement No. 952360).

THANK YOU FOR YOUR ATTENTION!

TAL
TECH

MariCybERA

European
Commission