Supervisory Control of a Storm Surge Barrier System

Final Assignment 2025-2026 (4SC080)

Introduction

The purpose of this final assignment is to allow you to demonstrate that you master the different subsequent steps encountered in synthesis-based engineering of supervisory controllers for cyber-physical systems as proposed in the course Supervisory Control of Cyber-physical Systems (4SC080). These steps are as follows:

1. Abstracting the hybrid components of the system.
2. Modeling an uncontrolled system (plant) using a network of discrete automata.
3. Using the simulation capabilities of CIF to validate this model.
4. Formulating system requirements, both informally and formally.
5. Synthesizing a supervisory controller that satisfies these requirements.
6. Validating the controlled system using simulation.

Storm surge barrier systems – background information

With rising sea levels, it is necessary to prepare for high water. To this end, countries at risk of flooding have built various structures, such as storm surge barriers and sluices, to hold back water. Because failures of such critical water infrastructures have a huge socioeconomic impact, reliable control of their systems is crucial.

Ensuring the reliability of control software is a multifaceted challenge that involves addressing various factors, from software complexity to effective testing. To be ahead of potential safety risks, the European STORM_SAFE project[1] seeks to improve the digital resilience of crucial water infrastructures in the North Sea area by investigating methods that support the development of reliable control software.

In [1], Supervisory Control Synthesis is applied to a part of a storm surge barrier control system (the 'Maeslantbarrier' in the Netherlands). The synthesized supervisory controller is guaranteed to meet all formalized safety requirements and can be used to automatically generate controller software. The method showed sufficient versatility and scalability to be applied to a subsystem of a critical water infrastructure.

[1] See `https://www.interregnorthsea.eu/stormsafe` for more information about this project.

Figure 1: Storm surge barrier at Hvide Sande (from [2])

In this final assignment of the course Supervisory Control of Cyber-physical Systems, we focus on developing a supervisory controller for a different storm surge barrier that also participates in the STORM_SAFE project: the barrier at *Hvide Sande*, Denmark. See Fig. 1.

Note that, while this assignment is inspired by the real system located at *Hvide Sande*, various aspects (mainly the water levels) have been simplified to make it suitable for this assignment.

Problem setting

The storm surge barrier considered in this assignment consists of multiple gates placed side-by-side, separating the *Ringkøbing Fjord* from a canal. The canal connects the fjord with the sea. On either side of the canal is a harbor. A satellite image of the situation is given in Fig. 2.

Each gate is vertically actuated by its own motor. The actuation speed is relatively low: it takes 6 minutes to fully lift or lower a gate. It requires a lot of power for the motor to start raising or lowering the gate, resulting in a short power peak. Thus, it is not allowed to start operating all gates at the same time.

The barrier's gates are operated for various reasons.[2] When there is a storm surge, the gates close to protect the land behind. When there is a lot of rain, resulting in high water levels in the fjord, the gates open to let the water flow towards the sea. This gravitational discharge is only possible when the sea water level is lower than the fjord water level. With rising sea levels, the window of opportunity for this discharge is ever-shrinking and should be used optimally.

[2] For those interested, current sluice data can be found at `https://kyst.dk/hav-og-anlaeg/maalinger-og-data/slusedata/slusedata-og-sluselog-fra-hvide-sande`

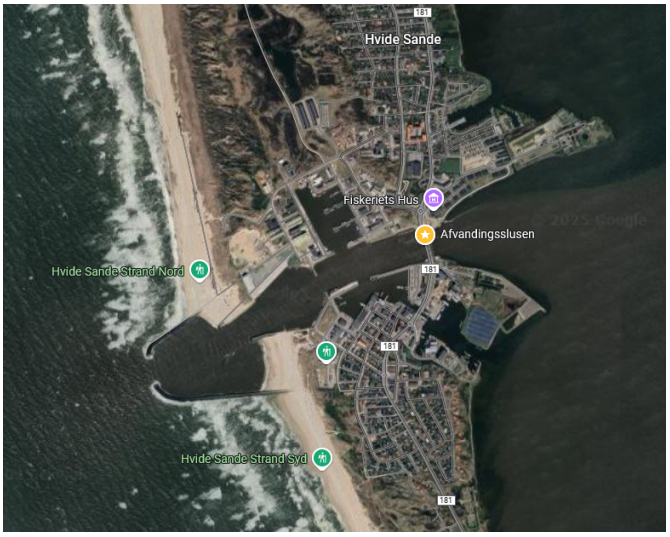

Figure 2: Satellite view of the area (from Google Maps)

In addition to the previously mentioned reasons for operating, the barrier operators also have to consider the nearby harbors. Ships enter and leave the harbors through the canal. If there is a large flow in this canal, this endangers the ships. The flow in the canal is largely determined by the barrier. Thus, when ships arrive at a harbor or want to depart, the barrier closes to prevent dangerously large flow.

The safe behavior of the system must be ensured, especially since flooding has great socio-economic impact. Eventually (or ideally), it is desired to have a supervisory control system that ensures safe behavior in an environment with faults. An example of such a fault is a gate sensor not working. We assume that any other control systems are in place and designed correctly (which does not imply that faults cannot happen).

Design of the supervisory controller

In this project, you will carry out the start of a typical design process where some specifications of the used hardware and desired control system are given initially by the infrastructure providers. The specifications in this document act as a starting point. You may find they are incomplete and vague. If needed, you may be able to make the specifications more specific by talking with the infrastructure providers (the TA's).

Model components

Sea water level. The water level of the sea l_s [m] depends on the tide. The tide of the sea can be roughly described as a sine. We propose the following equation:

$$l_s = A - A \cdot \sin\left(\frac{2}{60 \cdot 60 \cdot 24} \cdot 2\pi t\right) \tag{1}$$

where t is time, interpreted in seconds. The amplitude A of the sine may be assumed to be 2.5 [m]. The period of the sine is such that the tide cycles twice a day. With this equation, l_s varies between 0.0 and 5.0 [m].

Fjord water level. The water level of the fjord l_f [m] depends on the inflow of rainwater from the surrounding area and the outflow of water through each of the gates:

$$\dot{l_f} = \frac{1}{A_f} \cdot (R(t) - \sum_{i=1}^{n} Q_i(t)) \tag{2}$$

where A_f [m^2] is the area of the fjord, $R(t)$ [m^3/s] is a function representing the inflow of rainwater, $Q_i(t)$ [m^3/s] is the flow through gate i (see definition below) and n is the number of gates. The inflowing rainwater $R(t)$ is positive when it is raining or 0.0 [m^3/s] when it is dry.

Gate actuators. Gates are actuated by a 3-phase induction motor. The motor is connected to a winch system, which raises or lowers the gates depending on the direction of rotation of the motor. The full range of the actuators results in an opening height between 0 and 6 [m]. Gates can also be opened to an intermediary height of 3 [m]. A distance sensor at the bottom of each gate informs the system of the opening height. A touch sensor at the top of the motion might be added in the future.

The change in height h_i [m] of gate i is determined by the actuator input $u_i(t)$ [m/s]:

$$\dot{h_i} = u_i(t) \tag{3}$$

where $u_i(t)$ is positive when gate i is raising, negative when the gate is lowering, and 0 otherwise.

The storm surge barrier considered in this assignment consists of 14 identical gates. Although eventually scaling up to 14 gates is desired, for this assignment it is sufficient to model 4 of the 14 gates. Still, the modularity of your model (an important part of scalability!) is an important part in the grading. Further information on modularity in CIF is given in [3].

Water flow. The flow through a gate is determined by the opening height and some constant c [m^2/s]:

$$Q_i = c \cdot h_i. \tag{4}$$

where c is a positive value c_1 when $l_s < l_f$, 0 when $l_s = l_f$ and $-c_1$ when $l_s > l_f$. A positive flow thus corresponds with flow from the fjord to the sea. You may assume that all gates have the same c.

Ships. Ships sail from sea to harbor and back through the canal by the barrier. Because the storm surge barrier generates a large flow when it is opened, the ships can not sail at such a time. Currently, the operators sometimes have to close the gates so that a large ship can safely enter or leave the harbor.

For this reason, the operators want to have some kind of controllable sign that instructs the ships to wait a little bit. Because this sign does not yet exist, it is flexible what the sign should look like or what it can do. You are free to make assumptions on the design of the sign.

Specifications

The storm surge barrier exists to protect the inland area from storms, but also to regulate the water level in the fjord. In consultation with the operators of the system, some specifications have been formulated. Besides the specifications given below, you are encouraged to propose your own requirements and functionalities, as long as you clearly describe and motivate them in the report.

Gate actuation.

G1 Gates must close when the sea water level is above 4.5 [m], to prevent flooding of the land behind.

G2 Gates are opened at most at an intermediary height of 3 [m] when the water level in the fjord is not near critically high or low levels.

G3 To prevent peak load on the electricity net, gate actuation (starting to open or close) has an interval time of 5 [s].

Water levels.

L1 The water level in the fjord should not exceed 4.0 [m].

L2 The water level in the fjord should not fall below 1.0 [m].

Ships.

S1 Ships will only enter the canal if the flow generated by the storm surge barrier is small enough (below 100 [m^3/s]).

S2 Ships should be allowed into the canal once in a while (stopping the ships from entering for eternity is not an acceptable solution).

Other remarks

Several details and design choices are not specified here to endow the project with a significant level of flexibility also on the formulation side. An important part of the project is therefore to make assumptions under which the proposed solution will function, resulting in significant progress towards storm surge barrier automation shaped by the expertise of the members of the group. When in doubt, consult with the TA's.

It is advised to start with a simple model and build from there. In other words, the first iterations of your models do not have to be perfect.

To obtain your abstract finite state model, you could start by assuming gates are opened and closed with constant velocity (not a valid assumption, but it helps to start) and compute an abstraction with transitions every 3 minutes. Additionally, you can also try to evaluate under what conditions the water level of the fjord can be maintained.

Handing in

You are required to submit a (short) report as a PDF file on Canvas. The deadline for the final report is April 17, 2026 (AoE). The report contains:

- Introduction of the problem, system description, assumptions and boundary conditions.
- A description of your abstract finite state model with gate heights and fjord water level being the model state, gate flow being the output.
- A description of any other models made, for example of the ship sign.
- The informal requirements and their models used for synthesis.
- A collection of event sequences that may be used to test the controlled system. Indicate whether sequences show the presence of relevant required behavior or the absence of relevant forbidden behavior.

In addition to the report, you should be able to demonstrate that you have performed synthesis. For this reason, you must provide:

- your model files
- the tooldef file used for synthesis
- the obtained supervisor

Evaluation

The final assignment will be evaluated on the following aspects:

1. Abstractions:
   (a) Correctness, clarity and elegance.
   (b) Explanation in the report.
2. Proposed CIF model of the uncontrolled plant:
   (a) Correctness, clarity and elegance.
   (b) Explanation in the report.
   (c) Modularity of the model.
   (d) Level of ambition.
3. The informal requirements and their (formal) models in CIF:
   (a) Correctness, clarity and elegance.
   (b) Explanation in the report.
4. Quality of the report.

Notes:

ad 2) If the uncontrolled system is too simple (and in this sense avoids problems in the uncontrolled system) this is not valued very much.

ad 1,2,3) Elegance and clarity are greatly helped by having a clear relationship between concepts from the informal description and their formal counterparts.

References

[1] M. A. Goorden, J. M. van de Mortel-Fronczak, K. van Eldik, W. J. Fokkink, & J. E. Rooda, "Lessons learned in the application of formal methods to the design of a storm surge barrier control system", *IFAC-PapersOnLine*, vol. 55, pp. 93–99, 2022. DOI: 10.1016/j.ifacol.2022.10.329

[2] Kystdirektoratet. Available: `https://kyst.dk/hav-og-anlaeg/vedligehold-af-havneanlaeg-sluser-daemning-og-sejlloeb/hvide-sande-og-thorsminde-sluser`

[3] CIF tooling, available at `https://eclipse.dev/escet/cif/index.html`