inf461 - Security of Cyber-Physical Systems

<table>
<thead>
<tr>
<th>Module name</th>
<th>Security of Cyber-Physical Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module code</td>
<td>inf461</td>
</tr>
<tr>
<td>ECTS credit points</td>
<td>6.0 KP</td>
</tr>
<tr>
<td>Workload</td>
<td>180 h</td>
</tr>
<tr>
<td>Used in degree programmes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Master's Programme Computing Science &gt; Mastermodule</td>
</tr>
<tr>
<td></td>
<td>• Master's Programme Engineering of Socio-Technical Systems &gt; Systems Engineering</td>
</tr>
<tr>
<td>Contact person</td>
<td></td>
</tr>
<tr>
<td>module responsibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sibylle Fröschle</td>
</tr>
<tr>
<td>authorized examiners</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Die im Modul Lehrenden</td>
</tr>
<tr>
<td></td>
<td>• Sibylle Fröschle</td>
</tr>
<tr>
<td>Prerequisites</td>
<td></td>
</tr>
</tbody>
</table>

Skills to be acquired in this module

Professional competences:
The students:

- are aware of the threats posed by cyber attacks to cyber-physical systems
- understand security solutions specific to CPS
- know examples of security architectures of CPS
- are able to apply this knowledge to assess the risk of cyber attacks to a given CPS as well as to develop a conceptual systems security architecture for it

Methodological competences:
The students:

- carry out a threat and risk assessment for a given CPS
- formulate security requirements for a given CPS
- develop a systems security architecture for a given CPS to meet them

(These are examples, the exact skills depend on the focus chosen by the student.)

Social competences:
The students:

- are able to master a new topic by self-study and interaction with experts and peers
- are able to explain the significance and facets of security for CPS to experts and non-experts
- are able to expertly discuss security risks and incidents of CPS

Self-competences:
The students:

- follow up and critically assess current developments in the security of CPS including relevant security incidents
- are security aware and foster a security culture with respect to CPS and the resulting critical infrastructures
**Module contents**

Embedded systems in the energy, transportation, and health domains are currently undergoing a technological transition towards highly networked automated cyber-physical systems (CPS). Such systems are potentially vulnerable to cyber attacks, and these can have physical impact. This includes targeted sabotage of a plant (e.g. Stuxnet), large-scale sabotage of infrastructure to cause economic damage (e.g. attacks against energy grids), and indiscriminate attacks to cause civilian casualties (e.g. by compromise of transportation systems). In this module we investigate and discuss security principles, solutions, and architectures for CPS as well as real-life security incidents. The topics include distance bounding protocols, location tracking and counter-measures, safety and security engineering of CPS, security in the automotive and maritime domain including car hacking and vehicle-2-x communication, hacking in the medical domain, attacks against energy grids, Stuxnet, CPS and society: benefits, risks, acceptance.

**Recommended reading**

Recent scientific papers and reports in the public domain news.

**Links**

http://vhome.offis.de/sibylle/

**Language of instruction**

English

**Duration (semesters)**

1 semester

**Module frequency**

once a year

**Module capacity**

Unlimited

**Module level**

AS (Akzentsetzung / Accentuation)

**Modulart**

Pflicht o. Wahlpflicht / compulsory or optional

**Lern-/Lehrform / Type of program**

S or V

**Vorkenntnisse / Previous knowledge**

Security

**Examination**

**Examination periods**

At the end of the lecture period

**Type of examination**

Presentation and written documentation, oral exam, or exam

**Course type**

course or seminar

**SWS**

2

**Workload attendance**

28 h