Information and Cyber Security (ICS)

Fields of education: Engineering and Information Technologies

1. Professional qualification

Professional career outline

The importance of Information and Cyber Security in industry, business, government and society is continuously increasing and it plays a crucial role to keep them resilient or at least up and running. The complexity of the topic grows dramatically and produces a high demand for specialists that have the necessary knowledge. Currently all UAS are aware of this situation and offer within their computer science bachelor programs a specialisation or major in this field. Only HSLU offers an information and cyber security bachelor program.

There is an increasing demand for higher qualified experts that have a deeper knowledge and are aware of the latest developments in security technologies than the one obtained in the bachelor course, even the one from HSLU. Preferred job positions for MSE graduates in ICS are senior positions in research and development as well as technical management in all kinds of service and production industry as well as in organisations in the private and public sector. The graduates with an MSE information and cyber security profile will be able to work in jobs such as:

- Security Architect
- Security Consultant
- Security Engineer of Products
- Analyst in Cyber Defence Centre
- Security Network Engineer
- Security Operator

In order to fulfil this demand, MSE graduates need master-level competencies in all important areas of information and cyber security such as security architecture and management, in-depth security, software security, digital forensics, as well as IoT security and industrial infrastructure security (Operation Technology). They must be able to research and develop, plan, specify and conceptualise innovative security solutions and architectures.

Professional skills

MSE graduates with the ICS profile can design, build and manage innovative security systems and architectures. They have the knowledge and competence to consider and obey the requirements from all relevant stakeholders as well as regulatory issues. They integrate the security aspects in heterogeneous environments and increase the resilience. MSE graduates apply and develop efficient and effective tools for analysis, management, simulation and modelling. They have a deep knowledge and understanding to systematically identify problems and weaknesses which will be eliminated with adequate measures. Risk analysis and appropriate mitigation is a common task for MSE ICS graduates.

MSE graduates can solve complex problems using adequate expert, data analysis, and decision-making tools. They have learned to analyse and evaluate new security technologies and research approaches in their area and to include explicit and implicit requirements and constraints in their decision processes.

They have acquired enough management competences to be able to lead smaller development teams in a productive way and to take the responsibility of managing IT infrastructures.

Entry skills

Specific skills are required to enrol in this profile. Students holding the following Bachelor degrees generally fulfil these entry requirements:

- BSc in Information and Cyber Security
- BSc in Computer Science
- BSc in Data Science

The assessment of the entry skills is part of the enrolment process of the respective school. Students who do not hold one of the above mentioned Bachelor degrees will be individually assessed for their suitability by the respective University of Applied Sciences.

Differentiation to bachelor level

In contrast to BSc students MSE graduates have a deeper theoretical and conceptual foundation in information and cyber security in general and more solid knowledge in one or more of the topics mentioned in the following section. They can easily apply research results in their field of competence and apply this to the problems within their professional field to generate efficient, effective and innovative solutions. In general MSE graduates have a broader information and cyber security view what gives them a deeper understanding of complex security systems and results in better and sustainable solutions.

2. Profile contents

MSE students in ICS have master-level skills and knowledge in the main areas of information and cyber security and can deepen their knowledge and skills in or more of the following areas. This specialization is conducted primarily through the Vertiefungsmodule and Master Thesis but also supported by technical scientific modules (TSM) in a selected number of topics.

The topic Security Management and Governance focusses on the accountability framework that provides an oversight to ensure that potential risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks based on a security strategy. MSE students have a deep knowledge and can concept, design, specify and maintain such complex and comprehensive systems.

MSE students with interest in Software based Security, that defines a set of practices help to protect software applications from attacks and threats, are able to incorporate these techniques into the software development lifecycle and testing process. They know the different phases in the secure software development lifecycle (SSDLC). They know the different techniques, evaluate them and can apply the suitable one.

Network Security covers all security aspects of networks. This includes physical, logical and software defined networks and aim to ensure the confidentiality, integrity, and availability of network resources and data by implementing various security measures such as firewalls, intrusion detection and prevention systems, encryption, authentication, and access control mechanisms. MSE students are able to research, develop, implement and run network security to protect sensitive information, maintain business continuity, and safeguard against financial losses and reputation damage. They also identify potential vulnerabilities and risks, and design, develop and implement strategies to mitigate them.

Security Architecture refers to the design and implementation of a comprehensive security framework that ensures the protection of information assets and infrastructure from threats and risks. MSE students are able to define policies, procedures, standards, and technologies that define the security requirements, objectives, and capabilities of an organization. Designing, implementing, and running are core competences and they can outline the roles and responsibilities of different stakeholders in the security process, including IT personnel, management, and end-users.

MSE students focusing on Security Assurance, Resilience and Safety are able to secure, develop, test and verify systems and know how they can be attacked and defended. They know relevant cryptographic building blocks, design principles and methods, processes and security controls to build and maintain

systems that are secure. The students know the threat landscape and they can take on the role of an attacker if needed. They can evaluate the security of a system and make recommendations on how to improve it. They can assess and adopt new security technologies emerging from research and investigate new threats emerging from practice.

MSE students with interest in Infrastructure Security (incl. OT, IoT) will learn all security aspects of critical infrastructures and how to deal with the secure operational phase of these infrastructures. They know the different types of infrastructure security and can apply, test and maintain this to and on real world systems and applications. This includes operations and maintenance of systems in a way the security is not downgraded, possible threats can be identified and mitigated, and security recommendation can be provided. A close cooperation with the system infrastructure should finally lead to a kind of DevSecOps setup.