Q&A Exam TEK5530 spring 2021 - **Update 10Mar2021**

L1-1: What are the challenges for operational control (OT)?

L1-2: What are the differences between an IT infrastructure and an operational control infrastructure with respect to connectivity, network posture, security solutions, and the response to attacks?

L2-1: Which are the domains being merged in the view of Internet of Things?

And what are the specifics and challenges of these domains?

What is the difference between the Web and the Semantic Web?

L2-2: Explain the manageability challenges with an IoT home environment!

Expected: inability to manage full depth, automatic configuration, multi-owner, privacy control.

L3-1: What is special with security of the Internet of Things?

Explain possible security problems with home IoT appliances!

L3-2: Comparing IT and automation equipment, what would you see as main difference?

What are the challenges in converged IoT infrastructure challenges?

Explain attacks, where IoT devices can play a role!

Why can tamper resistance be important in the IoT?

L3-8 Is over-the-air update a plus or a minus for the security of the system? Why?

L4-1: What is the motivation for introducing a Smart Grid?

What do you see as main security problems for an automated meter reader (AMR)?

L5-1: Why is QoS is an important question in automation?

What considerations would you take when analysing time aspects in automation?

L5-3: What is an operating envelope?
Provide examples of parameters of an operating envelope

Why is it important to follow up requirements and have some kind of tracking?

L7-1: Explain the difference between functional, non-functional and security components

Provide examples of security challenges in IoT

Provide at least 4 functional components of a system of system.

Provide at least 4 security or privacy components

What is the relation of safety and security?

L7-3: Provide the reasoning for Industrial Automation Control (IAC) in automation

How is integrity translated into components?

L8-1: Discuss the shortcomings of the traditional threat-based approach

L9-1: What is meant by Defense-In-Depth?

L9-2: Provide examples of hardening

L9-3: Which components does an industrial control system (ICS) have?

L10-1: What are the core elements of the Multi-Metrics approach? How can you achieve measurable security and privacy?

How is the Multi-Metrics analysis performed? What are the results being compared?

L10-2: Explain the effect of weighting in the Multi-Metrics analysis. What are the results of a linear weighting, as compared to a root-mean-square analysis?

L11-1: What are security functionalities and attributes? Name at least 3 of each type.

L13-1: What is an Intrusion Detection System?

Which components has an Intrusion Detection System?

Describe how to evaluate possible attacks on an automation system.

L13-3: Describe the differences between a signature-based and an anomaly detection-based IDS.

L14-3: What is a threat modeling tool? Use the example of the Microsoft

Thread modeling tool.

How can a threat modeling tool contribute to a better product?

L15-1: Tell the difference between the cloud delivery models IaaS, PaaS and SaaS.

Present the AWS shared responsibility model, tell the difference between security of the cloud and in the cloud.

L15-3: Logging and forensics in AWS: tell about possibilities to see what is happening in the cloud: VPC flowlogs, CloudWatch, CloudTrail

What is elasticity and scalability?

L15-5: What is cloud computing penetration testing, and what are the rules for penetration testing in the cloud?

L15-6: Security Controls: choose 3 of the 20 critical security controls and present them, explain why they are important and how they contribute to risk reduction.

Security Controls: Explain how physical security can contribute to security of a system.