**Study for the exams**

Overview of ICS

* Lecture 1 and Lecture 2 slides
* Chapter 2 from NIST 800-82

Differences between IT and OT systems:

* Lecture 3 slides
* Chapter 4 from:

Colbert, E.J.M., Kott, A. & SpringerLink (Online service) 2016, Cyber-security of SCADA and Other Industrial Control Systems, Springer International Publishing, Cham.

* https://blogs.getcertifiedgetahead.com/security-controls-implementation-3-of-3/ [Retrieved on 14/01/2019]

Advanced Persistent Threats:

* Lecture 4 and “5 and 6” slides

Cyber Kill Chain model (both IT version and ICS version)

* Lecture “5 and 6” slides
* SANS cyber kill chain (on Blackboard)
* LM-White-Paper-Intel-Driven-Defense.pdf (on Blackboard)

Defence in depth

* Lecture 7 slides
* Chapter 5 from NIST 800-82
* IEC/ISA 62443-3-2

ICS Risk Management (Security Categories and Impact Categories)

* Lecture 8
* Chapter 6 from NIST 800-82

Risk modelling/ Attack Graphs

* Lecture 9, 10 and 11 slides/videos (no new slides in lecture 10)
* Chapter 8 and 10 from:

Sheyner, O.M., 2004. Scenario graphs and attack graphs (No. CMU-CS-04-122). CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE.

* Chapter 8 from:

Colbert, E.J.M., Kott, A. & SpringerLink (Online service) 2016, Cyber-security of SCADA and Other Industrial Control Systems, Springer International Publishing, Cham

All the case studies we have discussed in the tutorials (material is on Blackboard either on the last page of the slides or as independent PDF documents.):

* Stuxnet
* Ukraine case study
* Havex