EES-UETP
Electric Energy Systems - University Enterprise Training Partnership

Course on:

Cyber-Physical System Security of the Power Grid

April 9-11, 2013

at KTH Royal Institute of Technology, Stockholm, Sweden

Background

Cyber Security is essential to today's power grid operation as well as tomorrow's smart grids. It is at the same a true challenge to achieve. Cyber security is a multifaceted area covering ICT-infrastructure, power control applications as well as the power grid as such. It ranges also over the threats, vulnerabilities, and risks. The purpose of this course is to provide insight to the latest research for raising awareness of cyber security and approaches for managing it. The course blends instructors from academia and industry and from Europe and the US.

Course Outline

Module 1: Cyber-Physical System Risk Assessment (Day 1, 3 Hours)
2-2:30 Opening Remarks by Chen-Ching Liu, Goran Andersson and Mathias Ekstedt
2:30 -3:30 pm Cyber-power risk assessment in the energy grids: risk factors and relevance in grid control (Giovanna Dondossola)
3:30-4:30 pm Cyber security analysis of SCADA system: security metrics, attack and defense graphs. (Mathias Ekstedt)
4:30-5:30 pm Risk assessment and mitigation of coordinated cyber attacks. (Manimaran Govindarasu)

Module 2: Cyber Security of SCADA Systems (Day 2, 6 Hours)
9-10 am Cyber-physical system security of the power grid, (Chen-Ching Liu)
10-11 am- Cyber security in substations: anomaly detection, impact analysis, (Chen-Ching Liu)
11-12 pm Experimental evaluation of cyber security in energy grids: set-up, control and attack scenarios, control infrastructures and countermeasures, attack tools, performance measures and security monitoring, (Giovanna Dondossola)
2-3 pm Role of experiments in the cyber-power risk assessment of energy grids: sample experiments, SCADA and DER communication protocols, from measurement to guidelines and risk index (Givanna Dondossola)

3-4 pm Cyber physical systems security SCADA testbed: architecture, vulnerability analysis, mitigation and defense evaluation. (Manimaran Govindarasu)
4-5 pm cyber security modeling language; combining defense graphs and system architecture models, tool demonstration, (Mathias Ekstedt)

Module 3: Cyber Security in Contemporary Control Systems for Power Grids (Day 3, 3 Hours)
9-10 am - Cyber attacks on SCADA system infrastructures and their consequences , (Gunnar Bjorkman)
10-11:20 am - Automatic Generation Control: potential attack vectors, impacts, and countermeasures, State estimation: potential attack vectors, impacts, countermeasures, (Goran Andersson)
11:20-12 pm Communication infrastructure for WAM and security requirements, Protection algorithms: potential attack vectors, impacts, and countermeasures. (Manimaran Govindarasu)

Course Instructors

Göran Andersson obtained his M.S. and Ph.D. from the University of Lund, Sweden. In 1980 he joined ASEA's, now ABB's, HVDC division in Ludvika, Sweden, and in 1986 he was appointed full professor in electric power systems at KTH (Royal Institute of Technology), Stockholm, Sweden. Since 2000 he is full professor in electric power systems at ETH Zürich (Swiss Federal Institute of Technology), where he also heads the powers systems laboratory. Professor Andersson is a Fellow of the Royal Swedish Academy of Sciences, and of the Royal Swedish Academy of Engineering Sciences. He is Editor-in-Chief of IET Proceedings Generation, Transmission and Distribution, and the recipient of the IEEE PES Outstanding Power Educator Award 2007 and the George Montefiore International Award 2010.

Gunnar Björkman is employed at ABB in the area of Network Management since 1976 and is since 1995 stationed in Mannheim, Germany. He has held several management positions within R&D and Product Management among them acting as global R&D Manager for ABB's range of Network Control products between the years of 1995 to 1999. Gunnar Björkman has been the Project Coordinator for the, in end 2011, finished EU/FP7 financed security project VIKING. Currently he is coordinating the ABB parts of another FP7 project, Grid4EU, which is focused on the operational aspects of Smart Grids. He is also pursuing a PhD study on SCADA security at Royal Institute of Technology (KTH) in Stockholm. He received is MSc. Electrical Engineering degree from KTH in 1972.

Giovanna Dondossola received her Master Degree in Computer Science from the University of Milan, Italy, in 1987 followed by a three-year post-master research at the CNR of Milan. Since then she spent her professional career in performing research on the resilience of Information and Communication Technologies for the power grids. She has been involved in many international research projects related to grid automation and control, fault tolerant distributed architectures and cyber security evaluation. She has been the Project Manager of the FP6-ICT European Project CRUTIAL (http://crutial.rse-web.it). She now belongs to the T&D Technologies Department of RSE research company where she leads national and European projects on the cyber security of smart grid communications covering cyber-power risk analysis and

experimental evaluation of cyber attacks to the grid control testbeds in the RSE Laboratory. Currently she is the Project Manager of the EPCIP European Project SoES (www.soes-project.eu) and the RSE responsible for the FP7-ICT Project SmartC2Net. She is a member of Cigrè and CEN/CENELEC/ETSI working groups on on Information Security in Smart Grid Standardization. She acted as an invited speacker in the Cyber Security Panels organised during the IEEE PES General Meeting 2011 in Detroit and the IEEE PES ISGT Europe 2012 in Berlin. She is co-author of more than 80 publications in International Conferences and Journals and co-author of the Book "Critical Information Infrastructure Protection and Resilience in the ICT Sector" published by IGI Global.

Mathias Ekstedt is Associate Professor at the Royal Institute of Technology (KTH) in Stockholm, Sweden. His research interests include systems and enterprise architecture modeling and analyses with respect to information and cyber security, in particular for the domain of power system management. He is the manger of the program IT Applications in Power System Operation and Control within the Swedish Centre of Excellence in Electric Power Engineering, and was the technical coordinator of the EU FP7 project VIKING, and the director of the Electric Power Engineering Master programme at KTH. He is the founder of the architecture network at the Swedish Computer Society and the secretary of Cigré WG D2.31 Security architecture principles for digital systems in Electric Power Utilities. He received his MSc. and Ph.D. degrees from KTH in 1999 and 2004 respectively.

Manimaran Govindarasu is a Professor in Electrical and Computer Engineering at Iowa State University (ISU). He received his Ph.D. in Computer Science and Engineering from Indian Institute of Technology (IIT) Madras, India, in 1998, and Masters in Computer Technology from IIT Delhi in 1994. His research expertise is in the areas of cyber-physical security of smart grid, cyber security, real-time systems, and QoS/overlay networks. He has published over 100 peer-reviewed research publications in international journals and conferences. He is co-author of the text, "Resource Management in Real-Time Systems and Networks," MIT Press, 2001. He has given tutorials in reputed conferences, including IEEE Infocom 2004, IEEE ComSoc TutorialsNow (2004), and IEEE ISGT 2012. He serves in the editorial board of IEEE Trans. on Smart Grid, served as guest co-editor for several journal special issues (IEEE Power & Energy - Jan. 2012, IEEE Network, Journal Systems and Software, Journal of High Speed Networks), and served as workshops/symposium chair, technical program vice-chair, and session chair for several IEEE conferences. He serves as the chair of the Cyber Security Task Force at IEEE PES PSACE-CAMS.

Chen-Ching Liu is Boeing Distinguished Professor at Washington State University, Pullman, USA, and Professor of Power Systems at University College Dublin, Ireland. At Washington State University, Professor Liu serves as Director of the Energy Systems Innovation Center. During 1983-2005, he was a Professor of Electrical Engineering at University of Washington, Seattle. Dr. Liu was Palmer Chair Professor at Iowa State University from 2006 to 2008. Dr. Liu received his Bachelor's and Master's degrees from National Taiwan University and Ph.D. from the University of California, Berkeley. Professor Liu received an IEEE Third Millennium Medal in 2000 and the Power and Energy Society Outstanding Power Engineering Educator Award in 2004. He chaired the IEEE Power and Energy Society Fellow Committee, Technical Committee on Power System Analysis, Computing and Economics, and Outstanding Power Engineering Educator Award Committee. Dr. Liu served as President of the International Council on

Intelligent System Applications to Power Systems (ISAP). He is a Member of the Board on Global Science and Technology, US National Academies. Professor Liu is a Fellow of the IEEE.

Registration

Cost
250 Euro for attendees coming from EES-UETP partner institutions.
600 Euro for attendees coming from non-member universities of the EES-UETP.
1000 Euro for attendees coming from non-member industries of the EES-UETP.
The course fees will include lectures, documentation, coffee breaks and lunches.

Registration and Payment procedure

Your registration is sent as an email to Annica Johannesson at KTH at Annica.Johannesson@ics.kth.se. After we have received your registration we will send you an invoice that should be paid before March 31. If you have any specific requirements regarding the information on the invoice, please make a note of this on your application.

There is a limit on 40 people attending the course. A first-come-first-served principle will be used.

Cancellation policy
Notifications should be sent in writing to the course coordinator. Cancellations received later than one week before the course will not be refunded.

Accommodation

Accommodation is booked and paid separately by the attendees. The following hotels are recommended:

Elite Arcadia
Körsbärsvägen 1
114 23 Stockholm
Tel +46 8 566 215 00
info.arcadia@elite.se

Central Hotel
Vasagatan 38
111 20 Stockholm
Tel +46 8 566 208 00
E-post centralhotel@profilhotels.se

Location
The course will take place at de department for Industrial Information and Control Systems (ICS), Osquldas väg 10-12, 7th floor. For further details see http://www.kth.se/ees/omskolan/organisation/avdelningar/ics/contact and map below:

Description from Arcadia to course location (ICS):