Schedule: ACCESS-FORCES CPS workshop 26-27 Oct

	Mon	Tue
8:00	8:00 Coffee 8:30 Welcome: Henrik Sandberg (KTH) 8:45 Saurabh Amin (MIT)	8:00 Coffee 8:30 Alessandro Abate (Oxford U.)
9:00	9:30 Henrik Ohlsson (C3 Energy)	9:15 Ling Shi (HKUST)
10:00	10:00 Coffee break 10:30 Linus Thrybom (ABB)	10:00 Coffee break 10.30: Group work
11:00	11:00 Erik Herzog (SAAB) 11:30 Lunch buffet and poster session	11:30 Martin Törngren (KTH)
12:00	12:30 Poster session continues	12:15 Lunch at Syster o Bror
13:00	13:30 Maria Henningsson (Modelon)	13:45 Serdar Yuksel (Queen's U.)
14:00	14:00 Mats Näslund (Ericsson) 14:30 Coffee break 14.45: Introduction to group work	14:30 Lillian Ratliff (UC Berkeley)
15:00	15.40: Group work	15.30: Group Presentations
16:00	16:30 Coffee break 16:45 Claudio De Persis (Groningen U.)	16:30 Coffee break 16:45 Xiaoming Hu (KTH)
17:00		17:15 Henrik Sandberg (KTH) + closing
18:00		
19:00	19:00 Dinner at Hasselbacken	
20:00		

Presentations Work in teams/posters Coffee/lunch/dinner

All presentations will be in F3, Lindstedtsvägen 26, KTH.

Titles and abstracts:

All presentations will be in F3, Lindstedtsvägen 26, KTH.

Monday

8:45 Saurabh Amin, FORCES/MIT

Title: Some Structural Results on Network Security Games Abstract: This work focuses on the analysis of attacker-defender interactions on distribution networks (DNs) using game-theoretic tools. Two attack models are considered: (i) strategic disruption of network links; (ii) manipulation of distributed generation (DG) nodes. In the first model, the defender chooses flow routing strategies to maximize the expected effective flow between source-destination pairs while facing strategic link disruptions and faces transportation costs. The attacker simultaneously disrupts one or more links to maximize her value of lost flow and faces cost of disrupting links. This game is strategically equivalent to a zero-sum game. Linear programming duality and the max-flow min-cut theorem are applied to obtain properties that are satisfied in any mixed Nash equilibrium. In any equilibrium, both players achieve identical payoffs. While the defender's expected transportation cost decreases in attacker's marginal value of lost flow, the attacker's expected cost of attack increases in defender's marginal value of effective flow. Interestingly, the expected amount of effective flow decreases in both these parameters. In the second model, the defender observes and responds to the adversary induced DG node disruptions by imposing partial load shedding and controlling supply. The loss to the defender includes loss of voltage regulation and cost of induced load control under supply-demand mismatch caused by the attack. Solving this sequential game is hard due to nonlinear power flows and mixed-integer decision variables. To address this challenge, the problem is approximated by tractable formulations based on linear power flows. The set of critical DG nodes and the set-point manipulations characterizing the optimal attack strategy are characterized. An iterative greedy approach to compute attacker-defender strategies for the original nonlinear problem is proposed. These results also provide guidelines for optimal security investment and defender response in pre- and post-attack conditions, respectively.

9:30 Henrik Ohlsson, FORCES/C3 Energy

10:00 Coffee break

10:30 Linus Thrybom, ABB

11:00 Erik Herzog, SAAB

11:30 Lunch buffet and poster session

12:30 Poster session continues

13:30 Maria Henningsson, Modelon

14:00 Mats Näslund, Ericsson/KTH

14:30 Coffee break

14:45 Introduction to group work

15:40 Group work

16:45-17:30 Claudio De Persis, Groningen University

Title: Cyber-physical systems and Lyapunov functions

Abstract: Control design based on energy functions is a powerful method for problems of coordination of network systems, for it leverages physical intuition to build Lyapunov functions which are instrumental in the analysis. In the presence of a cyber infrastructure, the use of energy as a candidate Lyapunov function is hampered by phenomena such as sampling, delays and data loss. In this talk, I will present some recent results on the redesign of energy-based Lyapunov functions that permit to take into account these cyber constraints. Within this framework, I will introduce a deterministic set-up to deal with data loss, possibly induced by malware actions such as Denial-of-Service attacks. Some of the results will be illustrated using microgrids as a case study. Along the way, I will point out challenging open problems that are, in my opinion, worth of investigation. This is joint work with P. Tesi, R. Postoyan and N. Monshizadeh.

19:00 Dinner at Hasselbacken

Tuesday

8:30 Alessandro Abate, Oxford University

Title: Data-driven and model-based quantitative verification and correct-by-design synthesis of CPS

Abstract: I discuss a new and formal, measurement-driven and model-based automated verification and synthesis technique, to be applied on quantitative properties over systems with partly unknown dynamics. I focus on physical systems (with spatially continuous variables, possibly noisy), driven by external inputs and accessed under noisy measurements, and suggest that the approach can be as well generalized over CPS. I formulate this new setup as a data-driven Bayesian model inference problem, formally embedded within a formal, model-based verification procedure. While emphasizing the generality of the approach over a number of diverse model classes, this talk zooms in on systems represented via stochastic hybrid models (SHS), which are probabilistic models with heterogeneous dynamics (continuous/discrete, i.e. hybrid, as well as nonlinear) - as such, SHS are quite a natural framework for CPS. With focus on model-based verification procedures, I provide the characterization of general temporal specifications based on Bellman?s dynamic programming. The computation of such properties and the synthesis of related control architectures optimizing properties of interest is attained via the development of abstraction techniques based on quantitative approximations. This abstraction approach employs methods and concepts from the formal verification area, such as that of (approximate probabilistic) bisimulation, over models and problems known in the field of systems and control. Theory is complemented by algorithms, all packaged in a software tool (FAUST^2) that is freely available to users.

9.15 Ling Shi, HKUST

Title: SINR-based DoS Attack on Remote State Estimation: A Game-theoretic Approach

Abstract: We consider remote state estimation of cyber-physical systems

(CPS) under signal-to-interference-plus-noise ratio (SINR)-based denial-of-service (DoS) attacks. A sensor sends its local estimate to a remote estimator through a wireless network that may suffer interference from an attacker. Both the sensor and the attacker have energy constraints and they need to consider how much transmission power to use and how much interference power to attack. We propose a Markov game framework to model this interactive decision-making process based on the current state and information collected from previous time steps. To solve the associated optimality (Bellman) equations, a modified Nash Q-learning algorithm is applied to obtain the optimal solutions. Numerical examples and simulations are provided to demonstrate our results.

10:00 Coffee break

10:30 Group work

11:30 Martin Törngren, KTH

Title: Characterization, analysis and recommendations for exploiting the opportunities of Cyber-Physical Systems

Abstract: Leveraging a comprehensive analysis of Cyber-Physical Systems (CPS) in Europe (the CyPhERS project - www.cyphers.eu), this talk presents overall findings focusing on (i) a characterization of CPS, (ii) opportunities and challenges in representative CPS application domains, and (iii) recommendations for action resulting from a cross domain analysis. The characterization enables the description of a CPS, or classes of CPS, according to their technical emphasis, cross-cutting aspects, level of automation and life-cycle integration. As opposed to many similar investigations on CPS and related concepts, CyPhERS adopted a broader sociotechnical perspective to CPS including societal, market and education/training aspects. Highlights from the recommendations will be discussed.

12:15 Lunch at Syster o Bror

13:45 Serdar Yuksel, Queen's University

Title: Convex Analysis in Stochastic Teams and Asymptotic Optimality of Finite Model Representations and Quantized Policies

Abstract: This talk is concerned with stochastic dynamic team problems and their optimal solutions. To facilitate a convex analytical approach, strategic measures for team problems are introduced; these are probability measures induced by admissible team policies. Properties such as convexity and compactness are studied. These lead to existence of and structural results for optimal policies. It will be shown that the set of strategic measures for a team problem is in general non-convex unlike single decision maker control problems, and cannot be convexified through the addition of common or independent randomness, but the extreme points of a relaxed set consist of deterministic team policies, which lead to their optimality. Refined characterizations of convexity for problems which include teams with a non-classical information structure will be presented. Finally, asymptotic optimality of finite model representations for a large class of dynamic team problems will be established. These lead to asymptotic optimality of quantized control policies, so that one can construct a sequence of finite models obtained through the quantization of measurement and action spaces whose solutions converge to the optimal cost. Witsenhausen's counterexample is an important special case that will be discussed.

14:30 Lillian Ratliff, FORCES/UC Berkeley

Title: The Emerging Data Market: Adaptive Incentives for Smart, Connected Infrastructure

Abstract: The next generation urban ecosystem empowered by the internet of things has at its core a shared economy where physical resources and data are easily aggregated and exchanged. In particular, advances in technology have lead to the proliferation of smart devices that provide access to streaming data and platforms for novel sharing mechanisms. This has, in turn, resulted in an emerging marketplace in which data is a commodity. The ease with which data and resources can be shared has led many urban constituents to become aware of the value of their data and its usefulness for operations. In such an environment, new learning and optimization schemes which consider users as strategic data sources and resource seekers are needed. In this talk, we will discuss the emerging data market, its incentive structure (players and their motivations), and tools for learning with strategic data sources. Focusing on the design of adaptive incentive mechanisms under adverse selection, we will construct an algorithm for online utility learning and incentive design and show convergence results for both the case where players are rational (play according to Nash) and myopic. We will see through a tutorial example how the algorithm performs, and conclude with some open questions and future directions.

15:15 Coffee break

15:30 Group presentations

16:30 Coffee break

16:45 Xiaoming Hu, ACCESS/KTH

Preliminary title: Crowd evacuation

17:15-17.45 Henrik Sandberg, ACCESS/KTH

Title: Information-Regularized Optimal LQG Control

Abstract: We consider a joint sensor and controller design problem for linear Gaussian stochastic systems in which a weighted sum of quadratic control cost and the amount of information acquired by the sensor is minimized. This problem formulation is motivated by situations where a control law must be designed in the presence of sensing, communication, and privacy constraints. We show that the optimal joint sensor-controller design is relatively easy when the sensing policy is restricted to be linear. Namely, an explicit form of the optimal linear sensor equation, the Kalman filter, and the certainty equivalence controller that jointly solves the problem can be efficiently found by semidefinite programming (SDP). Whether the linearity assumption in our design is restrictive or not is currently an open problem. This is joint work with Takashi Tanaka, MIT.

Challenges in CPS: working groups

SAAB	CPS-Systems Eng. & Edu.	**Modelon**	CPS-Modeling
Erik Herzog	SAAB	Maria Henningsson	Modelon
Saurabh Amin	MIT	Claudio De Persis	Groeningen U.
Bart Besselink	KTH	Viktoria Fodor	KTH
Liang Dai	Uppsala university	Håkan Hjalmarsson	KTH
Dimos Dimarogonas	KTH	Johan Karlsson	KTH
Per Enqvist	KTH	Alexander Medvedev	Uppsala university
Pedro Gomes	KTH	Jezdimir Milosevic	KTH
Meng Guo	KTH	Axel Ringh	KTH
Xiaoming Hu	KTH	Cristian R. Rojas	KTH
Ivan Stenius	KTH	Henrik Sandberg	KTH
Gustav Söderlind	MSB	Jana Tumova	KTH
Martin Törngren	KTH		
ABB	CPS-Communication	**Ericsson**	CPS-Security
Linus Thrybom	ABB	Mats Näslund	Ericsson/KTH
Alessandro Abate	Oxford	Christoph Baumann	KTH
James Gross	KTH	Mads Dam	KTH
Nicolas Innocenti	KTH	Elena Dubrova	KTH
Karl H. Johansson	KTH	Majid Gerami	KTH
Hojat Khosrowjerdi	KTH	Anders M	Försvarsmakten
Chanhwa Lee	Seoul National U.	Tobias Oechtering	KTH
Farshad Naghibi	KTH	Rafael Pasquini	KTH
Misbah Uddin	KTH	Emil Ringh	KTH
Jieqiang Wei	Groningen U.	Ling Shi	HKUST
Jungfeng Wu	KTH	Ragnar Thobaben	KTH
Ming Xiao	KTH	Moritz Wiese	KTH
C3 Energy	CPS-Energy		
Henrik Ohlsson	FORCES/C3 energy		
Claudio Altafini	Linköping University		
Martin Andreasson	KTH		
Gyrgy Dán	KTH		
Adam Molin	KTH		
Kaveh Paridari	KTH		
Lillian Ratliff	FORCES/UC Berkeley		
Emma Tegling	KTH		
Bo Wahlberg	KTH		
Serdar Yuksel	Queen's university		
Silun Zhang	KTH		