Editorial

Unal Tatar*

Department of Engineering Management and
Systems Engineering,
Old Dominion University,
Norfolk, Virginia, USA
Email: utatar@odu.edu
*Corresponding author

Gabriele Oliva

Unit of Automatic Control,
Department of Engineering,
University Campus Bio-Medico of Rome,
via Álvaro del Portillo 21,
00128, Rome, Italy
Email: g.oliva@unicampus.it

James Moreland Jr.

Office of Secretary of Defense,
3090 Defense Pentagon, Room 3B914,
Washington, DC 20301-3090, USA
Email: jmorelan@odu.edu

Biographical notes: Unal Tatar worked as a Principal Cyber Security Researcher in the government and industry for ten years. He is the former coordinator of the National Computer Emergency Response Team of Turkey. He worked in various cyber risk assessment projects in critical infrastructure sectors as a researcher and project manager. He holds a BSc degree in Computer Engineering, an MS degree in Cryptography. He is currently pursuing his PhD in ODU Engineering Management and Systems Engineering Department. His main topics of interest are information/cyber security risk management, cyber resiliency, cyber insurance, and policy and strategic issues in cyber security.

Gabriele Oliva received his Laurea degree and PhD in Computer Science and Automation Engineering in 2008 and 2012, respectively, both at the University Roma Tre of Rome, Italy. He is currently an Assistant Professor in Automatic Control at the University Campus Bio-Medico of Rome, Italy. His main research interests include critical infrastructures, distributed systems, distributed optimisation, and applications of graph theory in technological and biological systems.

James Moreland Jr. entered the Senior Executive Service in September 2014, and currently serves as the Deputy Director for Naval Warfare within the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD AT&L). He earned his PhD in Systems Engineering from the

George Washington University in 2013, an MS in National Resource Strategy from the Industrial College of the Armed Forces in 2001, an MS in Systems Engineering from the Virginia Tech in 1997, and a BS in Mechanical Engineering from the University of Maryland in 1988, his awards include three Joint Meritorious Unit Awards and one Navy Meritorious Unit Award for exceptional meritorious achievement in support of the Joint Chiefs of Staff, OSD, and Naval Sea Systems Command (NAVSEA), the Navy Superior Civilian Service Award, and the Navy Distinguished Civilian Service Award.

As demonstrated by recent events [e.g., the blackout experienced in Ukraine in 2015 (Liang et al., 2017) or the WANNACRY (Mattei, 2017) Ransomware], Critical Infrastructures (e.g., telecommunication or transportation networks) are particularly vulnerable to cyber attacks, which may generate cascading failures, possibly leading to the complete or partial halt of the services provided to the community, with dramatic and often life-threatening consequences.

Enhancing the protection of Critical Infrastructures to cyber threats is, therefore, one of the main challenges of the immediate future. To this end, it is fundamental to provide reliable architectures, effective risk assessment procedures and methodologies able to detect cyber attacks.

These tasks are extremely important, as highlighted for instance by the recent NIS EU Directive (European Commission, 2016), which requires critical infrastructure operators, and in particular IT providers, to take adequate measures in order to manage risk, report security incidents to the national competent authorities and provide early threat warnings.

This special issue intends to contribute in this sense, and several specific themes are addressed, such as risk management, cyber-event detection, intrusion detection and governance, to name a few.

In their paper ‘On the detection of cyber-events in the grid using PCA’, Wallace and Atkinson provide a methodology to detect data manipulations or data injections, based on principal component analysis. Wood et al. in their work ‘A security architectural pattern for risk management of industry control systems within critical national infrastructure’ propose a security architectural pattern to address cyber security risks, based on the Sherwood Applied Business Security Architecture (SABSA). Limbasiya and Shivam, in their paper ‘A two-factor key verification system focused on remote user for medical applications’ focus on telecare medicine information systems (TMIS) and provide a two-factor authentication and key agreement scheme. The paper ‘Towards effective cyber security resource allocation: the Monte Carlo predictive modelling approach’ by Fagade and Tryfonas provides a methodology based on Monte Carlo predictive simulation for improving the resource allocation in the context of security management. Katina et al., focus their attention on the governance, and in their paper ‘Complex system governance for critical cyber-physical systems’ stress the role of complex system governance (CSG) as a way to increase cohesion in order to face cyber threats in cyber-physical system (CPS) and critical infrastructures. In their paper ‘A process-based dependency risk analysis methodology for critical infrastructures’, Stergiopoulos et al. provide a methodology to dynamically assesses the evolution of cascading failures in critical infrastructures. In their paper ‘Preemptive: an integrated approach to intrusion detection and prevention in industrial control systems’, Etcheves Miciolino et al. provide an overview of the results attained by the preemptive project to improve the cyber-security of industrial control systems (ICS). Huang and Nicol in their work ‘An anatomy of trust in public key infrastructure' provide an in-depth analysis of the trust mechanism used in public key infrastructuress (PKI). The paper 'Achieving desired performance objectives in the energy sector through data analytics' by Hurley stresses the need of focusing on the analytic capability of the sectors and the need to meet the requirements and demands through more data-driven decision making across the entire enterprise. Finally, in 'Resilient industrial control systems based on multiple redundancy' by Alcaraz, a new repair approach for industrial control systems is provided based on multiple redundant pathways.

References

European Commission (2016) *The Directive on Security of Network and Information Systems (NIS Directive)*, Tech. Rep.

Liang, G., Weller, S.R., Zhao, J., Luo, F. and Dong, Z.Y. (2017) 'The 2015 Ukraine blackout: implications for false data injection attacks', *IEEE Transactions on Power Systems*, Vol. 32, No. 4, pp.3317–3318.

Mattei, T.A. (2017) 'Privacy, confidentiality and security of healthcare information: lessons from the recent WannaCry cyber attack', *World Neurosurgery*, Vol. 104, pp.972–974.