Dr Sokratis Katsikas,
CCIS – Center for Cyber & Information Security of Norway

Short Curriculum Vitae (C.V.)

Sokratis K. Katsikas was born in Athens, Greece, in 1960. He received the Diploma in Electrical Engineering from the University of Patras, Patras, Greece in 1982, the Master of Science in Electrical & Computer Engineering degree from the University of Massachusetts at Amherst, Amherst, USA, in 1984 and the Ph.D. in Computer Engineering & Informatics from the University of Patras, Patras, Greece in 1987. Currently he is a Professor with the Center for Cyber and Information Security, Norwegian University of Science and Technology, Norway, Professor of the Dept. of Digital Systems of the University of Piraeus, Greece (on leave), member of the pool of experts of the Institutional Evaluation Programme of the European University Association and chair of the Steering Committee of the same programme. He has been the Rector (2003-2006) and Vice-Rector (1997-2003) of the University of the Aegean, member of the Board of the Hellenic Quality Assurance Authority for Higher Education (2006-2008), member of the Board of the Hellenic Authority for Information and Communication Security and Privacy (2008-2009), Vice-President of the Panhellenic Federation of University Faculty Members (2009), the National Representative of Greece to the Management Committee of the 7th EU R&D Framework Programme "People" (2007-2009), the General Secretary for Telecommunications & Post of the Ministry of Infrastructures, Transport and Networks of the Hellenic Republic (2009-2012), member of the Committee for Information and Communication Technologies of the Greek Government (2011-2012), Chairman of the Technical Advisory Board on Information and Communication Technologies of the Ministry of Administrative Reform and Electronic Government (2011-2012), the President of the National Education Council of Greece (2013-2015), and the President of the Council of University Education of Greece (2013-2014). His research interests lie in the areas of information and communication systems security and of estimation theory and its applications. He has authored or co-authored more than 230 journal publications, book chapters and conference proceedings publications and he has participated in more than 60 funded national and international R&D projects in these areas. He is serving on the editorial board of several scientific journals, he has authored/edited 26 books and has served on/chaired the technical programme committee of more than 400 international scientific conferences.

"Cybersecurity issues in the Oil & Gas industry"

Cyber-physical systems (CPS) are physical and engineered systems that interact with the physical environment, whose operations are monitored, coordinated, controlled and integrated by information and communication technologies. These systems exist everywhere around us, and range in size, complexity and criticality, from embedded systems used in smart vehicles, to SCADA systems in smart grids, to control systems in water distribution systems, to smart transportation systems, to plant control systems, engineering workstations, substation equipment, programmable logic controllers (PLCs), and other Industrial Control Systems (ICS). The oil and gas industry is not an exception to the rule. Such systems are routinely used to monitor and control physical processes in the oil and gas industry. Their role is the acquisition of data coming from processes (temperatures, pressures, valve positions, tank levels, chemical compositions, flow demands, etc.), human operators and the direct control of electric, mechanical, hydraulic or pneumatic actuators. Failure of such systems can cause production stoppages, a decrease in product quality or even destruction of infrastructure. In the past, such systems were isolated, invisible to the outside world and using proprietary hardware, software, and communication protocols. Today, these systems are increasingly being integrated into the enterprise IT systems; this enhances the business intelligence capabilities of the enterprise, but there is a price to pay: these mission-critical systems are now vulnerable to cyber attacks and must, therefore, be properly protected against those. This talk will address critical concerns and trends regarding cyber security for the oil & gas industry, and will also discuss ways of addressing these concerns.