Digital enterprise and Cyber security evolution

A. Raicu[1,*], G. Raicu[2]
Department of General Engineering Sciences, Constanta Maritime University, 104 Mircea cel Bătrin Street, 900663 Constanta, Romania, alexandra.raicu@cmu-edu.eu
Department of Navigation, Constanta Maritime University, 104 Mircea cel Bătrin Street, 900663 Constanta, Romania, gabriel.raicu@cmu-edu.eu

Keywords. PLM, cyber security, digital enterprise, cloud computing, Internet of Things and Services

Abstract.
Industry 4.0 requires increased connectivity and the use of standard communication protocols which nowadays implies an increased need to protect critical industrial systems and manufacturing lines from cyber threats. We can not talk about the evolution of the digital enterprise without cyber security. There are a lot of Cyber Security incidents related to Industry 4.0 and IoT developments. PLM, as a whole concept, are prone to cyber threats due to complex interactions between management of design data, quality management, process management, portfolio management, Supply Chain Management (SCM), Customer Relationship Management (CRM) and management of whole things which are related to the product. The paper address the evolutionary cyber threats in last decade using public resources. At present, the large companies that supply industrial equipment have also taken into account the aspects of cyber security. The paper, also presents certain approaches from a scientific point of view in Constanta Maritime University (CMU) research center for the cyber security. To address this complex research field, CMU started several years ago, a complex research and innovatived project related to advanced research, training and development of new technologies in maritime cyber security. Using the CMU complex cybersecurity simulator, we are able to generate some massive scenarios in technical related fields such as maritime operations, technical design, technical simulations and detect potential vulnerabilities. One of these kinds of activities was treated as potential long term risks due to the nature of induced vulnerabilities in PLM software's.