1 THE (IN)SECURITY OF THE INFORMATION FLOW WITHIN THE PLM

The classic PLM principles are only intended to provide control over the information and tools that allow the management of the overall life cycle of products. Product development is accompanied by many changes, such as changes in customer requirements, errors in design and planning, availability of resources, etc. Thus, the entire PLM process processes an enormous amount of data flow, and to be efficient in a PLM system, the product data must be dynamically shared, easily, accessible, and inherently secure.

The classic approach to the concept of PLM does not consider cybersecurity problems, the principle of design of the concept being prior to the emergence of global security problems. And here we can refer to all the stages, aspects of the life of a product, stages that involve each interaction between entities that use the information available and share it further.

2 PLM Casuistry – unsecured SCENARIOS

LOCALIZED COMPROMISE OF PLM MANAGEMENT SYSTEMS – THE FOXCONN CASE

COMPROMISING A GLOBAL INDUSTRIAL SOLUTION – THE SIEMENS CASE

SIMULTANEOUS RISK ACCUMULATION – OT – SIEMENS – SCHNEIDER ELECTRIC

COMPROMISING A GLOBAL INDUSTRIAL SOLUTION – THE AUTODESK CASE

3 CMU scalable micro-Smart Factory

In terms of command-and-control technologies, the Industry 4.0 systems in the UMC laboratory inventory have an effective general connectivity but with potential vulnerabilities to "low and slow" attacks. The design elements are available on laptop computers connected via a VPN (OpenVPN / SoftEther) to a Smart Factory resource management node. Access to C&C resources is restricted internally within a virtual LAN available only within a Hypervisor that manages local resources and applications. There is a dual access authorization (2FA + certificate authentication).

CMU MISP

ICS malware

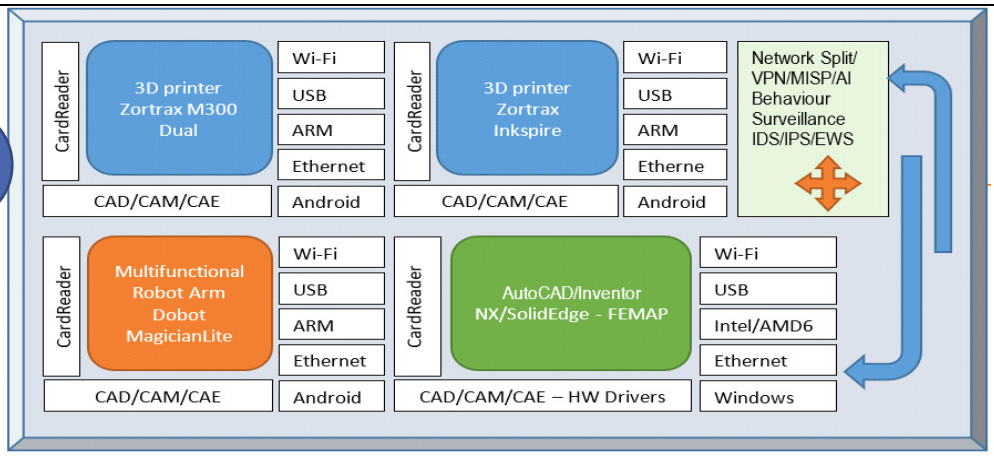
A proactive approach to ensuring the cyber security of the micro factory is obtained using examples and models focused on ICS / SCADA. The following graphical examples refer to the well-known IRONGATE family of malware identified by FLARE from FireEye (Mandiant).

Alexandra Raicu*[a], Gabriel Raicu[b]

[a]Department of General Engineering Sciences, Faculty of Naval Electromechanics, Constanta Maritime University, 104 Mircea cel Batrân Street, 900663, Constanta, Romania; [b]Department of Navigation and Waterborne Transport, Faculty of Navigation and Naval Transport, Constanta Maritime University, 104 Mircea cel Batran Street, 900663 Constanta, Romania

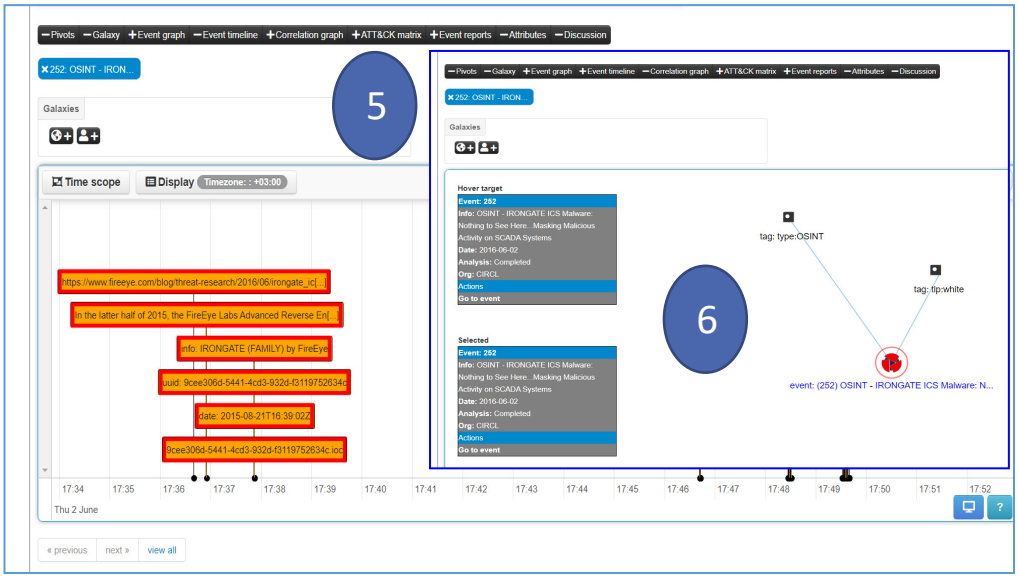
In the last five years, there has been a major change in approach from a conceptual point of view in terms of cybersecurity that needs to be ensured at the level of a complete industrial chain from the perspective of a Smart Factory. In this paper we proposed to develop a complete Product Lifecycle management (PLM) system in conditions of cybersecurity. We started from conclusive global examples and analyses (in)security of the flow of information within the PLM, such as the incidents of Foxconn, Siemens, Schneider Electric, Autodesk. Using the paradigm imposed by the efficiency of PLM processes, we have developed an intelligent scalable micro factory at the Maritime University of Constanta, within the PLM Center.

4



DEVELOPING A COMPLETE PLM SYSTEM IN CYBERSECURITY CONDITIONS

5



6