The 5th GI/ACM Workshop 2020 Scope and Draft Programme on Standardization of Secure and Safe Smart Manufacturing Systems with respect to IEC 62443 IACS

Jan deMeer[1] Karl Waedt[2] Axel Rennoch[3] Hans-Joachim Hof[4]

Abstract: The 5th GI/ACM Workshop Programme on Standardization of Secure and Safe Production within Industrial Automation and Control Systems (IACS) took place virtually at September 28, 2020 at the Karlsruhe Institute of Technology (KIT) that hosted the 50th GI's yearly assembly (GI Informatik 2020 Jahrestagung): https://informatik2020.de/programm/workshops/

Keywords: I4.0; Security & Safety; Industrial Automation and Control Systems; Digital Twin; Production Ontologies; Smart Manufacturing; Asset Administration Shell; OPC-UA; AutomationML; OT/IT Security; Syntactic and Semantic Interoperability; Edge Computing

1 Organization of the IACS Standardization Workshop 2020

The IACS workshop call has been closed August 31 2020 due and 10 up-to-date papers from the realms of Standardization, Best Practice and I4.0 Research have been presented. The preparation of the IACS Workshop has been achieved by means of the platform: https://easychair.org/conferences/?conf=i40acsws20 in co-operation with the IACS Standardization WS Programme Committee. All accepted contributions (with the exception of abstracts) that coincide to Springer Publisher's author guidelines of LNI: https://gi.de/service/publication/ini/ are listed below and are ready for publication in the Conference Proceedings of the GI Informatik Jahrestagung 2020.

The PC decided on the WS' Programme that comprises the following presenters and IACS topics. Notice the 1st (‚IACS Scope and Semantics') and the 10th (‚Quo Vadis IACS') presentation embrace the WS' Programme of Work in an introducing and concluding part:

1. *Jan deMeer et al.: Introduction into IEC 62443 IACS Scope and Semantics*
2. *Vitaly Promyslov et al.: Validation of Control Systems with Heterogeneous Digital Models and Virtualization Technologies*

[1] smartspacelab.eu GmbH, Berlin, 12205, demeer@smartspacelab.de
[2] FRAMATOME GmbH, Erlangen, 91058, karl.waedt@framatome.com
[3] Fraunhofer FOKUS, Berlin, 10589, axel.rennoch@fokus.fraunhofer.de
[4] Technische Hochschule Ingolstadt, hans-joachim.hof@thi.de

doi:10.18420/inf2020_26

3. *Mithil Parekh et al.: Aligning with Cyber Security Framework by modeling OT Security*
4. *Yuan Gao et al.: Operational Security Analysis and Challenge for IoT Solutions*
5. *Axel Rennoch et al.: Edge Computing Standardization and Initiatives*
6. *Vanesa Watson et al.: MAC-layer Security for Time-sensitive Switched Ethernets*
7. *Joseph Schindler et al.: Gossip Protocol Approach for a Decentralized Energy Market with OPC-UA Client Server Communication*
8. *Nikolas Mühlbauer et al.: Feature-based Comparison of Open Source OPC-UA Implementations*
9. *Deeksha Gupta et al.: Simulation Model for Threat and Impact Analysis on Modern Electrical Power Systems*
10. *Pierre Kobes: Quo Vadis IEC 62443 IACS?*

The Board of GI/ACM WS Co-Chairs and the WS Programme Committee appreciated the technical support from:

2 Scope of IACS Standardization

The scope of IACS Standardization and thus of the Workshop included but is not limited to the full bandwidth of the current 13 parts of the IEC 62443 IACS Standards series, i.e.:

1. IACS Modeling and Concepts
2. System Security Conformance Metrics
3. Security Lifecycle and Use Cases
4. Patch and Security Management Systems
5. IACS Security Risk Assessment and Security Levels
6. Product Development
7. Security Requirements for IACS Components,

which includes requirements to security und safety measures to be applied during the full IEC62443 IACS live cycle comprising:

1. Rules and procedures for operation and maintenance of IACS
2. Planning and installation of Basic Process Control Systems (BPCS), Safety Instrumented Systems (SIS), other hard and software of IACS
3. Development and implementation of IACS components comprising
    1. embedded devices
    2. network components
    3. host devices
    4. applications

Additionally Security and Safety Requirements of IEC 62443 production sites and devices comprise the following measures and concepts:

1. to identify security contexts in order to condemn threats;
2. to identify security aims in order to enable automatization of production plants with the base line of ‚Safety first';
3. to identify production safety based on minimal right restrictions without influencing IACS availability too much;
4. to organize staggered defense measures in order to harden the IACS assets against attacks;
5. to perform Risk Analysis in order to evaluate Threats and Vulnerabilities of Assets;
6. to identify Guidelines and Processes of enterprises for the purpose of a holistic view on the enterprise's and plant's security;
7. to invent concepts of security into the whole chain of production in order to avoid vectors of threats and vulnerabilities.

3 Semantics of IACS Standardization

3.1 Complexity in Standardization

Industrial Standards such as the multi-part IEC 62443 standard on Security of Industrial Automation and Control Systems that is currently elaborated by a couple of standardization committees such as ISA99, ISO JTC1/SC27/WG4, IEC TC65/WG23 etc. become more and

more complex in the sense of yielding a common understanding with respect to a unique interpretation, e.g. for an implementation of a production system to be conform to the given set of complex standards.

3.2 Semantic Classification

With respect to the issue of yielding a common interpretation of standardization texts the so-called ‚System Committee on Smart Manufacturing (SyC SM)' has started the task force ‚ISO/IEC Joint Smart Manufacturing Standards Map (TF SM2)' to solve the issue of a common understanding by inventing the methodology of classification supported by a platform of integrated tools comprising visualization and a central repository of classified text passages.

The process of SM Standards Classification comprises three steps:

to collect formats and characteristics of products or of processes of production prescribed and constrained in related standards (Notice: In future this step needs to be supported by a SM2 Vocabulary that is do-day not available);

to actualize parameters of SM standards by assigning specific values to the characteristics of standards identified in the SM2 catalogue;

to perform tool-supported semantic analysis in 2D or 3D graphic representations to standards contained in the SM2 catalogue.

The method of graphic analysis means the mapping of product or production characteristics to two, three or more dimensional axes of a standardized reference model, e.g. life-cycle phases of product types or of production systems.

When inspecting the SM2 catalogue for retrieving features of PLC (Production Life Cycle of IEC 61131-4) Languages then you may get the following ‚answers' depending of the used classification scheme:

```
product class := control> & <production system phase := design |
implementation> & <product usage := functional layer>;
```

where ‚product class', ‚production system phases', ‚product usage' are dimensional components and ‚control', ‚design', ‚implementation', ‚functional layer' are values that are assigned to the dimensional components.

3.3 Semantic Interoperability

The standardization documentation series of JTC1/SC41 of the IIoT project ‚ISO 21823 - IoT Framework, Transport Interoperability, Semantic and Syntactic Interoperability',

distinguishes explicitly between syntactic and semantic 'Interoperation among Industrial Things' - whereby 21823 part 4 describes syntactic and 21823 part 3 describes semantic "Interoperability between IoT Models".

Thus syntactic interoperability means syntactic data exchange among entities with multiple options of information representation of IoT data - semantic interoperability means data exchange among multiple and different IoT device ontologies.

In the IEC white paper(2019) ‚Semantic Interoperability' it is defined that 'semantics and semantic interoperability' comprises 'linked (data) structures onto which data is mapped and then it is propagated across these structures to produce new data; the latter operation is called inferencing'.

The Standardization Committee SC42/WG3 on AI in the documents of ISO SC42/WG3 24029-2 and SC42/WG3 TR24029-1 does not explicitly address semantics even not in the realm of validation and verification of robustness of *Neural Networks (NN)*. However Formal Description Techniques (FDT) should help 'to determine strong (robustness) properties that are proven true on a whole domain of inputs to a NN and not just isolated ones' of ISO SC42/WG3 24029-2.

The essence is on proving properties with formal methods - which is also applied by the DKE/VDI DINCONNECT:2020 SemNorm Approach. In SemNorm the properties to be proven are directly represented by semantic Graph artifacts and indirectly by language term artifacts (e.g. such as *CSlang* of ETSI in GS ISI006). Here the formal method is the mathematics of many-sorted Algebraic Theories and because of mathematics it is designed to be computational. The textual language terms share the semantics of the given formal methods. Thus a language term may have the same semantical meaning as a programmed piece of behavior of a Digital Twin (Model) in the semantic domain.

4 Workshop Conclusions

More information about various technical aspects of I4.0/IACS industrial semantics have been presented in the submitted paper work to the workshop. The contained publication ‚Semantics for I4.0 Smart Manufacturing' gives a rough overview of standardization activities in the realms of I4.0 language design, declarative semantics and operational Digital Twin simulations.

The next 6th Workshop on IACS is to be announced for Berlin at GI INFORMATIK2021!