IFAC
INTERNATIONAL FEDERATION OF AUTOMATIC CONTROL
INCOM 2021 BUDAPEST
INCOM 2021
17th IFAC Symposium on
Information Control Problems in Manufacturing
7-9 June 2021, Budapest, Hungary

https://incom2021.org/
http://ifac.papercept.net/

Open Track Session on "Security of large-scale complex systems"
for 17th Symposium on Information Control Problems in Manufacturing

Track Chairs: **Dr. Vitaly Promyslov, Dr. Elena Jharko, Prof. Roman Meshcheryakov, Dr. Alexey Poletykin**
(*V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia; E-mail:* *v1925@mail.ru*)

Scope

The components of the modern world including enterprises, facilities tend to be more and more interconnected and form a large-scale complex system. Their control systems rely on a top of complex and distributed architecture, implementing multiple functions, and integrates numerous digital components throughout the facility. A more profound automation of large-scale systems has the potential to increase operation safety, to enhance production and to reduce development costs. Nevertheless, it also brings new cyber security threats inside the system.

Logically, the technical evolutions of control and safety systems and the rapid evolution of the threat landscape has turned cyber and information security into a high-priority issue for modern society. To face this challenge, innovation and research are needed: this session aims at contributing to this effort. It is open to both industrial and academic contributions in the area of cybersecurity of large scale and complex systems. High-quality scientific papers are expected, but industrial use- cases and application reports are also most welcome.

Abstract

The last decades, controls systems of many large and medium scale facilities and enterprises in industrial, energy, transport and public sectors reached a whole new level of development owing to the increased level of automation of the control with expanded functionality. This new level is a result of transferring from hard-wired, mostly analog control systems to the digital, highly interconnected distributed structure and accompanied the almost exponential growth in available computational performance. These features enable the realization of much more sophisticated algorithms for object control and in the processing of the sensor's data. The other immediate result of a digital revolution in control systems is extensive usage of artificial intelligence and big data analysis algorithms in the control process. That allows increased operation safety and to enhance output and performance in the target system.

The drawbacks of this are not only increasing complexity, maintenance cost, and production time for controls system but also the introduction of a new 'cybersecurity' type of threats for the system itself and object at the whole. Therefore, it is commonly accepted that insecure digital controls system may lead to catastrophic disruptions, disclosure of sensitive information, and frauds that might disrupt the operation and safety of the primary system. A clear view exists that security is a part of more general safety provision on the facility, and It is associated with the whole spectrum of the security domain, including informational and technological issues.

It was generally recognized that solution of the problem should be based on combination of many approaches found in different fields of fundamental and application sciences.

Then security problem of large scale complex systems shell be considered as a set of a few particular issues, such as:

- Security policy and security architecture design of the complex systems;
- Developing of new mathematical approaches for security modeling of hybrid and discrete event systems;
- Quality assurance and maintenance on system and components level.

The security policy forms the basis for the understanding of how various components involved in a security architecture relating to each other in a complex system. The security policies delimit expectations and system's requirements to handle the system's goals inside and beyond the system. The policies are built based on risk analysis that is recognized real for an organization operating the nuclear facility.

The establishing of the security goals is the main procedure in the process of developing a security policy. The security goals are forming in different layers of the system hierarchy: managers, operators, engineers for enterprises or smart devices in the internet of things. The goals are mixed and heterogeneous, and input data used in the process of goals identification may be weak and incomplete. That all makes the security goals identification process time consuming, challenging, and iterative. The goals undertenancy is manifested, for instance, in existence of mutual subordination (loops), incompleteness or internal contradictions or incompleteness in the security policy which was not verified during the manual assessment of the security policy.

Even the existence of the right security policies does not guarantee that its realization will maintain the security risk for large scale complex system an acceptable level due to uncertainty in input data or policy formulation.

Considerable complexity of the security policy large scale, involving a large number of assets and relationships between them may lead a dropping some aspects of the security policy in security architecture implementation or into security controls.

To face this challenge, innovation and research are needed: this session aims at contributing to this effort. It is open to both industrial and academic contributions in the area of security of large-scale control systems and their components. High-quality scientific papers are expected, but industrial use- cases and best practice application reports are also most welcome.

Topics

The list of topics includes, but is not limited to:

- Secure architecture design of large-scale complex systems
- Developing of new mathematical approaches to model of hybrid and discrete event systems
- Cybersecurity maintenance and patch management over time
- Risk assessment approaches adapted to the security context
- Quality assurance and maintenance on system and components level
- Cybersecurity exercises and contingency plans
- Intrusion-tolerant and resilient systems and architectures
- Coordination between functional and cybersecurity requirements or provisions
- Threat and attack modeling and security metrics
- Security assessment tools and methodologies
- Security Incidence response
- Forensics for industrial control systems
- Cryptography
- Authentication and Authorization
- Policy, regulations, normative frameworks
- Smart devices and internet of things security
- Security in industrial and infrastructure facilities (avia, nuclear and energy sector, transport)

Important dates and submission information

Important dates:

- Draft manuscript submission – November 13, 2020
- Late Breaking Results Submission Deadline – December 15, 2020
- Final paper submission deadline – February 1, 2021

For author guidelines, please refer to www.ifac-control.org . All papers must be submitted electronically at https://ifac.papercept.net/ . All papers must be prepared in a two-column format in accordance with the IFAC manuscript style. Please use the official IFAC instructions and template to prepare your contribution as full-length draft paper and submit it on line.

Submission details are available on the symposium website. All submissions must be written in English.

The corresponding author submits the paper online (pdf format) as Open Track Paper. Submission as an invited paper requires the use of Open Track code: **b5kv5**.

Proposal 30 submitted to 17th IFAC Symposium on Information Control Problems in Manufacturing. Received October 17, 2020.