Provable cyber security for industrial control systems

Tomas Kulik

Department of Engineering, Aarhus University, Denmark

Abstract. Industrial control systems are becoming more complex and interconnected. These systems are moving from *isolated, locally accessible* to *distributed and cloud connected* architectures. This paradigm shift brings challenges especially in the area of cyber security. Often the systems in question control vast amounts of physical devices or critical infrastructure, hence strong assurance of security is required. Formal verification can provide this assurance, but complexity of these systems requires finding the right compromises and correct tools for the task. This research project investigates usage of formal verification in the setting of cloud connected industrial control systems. The goal is to provide methods and frameworks adaptable for industrial use.

Keywords: Formal verification · Model checking · Cyber security · Control systems · VDM-SL

1 Introduction

Cloud technologies are revolutionizing computation [3]. The rise of scalable and cheap computing has changed the consumer sector, where companies outsource their computing infrastructure to cloud providers. The situation is different in the field of industrial control systems. While the benefits of migration of the control system to the cloud, such as readily available data analysis tools, scalable storage and cost savings are known, industrial entities are often skeptical of security and privacy of these systems [2]. This leads to retention of on premises data-centers, which are often not ready for inclusion of other new technologies such as Industrial Internet of Things (IIoT). One way of enabling the industrial entities to use the benefits of cloud computing is by providing strong assurances of cyber security. Formal methods are well suited to step into the area with several options such as theorem proving, model checking and formal validation. Currently the model checking and formal validation approaches are gaining acceptance in industry [8],[7] and hence this work is focused on them. In both cases a formal model of the system is created which is then verified against security properties of choice. The creation of formal model is an important step as the model must be close enough to the actual system to enable for meaningful early verification [9]. The modeling provides further benefits such as design space exploration, where different parts of the system could be given different behavior, where the analysis helps to determine the best choice for the actual system. In case of migrating an existing industrial control system to the cloud, the analysis can reveal weak points, hence both the choices of cloud provider and behavioral aspects of the system could be adapted to the security needs.

The cloud connected industrial control system consists of remote clients, used by users to login to the system, the cloud platform and the control part of the system often consisting of local terminal and the control network. A typical architecture is shown in Fig. 1. The architecture itself hints on possible attack vectors, which could be a remote client, the network connection, the cloud infrastructure, a local terminal or even the control network itself.

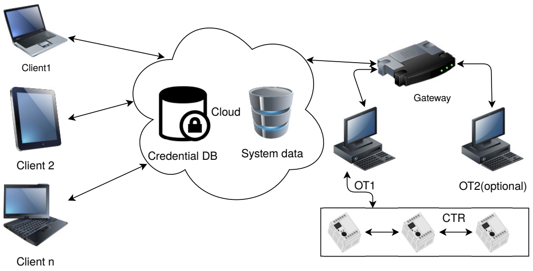

Fig. 1. Cloud connected industrial control system

Model checking is applicable to the system at a high level of abstraction, as it is prone to potential state space explosion, while partial model checking allows for increased level of detail [1]. Formal validation, such as combinatorial testing using VDM enables high detail of the model, however is not exhaustive. In order for further acceptance of this approach the security properties need to be based on well know mitigations to security attacks or cyber security standards. This research project considers this and uses the IEC-62443 cyber security standard as a basis for the cyber security properties. The research is carried out in close cooperation with an industrial partner in a form of extensive case studies and has lead to several publications, described in more detail below.

2 Methodology

This section presents the methodology being used within the research project. In order to formalize the architecture provided by the industrial partner, different cyber attacks and mitigations to these attacks, the project started with modeling and verifying the control network. Next, the aspects of cyber security standard has been added as mitigations and the operations terminal has been introduced. The verification has been carried out using the Alloy Analyzer. The research then progressed into including the cloud platform and the remote clients and formally defining the behavior of these components. Later this has been again extended to include different aspects of the cyber security standard. In the last two cases the formal verification has been carried out by means of model checking using TLC model checker as it provided improved scalability over Alloy. Currently the work focuses on introducing more detail and notion of time, including the real-time aspects of control into the system behavior by usage of technologies as VDM-SL and partial model checking using UPPAAL.

In order to be able to switch verification technologies and modeling frameworks, the behavior is formally defined using Labeled Transition System (LTS) and the properties are defined using Linear Temporal Logic (LTL) and Computational Tree Logic (CTL). From the perspective of the industrial partner this approach also enables them to understand the way the behavior is formalized without setting up a specific toolkit.

3 Status

The research project has so far generated results primarily in terms of formalization of industrial control systems and cyber security standards. The first publication [4] has demonstrated formalization of a distributed control network with focus on several cyber attacks. The main contribution of the work was to create a formal framework defining atomic actions that can form interaction patterns, based on which a formal model of an IIoT based control network could be created. Within this work we have carried our formal analysis of a control network against several security properties. We have increased the amount of control units until we have reached the practicality limit of the verification. Using Alloy analyzer we verified control networks with up to 100 control units.

The second publication [5] has been an extension of the formal framework that allowed for verification of the control network including a local terminal against security properties formalized from the industrial automation cyber security standard. Here we have demonstrated formalization aspect of natural language based cyber security standards. The analysis have been carried out using Alloy analyzer, demonstrating effectiveness of formally defined mitigations against considered cyber attacks.

In the third publication [6] we have included the cloud connectivity and remote clients interaction to the model of the system. The client interactions include authentication, remote firmware updates and data review. Further we have formally specified cyber attacks aimed at the cloud connected parts of the system and mitigations to these. The control network has been abstracted away as it has been verified in previous analyses. The formal specification has been carried out in modular way building on top of techniques from our previous work. The verification of security properties has been carried out on TLA+ model using the TLC model checker, where the verification has been shown to be feasible with verification times less than five minutes.

The fourth publication, accepted for presentation has extended the TLA+ model with cyber attack mitigations based on the cyber security standard. This work has demonstrated the possibility of analyzing a complex control system against cyber security standard in early stages of the system development.

4 Conclusion and Future Work

The primary contribution of the research so far has been creation of a formal framework for formalization of industrial control systems behavior in an IIoT setting and demonstration of feasibility of formal verification of security properties of complex cloud connected industrial control systems. Further contribution is the demonstration of formalization of natural language based cyber security standards and their role in formal security verification.

We expect to deliver further contributions, specifically by demonstrating formal analysis of complex industrial control systems using partial model checking with high level of detail, demonstrating uses of combinatorial testing in VDM as a viable alternative to model checking. Furthermore, we expect to demonstrate a model-in-the-loop approach, where machine learning anomaly detection sends potentially malicious traces to the formal model for formal analysis.

Acknowledgments This work is supported by Manufacturing Academy of Denmark (MADE).

References

1. Andersen, H.R.: Partial model checking. In: Proceedings of Tenth Annual IEEE Symposium on Logic in Computer Science. pp. 398–407 (1995). https://doi.org/10.1109/LICS.1995.523274
2. Baker, T., Mackay, M., Shaheed, A., Aldawsari, B.: Security-Oriented Cloud Platform for SOA-Based SCADA. In: 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. pp. 961–970 (May 2015)
3. Buyya, R.: Cloud computing: The next revolution in information technology. In: 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010). pp. 2–3 (Oct 2010). https://doi.org/10.1109/PDGC.2010.5679963
4. Kulik, T., Tran-Jørgensen, P.W.V., Boudjadar, J., Schultz, C.: A Framework for Threat-Driven Cyber Security Verification of IoT Systems. In: 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW). pp. 89–97 (Apr 2018). https://doi.org/10.1109/ICSTW.2018.00033
5. Kulik, T., Larsen, P.: Towards formal verification of cyber security standards. vol. 30, pp. 79–94. Institute for System Programming, Russian Academy of Sciences (ISPRAS) (2018). https://doi.org/10.15514/ISPRAS-2018-30(4)-5
6. Kulik, T., Tran-Jørgensen, P.W., Boudjadar, J.: Formal Security Analysis of Cloud-Connected Industrial Control Systems. In: International Conference on Security for Information Technology and Communications. pp. 71–84. Springer (2018)
7. Larsen, P.G., Fitzgerald, J.: Recent industrial applications of VDM in japan. In: Proceedings of the 2007th Internatioanal Conference on Formal Methods in Industry. pp. 8–8. FACS-FMI'07, BCS Learning & Development Ltd., Swindon, UK (2007)
8. Newcombe, C.: Why amazon chose TLA + . In: Ait Ameur, Y., Schewe, K.D. (eds.) Abstract State Machines, Alloy, B, TLA, VDM, and Z. pp. 25–39. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
9. Pedroza, G., Apvrille, L., Knorreck, D.: Avatar: A SysML environment for the formal verification of safety and security properties. In: 2011 11th Annual International Conference on New Technologies of Distributed Systems. pp. 1–10 (May 2011)