On Reliability and Resilience of Power Systems Automation using Stochastic Timed Automata

Kai Heussen, Hugo A. López and Hanmin Cai

***Abstract*—Automation standards such as IEC61499 support the specification of distributed event-based functions that can be applied to for example voltage control applications. Such distributed automation systems can contribute to improved power quality and reduced outages by being partially reliant on communication. Such resilience oriented automation concepts account for and accommodate partial system failures, e.g. by defining operation modes at a reduced service level. The reliability performance assessment of such extended control strategies requires a detailed modeling of their internal logic and dependence on communication. In this work we outline an approach to the development and assessment of such distributed automation functions based on networks of timed automata and their extension as networks of stochastic timed automata. Reliability and resilience properties are formalized in terms of logical formulae whose satisfaction can be evaluated by contemporary assessment methods.**

***Keywords*—Timed automata, communication, cyber-physical systems, control, reliability, resilience**

I. Motivation

Power systems and automation is increasingly perceived as a cyber-physical system, where physical operating constraints have to be complemented with constraints representing both the communication and the computation infrastructures. Analysis of cyber-aspects in power systems is conventionally not addressed directly due to engineering reliance on decentralized control and modeling of operating modes on the basis of local control objectives. The activation of distributed resources for power system management and control makes power system operation increasingly reliant on higher number of individually less reliable communicating devices. Due to the relatively small impact of individual component failures, appraisal of overall reliability performance is difficult to achieve. Alternative formulations to the conventional reliability assessment based on $(N-1)$-security are being formulated [1], but also entail computational challenges. Alternative approaches are required to scale up these assessment methods, and that can account for discrete behaviour and logic of the combined cyber- and physical system. The systematic appraisal of reliability performance is also required for distributed control applications which are dependent on communication. Here two basic challenges await: the validation of functionally correct distributed control applications as well as the appraisal of achieved reliability performance [2]. Timed automata have long been established in the design and assessment of automation components but are not yet commonly applied in power systems. Distributed control applications can be formulated using IEC61499 standard which defines event-based aspects of function blocks as automata, such that IEC61499 applications and can be interpreted as networks of timed automata.

An often cited issue with product automata is that of state explosion, which has previously been addressed by the use of petri nets [3]. However, there are drawbacks to petri nets, such as the need to design them as a global model, independently from available implementations or specifications of component behaviours. Recent developments in the field of stochastic model checking based on automata mitigate such challenges [2], and related methods promise alleviation of some fundamental limitations [4].

The assessment itself is faciliated by logical formulae in e.g. Linear temporal logic (LTL). To apply the rich toolsets to power systems automation assessments, two main developments are required: firstly, the practice of defining automation solutions as networks of timed automata; secondly, a set of standard logical query formulations that address the typical power systems requirements and reliability performance criteria.

II. Approach and Expected Results

This paper will outline the principles of engineering first for functional correctness then for reliability. The approach will be described on two case studies (one illustrative on frequency control, the other on coordinated demand response [5]). The approach comprises the following steps: *1.* develop jointly discrete system model and basic controller; *2.* validate requirements (formulated as logical queries on the formal (non-stochastic) automata network); *3.* add fault events and states: a. validate fault behaviour b. extend to stochastic automata to evaluate reliability performance; *4.* develop fault awareness extensions of controller behaviour; *5.* evaluate final response behaviour as stochastic automaton.

A core contribution will be the formulation of query types that correspond to classical power systems reliability, security, resilience assessment criteria. Following a concise definition, each of these terms are formulated as a formal logical query logical on the respective model.

References

[1] E. Karangelos and L. Wehenkel, “Probabilistic reliability management approach and criteria for power system real-time operation,” in *Power Systems Computation Conference (PSCC), 2016.* IEEE, 2016, pp. 1–9.

[2] C. Baier, B. Haverkort, H. Hermanns, and J. Katoen, “Performance evaluation and model checking join forces,” vol. 53, no. 9, pp. 76–85, 9 2010, 10.1145/1810891.1810912.

[3] Z. Lin, F. Wen, C. Y. Chung, and K. P. Wong, “A survey on the applications of petri net theory in power systems,” in *2006 IEEE Power Engineering Society General Meeting*, 2006, pp. 7 pp.–.

[4] H. A. Lopez and K. Heussen, *Choreographing Cyber-Physical Distributed Control Systems for the Energy Sector.* Association for Computing Machinery, 2017.

[5] H. Cai, S. You, H. W. Bindner, and S. Klyapovskiy, “Load Situation Awareness Design for Integration in Multi-Energy System,” in *2017 IEEE International Conference on Energy Internet (ICEI)*, 2017, pp. 42–47. [Online]. Available: http://ieeexplore.ieee.org/document/7926847/