On the Applicability of State Machine Replication for Dependability in Smart Grids

Armin Stocker*
stockera@fim.uni-passau.de
University of Passau
Passau, Germany

Hermann de Meer
demeer@uni-passau.de
University of Passau
Passau, Germany

Franz J. Hauck*
franz.hauck@uni-ulm.de
Ulm University
Ulm, Germany

ABSTRACT

The frequency of a power system is a critical parameter to maintain for power system stability. Any imbalance between generated and consumed power leads to fluctuations in frequency. These imbalances must be compensated for immediately. Compensation of power imbalances requires sufficient backup reserves. These reserves used for the stability of the power system are called ancillary services.

In traditional power systems, ancillary services are concentrated at relatively few, large synchronous generators in the transmission network. Because they are often based on fossil fuels or nuclear power, these synchronous generators are phased out in favour of renewable energy resources, such as solar panels and batteries, located in distribution networks. This change implies that the provision of ancillary services must also be decentralized. At the same time, the complexity of the power system has increased due to a large number of controllable components.

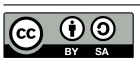
Decentralization and increasing system complexity lead to bottom-up aggregation approaches, such as energy cells. In this research, energy cells refer to a delimited grid area that operates autonomously while remaining connected to the power grid at large. Thus, an energy cell as an aggregate can still exchange power with the grid. Based on this concept of an energy cell, this research investigates the provision of dependable ancillary services. Automatic frequency restoration reserves (aFRR) are chosen as an exemplary service, as they require accurate coordination of the energy cell with the transmission system in close to real-time.

The control of the energy cell must be fault-tolerant with respect to ICT faults affecting the communication within the cell, ICT faults affecting the control centre and ICT and power system hardware faults affecting the distributed energy resources in the energy cell. We assume that the ICT faults affecting the communication and the ICT and power system hardware faults affecting the distributed energy resources can be handled by the control of the energy cell, we focus specifically on ICT faults that can affect the control of the aggregate cell as a potential single point of failure. State-machine replication (SMR) is applied to provide guaranteed continued operation despite faulty replicas, assuming not only crash but also Byzantine faults.

Yet, when deploying the energy cell control software with state-machine replication three challenges arise that were not yet adequately addressed in previous research: First, sending of monitored status information from the cell to the control, sending of targets for automatic frequency restoration reserve from the transmission system operator to the control, and the sending of decision points to the cell components must be integrated into the state-machine replication system model. Second, the resulting requests have to be scheduled as concurrently as possible to ensure fast reaction speeds, which requires deterministic multithreading. As part of this, requests must be coordinated, e.g., request executions for new set points need to wait until a decision is computed. This requires deterministic coordination primitives, such as *wait* and *signal*. Third, the used decision algorithm is based on a meta-heuristic that enables fast execution, which requires good random numbers, and only recent messages must be processed, which requires real-time time stamps. These random numbers and time stamps must be computed in a deterministic way.

All challenges are solved by using BFT-SMaRt with an integrated UDS deterministic scheduler and a Byzantine fault-tolerant mechanism to deterministically create secure random numbers and real-time time stamps. For the replicated control software, the impact on runtime and accuracy is investigated. A scenario with a faulty leader node is simulated to estimate worst-case performance. In summary, the results show that state-machine replication contributes to an increase in latency for control in the energy cell during normal operation. In case of a leader fault, the operation of the replicated state machine stalls for a few seconds until a new leader is elected. The deviation from the target are found to be only slightly outside of the tolerance bands for these few seconds and the control recovers to within the band quickly once a new leader is elected. Thus, the results

*Both authors contributed equally to this research.



confirm that state-machine replication is suitable for this use case and can effectively reduce costs for ICT faults affecting the cell control. Further, it is very likely that certain implementation aspects can be further optimised as this paper reports preliminary results.

CCS CONCEPTS

• **Hardware → Smart grid**; • **Computer systems organization → Dependable and fault-tolerant systems and networks**; • **Software and its engineering → Scheduling**.

KEYWORDS

Ancillary Services, State Machine Replication, Dependability, Energy Cells, Smart Grids

ACKNOWLEDGMENTS

The work that lead to this research was funded in part by the FFG (Austrian Research Promotion Agency) and the BMIMI (Austrian Federal Ministry of Innovation, Mobility and Infrastructure) as part of the cells4energy project (project number: FO999904664; www.ffg.at)