Poster: Communication Failover Strategies for Dependable Smart Grid Operation

Elisei Ember[1], Konrad Diwold[1,2], Kay Römer[2], Carlo Alberto Boano[2], Markus Schuß[2], Albin Frischenschlager[3], and Alfred Einfalt[3]

[1]Pro2Future GmbH, Graz, Austria {firstname.lastname}@pro2future.at

[2]Institute of Technical Informatics, Graz University of Technology, Austria, {markus.schuss, roemer, cboano}@tugraz.at

[3]Siemens AG Österreich, Austria, {firstname.lastname}@siemens.com

Abstract

This poster presents a concept for multi-radio fail-over strategies to achieve dependable communications in decentralized smart grid operation. By assessing currently-available link qualities (across multiple radios) and by adjusting the used communication channels and payloads size accordingly, robust and dependable communications and operations can be achieved. The concept was realized in a demonstrator and first evaluation results are presented.

1 Introduction

Due to the ongoing integration of distributed energy resources (e.g., domestic photovoltaic systems), energy is now actively produced in low-voltage grids, which were originally designed for distribution only and are therefore mostly uncontrolled [6]. Providing automation technology is challenging due to the large amount of low-voltage grids, which will require active monitoring/control schemes, and the current lack of automation and communication infrastructure within them. In response to this challenge, research on smart grid technologies has increased [3]. While local grid control strategies, that do not require any form of communication between grid automation and operator, exist [5], the implementation of higher-level ancillary and monitoring services [2] requires continuous and dependable communication between a field device and the operator.

Wireless connectivity will play a key role in future smart grid solutions. Its suitability, however, depends heavily on the exact deployment location and is often subject to external influences [1]. As monitoring and control mechanisms are implemented independently of the exact communication arrangement, multilayered communication schemes must be provided to enable fail-over mechanisms and ensure continuous availability of these critical services.

This poster presents a communication fail-over concept for smart grid automation, which aims to provide continuous communication and adaptive fail-over mechanisms for dependable communications between device and back-end.

2 System Design

An overall system architecture and the resulting prototype are presented in Fig. 1. The system consists of two main components: the back-end of a distribution system operator and a field device. The application of a field device can be manifold: it could monitor grid parameters (e.g., voltage or frequency) and provide this information in real-time to the operator. Additionally, it could be used to locally implement control commands provided by the system operator during operation. For decentralized monitoring/control schemes, connectivity is crucial: to ensure a stable connectivity, the field device provides several independent communication interfaces. These interfaces are abstracted be-

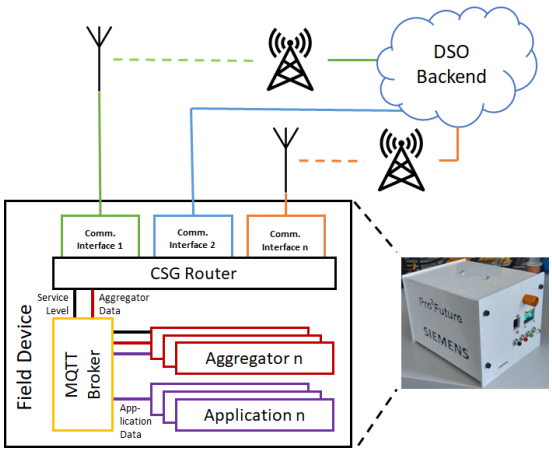

Figure 1. Sketch of prototypical system architecture, field device-middleware and resulting prototype

hind a routing application called `CSG router`. In addition to realize the communication between field device and back-end, `CSG router` continuously monitors communication metrics (such as connection state and signal strength) for each independently-available communication interface. These metrics are used to calculate interface-dependent service levels, which are continuously used to evaluate the current communication quality and switch between communication interfaces, if necessary. Depending on the interface in use, information sent from and to the field device is adapted, as different communication interfaces (e.g., NB-IoT vs. LTE) differ significantly in their throughput and priority must be given to operation-critical information. As field device applications are agnostic to the current connectivity to the back-end, an MQTT-based device-middleware is used to realize a communication-dependent payload adaption and route information from the applications (via `CSG router`) to the operator. The structure of the device-middleware is outlined in Fig. 1: outgoing application data is routed from an application to `CSG router` via so-called `Aggregator` instances. These instances are application-dependent and receive full data streams from their respective applications. In addition, they receive prevailing service level from `CSG router`, which is used by an `Aggregator` to adjust outgoing application information. How information is adjusted in case of limited connectivity is dependent on the application, as different applications might require different forms of aggregation. Therefore, `Aggregators` are designed as freely programmable `python` scripts, which can be realized independently as part of an application's configuration.

3 Initial prototype validation

To test the proposed concept, a prototypical field device was developed (see Fig. 1 bottom right). The initial prototype hosts one wired (Ethernet) and two wireless interfaces (LTE, and NB-IoT). NB-IoT was chosen as it provides connectivity even in deep indoor application scenarios [4]. `CSG router` calculates a service level in the range 0-100 for each available interface, with 0 corresponding to best service level. For each technology T, the service level is calculated as $S_T = min\{(O_T + SS_T), 100\}$, with O_T denoting a technology offset ($O_{LAN} = 0$, $O_{LTE} = 10$ and $O_{NB-IoT} = 60$; which were chosen to reflect the available data-throughput of the interfaces) and SS_T denotes the received signal strength at a respective interface[1]. The interface providing the best service level is selected by `CSG-Router` for communication and the resulting system service level S is continuously provided to the `Aggregator` instances.

For a first assessment, applications in the prototype produce a sine with a rate of 0.1 Hz and a resolution of 100. Given a service level of $S = 0$, all data will be forwarded to the back-end; for service levels between 1 and 90, data will be compressed by the `Aggregator` with a sample size of $S/5$; given a service level of 90+, only peak values are sent (which could correspond, for example, to the transmission of alarms in a real-world application).

[1]Note: as no signal strength value can be measured at the Ethernet interface, it will always have a service level of 0, if a connection to the back-end is present. For other interfaces, the signal strength is based on the perceived signal quality and normalized across technologies.

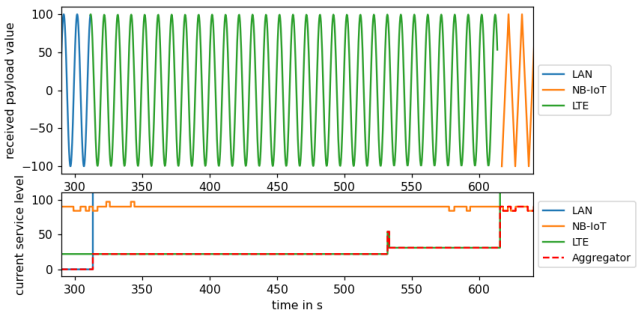

Figure 2. Test of fail-over capability. Payload received at backend (top) - service levels at device (bottom).

Fig. 2 outlines a first system verification using a test lasting 640 seconds. The service levels of the interfaces were manually altered after 310 seconds (by disabling Ethernet) and 620 seconds (by damping the LTE radio). The system adjusts to changing service levels by (i) switching between different radios and (ii) adjusting the transmitted payload. When the Ethernet connection is lost, the system will switch to the LTE interface, which results in a loss of connectivity for around 4 seconds (i.e., the time required until connectivity loss manifests itself and a switch to the next interface is completed). In the case of damping the LTE signal, the interface switches towards NB-IoT and an adaptation (i.e., transmission of peak values only) is realized instantly.

4 Conclusion

This poster outlined an initial fail-over concept for smart grid communication. To apply the concept, a correct assessment of communication service levels is crucial. Within this work received signal strength was used to calculate the service levels of the available interfaces. Current experiments aim to establish detailed connection qualities based on available radio metrics across different wireless communication technologies to provide better service level estimations and robust fail-over via dedicated routing applications.

Acknowledgements

The authors gratefully acknowledge the support of the Austrian Research Promotion Agency (FFG) (#6112792).

5 References

[1] M. Cattani, C. A. Boano, and K. Römer. An Experimental Evaluation of the Reliability of LoRa Long-Range Low-Power Wireless Communication. *Journal of Sensor and Actuator Networks*, 6(2):7, 2017.

[2] M. Faschang, S. Cejka, M. Stefan, A. Frischenschlager, A. Einfalt, K. Diwold, F. P. Andrén, T. Strasser, and F. Kupzog. Provisioning, Deployment, and Operation of Smart Grid Applications on Substation Level. *Computer Science-Research and Development*, 32(1-2), 2017.

[3] M. Hossain, N. Madlool, N. Rahim, J. Selvaraj, A. Pandey, and A. F. Khan. Role of Smart Grid in Renewable Energy: An Overview. *Renewable and Sustainable Energy Reviews*, 60:1168–1184, 2016.

[4] I. Z. Kovács, P. Mogensen, M. Lauridsen, T. Jacobsen, K. Bakowski, P. Larsen, N. Mangalvedhe, and R. Ratasuk. LTE IoT Link Budget and Coverage Performance in Practical Deployments. pages 1–6, 2017.

[5] A. Singhal, V. Ajjarapu, J. Fuller, and J. Hansen. Real-Time Local Volt/Var Control under External Disturbances with High PV Penetration. *IEEE Transactions on Smart Grid*, 10(4):3849–3859, 2018.

[6] J. Von Appen, M. Braun, T. Stetz, K. Diwold, and D. Geibel. Time in the Sun: The Challenge of High PV Penetration in the German Electric Grid. *IEEE Power and Energy magazine*, 11(2):55–64, 2013.