Open Source Software for the Smartgrid: Challenges for Software Safety and Evolution

Tosin Daniel Oyetoyan, Reidar Conradi, Daniela Soares Cruzes
Department of Computer and Information Science, NTNU, Trondheim, Norway.

Abstract

The growing Smartgrid behind today's electricity supply introduces many challenges. One aspect is the management of various software that drive these new systems at different domains (generation, transmission, distribution and consumption) and nodes of the Smartgrid network. Managing such concerted, distributed, evolving and heterogenous System of Systems requires a methodical approach to support more standardized processes and products to reach the Smartgrid vision. This paper presents a recent research project focusing on assessing the adoption of OSS for the Smartgrid by investigating its safety and evolution criteria.

1. Introduction

This work introduces current research in the field of software management for Smartgrid applications [1]. It is based on literature reviews and initial formulation of requirements for both the Smartgrid and its software, and case studies that will be established with industrial partners.

The emerging Smartgrid has introduced new challenges for the management of software across different electricity domains and organizational boundaries. The Smartgrid is made up of loosely coupled system of systems [2]. This means that many systems and software with various ownership and management boundaries are interconnected to provide end-to-end services among stakeholders, as well as among intelligent devices [2].

Maier [4] stated five key traits of a System of Systems (SoS) to be; operational independence of the elements, managerial independence of the elements, evolutionary development, emergent behaviour and geographical distribution. The Smartgrid is a relatively new concept and emerging with sparse existing literatures. Some of the characteristics of Smartgrid as SoS (see Figure 1) have been discussed in [2, 5].

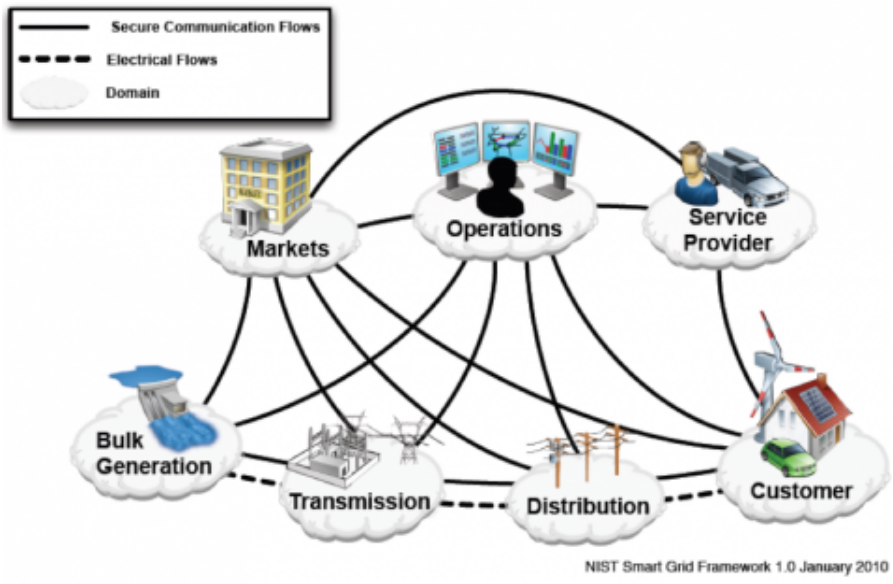

Figure 1 Smartgrid as SoS [2].

This paper was presented at the NIK 2011 conference. For more information see http://www.nik.no/

We will focus on software evolution and safety criteria in Smartgrid applications. How should the Smartgrid software be designed to make the Smartgrid safe and resilient to failure, as well as allowing better management of its software evolution? Assuming that we have an operational Smartgrid as a System of Systems, this means that the internal state of a distributed Smartgrid "node" (its code, code activation pointers and data) may not be fully visible or controllable from the outside. How can we then enforce a "safe" behaviour, like avoiding blackouts? That is, how can we ascertain that the local nodes (with all their collaborative and decision-making incompleteness, defects, version skews, etc.) will manage to offer a concerted and safe state at most times?

This paper further discusses some challenges with the management of the Smartgrid software in section 2 and also introduced related questions with the adoption of Open Source Software (OSS) approach for Smartgrid applications in section 3. The conclusion of this position paper is given in section 4.

2. Open Challenges with the Management of Software in Smartgrid

There are many open challenges around software management in Smartgrid and which need a proactive and pragmatic research approach [2]:

i. The Smartgrid is an evolution of the traditional electricity grid. In other words, the traditional electricity supply will be modernized through re-engineering, adaptation, modification and updates.
ii. The Smartgrid is a web of heterogeneous systems and networks with diverse software running at the different domains.
iii. The Smartgrid introduces a distributed approach to electricity generation and supply in contrast to a more centralized approach in the existing grid. The injection of "green" sources (wind, solar, etc.) of energy to the grid, both from bulk generation centres and households, is a main feature in today's Smartgrid.
iv. The Smartgrid will feature various software, stakeholders, owners, management boundaries, governmental boundaries and regulators.
v. The Smartgrid market will introduce a new dynamic in terms of buying, selling and distribution of electricity.
vi. Cyber security is significant to the Smartgrid. The Smartgrid is envisioned to come with high robustness and safety.

In view of the aforementioned Smartgrid features, we summarize some of the software management implications of the Smartgrid features in Table 1.

Table 1 – Smartgrid features and challenges for Software management.

Smartgrid features	**Challenges for Software Management**
Distributed systems	Software configuration management issues with coordination, change control, negotiation etc.
Evolution from traditional grid	Integration challenges with legacy systems.
Heterogeneous system (s)	Interoperability challenges, open architectures, open standards.
Interdependence and interconnections	Interoperability, network-system reliability.
Multiple stakeholders and owners	Multiple sources of unpredictable changes that can affect system quality, governance and ecosystems.
Cyber-based systems	Security challenges, life-critical system design and development approaches.

3. OSS for Smartgrid applications – Implications for Research

A high level of complexity is obvious in managing the various software, owners, management boundaries, governmental boundaries and regulators involved in the Smartgrid. Today, consensus favours Smartgrid initiatives at strategic levels that can accommodate the coexistence of and evolvement through several generations of IT standards and technologies (models, software and devices) [2, 3]. A possible approach is thus to investigate the adoption of OSS in the Smartgrid SoS products.

A SoS typically have different sources of risks and challenges that are related to software safety and evolution as discussed in [7]. Some of these risks are:

1. Potential for change in the system(s) from any direction (that is, from stakeholders or constituent system as well as from evolving business requirements).
2. Less predictability regarding stakeholders needs, technology advances and component behaviour that is typical in an environment with no central control.
3. Failures with causes or impact beyond the individual system boundary.
4. Constrains in terms of new development and evolution because of existing collection of design choices.
5. Limited knowledge of individual system state and behaviour

Cowling and Cloutier [8] showed how SoS and OSS share certain similarities along OSS features of communities, governance and development in relation to SoS characteristics discussed in Maier [4]. This comparison is useful background to study OSS in a Smartgrid SoS environment. Sharma et.al [6] also, described a framework for creating a hybrid-OSS community that can be leveraged for managing OSS Smartgrid artefacts involving heterogeneous stakeholders and communities with different development practices. Thus, we propose some relevant **research questions** for OSS in Smartgrid SoS products as follows:

1. What are the risks and challenges of an OSS approach to the Smartgrid and how can they be mitigated?
2. How are OSS-Smartgrid communities created?
    a. That is, what are the different ecosystems involved (software vendors, integrators, hardware vendors etc.)
    b. How are business models pursued to satisfy all or some of the different stakeholders' interests?
    c. What are the practical challenges of such heterogeneous community?
3. How can the evolution of an OSS artefact in Smartgrid products be controlled to have consistent and safe states? (See Figure 2)
    a. How to develop configuration management policies in a distributed and heterogeneous stakeholders community?
    b. How can the existing process models be improved for safe and consistent states in the Smartgrid?

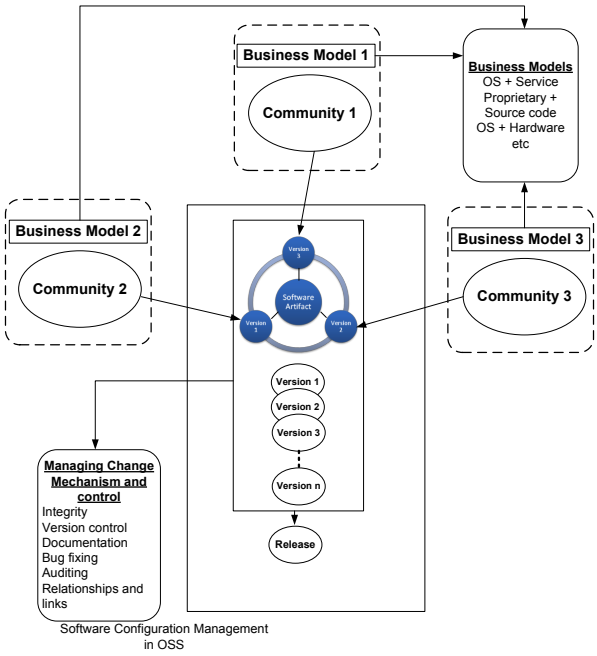

Figure 2 Software Configuration Management for OSS in Smartgrid applications.

4. Conclusion and future work

This position paper has proposed a collaborative OSS approach to manage and evolve the Smartgrid products. We have highlighted the software management challenges dictated by the Smartgrid`s inherent features as a SoS. Our future work will involve empirical studies of industrial OSS in Smartgrid products in collaboration with Norwegian energy companies with the aim to explore and explain some of the mentioned research questions. These studies will typically include literature reviews, interviews, surveys and industrial case-studies.

References

[1] IME, NTNU. *"F: Improved Management of Software Evolution for Smartgrid Applications."* http://ime.ntnu.edu/research/Smartgrid/f (accessed January 10, 2011).

[2] NIST. *"NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0"*, NIST Special Publication 1108. January, 2010.

[3] DAF, *"Electricity: Renewables And Smart Grids"*, Directorate For Financial And Enterprise Affairs Competition Committee, Norway. January. 2010.

[4] Maier, M.W., *"Architecting Principles for System of System"* Systems Engineering, Vol. 1, No. 4, pp. 267-284. 1998.

[5] K. Mani Chandy, Jeff Gooding and Jeremy McDonald. *"Smart Grid System-of-Systems Architectures"* http://www.gridwiseac.org/ (accessed July 5, 2011).

[6] Srinarayan Sharma, Vijayan Sugumaran and Balaji Rajagopalan. *"A framework for creating hybrid-open source software communities"* Blackwell Science Ltd, Information Systems Journal 12, 7-25. 2002.

[7] Rita Creel and Bob Ellison. *"System-of-Systems Influences on Acquisition Strategy Development."* Carnegie Mellon University. 2008.

[8] James Cowling and Robert Clouting. *"A System of System perspective on Open Source Software Projects"* 7th Annual Conference on Systems Engineering Research 2009 (CSER 2009).