Organizational Control Reconfigurations for a Robust Smart Power Grid

Evangelos Pournaras, Mark Yao, Ron Ambrosio, Martijn Warnier

Abstract Large-scale cyber-physical infrastructures, such as the Smart Power Grid, are envisioned as some of the core elements of the future Internet of Things. These critical infrastructures move more and more beyond centralized management and control by system operators and administrators. Overloading and failures in the Smart Power Grid threaten the matching of demand-supply especially when new emerging technologies are integrated such as micro-generation, renewable energy resources and electrical vehicles. The integration of these technologies in the Smart Power Grid make the concept of Internet of Things highly applicable in the energy domain. The introduction of automated and decentralized protection mechanisms requires embedded control elements that perform organizational reconfigurations themselves in a spatially distributed environment. The dynamic input and output binding between such control elements is an example of an organization reconfiguration that is traditionally managed offline during the design phase of a cyber-physical system. An introduced computational intelligence for the purpose of such organizational control reconfigurations requires the interoperation with the rest of the control logic during runtime. This book chapter illustrates a model that makes this interoperation possible: ALSOS-ICS, the Application-level Self-Organization Services for Internet-scale Control Systems. Four incremental protection levels for the robustness of the Smart Power Grid illustrate the requirements of organizational control reconfigurations and the applicability of ALSOS-ICS in this domain.

Evangelos Pournaras, Martijn Warnier
Delft University of Technology, Section Systems Engineering
e-mail: {e.pournaras,m.e.warnier}@tudelft.nl
Mark Yao, Ron Ambrosio
IBM Thomas J. Watson Research Center
e-mail: {markyao,rfa}@us.ibm.com

1 Introduction

Cyber-physical systems within the Internet of Things are built by physical and software elements of embedded control whose organization has traditionally been an offline design aspect. Input and output (I/O) of control elements are bound manually to form the control loops of a control application [27]. This is a design phase that is usually not automated and occurs before system runtime [9]. However, the Internet of Things require online and automated organizational control reconfigurations as cyber-physical systems scale and their elements become more interconnected, distributed and interactive. Reconfigurations become an integral part of the computational intelligence that control elements should have. In this case, organizational control means that the feedback control loops formed by the I/O binding of the control elements are organized within a large-scale networked and distributed environment of Internet of Things. Network abstraction, fault-tolerance, latency, limited connectivity and shared resources are some of the challenges that need to be addressed [24]. Introducing and modeling dynamic reconfigurations of the organizational control in an Internet-scale control system is challenging. This is because the physical assets of a cyber-physical system interoperate based on I/O signals and feedback loops, whereas, distributed software elements are usually event-based, information-driven and are built by multiple layers of network abstraction. This modeling gap introduces various integration and interoperation issues that are identified in literature [15, 24]. Cyber-physical systems without organizational control reconfigurations cannot support the emergent application requirements of Internet of Things. Therefore, the modeling of organizational control reconfigurations is relevant and connects both of these related research areas [22]. This book chapter illustrates a modeling approach of organizational control reconfigurations in the application domain of the Smart Power Grid. This is a critical application domain for the Internet of Things as a large number of physical and software assets of the traditional electrical grid become more interconnected, intelligent and self-aware of socio-technical factors that mandate their design and operation [20].

The protection of the Smart Power Grid from overloading or failures is a critical requirement that involves various organizational control reconfigurations such as adjusting the load of a power line, switching the power flow to alternative distribution lines, turning on backup generators and restoring the system after a black-out. Traditionally, these reconfigurations are coordinated manually by experienced systems operators supported by usually centralized data acquisition information systems [12]. This approach is limited and cannot remain as a long-term solution in the future Smart Power Grid. The introduction of micro-generation, renewable energy resources and electrical vehicles are some examples that indicate the future challenge and complexity of matching demand and supply within a robust and dynamic Smart Power Grid. Therefore organizational control reconfigurations in an environment of Internet of Things need to be dynamic, automated and coordinated by the computational intelligence of control elements able to interoperate for this purpose.

The first contribution of this book chapter is to illustrate how the interoperation of the organizational control reconfigurations with the rest of the control application

logic, e.g. the protection of the Smart Power Grid, is made possible by modeling the dynamic I/O binding of control elements as a control system within the Internet of Things. This means that a number of software embedded control elements, running as a control application, dynamically configure the I/O binding of a second control application that requires this dynamic I/O binding.

The second contribution of this book chapter is the illustration of four incremental protection levels for the robustness of the Smart Power Grid. These protection levels are actual application scenarios of organizational control configurations concerning the Internet of Things in the domain of the Smart Power Grid. The application scenarios show why control elements need to dynamically bind with each other on-the-fly and which protection measures these reconfigurations support. Within the domain of the Smart Power Grid, dynamic I/O binding is not introduced as an alternative protection mechanism such as the ones of [8], but as the means to make these mechanisms more applicable within dynamic environments of the Internet of Things.

This book chapter is organized as follows: Section 2 illustrates the model for organizational control reconfigurations: ALSOS-ICS, the Application-level Self-Organization Services for Internet-scale Control Systems. Section 3 outlines four incremental application scenarios for the robustness of the Smart Power Grid that require dynamic organizational control reconfigurations. Section 4 discusses the approach of ALSOS-ICS in the application domain of the Smart Power Grid and in the more general development life-cycle of distributed embedded control systems. Finally, Section 5 concludes this chapter and outlines future work.

2 Dynamic I/O Binding Reconfigurations

Two control elements are bound if there is at least one output from the first control element wired to the input of a second control element. A binding reconfiguration is defined by the rewiring of the input/output of a control element to a different output/input respectively of the same or of another control element. A dynamic binding reconfiguration means that this rewiring is automated during system operation (online) with a minimum or absent centralized intervention. Dynamic I/O binding reconfiguration requires system elements that should be capable to perform these reconfigurations and should be able to interoperate with the rest of system control logic. Existing solutions provide an offline [9], external [33] and/or centralized [10, 14, 23] configuration of I/O bindings.

Our earlier work [29] introduces a model for application-level reconfiguration of dynamic I/O binding in Internet-scale control systems that is referred to in this chapter as ALSOS-ICS, the *Application-Level Self-Organization Services in Internet-scale Control Systems*. This model introduces a new type of control application that provides reconfiguration services for dynamic I/O binding to other control applications. This type of control application is modeled as a control system, built by control elements that are able to interact with other control elements of the same API

but implemented for a different application scope. This approach allows a higher interoperability and modularity between control applications and a higher flexibility, integration and applicability of dynamic I/O binding reconfigurations in the domain of cyber-physical systems and Internet of Things.

ALSOS-ICS is composed of three types of control elements: (i) the *I/O discovery sensor*, (ii) the *I/O decision controller* and (iii) the *I/O reconfiguration actuator*. These elements are bound to each other and also to elements that compose a different control application. The later application is the one that experiences dynamic I/O binding capabilities provided by an ALSOS-ICS control application. The I/O discovery sensor senses for possible I/O bindings and outputs these possible bindings to the I/O decision controller. The possibility of gossip-based discovery sensors is discussed in our earlier work [29]. The I/O decision controller selects to add or remove I/O bindings based on the objectives of the control application that ALSOS-ICS supports. These objectives may be represented as a fitness function or high-level business rules and policies. The added and removed I/O bindings are the output to the I/O reconfiguration actuator that modifies the I/O binding of the served control application.

The coupling of ALSOS-ICS with control applications can be performed at different levels as illustrated in our earlier work [29]: (i) *system-level*, (ii) *node-level* and (iii) *element-level*. This book chapter shows more specifically the relevance of these levels in the Smart Power Grid. Figure 1 illustrates an overview of ALSOS-ICS and its coupling to the Smart Power Grid.

In the system-level coupling, ALSOS-ICS is linked to a Distribution Automation System (DAS) that may perform various system optimizations such as power flow optimization [5], secure fault isolation [2] etc. Data acquisition is, to an extent, centralized. A node-level deployment of ALSOS-ICS distributes I/O binding control over the Smart Power Grid at different control points such as power lines, substations, etc. Because of a higher decentralization in node-level compared to system-level, the ALSOS-ICS control elements require in this case more complex interactions that guarantee access to remote information. Finally, coupling ALSOS-ICS at the element-level introduces dynamic I/O binding control at the very low-end control elements of the Smart Power Grid. In this case, control elements reconfigure their I/O binding autonomously and in a fully decentralized fashion.

3 Application Scenarios

The Smart Power Grid may experience various (cascading) system failures or malfunctions such as overloaded power lines, failures of power lines, physical disasters, demand-supply imbalances or black-outs. These events require a broad range of system reconfigurations and stabilizations to guarantee robustness and a continuous system availability of the Smart Power Grid. Power reconfigurations that prevent system failures or minimize their impact by isolating them, require a period of time to be applied, depending on the type of reconfiguration. Time is a critical factor
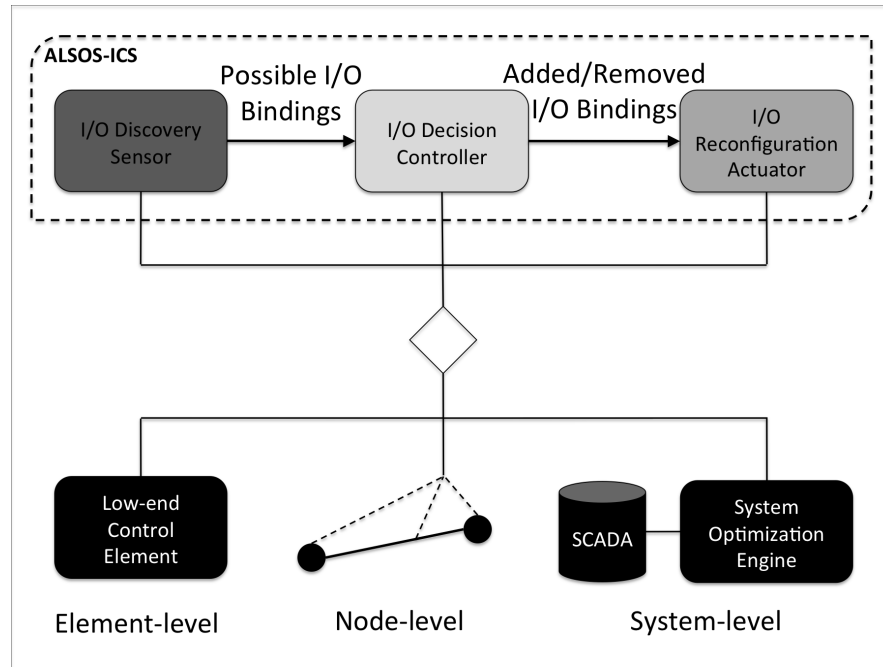
Fig. 1 Positioning of ALSOS-ICS in the context of the Smart Power Grid.

for the prevention of system failures or the minimization of their impact by, for example, isolating these failures. System operators cannot always make optimum decisions especially when multiple transmission lines are affected simultaneously. Automated and dynamic I/O binding reconfigurations are required to stabilize the operation of the Smart Power Grid using computational intelligence embedded in control elements.

This book chapter illustrates four application scenarios that together suggest an incremental four-level protection approach based on dynamic I/O binding reconfigurations. The purpose of these application scenarios is not to introduce a new concrete protection mechanism but to underline the importance of dynamic I/O binding requirements for the robustness of the Smart Power Grid. The four levels of Smart Power Grid reconfigurations are the following:

1. *Dynamic load-balancing of power lines*: Power flow may exceed the capacity of certain power lines when demand increases or neighboring power lines fail. Rerouting power to alternative parallel power lines requires rapid I/O binding reconfigurations to prevent cascading failures to a certain extent.
2. *Dynamic switching of power flow*: Generation, transmission and especially distribution networks are supported by multiple backup power lines and switches that provide alternative power flow of the load served by a substation but also between different substations. System failures and maintenance can be managed by

dynamic and automated I/O binding reconfigurations of power lines and switches instead of manual actions by system operators.

3. *Dynamic allocation of operating reserves*: Demand-supply imbalances due to system failures or a sudden demand peak require system scaling. Operating reserves are back-up power generation that can be made available within a varied time span depending on various technical constraints. Dynamic I/O binding reconfigurations are required to activate/deactivate operating reserves for a given system situation.

4. *Dynamic restoration after blackout*: If a system failure occurs despite the above mentioned protection actions, the power system is islanded and the restoration of the system back to its normal operation is challenging. Islands should be integrated again, generators should be activated gradually and this activation should be coordinated with the rest of the generation available in the system.

This four-level protection approach can be realized by one or more cyber-physical control applications built by three types of control elements bound in an overlay network (application graph):

- *Load sensor*: This control element monitors load information from various physical assets of the Smart Power Grid. It is bound to protection controllers to provide them with the necessary information.
- *Protection controller*: This control element coordinates the stabilizations required to guarantee the protection and robustness of the Smart Power Grid.
- *Stabilization actuator*: This control element adjusts the operation of various underlying physical assets that contribute to the stabilization of the Smart Power Grid.

The power supply required for the overlay network to function is crucial and is designed to be independent of the state in the underlying infrastructure. This can be technically achieved by the availability of dedicated small-scale backup generators or the utilization of batteries [7]. This section shows the dynamic I/O binding requirements and services that such a control application can meet and consume respectively by using ALSOS-ICS.
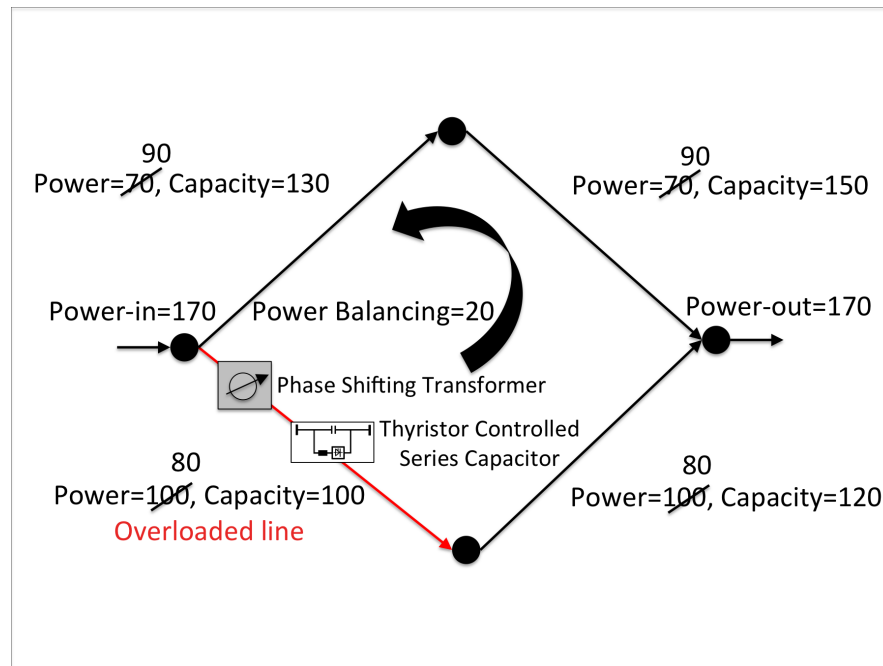
3.1 Dynamic Load-balancing of Power Lines

This is the first level of dynamic reconfigurations applied for the prevention of cascading and other failures. It concerns the load-balancing of power lines positioned in parallel within the generation and transmission system. If a heavily loaded line transmits an excess power load, this excess load can be rerouted to another under-loaded power line positioned in parallel.

This load rerouting is possible in two ways: (i) Shifting the phase angle between the voltages in the nodes adjacent to a power line or (ii) altering the line impedance. The first approach is technically possible via a *phase shifting transformer* device

mainly used for the load-balancing of power lines [31, 32]. The second approach is possible via a *thyristor controlled series capacitor* [13, 26]. This device is mainly used for minimizing power oscillations. Other more complex devices that combine these two functionalities with additional features are proposed in literature [1, 19] resulting in improved stability of power lines.

Figure 2 illustrates the concept of load-balancing between two power lines. When the power of a line reaches its capacity of 100 units, power balancing is performed by rerouting 20 units to a line with power flow of 70 units and capacity of 130 units. These 20 units are the result of either the alteration in the voltage phase angle or in the impedance of the power line. Note that, from an engineering point of view, these alterations can be performed rapidly. However, the balancing compensation that can be achieved is related to the technical specification of the lines and therefore this approach has limitations. These limitations are out of the scope of this book chapter and are discussed in related work [13, 26, 31, 32].

Fig. 2 Load-balancing of power lines by rerouting load from an overloaded line to an underloaded one.

Figure 3 illustrates the bound control elements that manage the load-balancing of transmission lines. Note that the control elements are bound in an overlay network that manages the information generated by the physical assets of the transmission lines. The load sensors in every power line output the load information to the protection controllers of the adjacent nodes. Based on this information, the balancing

controllers perform decision-making about the power rerouting. This decision is executed by a stabilization actuator that controls the phase angle or the impedance of its controlled power line. More specifically, the information about the rerouted load is translated by the stabilization actuator to an actual configuration in the phase shifting transformer or the thyristor controlled series capacitor.
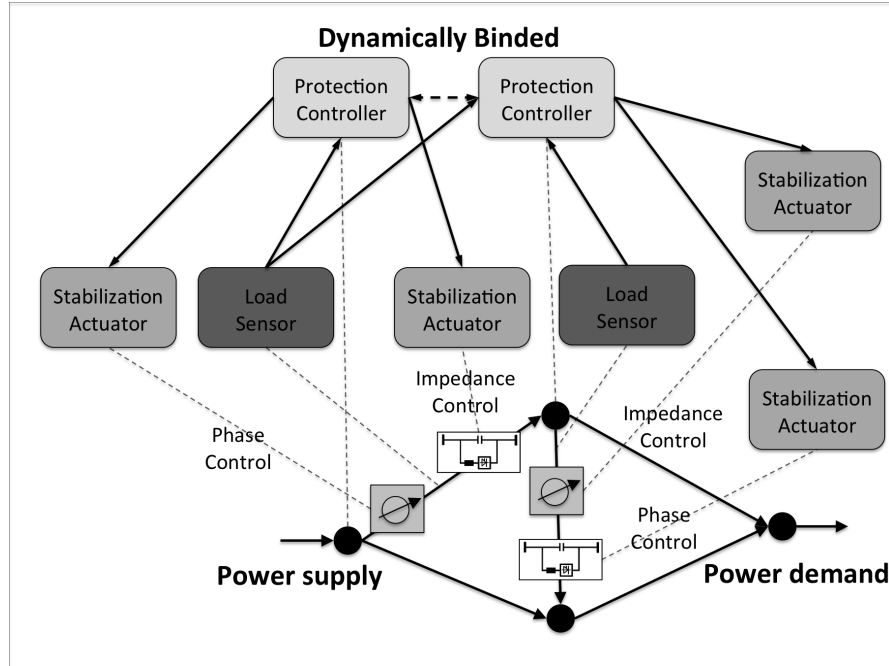
Fig. 3 The overlay network of control elements that balances the load between parallel transmission lines.

Note that, protection controllers require coordination. This is because a load-balancing action should not cause an overload to other power lines in the transmission topology. Therefore, the protection controllers require an on-demand dynamic I/O binding provided by an ALSOS-ICS control application. Both (i) the I/O binding control application and (ii) the load-balancing control application are realized by embedded software control elements and therefore interoperation between these two control applications is possible.

For example, assume a (tree) branch of nodes that after a load-balancing action is fed with a higher amount of power. Coordination can be performed by discovering generator nodes within this branch that can decrease their energy supply after load-balancing is performed to compensate. The protection controller of this generator node and the protection controller of the power line, in which a higher load is rerouted can dynamically bound by an ALSOS-ICS control application to negotiate

and coordinate these operations. This coordination can be performed on-the-fly and in an automated fashion without the intervention of systems operators.
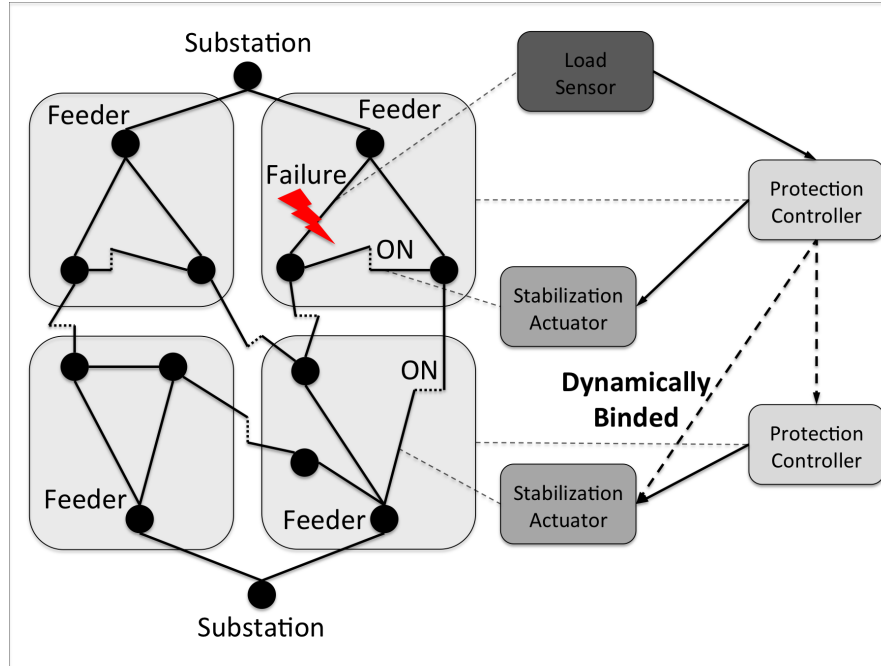
3.2 Dynamic Switching of Power Flow

Within (i) a generation and transmission system as well as (ii) a distribution system, power is possible to flow in different ways. This is crucial for (i) the protection of the power grid [11] and (ii) its optimization based on market strategies or economic and environmental policies [17, 25]. One way to control the power flow is by switching the power flow on or off between different nodes in a topology, e.g. in the topology of the distribution system. Switching is technically possible by using relays, switches, circuit breakers or reclosers [11]. Switching provides some form of redundancy or flexibility as power can be made available via alternative distribution paths. This provides the option to perform several critical operations [11, 27] such as (i) system clearance, maintenance, repair or construction, (ii) load-balancing and (iii) system restoration after blackouts as discussed in Section 3.3.

Figure 4 illustrates a dynamic switching scenario in a distribution system. The topology consists of nodes that represent loads, such as households, that draw power from specific feeders that are connected to substations. The control of the distribution system is hierarchical and is managed by nested control areas [11]: (i) A substation defines its control area, (ii) within which the feeders have their own control areas, (iii) within which feeder lines may also form their own control area. Therefore, the distribution system can be controlled at different granularity levels. For illustration purposes, Figure 4 focuses only on the control areas defined by the feeders.

Assume that a number of simple closed switches can transfer power between loads (i) within a control area and (ii) between different control areas. The switches are configured at 'on' or 'off' according to a system optimization [11, 17, 25]. This optimization guarantees that all loads are served and that there are no overloaded feeder lines. However, as it is mentioned before, failures may happen due to demand peaks, physical disasters or even cyber-attacks in the power grid. Failures result in power outage in one or more households and may even cascade and cause new failures in the distribution system. A coordinated switching of power flow is required to stabilize the distribution system. Note that an automated control of switches is possible via pole-top remote terminal units (RTUs) [30].

Control elements undertake this coordination by dynamically binding themselves to control the switches and, therefore, manage the power flow in a distribution system. Load sensors monitor the power flowing in a power line. This information is output to the protection controller of the feeder control area. If a failure is detected by this controller based on the input load information, an alternative power flow needs to be discovered and utilized. Protection controllers are dynamically bound and communicate to guarantee that switching of power flow does not influence other parts of the system. Next, the protection controller of the affected control area is dy-

Fig. 4 Dynamic switching guarantees the power delivery in the loads of a distribution system when a failure of power lines occurs. One or more switches can close enabling a load to draw power from a neighboring control area that is served by a different feeder. Control elements are dynamically bound with each other to coordinate the dynamic switching of power flow.

namically bound with stabilization actuators that control switches within the same control area and in neighboring ones. These switches are turned on for a period of time to deliver power to the affected households. This binding configuration may last as long as the failures occurs and during repair/maintenance operations. Manual actions by system operators are not required as long as the protection controllers are able to coordinate the switching of the power flow.

Similarly to the previous scenario, the dynamic switching of power flow forms a control application that is served by an ALSOS-ICS control application. The I/O discovery sensors of ALSOS-ICS locate the feeder control areas and the switches that when closed deliver power to the affected nodes. The I/O decision controllers select the I/O binding reconfigurations required given state information provided by the protection controllers. Finally, the I/O reconfiguration actuators of ALSOS-ICS bind the load sensors, protection controllers and stabilization actuators to handle a failure occurred in the distribution system.

3.3 Dynamic Allocation of Operating Reserves

The first two protection levels illustrated in Section 3.2 and 3.3 may not be adequate in some cases. For example, there are power lines that do not support the technology for power balancing or do not have automated switches. Furthermore, load-balancing has its limits especially when the power demand increases and additional power supply is needed in the system. Backup generation is required in the power infrastructure to match supply and demand without causing cascading failures by overloaded power lines. This backup generation is the *operating reserves* of a power grid.

Traditionally, an operating reserve is a generating power capacity available on-demand to the system operator within a period of time. An operating reserve is usually activated to meet power demand in case of system disruptions, such as power line failures or system maintenance. Although there are various operating reserves that match different system requirements, two main types of operating reserve are used by system operators [4]:

- *Spinning reserve*: This is additional synchronized generated capacity available in the system by increasing the power output of the online power generators. Spinning reserve can also refer to responsive loads as a result of demand-side energy management [21, 28].
- *Non-spinning reserve*: This is additional non-synchronized generated capacity that can be made available to the system by offline power generators within a longer period of time than spinning reserve. The power exchanged via power flow gates between different transmission zones is also a form of non-spinning reserve.

Figure 5 shows a simplified illustration of spinning and non-spinning reserves. This extra capacity can be made available within 10 minutes approximately for a period of approximately 30 minutes depending on the type of reserve and the technical features of the physical assets that enable it [6]. Failures of power lines and cascading failures can be prevented by choosing the point where the additional power is injected. For example, if the power lines adjacent in the main power supply of Figure 5 cannot support the extra power of spinning reserve, an alternative reserve that is adjacent to lines with higher capacity can be selected. Furthermore, offline power generators have a varying startup time that is also related to the actual power activated, referred to as *ramp rate* [6]. Multiple reserves can be activated and combined to ensure the robustness of power transmission. Finally note that the traditional spinning reserve is usually more expensive than the non-spinning one and therefore the cost can also be a selection factor.

Operating reserve is traditionally activated manually by system operators as agreed offline by market contracts [6]. As Smart Power Grids scale and becomes more complex and dynamic, failures and their cascading effects cannot be managed by system operators. An online, automated and dynamic allocation of operating reserves is required. Therefore, this section proposes the dynamic allocation of operating reserves by software embedded control systems. Figure 6 illustrates the
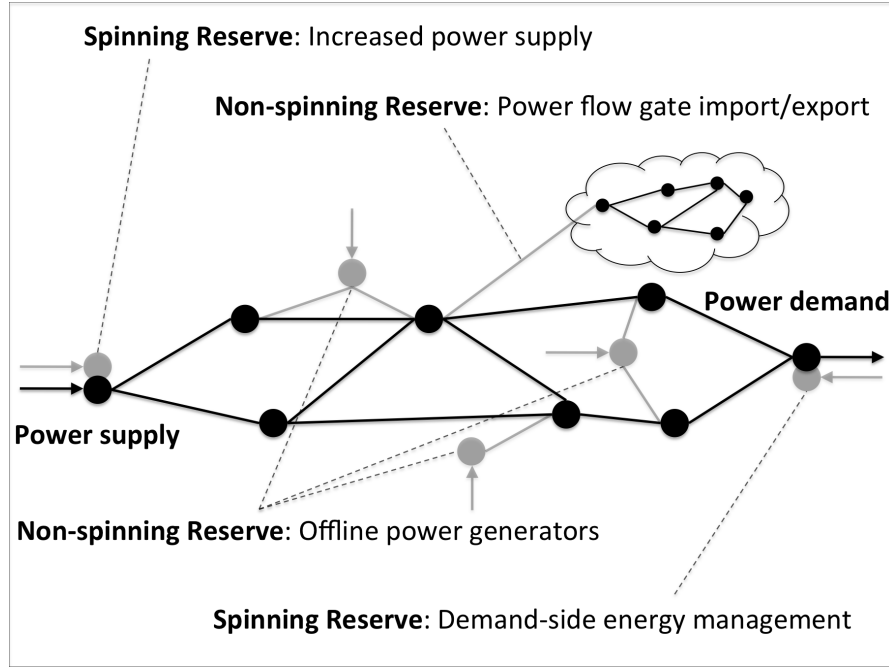
Fig. 5 A power system with different operating reserves.

control elements of a power line that is protected by three operating reserves: (i) A spinning reserve in the supply node, (ii) a second spinning reserve that acts as a responsive load enabled by a demand-side energy management mechanism and (iii) a non-spinning reserve that remains offline under normal system operation. Each power line and node, including the ones of the non-spinning reserves, have a load sensor and a protection controller respectively. Furthermore, every node that acts as an operating reserve has a stabilization actuator that activates and deactivates the operating reserve. The protection controllers, that are adjacent to an overloaded power line, check if a first-level reconfiguration is possible and adequate to balance the load of the affected power line as illustrated in Section 3.1. If the first-level reconfiguration cannot be applied, the protection controllers either activate their local reserve, if they have one, or coordinate with other remote protection controllers the allocation of their reserves.

Dynamic binding is required between the remote protection controllers to coordinate the activation of operating reserves in a cost-effective manner. Furthermore, if a non-spinning reserve is activated, the load sensor of its adjacent power lines may need to be dynamically bound with the other adjacent nodes. An ALSOS-ICS application can perform this service by inter-operating and configuring the I/Os bindings in the control application of dynamically allocated operating reserves.
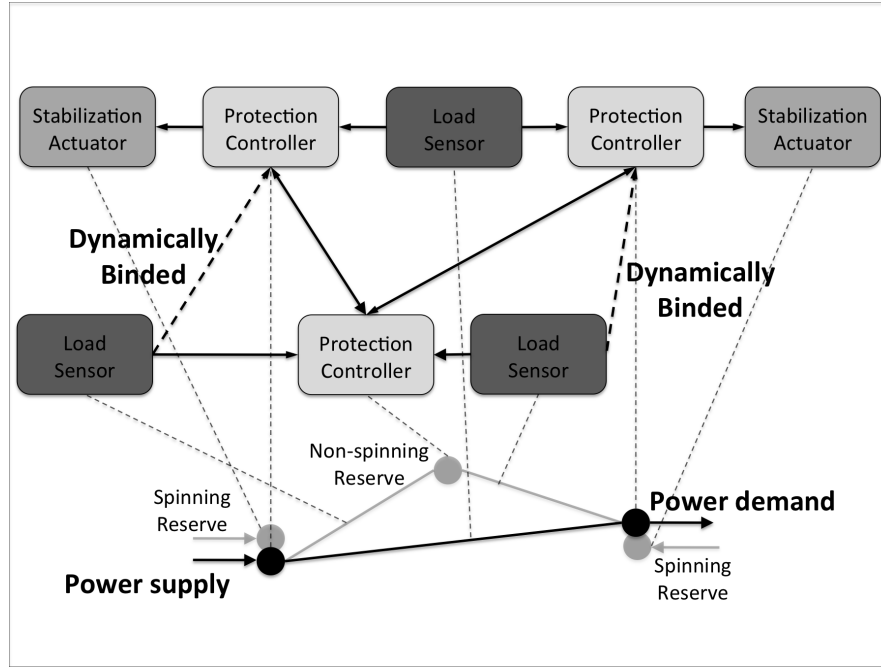
Fig. 6 The overlay network of control elements that allocate and control operating reserves for the protection of a power line from an overload.

3.4 Dynamic Restoration after Blackout

Despite the aforementioned levels of protection, blackouts may still occur. Blackouts in the USA have not decreased the last years and occur with higher frequency during peak times [16]. During a blackout condition, the transmission and distribution system is clustered in one or more islands that cannot exchange power due to failed power lines or nodes. These failures may be isolated or cascading. The latter is the main cause of blackouts in power systems. During a cascading failure, a power flow is forced to a rerouting that makes other lines and nodes overloaded and failing. This failing process is recursive. The system restoration after such a condition is highly complex. A simple and arbitrary restoration of the failed units does not guarantee the system restoration back to normal operation. Demand draws the power that is made available after restoration causing a new failure. Coordination is required during the restoration process by interconnecting the islands and synchronizing the power flow that is made available after a blackout. This coordination means that the I/O binding of the cyber-physical control elements should be adjusted dynamically during this process. Existing restoration approaches are mainly managed by system operators that apply manual actions based on their experience [12].

Figure 7 illustrates an example of coordination performed for the restoration of a system after a blackout. Note that this scenario assumes that there is available re-

served power for the control elements to perform their control tasks. Therefore, the overlay network of the control elements is energized, connected and manageable compared to the affected physical infrastructure. A simple cascading failure causes this blackout. The sequence, in which the events occur, is numbered and illustrated in order as follows: First, an unexpected failure occurs to one of the generators that causes (i) a lower power injection in the system and (ii) the unavailability of its adjacent transmission lines (event #1). Because of this failure, two events follow: (i) The power of the second generator is rerouted to its second power line and (ii) the spinning reserve of the second generator is activated. The activation occurs because of the frequency drop that the failure of the first generator causes (event #2). This increased load makes a second node overloaded and failing (event #3). This cascading failure clusters the power network in two islands. A blackout has occurred and the system needs to be restored in a coordinated and timely fashion.
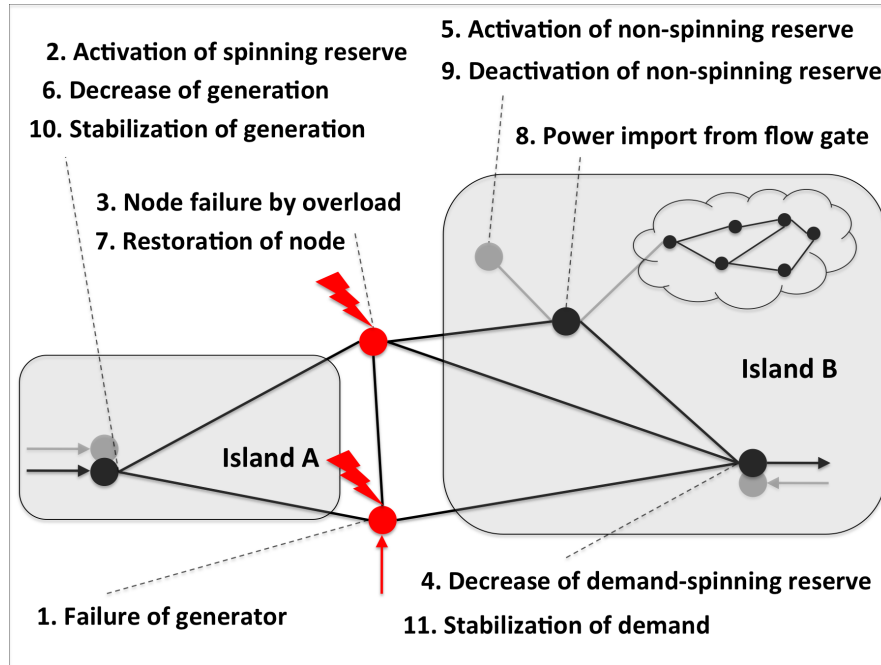
Fig. 7 A sequence of coordination actions for a blackout restoration.

The goal of the restoration strategy is to interconnect the islands that resulted after the blackout. This can be achieved by reversing the overload in the failing node. Three actions are applied: (i) Activation of spinning reserve using demand-side energy management (event #4), (ii) activation of non-spinning reserve by turning on a backup generator (event #5) and (iii) adjusting the generation in island 'A' to restore the failed node (event #6). After these actions, the islands are again interconnected (event #7). However, the activated non-spinning reserve cannot run for long and it is

an expensive power source. Therefore, power is imported from a neighboring zone via a flow gate that interconnects the two zones (event #8). At the same time, the non-spinning reserve turns off (event #9), the initial power generation is stabilized (event #10) and demand is fully served again (event #11). These actions complete the system restoration. Later on, if the failed generator is fixed, new adjustments can be applied to remove the power dependency from the neighboring transmission zone.

All these actions should be executed in a certain priority and timely fashion. Synchronization is crucial. For example, the generator in island 'A' should be dynamically bound to the back-up generator in island 'B' to coordinate and adjust the allocation of power that will enable the overloaded node to be available again and interconnect the two islands. If actions are not coordinated, then new failures may occur that may result in more isolated islands that cannot be energized. For this reason, an islanding situation in the physical layer should not be reflected in the overlay network of control elements. The overlay network should remain connected and allow the control elements of ALSOS-ICS to inter-communicate between different islands and therefore support the coordination and restorations actions. Note that, as mentioned in Section 2, a gossiping protocol implementation for the I/O discovery sensors is a relevant choice in this case. Gossiping builds and maintains a dynamic well connected and non-clustered overlay network that remains robust even in case of catastrophic failures [18].

Note that, dynamic blackout restoration actions are based on dynamic load-balancing of power lines, switching of power flow and allocation of operating reserves. Therefore, more effective mechanisms for blackout prevention support a more effective blackout restoration in case it occurs.

4 Discussion

The protection of the power grid is a highly challenging and complex problem that should be decomposed and managed at different levels. This book chapter illustrates coordination scenarios within four incremental Smart Power Grid protection levels. The protection requirements in each scenario are traditionally satisfied by experienced system operators that apply manual actions assisted by centralized data acquisition and supervisory systems. However, as micro-generation scales and becomes more decentralized, such an approach becomes cost-ineffective. A higher level of automation is required, which means that control elements managing various physical assets need to become more interactive and intelligent. Distributed computational intelligence requires a situational awareness that can be attributed to a system if and only if its elements have the potential to be dynamically bound with each other on-demand. Without dynamic I/O binding of control elements, coordination cannot always be achieved. This is exactly what the four incremental scenarios for the protection of the Smart Power Grid show. For example, binding an offline generator to the rest of the control elements when operating reserves are utilized is

required to control and coordinate the injected power flow in the system. Without such a binding, a protection measure may cause new cascading failures.

The modeling approach of ALSOS-ICS couples dynamic I/O binding capabilities with the rest of the control logic of a cyber-physical system. he Internet of Things requires reconfigurable physical and software control elements that ALSOS-ICS can dynamically bind and organize. ALSOS-ICS control elements are able to interoperate as a control application with the rest of the control elements. This distinction suggests a split of concerns for system developers, yet, the context remains within control systems of Internet of Things and their applications. More specifically, ALSOS-ICS developers, extending the work of application integrators, build control elements that provide dynamic I/O binding capabilities to another group of control elements, developed by domain-experts, that embed the main control application logic. In the four application scenarios illustrated in Section 3, the main domain-expert developer has knowledge about the protection of the Smart Power Grid, and more specifically about the available repair and maintenance mechanisms. This developer provides the load-sensors, protection controllers and stabilization actuators. It assumes a certain level of interaction and communication capabilities that ALSOS-ICS developers expose via, for example, interfaces. The actual I/O binding discovery, selection and reconfiguration is handled by the control elements of ALSOS-ICS developed by network communication experts.

5 Conclusions and Future Work

This chapter illustrates application scenarios of organizational control reconfigurations for the robustness of the Smart Power Grid. Each of these scenarios requires some degree of coordination between control elements that manage various physical assets. With the emergence of micro-generation and renewable resources, matching supply and demand becomes challenging with an impact on the robustness of the power grid. Coordination needs to evolve beyond the control of system operators, become more automated, decentralized and manageable by control elements themselves. The coordination and computational intelligence of control elements requires capabilities for dynamic binding reconfigurations in this case. The application scenarios illustrated and discussed in this book chapter exactly show such required capabilities for the protection of the Smart Power Grid. Dynamic binding reconfigurations required for applications of the Internet of Things can be modeled as a control application using the ALSOS-ICS model summarized in this chapter. ALSOS-ICS allows a higher interoperation and modularity between control applications and a higher flexibility, integration and applicability of dynamic binding reconfigurations in the domains of the Internet-scale cyber-physical control systems.

Organizational control reconfigurations are required in other application domains beyond the Smart Power Grid. ALSOS-ICS is application-independent and therefore various domains of Internet of Things, such as transportation systems, air vehicles [34] etc., can make use of it.

Future work includes the actual implementation, testing and evaluation of Internet of Things applications that are based on dynamic I/O binding of their control elements. iCS [3] is a Java Micro Edition (JME) lightweight runtime environment for distributed control applications that can be used for exactly this purpose. Furthermore, a critical aspect that needs to be studied in the future Smart Power Grids is the higher interdependence of the power infrastructure to the communication infrastructure.

References

1. M. Abdel-Moamen and N. Padhy. Optimal power flow incorporating FACTS devices - bibliography and survey. In *Transmission and Distribution Conference and Exposition, 2003 IEEE PES*, volume 2, pages 669 – 676, Sept. 2003.
2. M. Ahmed and W. Soo. Development of customized distribution automation system (DAS) for secure fault isolation in low voltage distribution system. In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, pages 1 –7, July 2008.
3. R. Ambrosio, A. Morrow, and N. Noecker. e-Business Control Systems. In *Proceedings of the 2nd International Conference on Computing, Communications, and Control Technologies*, pages 91–96, University of Texas, Austin, TX, 2004. IEEE Computer Society.
4. F. D. M. Ch, D. B. Bedoya, G. D. M. Jannuzzi, and L. C. P. Da Silva. Operating reserves provided by distributed generation. In *Proceedings of the 3rd IASME/WSEAS International Conference on Energy & Environment*, pages 219–224, Stevens Point, Wisconsin, USA, 2008. World Scientific and Engineering Academy and Society (WSEAS).
5. C.-S. Chen, C.-T. Tsai, C.-H. Lin, W.-L. Hsieh, and T.-T. Ku. Loading balance of distribution feeders with loop power controllers considering photovoltaic generation. *Power Systems, IEEE Transactions on*, 26(3):1762 –1768, Aug. 2011.
6. J. Chen, J. Thorp, R. Thomas, and T. Mount. Locational pricing and scheduling for an integrated energy-reserve market. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, page 10 pp., Jan. 2003.
7. K. Divya and J. stergaard. Battery energy storage technology for power systemsan overview. *Electric Power Systems Research*, 79(4):511 – 520, 2009.
8. X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid - the new and improved power grid: A survey. *Communications Surveys Tutorials, IEEE*, PP(99):1–37, 2011.
9. T. Gensler and C. Zeidler. Rule-Driven Component Composition for Embedded Systems. In *International Conference on Software Engineering (ICSE): Workshop on Component-Based Software Engineering*, 2001.
10. I. Georgiadis, J. Magee, and J. Kramer. Self-organising software architectures for distributed systems. In *Proceedings of the first workshop on Self-healing systems - WOSS '02*, page 33, New York, NY, USA, Nov. 2002. ACM Press.
11. R. Greer, W. Allen, J. Schnegg, and A. Dulmage. Distribution automation systems with advanced features. In *Rural Electric Power Conference (REPC), 2011 IEEE*, pages C4–1–C4–15, Apr. 2011.
12. F. L. Greitzer, R. Podmore, M. Robinson, and P. Ey. Naturalistic decision making for power system operators. *International Journal of Human-Computer Interaction*, 26(2-3):278–291, 2010.

13. R. Grunbaum and J. Pernot. Thyristor-controlled series compensation: A state of the art approach for optimization of transmission over power links. In *1st International Forum on Innovations in Power Links*, pages 15–20, Mar. 2001.

14. M. Guler, S. Clements, N. Kejriwal, L. Wills, B. Heck, and G. Vachtsevanos. Rapid Prototyping of Transition Management Code for Reconfigurable Control Systems. In *Proceedings of the 13th IEEE International Workshop on Rapid System Prototyping (RSP'02)*, Washington, 2002. IEEE Computer Society.

15. D. Hammerstrom, T. Oliver, R. Melton, and R. Ambrosio. Standardization of a hierarchical transactive control system. In *Proceedings of the Grid Interop '09 Conference*, 2009.

16. P. Hines, J. Apt, and S. Talukdar. Large blackouts in North America: Historical trends and policy implications. *Energy Policy*, 37(12):5249 – 5259, 2009.

17. S. Jalilzadeh, H. Hosseini, V. Nabaei, G. Govar, and M. Zandi. Multipurpose reconfiguration of deregulated distribution networks using BGA. In *Power and Energy Conference, 2008. PECon 2008. IEEE 2nd International*, pages 1222 –1226, Dec. 2008.

18. M. Jelasity, S. Voulgaris, R. Guerraoui, A.-M. Kermarrec, and M. van Steen. Gossip-based peer sampling. *ACM Trans. Comput. Syst.*, 25(3), Aug. 2007.

19. X. Jiang. *Operating Modes and their Regulations of Voltage-sourced Converter Based Facts Controllers*. PhD thesis, Faculty of Rensselaer Polytechnic Institute, Rensselaer Polytechnic Institute, 2007.

20. S. Karnouskos. Cyber-physical systems in the smartgrid. In *Industrial Informatics (INDIN), 2011 9th IEEE International Conference on*, pages 20 –23, july 2011.

21. B. Kirby. Load response fundamentally matches power system reliability requirements. In *Power Engineering Society General Meeting, 2007. IEEE*, pages 1–6, June 2007.

22. A. Koubaa and B. Andersson. A Vision of Cyber-Physical Internet. In *8th International Workshop on Real-Time Networks (RTN'09)*, 2009.

23. J. Kramer and J. Magee. Self-Managed Systems: an Architectural Challenge. In *Future of Software Engineering (FOSE '07)*, pages 259–268. IEEE, May 2007.

24. E. Lee. Cyber physical systems: Design challenges. In *Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on*, pages 363 –369, May 2008.

25. X. Mamo, S. Mallet, T. Coste, and S. Grenard. Distribution automation: The cornerstone for smart grid development strategy. In *Power Energy Society General Meeting, 2009. PES '09. IEEE*, pages 1 –6, July 2009.

26. N. I. Maruf, A. Mohsin, A. Shoeb, K. Islam, and M. Hossain. Study of Thyristor Controlled Series Capacitor (TCSC) as a Useful Facts Device. *International Journal of Engineering Science and Technology*, 2(9):4357–4360, 2010.

27. A. Meier. *Electric power systems: a conceptual introduction*. Wiley survival guides in engineering and science. IEEE Press, 2006.

28. E. Pournaras, M. Warnier, and F. M. Brazier. Local Agent-based Self-stabilisation in Global Resource Utilisation. *International Journal of Autonomic Computing*, 1(4):350 – 373, Dec. 2010.

29. E. Pournaras, M. Yao, and R. Ambrosio. Dynamic composition and reconfiguration of internet-scale control systems. In *Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on*, pages 233 –240, June 2011.

30. J. Santos, N. Silva, P. Rodrigues, A. Rodrigues, D. Marsh, F. Gomes, C. M. Pinto, A. Blanquet, and A. Carrapatoso. Electric grid versus data network architectures and standards Smart Grid as plug & play. *IET Conference Publications*, 2009(CP550):912, 2009.

31. D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, and W. Kling. Usefulness of DC power flow for active power flow analysis with flow controlling devices. In *AC and DC Power Transmission, 2006. ACDC 2006. The 8th IEE International Conference on*, pages 58 – 62, Mar. 2006.

32. J. Verboomen, D. Van Hertem, P. Schavemaker, W. Kling, and R. Belmans. Phase shifting transformers: principles and applications. In *International Conference on Future Power Systems, 2005*, page 6, Nov. 2005.

33. L. Wang, S. Balasubramanian, and D. H. Norrie. Agent-based Intelligent Control System Design For Real-time Distributed Manufacturing Environments. pages 115–152. In Working Notes of the Agent Based Manufacturing Workshop, 1998.

34. L. Wills, S. Kannan, S. Sander, M. Guler, B. Heck, J. V. R. Prasad, D. Schrage, and G. Vachtsevanos. An open platform for reconfigurable control. *IEEE Control Systems*, 21:49–64, 2001.

Index