PAC World Conference 2012

Budapest, Hungary, 25 – 28 June 2012

# Adaptivity of Protection in Smart Grids

Sampo Voima & Kimmo Kauhaniemi
University of Vaasa
sampo.voima@uwasa.fi
Finland

## Abstract

In this paper the adaptivity of protection required in Smart Grids is discussed with focus being in the MV level. As the network topology is changing and active resources are connected or disconnected the protection requirements are changing at the same time. The change in the system conditions creates a need for adaptive protection schemes that are self-aware to the changes happening in the system and can adapt to the changed system conditions. The grid conditions requiring adaptivity are discussed and adaptivity is divided into two categories based on the decision making strategy. Finally the adaptivity required from Smart Grid protection is demonstrated.

## Introduction

Today’s passive medium voltage (MV) distribution networks are in the beginning of the transition towards future Smart Grids. Smart Grid does not have a single clear definition and there is a great deal of variation what is considered a Smart Grid. One of the many definitions for Smart Grid is given by The European Technology Platform SmartGrids that states [1]: *"A SmartGrid is an electricity network that can intelligently integrate the actions of all users connected to it - generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies"*. Basically what that means is that a Smart Grid is a network that can employ a wide range of different active resources, which include distributed generation (DG) and energy storages connected together with telecommunication. The concept of Smart Grid seems very attractive, but there are still many challenges before fully integrated Smart Grids can be enabled. One of the challenges is protection, and the transition towards Smart Grids brings up new requirements for protection, that needs to be adaptive for changes in the network topology and configuration along with connecting of active resources. The effects of adding DG and other active resources to networks are numerous including changing network topologies, changing power flow direction and increased or decreased short circuit levels among other effects. Furthermore, in networks with DG new possibilities arise as DG makes it possible to use part of the network as a self-sufficient island which is also known as microgrid. Using part of the network as microgrid contributes to self-healing in Smart Grids by enabling the service of supply to continue to the parts of the network that otherwise would be negatively affected by faults in the network. Self-healing is a feature strongly related to protection and control. Self-healing means, for example, that it is possible to continue to supply a part of the network after contingency by taking backup supply into use or by operating a part of the network as microgrid. Microgrid can therefore be counted as one aspect of the required adaptivity. A distribution network may have several self-healing strategies from which the most suitable one to the prevailing network conditions is selected. The protection and control system should be able to take action in order to continue to deliver power to areas not affected by contingency after it has occurred.

Today’s passive electric system lacks the capabilities to perform the required adaptive functions to cope with changes in network topology, operating mode of DG etc. The traditional protection of distribution networks has followed the same concept for decades, that is, the assumption of unidirectional power flow from higher voltage level to lower, and protecting the network mainly with overcurrent sensing devices. Therefore, the traditional protection system does not always satisfy the protection requirements and new protection solutions will be needed. Adaptivity in protection can mean, for example, dynamic protection which is capable of adapting to a situation where adding of DG changes the protection requirements. The decision making behind the adaptivity of protection can be either centralized or distributed which in other words can be described as centralized or distributed intelligence.

First in this paper the adaptive protection concept is described. Then the changing grid conditions that require adaptivity form the protection are discussed. A short review of protection and control functions is made and different levels of adaptivity are introduced. After that some technical considerations are reviewed and the centralized and distributed intelligence behind the decision making is discussed. Finally the required adaptivity of Smart Grid protection is demonstrated.

## Adaptive protection

The adaptive protection was developed in the 1980's. The development was enabled by the increase of computer based relaying which allowed the possibility to change relay characteristics, and the development has been ongoing ever since [2]. The need to create adaptive protection comes from the evolving networks which can make the existing relay settings to be inappropriate. This creates the need for relays whose settings can be controlled in response to external conditions [2]. It should also be noted that some of the traditional protection functions have adaptive characteristics in them, for example, the inverse time overcurrent relay adapts its operating delay to the prevailing fault current magnitude [2]. In [2] the adaptive relaying has been defined as *"adaptive protection is a protection philosophy which permits and seeks to make adjustments in various protection functions automatically in order to make them more attuned to prevailing power system conditions"*. In [2] it is also mentioned that the definition creates requirements that are necessary to obtain an adaptive protection system. The requirements include that the system itself allows predetermined adjustments to be made when receiving external information, or tries to find adjustments within itself, and information can be extracted from the normal measurements or from external sources [2].

The flow of functions of any adaptive relaying system consists of four steps that have been depicted in [2]:

1. Determination of changed condition
2. Decision for adaption
3. Adjustment of protection
4. Report to the personnel responsible.

Furthermore, the possibilities to use adaptive protection schemes at transmission level are discussed and identified for example in [2] and [3].

## Changing grid conditions requiring adaption of the protection

Nowadays with the increasing number of local production, for example DG, the need for adaptive protection also in the distribution level becomes apparent. In Smart Grids where the number of connected DGs and other distributed energy resources varies the grid becomes more active and needs adaptive protection schemes. In a typical radial distribution feeder the protection assumes power flow from only one direction, and an example of how the situation is changed when DG is added to the network is depicted in the figure below (Fig. 1). In the figure below a DG connected to the network can affect the fault current levels and the current flow direction as is shown in the figure when the DG feeds a fault at an adjacent feeder. In the worst cases this could lead to false tripping of the feeder where the DG is located or sympathetic tripping of the DG unit. The impacts of DG on the protection of distribution networks have been more thoroughly studied for example in [4].

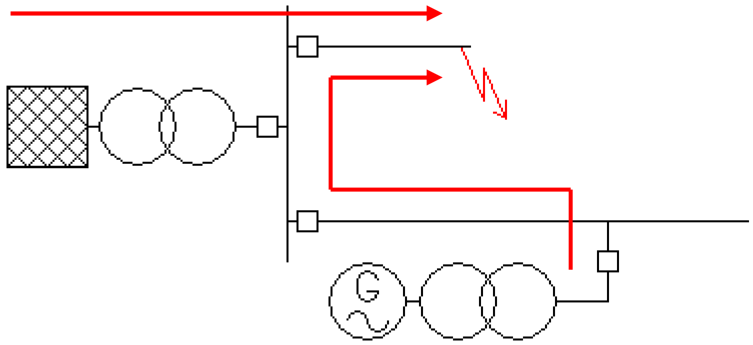

Figure 1. DG feeding a fault at an adjacent feeder.

In order for the protection system to be adaptive it needs some information of changes occurring in the network that might have an effect on the protection requirements, and furthermore on the protection settings. It can even be possible that the new requirements cannot be fulfilled by adjusting the settings, but also totally different protection functions must be taken into use. Some of the most important information of the state of the distribution network regarding to the protection requirements are listed below:

- Network configuration
- Operation status of DG units
- Earthing arrangements.

Events in the distribution system affecting the network configuration (topology change) need to be detected. In other words the network configuration basically means taking into account the connection status of switching devices and circuit breakers and therefore the network structure.

In many countries the typical MV network consists of feeders that are operated in radial while they have one or more backup connections to the neighboring feeders. In the border between the feeders there is typically an open disconnector or switch. By selecting some other switches to be open the radial configuration of the feeder may be easily changed. This might be necessary, for example, in order to reduce the feeder losses or the voltage drop. In the future Smart Grids there are also other reasons to change the system configuration, which are for example originating from the market or energy management actions. The different network structures may have different protection requirements. For example, the protection requirements and settings are different for radial and closed ring operated feeders.

As the production in Smart Grids is varying the connection status of DG units must be known. Possibly even information on the fault current producing capability of DG units has to be available. The operation status of DG units translates to knowing their short-circuit producing capabilities. One example of this is a wind farm with multiple wind power plants with all of them connected to one point in the distribution network. The varying number of operational units affects the total short circuit current that the wind farm is able to produce.

Earthing arrangements need to be considered especially in the case where operating part of the network as microgrid is possible. The earthing arrangements can change upon transitioning to island operation, for example, in a case where normally the distribution network is centrally compensated. When the island is formed the connection to the central compensation is lost, and therefore the earthing is changed to isolated. Further complications may rise in cases with a decentralized compensation. The decentralized compensation is designed in a way that each compensation device compensates a predetermined length of the feeder. If the feeder length is suddenly changed due to changes in the network topology, such as opening or closing back-up connections or transitioning part of the network to microgrid operation, the length of the feeders and the compensation degree may change.

### Protection and control

As relays and protection systems become more advanced the difference between the protection and control functions becomes harder to distinguish as the functions are often present in the same physical devices [2], and perform the same functions. Some functions performed by relays such as reconfiguring the network after contingency are hard to categorize to either category as it has functions of both. Furthermore, [2] points out that as the adaptive protection concepts evolve the distinction between protection and control will become less precise. Similarities between the adaptive protection strategies and control can be found in the basic fundamentals of adaptive protection as adaptive protection requires feedback, and feedback is also an essential element of control. Some Smart Grid functions such as self-healing are closely related to both the protection and control. Self-healing of a faulted distribution network consists of both the protection and control actions. In a traditional sense the protection system isolates the fault and the control system automatically closes back-up connections or initiates the transition to microgrid. However, the line between the protection and control is not that straightforward as often both operations can be carried out from the same device and perform the same actions.

### Different levels of adaptivity

The adaptivity of the protection can be accomplished in different ways, but there can also be distinguished different levels of implementation of the adaptivity. Here a simple categorization is introduced ranging from traditional protection with no adaptivity to the future Smart Grid protection applying extensive adaptivity.

With the traditional distribution network protection as shown in Figure 2 the network configuration, which is typically fixed allowing only minimal variation, is first identified after which the appropriate settings are chosen basing on calculations made. After that the protection is ready to operate in the required way. Here the “protection” refers to the sequence of actions taken in any fault case. The sequence includes three steps: indication of fault, locating the fault (typically the faulted feeder) and isolating the fault by opening the breaker(s). This kind of scheme is passive and does not take into account any major changes in the network, such as possible connection of DG, because of which the protection performance may diminish due to the changes if the setting procedure is not repeated.

In an adaptive protection scheme the status of the network is constantly monitored and when a change is detected the protection settings are modified accordingly, and possibly even different protection functions and methods are taken into use. The protection from fault indication up to fault clearing follows the same principle as before. A clear difference when comparing to the traditional system is that some monitoring of the system status is needed. Typically this means that data of the system status is available from distribution automation system.

The Smart Grid protection goes one step further by introducing self-healing of the network. Self-healing can be based on several different predetermined specific strategies from which the most suitable one is chosen according to the prevailing system conditions. The protection and self-healing strategy can work simultaneously when the protection system isolates the fault and at the same time the self-healing strategy is executed. In this case the protection and control system operate in close cooperation where the latter one is responsible of the self-healing functionality. The essential feature here is that the adaptivity is extended both to the protection and control or automation functions.

In the figure below (Fig. 2) the realization of protection has been divided into three stages separated by the horizontal dashed lines. The first stage (Information) is a stage where information of the network configuration is gathered. In Smart Grids the first layer becomes dynamic since information of the system status and changes in it is continuously available. In the second stage (Adaption) the protection system is adapted to match the current requirements basing on the received information. In the adaptive and Smart Grid protection the settings and functions of the protection are constantly adjusted and in the Smart Grid protection also the self-healing strategy is chosen according to the current system status. All this is done automatically without human intervention while in the traditional protection the adaption phase consists of manual work and it is usually also done only once for the whole lifetime of the target system. The third stage (Operation) represents the actions to be taken. In all cases it includes the operation of the protection devices. For the Smart Grid protection stage there is also the self-healing after the protection. This includes the self-healing actions taken care by the automation system right after the fault is isolated.

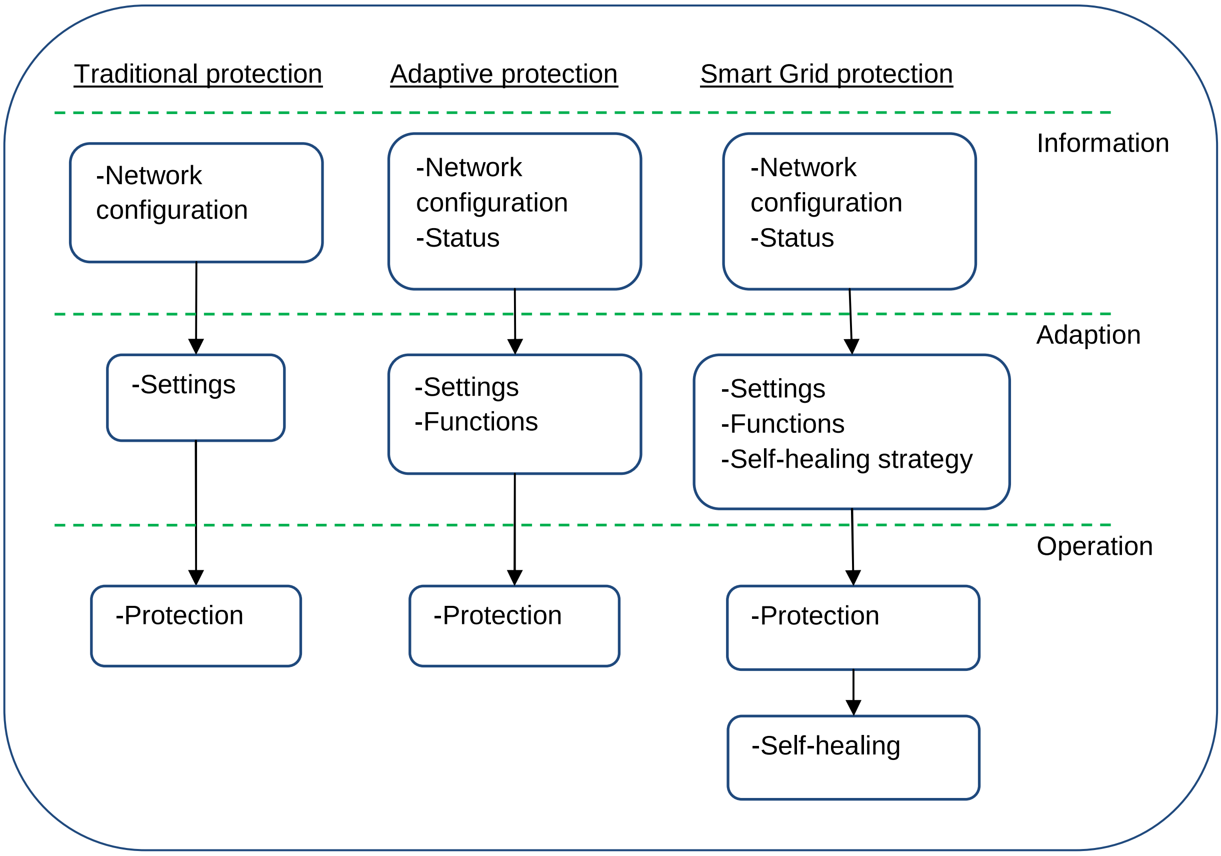

Figure 2. Different levels of adaptivity.

### Technical considerations

An increasing number of active resources will be connected to the Smart Grid. All these resources also need to be connected to each other with a communication channel. This is also the case with Smart Grid protection. The protection devices in Smart Grid must have communication capabilities to better use their potential and to achieve adaptive protection. Relating to communication also in most adaptive protection schemes more measurements are needed. The measurement data has to be swiftly transferred to any device that might need it.

The protection of the whole distribution network has to be based on well defined protection zones. Using protection zones allows isolating the fault to a single zone which can then be disconnected and separated from the rest of the network. The protection requirements of each zone not only depend on the zone configuration, for example if there is DG or not, but also on the configuration of adjacent zones as shown in Figure 3. In the Figure 3 the different protection zones are marked with different colors. The zones in the Figure 3 depict some of the different types of zones such as radial, ring and busbar. The configuration of zones can change with the switching status of the network, for example two or more radial zones can create a ring topology network. Smart Grid brings further considerations as varying amounts of DG can be connected to any protection zone. Ultimately even all the zones connected galvanically together affect to the protection requirements, as is the case with the earth fault protection in non-effectively earthed systems.

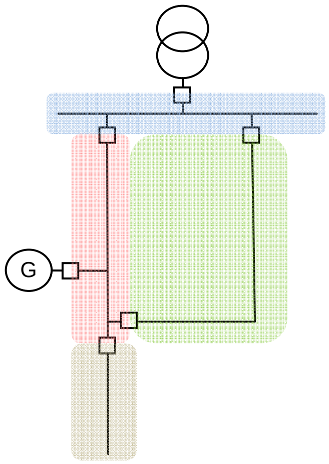

Figure 3. Division of the power system to protection zones.

The Smart Grid applications require interoperability between the different components of the power system, which can be provided by linking them together with communication and information technology [5]. The interoperability is needed not only for the protection devices, but also all the active devices connected to the Smart Grid require interoperability between them. This is supported in [5] and [6], which both identify reliable and real-time two-way communication as key factors of the Smart Grid infrastructure. For this reason a common communications standard is required, and today the IEC 61850 standard is looking like it will be a complete telecommunication solution for the future.

In certain cases it may be advantageous to change the protection method within a relay from one to another. With adaptive protection system this becomes possible. In changing system conditions the protection requirements may initiate a change to another protection method which better matches the requirements set by the new system conditions. In practice, this could mean that the active protection functions in each IED together with their settings are changed according the changes in the primary system in order to achieve optimal protection system performance. Enabling the use of different protection methods for different network configurations and even the use of different methods in different protection zones may be necessary to have acceptable protection speed and selectivity. Additionally, new protection functions and algorithms based on more than one method, so called multi-criteria, can be realized. More measurements will be needed if the network protection is to be realized with methods that require voltage to be measured in addition to current, therefore, the measurements needed in Smart Grid increase.

### Centralized and distributed decision making

Several adaptive protection concepts and strategies have been developed and presented for example in [7][8][9][10]. Among the different concepts some have been especially developed for Smart Grids and some others can be applied to Smart Grids. The adaptive schemes can be divided into two different approaches based on decision making behind the adaptivity; centralized and distributed decision making strategy.

The basic architectures of centralized and distributed decision making based systems are showed in the figure below (Fig. 4). Also on the figure (Fig. 4) the red color illustrates where the decisions considering the protection settings etc. are made. In the system based on centralized decision making there must be some centralized intelligence and decision making unit which constantly monitors the status of the network. Here this unit is named as the protection management system (PMS). When some change in the status of the network is detected the PMS provides new matching settings and setups for protection devices in the network. The IEDs in the network communicate with the PMS which handles all the communications needed to accomplish the adaptivity; collecting various information from the system and sending commands to IEDs to change settings and active functions. The communication channel used in controlling the adaptivity of the protection is required to be reliable and dedicated communication channel only for this purpose could be used. In practice the same communication media that is at least partially used directly for protection purposes (e.g. transfer trip and interlocking) can be utilized also for adaptivity management.

When the computing power of IEDs located in the network increases it enables more efficient local calculation and decision making. Tasks and functions can be distributed among several IEDs to increase the system performance and flexibility. This means that distributed decision making and intelligence is being used. One way to look at distributed decision making is that each IED is responsible of its own protection zone and adjusts the protection settings the best they can to accomplish this. A simple example of distributed decision making system is shown in Figure 4.

In reality a third option would be to use some kind of hybrid scheme where some decisions are made for instance at the substation and some at the local level. One example of this could be that the protected area for each IED and the network topology information are given from the PMS, but each IED then chooses the protection method, functions and settings to best suit the situation.

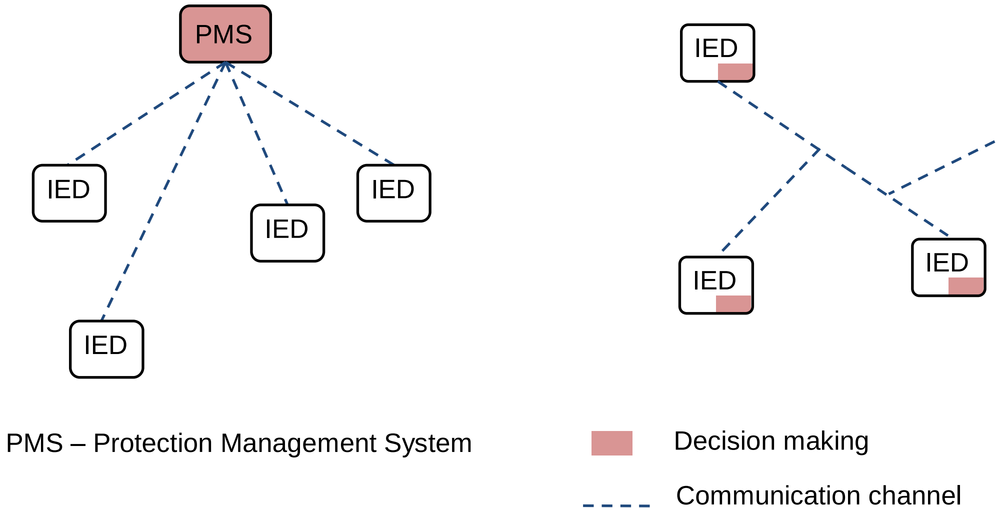

Figure 4. Adaptive protection schemes with centralized and distributed decision making.

The first version and at the same time the first steps of tackling protection related challenges and towards utilizing adaptive protection could be a centralized adaptive protection system where a number of predefined settings have been calculated for equal number of possible network configurations. In centralized adaptive strategy the connection and operating status of switching devices and DG units is transferred to the central management system which then calculates or takes into use predefined settings to match the new network status. This kind of centralized strategy is vulnerable to malfunctions in the communication network because the IEDs rely on the information sent from the central management system to change their settings. Some centralized adaptive strategies are proposed for example in [8] and [9]. In [9] the calculations of adaptive protection device's settings are carried out in the server of a centralized control center. The centralized control center uses status information and topology connection relations coming from SCADA system to confirm whether topology structure and operating mode change or not. Likewise in [8] the information of the network topology, which is changed when the operating status of DG units change, and the changes is it are transferred to the IEDs. The low pick-up setting for ground overcurrent protection is then dynamically adjusted based on local load current measurement.

In the distributed decision making scheme the different functions are divided between multiple devices. However, [7] reckons that when using distributed decision making challenges arise when functions need to be split over physical devices. In [7] it is also said that functions could be duplicated over several devices to handle this challenge and that active setting verification can be a distributed function meaning that the IEDs could locally verify the validity of their settings. One possible way to accomplish distributed adaptive protection is to use the agent technology [10]. When agent based technology is applied the system is generally called a multi-agent system which consists of several agents working together and communicating between each others to achieve a common goal. In [10] it is said that the agents are actually autonomous software entities that operate without human intervention, and they are also able to react to the changes in their environment. Furthermore, a multi-agent system has an interesting feature since they are proactive, so they may take initiatives in order to achieve the goal [10]. The control capabilities of multi-agent approach for Smart Grid have already been successfully demonstrated in [11], an adaptive protection concept based on multi-agents has been demonstrated in [10], and an agent based distance protection for Smart Grids is presented in [12].

The adaptive protection leaves some open questions remaining to be answered. One such question is that if some adaptive protection system would be implemented what would be needed for its successful implementation? The modern IEDs often support online change of settings but adding some new protection methods is usually not possible. Thus it would be worth to consider the possibilities to reprogram some of the IED functions online by uploading new protection functions or algorithms directly into the IED. For example if the admittance based earth-fault protection present in [13] would be intended to be used, could it be uploaded to the IED and taken into use. Another important question is how the functionality of the whole protection system can be tested?

## Required adaptivity of Smart Grids protection

In this chapter the most important adaptive features required from the Smart Grid protection will be presented through an example network shown in Figure 5. The different features include situations what will be needed for the adaptivity to take into account. The focus will not be on the protection methods or whether the used adaptivity is centralized or distributed. Instead, some different situations where adaptivity of the protection is needed will be presented. In the examples it is assumed that the IEDs can communicate with each other through fast communication channel, and that the IEDs form protection zones between them.

The successful protection of any network relies on the correct protection settings used at any given time. Therefore the key question is what the IED measures and how it will detect abnormal network conditions? Changing network conditions change the measured values in different fault cases. With this in mind the IEDs have to adapt to the new situation by altering their settings or taking new functions into use. Furthermore, in Smart Grids adjusting the protection settings is constant since active resources and distributed energy resources can change their operating status. The protection system needs to adapt to the changes in the network topology. Opening or closing switches changes the network topology and possibly affect the way relays detect fault conditions. Changing the connection status of the switch at IED 4 in Figure 5 changes the network topology. By closing the switch the network topology can change, and the network can become a part of either a closed ring or meshed network depending on the surrounding connections, or create a longer radial feeder. Opening the switch can shorten the radial feeder or change the topology from closed ring or meshed to radial. In addition, in Smart Grids different types of DG units can be connected to the network and the change in the operation status of the DGs can also change the network conditions in such a way that protection system should adapt to the new situation.

Adding DG to the network also creates the possibility to use part of the network as a microgrid. The transition to island operation creates challenges for protection which the protection system should adapt itself to. Additionally, the protection requirements for island and grid connected modes of operation can differ from each other greatly. The traditional overcurrent protection may be sufficient for grid connected mode but when operating in an island mode the traditional protection might not be sufficient anymore due to lack of short circuit current. The protection system should adapt itself to the new situation by taking protection settings designed for island operation into use. Likewise, when transitioning back to grid connected mode the protection settings should also be changed back to match the grid connected mode.

Self-healing can be achieved by transitioning part of the network to microgrid operation. An example of this is shown in Figure 5 where a fault is detected in the zone between IED 1 and IED 2. The remaining zones from

IED 2 to either IED 3 or 4 could then be operated as a microgrid and continue to supply the remaining customers. As shown in the Figure 5 it is possible to form different sizes of microgrids depending on the state of generation and load. The protection system should adapt itself to match the protection settings of the island size. When transitioning to island the earthing arrangements can in some cases change. One example of this would be if the network shown in Figure 5 is for example resonant earthed applying central compensation with one Petersen coil at the substation, and when the microgrid is formed the connection to the compensation coil is lost and therefore the earthing method changes. The protection settings must be changed to match the new earthing status of the network. Self-healing can also be achieved by closing a backup switch as shown in Figure 5. The whole self-healing strategy for the example network in fault case as depicted before could be to transition the zone between IEDs 2 and 3 to microgrid and closing the backup connection at IED 4. When using self-healing strategy where one or more back-up switches are closed the protection requirements and possibly current flow direction at the IEDs change and they must adapt to the new situation.

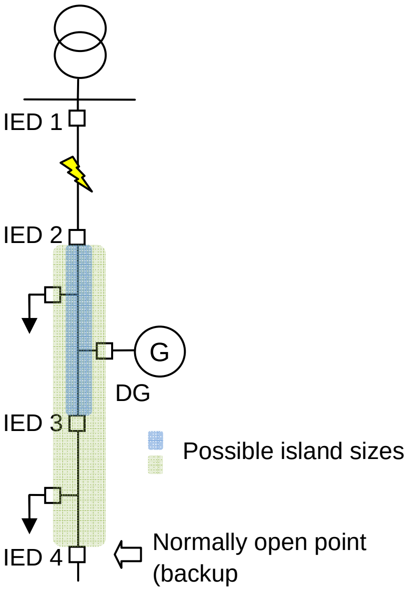

Figure 5. An example network.

## Conclusions

Adaptive protection has been studied to some extend since it was first introduced in the 1980's but still there is no unified adaptive protection solution describing precisely how the protection system should be realized. In this paper the adaptivity of protection required in Smart Grids has been discussed. An adaptive protection system for Smart Grids can be realized with two different decision making architecture. One is centralized strategy where the decisions are made centrally and the other is distributed strategy in which the decision making is distributed to different IEDs in the network.

Adaptivity of the protection is required due to various frequently happening changes in the Smart Grid; few examples are the changing grid topology due to switching actions, changes in the operating status of DG units and islanding of part of the network due to a fault and subsequent self-healing actions. Finally it can be stated that in order to fully utilize the potential benefits of various Smart Grid capabilities an adaptive protection system is needed that is actually self-aware of the changes happening in the network, and can select correct settings and protection methods matching the changed network topology and state.

## Acknowledgments

This work was supported by *Smart Grids and Energy Market (SGEM)* research program of CLEEN Ltd, the Strategic centre for science, technology and innovation of the Finnish energy and environment cluster.

## References

[1] European Technology Platform SmartGrids, “Strategic Deployment Document for Europe’s Electricity Networks of the Future”, Final Report, 20 April 2010. Available at: http://www.smartgrids.eu/

[2] Adaptive Protections and Control Final Report. CIGRE. 1995.

[3] D. Tholomier, D. Paraiso, A. Apostolov, Adaptive Protection of Transmission Lines, *Power Systems Conference 2009,* Clemson, USA 10-13 March 2009.

[4] K. Kauhaniemi, L. Kumpulainen, Impact of Distributed Generation on the Protection of Distribution Networks, *Developments in Power System Protection,* Amsterdam 5-8 April, 2004.

[5] V.C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati, G.P. Hancke, Smart Grid Technologies: Communication Technologies and Standards, *IEEE Transactions on Industrial Informatics, vol. 7 n.* 4, November 2011, pp. 529-539.

[6] D.M Laverty, D.J. Morrow, R. Best, P.A. Crossley, Telecommunications for Smart Grid: Backhaul solutions for the Distribution Network, *IEEE Power and Energy Society General Meeting 2010,* 25-59 July 2010.

[7] I. Abdulhadi, F. Coffele, A. Dysko, C. Booth, G. Burt, Adaptive Protection Architecture for the Smart Grid, *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies,* Manchester, United Kingdom 5-7 December 2011.

[8] H. Cheung, A. Hamlyn, C. Yang, R. Cheung, Network-based Adaptive Protection Strategy for Feeders with Distributed Generations, *2007 IEEE Canada Electrical Power Conference,* Montreal, Canada 25-26 October 2007.

[9] Zhongwei Li, Weiming Tong, Fengge Li, Shenghu Feng, Study on Adaptive Protection System of Power Supplu and Distribution Line, *2006 International Conference on Power System Technology,* 22-26 October 2006.

[10] K. Kauhaniemi, S. Voima, Adaptive Relay Protection Concept for Smart Grids, *Renewable Efficient Energy II Conference,* Vaasa, Finland 21-22 March 2012.

[11] M. Pipattanasomporn, H. Feroze, S. Rahman, Multi-Agent Systems in a Distributed Smart Grid: Design and Implementation, *IEEE/PES Power Systems Conference and Exposition, PSCE '09*, 2009.

[12] F. Kawano, G.P. Beaumont, K. Fukushima, T. Miyoshi, T. Shono, M. Ookubo, T. Tanaka, K. Abe, S. Umeda, Intelligent Protection Relay System for Smart Grid, *10th IET International Conference on Developments in Power System Protection (DPSP 2010),* March 29 – April 1 2010.

[13] A. Wahlroos, J. Altonen, T. Hakola, T. Kemppainen, Practical Application and Performance of Novel Admittance Based Earth-fault Protection in Compensated MV-Networks, *21st International Conference on Electricity Distribution,* Frankfurt, Germany 6-9 June 2011.