A Dynamic Modelling Environment for the Evaluation of Wide Area Protection Systems

I. F. Abdulhadi, R. M. Tumilty, G. M. Burt & J. R. McDonald
Institute for Energy and Environment, University of Strathclyde, UK
iabdulhadi@eee.strath.ac.uk

Abstract- This paper introduces the concept of dynamic modelling for wide area and adaptive power system protection. Although not limited to these types of protection schemes, these were chosen due to their potential role in solving a multitude of protection challenges facing future power systems. The dynamic modelling will be implemented using a bespoke simulation environment. This tool allows for a fully integrated testing methodology which enables the validation of protection solutions prior to their operational deployment. Furthermore the paper suggests a distributed protection architecture, which when applied to existing and future protection schemes, has the potential to enhance their functionality and avoid mal-operation given that safety and reliability of power systems are paramount. This architecture also provides a means to better understand the underlying dynamics of the aforementioned protection schemes and will be rigorously validated using the modelling environment.

I. INTRODUCTION

It is envisaged that future power systems will have different requirements so that they can operate more efficiently and meet security of supply regulations fully [1]. Future power system will be more flexible such that they can be operated optimally for pre- and post-fault conditions as well as be able to accommodate future generation mixes. Flexibility is also manifested by the advent of Flexible AC Transmission Systems (FACTS) such as series and shunt compensation in addition to power electronics based tap changers. Distributed Generation (DG) and especially generation capacity connected at the LV network in the form of micro-generation also poses new challenges in terms of protection and control [2].

Prevailing protection practices employ a fit and forget strategy where changes in settings usually involve manual adjustment by engineers when necessary (e.g. during network maintenance and reconfiguration). As the aforementioned system changes come into play, it becomes more difficult to sustain a satisfactory protection scheme performance. Adaptive/pseudo adaptive and Wide Area Protection Systems (WAPS) are foreseen to be important enabling technologies for the development of future power systems. Although at first glance WAPS may only be considered for transmission networks, some distribution network schemes may benefit greatly with system wide information. This is particularly true in MV networks with relatively higher levels of interconnection and distributed generation capacities. Due to the inherent risks associated with such protection schemes it is important to fully understand and qualify their performance. The main risk lies in using protection schemes with changeable settings in a safety critical system without having an appropriate level of confidence in their performance. In contrast to conventional distributed (non-centralised) protection where functionality is determined by local measurement and fixed settings, the dynamic nature of WAPS and adaptive protection poses new challenges that impede their wide scale adoption [3]. Nevertheless, it is possible to devise schemes where WAPS, including adaptive functionality, can be monitored and verified continuously to ensure their correct operation in response to system events. Where the protection fails to operate satisfactorily, contingencies are in place to avoid catastrophic system collapse caused by cascades. Additionally monitoring the response of more conventional forms of protection can aid in the mitigation of such risks.

This paper proposes a distributed protection architecture which aims to enable greater power system flexibility by continuous monitoring and management of protection schemes such that optimal operating conditions are created. Moreover, the dynamic modelling environment in question will act as a test harness through which the protection architecture can be validated by providing appropriate software modules to model the architecture and by managing inputs and outputs of a primary power system representation.

II. WIDE AREA PROTECTION SYSTEMS

A. Overview of Challenges

Modern power systems are increasingly operating close to their stability limits [4]. A number of recent blackouts have raised awareness of this issue. Steps have been put forward to prevent such occurrences including the use of WAPS which usually utilize information generated by phasor measurement units (PMUs) placed in strategic positions in a power system. WAPS mainly carry out protection functions such as load shedding and voltage collapse protection to avoid the cascade effect of blackouts. There are two major areas where protection schemes can benefit from wide area measurements – improved coordination as well as the potential for faster operation.

There are, however, a number of challenges that impede the deployment of WAPS on a wider scale or even on lower levels of the power systems (i.e. the distribution network). Customised WAPS may not be able to cope with all network events if not designed correctly. Improving their

performance lies in the efficient and timely use of the wealth of information generated by wide area measurements. Increased levels of information, however, may come at the detriment of slower operation of the protection due to the processing time required. Problems may also arise if the WAPS is of an adaptive nature. Changing settings in a flexible power system require concrete procedures to produce valid protection scheme states.

B. Current WAPS Practices

WAPS schemes currently in use can range from voltage collapse protection to under frequency load shedding (UFLS) that serve the purpose of maintaining system stability and avoiding blackouts. Conventional protection schemes, as of yet, have not made use of system wide information to enhance their functionality. A number of such schemes have been discussed but they are limited to simulation studies [5].

Different WAPS regimes may be used. These include enhancements to SCADA/EMS, flat architectures and multilayered architectures. This structural aspect is critical when considering the flow of system wide information and the overall coordination of the scheme. Particular regimes tie in closely with the distributed protection architecture under consideration. Consequently, the information exchange can be modelled readily which facilitates the understanding of the dynamics of WAPS data and its use.

III. Adaptive Protection Schemes

Adaptive Protection Schemes (APS) will be split into two types to simplify the following discussion. The first type will be called fully adaptive where the protection scheme or relay calculates the optimum setting at any given time. The second type will be referred to as pseudo adaptive where a number of predefined settings groups are available and selected from according to prevailing network conditions. The latter has been chosen for consideration in this paper due to its relative simplicity and the opportunity to validate such schemes in a more straightforward manner. It is also thought to bridge the gap between fully adaptive protection and conventional fixed setting protection. Moreover, adaptive settings can be applied in a WAPS based scheme.

The adoption of adaptive protection schemes have been slow and largely confined to an academic environment. However a number of widespread schemes that are simple in nature and are taken for granted do actually represent a form of adaptive protection such as voltage controlled over current protection [6].

When settings groups are used, network conditions can be covered for by assigning predefined protection settings. Fig. 1 illustrates the universal space 'U' where all possible network conditions are represented. A, B, and C represent three viable subsets of U, each of which defines a set of conditions for which one settings group holds. It may be difficult to demarcate the boundaries of each subset so that it can only be protected by a distinct settings group – this is depicted by the shaded area in Fig. 1. Such circumstances can be addressed in the design stage where specific criteria can be assigned to distinguish between the settings groups more clearly.

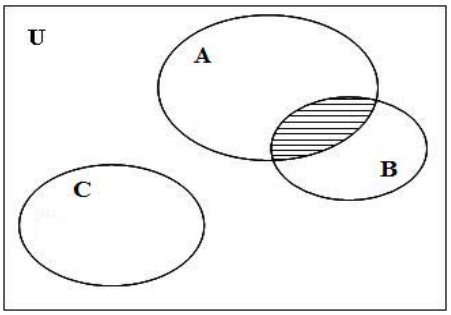

Fig. 1. System states and settings groups.

IV. The Distributed Protection Architecture

To better understand and facilitate the validation of future protection schemes, it is important to model such schemes and consider the various factors affecting their performance [7]. In order to achieve that, two steps must be taken. First of all, a representative protection scheme model devised, namely the protection architecture which is illustrated in Fig. 2. Secondly, a validation process must be must be applied to the model. This process is delivered by the dynamic modelling environment where it provides the means to emulate primary power system conditions and protection communications.

The distributed architecture assumes a multi-layered (stacked) structure. Each layer serves an abstract function in an overall attempt to create a suitable structure for the modelling of WAPS and APS. The following is a brief description of the individual layers.

A. Power System Information

Information used by the protection architecture is made available through a pool of data. This can be categorised into three subsets – primary quantities, phasor measurements and status data. Primary quantities are those voltage and current measurements made by local instrument transducers. On the other hand, system-wide phasor measurements are produced by PMUs. Finally, status data generated by different apparatus are also utilised by the architecture. Status data is usually in the form of binaries or indications of the present state of particular pieces of equipment.

B. Management Layer

Utilising power system information and identifying the required scheme response are the main functions of the management layer. It consists of two main functional elements: information handling algorithms and verification algorithms. The former manages the information available to protection relays. Each relay will require different amounts of information from different sources. This is governed by

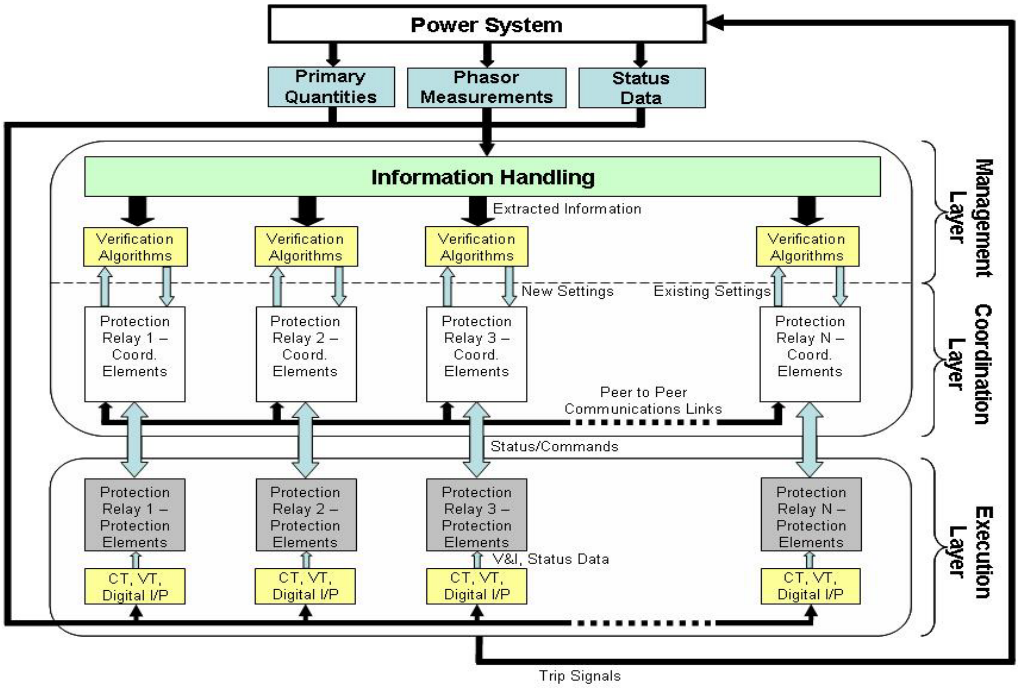

Fig. 2. The Distributed Protection Architecture.

factors such as redundancy (for reliability purposes) and the type of information. Special algorithms deal with information passed to it from the power system information pool. Relays are consequently fed with "filtered" information as appropriate. Although the information handling element is shown as a single entity in Fig. 2, it is possible to use a distributed architecture where individual protection relays are capable of selecting relevant information from a broadcast or otherwise. The verification algorithms, on the other hand, require two input streams to serve their function; these are information from the previous layer in addition to the protection scheme status which is represented by existing protection settings. These inputs allow the verification algorithms to continuously monitor the status of the protection scheme with reference to network conditions. Consequently, these algorithms can authorise the operation of the protection scheme or block it accordingly. Moreover, it can request the change between a set of predefined settings to create a more optimum state. The process in Fig. 3 shows, at a high level, how a typical verification algorithm may operate. As stated earlier, two sets of variables are continuously considered to determine the best choice of settings. It is possible that the verification algorithms may use some form of reliability or fault tree analysis for decision support [8].

C. Coordination Layer

This layer is responsible for ensuring that the coordination between protection relays in a scheme is maintained. Coordination includes time grading, protection zone arrangement, etc. Communication links are necessary to achieve the desired level of coordination. The architecture of the communications infrastructure can take many forms, the choice of which is depicted by the protection scheme requirements and relative merits of each communications topology (i.e. cost, redundancy, throughput, etc). Status data is most relevant to the coordination elements where a better understanding of the power system and protection topologies assists in delivering optimal protection settings.

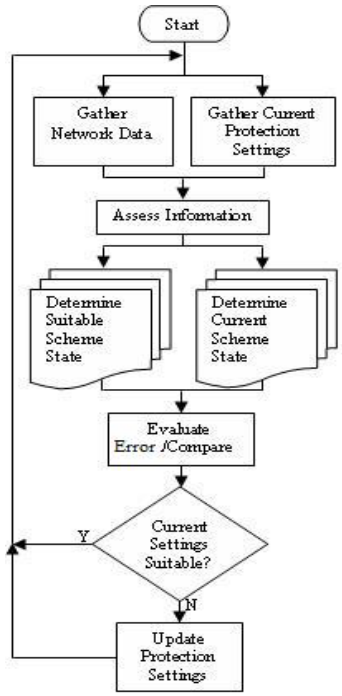

Fig. 3. Generic verification algorithm.

D. *Execution Layer*

This layer consists of conventional or adaptive protection algorithms with the latter having the ability to change between settings while in service. The settings changes are managed and coordinated by the previous functional layers according to the network and protection scheme states. In other words, the management and coordination layers are able to override or update the protection settings as appropriate. It thus forms a closed loop feedback system where the relay performance can be continuously assessed. The actual functionality of this layer can be delivered by either physical protection relays or dynamic software models of protection relays [9]. Although numerical protection relays are ideal for schemes where changing of settings is required, legacy relays can also be accommodated. The protection scheme with associated management and coordination functions will acknowledge this fact and operate accordingly.

V. The Dynamic Modelling Environment

A. *Environment Functions*

The distributed protection architecture discussed in the previous section requires a laboratory-based validation procedure. This is partly catered for by the dynamic modelling environment which performs three main functions. First of all, the environment feeds the appropriate primary power system information to the protection architecture under testing. It also routes tripping signals from the architecture back to the appropriate power system apparatus in a format suitable for the particular test setup in place (the test setup is discussed in section VI). Secondly, the environment provides a representative communications infrastructure fit for the protection scheme under consideration. This infrastructure also enables internal information exchange between layers to ensure compatibility. The third function is responsible for dynamically simulating different network states with the assistance of the power system information pool. Moreover, a user interface will be developed to allow monitoring the architecture's behaviour as well as changing its underlying functional parameters if required.

B. *Environment and Architecture Implementation*

The environment requires a degree of modularity in order to carry out its functions fully, facilitate testing and easily encapsulate the distributed protection architecture for validation purposes. This will be delivered to by a C++ based, object oriented engine. Moreover, precompiled libraries such as "SIM" and "CNCL" provide means of simulating discrete and event based dynamics which are applicable to the proposed protection architecture [10].

The modelling environment will be designed to be part of a larger integrated simulation system consisting of both software tools and hardware. This integrated simulation system can be thought of as a small scale power system simulator. Issues concerning interfaces and compatibility between the different components of the simulator need to be taken into account. Sound modular implementation and timely testing are key to mitigating these problems.

VI. Validation and Case Study

The modelling environment is an integral part of the protection architecture's validation. However, a dedicated test setup is needed to complement the environment's function. Fig. 4 shows a typical test setup. It includes a Real Time Digital Simulator (RTDS) to generate the power system information pool [11, 12]. On the other hand, the execution layer of the architecture is replaced by physical or modelled protection relays. The modelling environment manages the information exchange between the relays and the remaining layers of the embedded protection architecture.

A simple test scenario is presented here to illustrate the dynamics of the distributed protection architecture. This is not meant to be a new protection scheme design. The scenario is simply used to highlight the architecture's functional layers when viewed from a pseudo adaptive protection scheme standpoint. This scenario is an example of a problem encountered in a UK distribution system. This issue can be addressed using an adaptive protection scheme capable of changing between settings groups. Consider Fig. 5 which shows part of a primary substation. A graded overcurrent scheme is in operation where the protection for circuit breaker 2 (CB2) is a backup of protection devices downstream of it. Different current transformer (CT) ratios are used for the protection relays of CB1 and CB2. Should CB1 fail to operate, the higher CT ratio used for CB3's protection results in the prolonged exposure of the transformer T1 to fault current. This is particularly true for lower fault levels downstream of CB1. An adaptive protection scheme applied to this circuit could have rectified the problem by adjusting the overcurrent time multiplier setting of CB2's protection in order to shorten the time delay and avoid stressing the network assets. The failure of CB1 will notify the protection scheme and the setting of CB2's protection relay will be promptly switched to an alternative faster tripping one. The operation sequence of the scheme is shown in Fig. 6 where the management and coordination functions run in parallel to the power system events and prompt the change of the protection setting controlling CB2 to rapidly clear the fault.

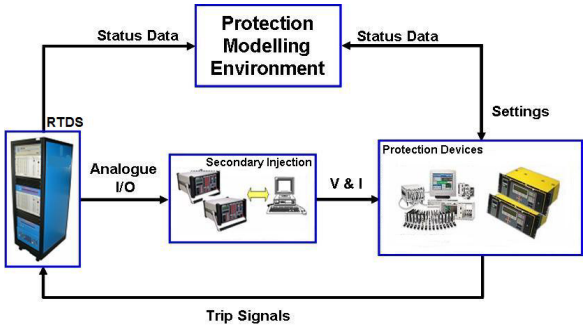

Fig. 4. Laboratory based validation setup for testing the protection architecture.

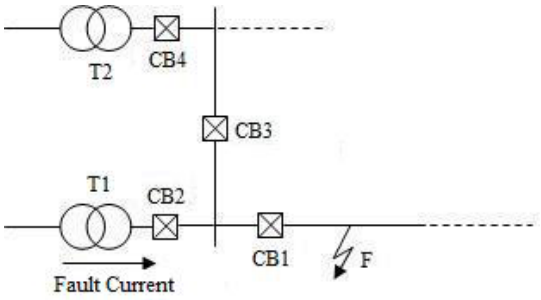

Fig. 5. Trip failure case study.

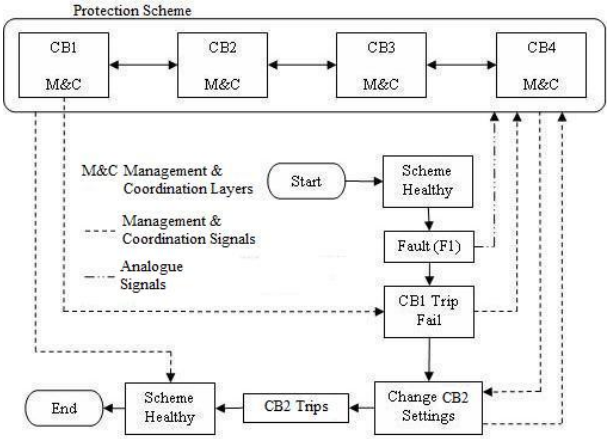

Fig. 6. Case study events sequence.

VII. Concluding Remarks

This paper has highlighted the main drivers behind the need for WAPS and APS. Their wide-scale adoption is challenged by the risk of unproven performance. In order to gain a better understanding of the dynamics of such protection schemes, a layer-based distributed protection architecture has been proposed. The architecture's layers are abstracted functionally, but at the same time provide a holistic representation of WAPS and APS that are able to optimise their performance in any given network condition.

Moreover, a laboratory based methodology is essential to validate the architecture. This is delivered by the dynamic modelling environment and is complemented by a set of peripherals including primary power system models and physical protection devices.

The environment effectively supports the architecture's internal and external information exchange as well as enables the user to have a better visibility of the dynamics of the underlying architecture. Further work is required to develop the functions of both the protection architecture and modelling the environment. Enhancements to the functional abstraction are also possible to improve the dynamic modelling of WAPS and APS.

Acknowledgment

The authors would like to thank the EPSRC for providing the financial support for this project as part of the SUPERGEN FlexNet consortium (Grant No. EP/E04011X/1). The authors would also like to extend their gratitude to ScottishPower EnergyNetworks for their comments and input.

References

[1] Elders et al., "Future Electricity Technologies and Systems", 1st Ed., Cambridge University Press, 2006, pp 24-79.

[2] R. M. Tumilty, M. Brucoli, G. M. Burt, T. C. Green, "Approaches to Network Protection for Inverter Dominated Electrical Distribution Systems", 3rd IET International Conference on Power Electronics Machines and Drives, 2006.

[3] A. G. Phadke et al., "Adaptive Protection as Preventive and Emergency Control", IEEE PES Summer Meeting, 2000.

[4] M. Begovic et al., "Wide-Area Protection and Emergency Control", Proceedings of the IEEE, 2006.

[5] J. Xiao, F. Wen, C. Y. Chung, K. P. Wong, "Wide-Area Protection and Its Applications – A Bibliographical Survey", IEEE PES Power Systems Conference and Exposition, 2006

[6] AREVA Transmission and Distribution, "Network Protection and Automation Guide", Chapter 17, pp 287-288.

[7] A. Dysko, J. R. McDonald, A. M. Carter, D. C. Humphreys, "Practical Use of a Dynamic Protection Modelling System", IEE 7th International Conference on Developments in Power System Protection, 2001.

[8] H. Seyedi, M. Fotuhi, M. Sanaye-Pansand, "An Extended Markov Model to Determine the Reliability of Protective Systems", IEEE Power India Conference, 2006.

[9] A. Dysko et al., "Dynamic Modelling of Protection System Performance", IEE 6th International Conference on Developments in Power System Protection, 1997.

[10] G. K. Fourlas, K. J. Kyriakopoulos, C. D. Vournas, "Hybrid Systems Modelling for Power Systems", IEEE Circuits and Systems Magazine, Vol. 4, Issue 3, 2004, pp 16-23.

[11] R. Kuffel et al., "A Fully Digital Power System Simulator Operating in Real Time", Canadian Conference on Electrical and Computer Engineering, 1996.

[12] Z. Q. Bo et al., "An Advanced RTDS Based Test System for Protection Relays", Proceedings of the 41st International Universities Power Engineering Conference, 2006.