21, rue d'Artois, F-75008 PARIS
http: //www.cigre.org

B5-117

CIGRE 2012

PERFORMANCE VERIFICATION AND SCHEME VALIDATION OF ADAPTIVE PROTECTION SCHEMES

I. Abdulhadi[1], F. Coffele, A. Dyśko
C. Booth, G. Burt
University of Strathclyde
UK

G. Lloyd
B. Kirby
Alstom Grid
UK

SUMMARY

A strong technical evidence base has demonstrated that existing protection scheme performance is suffering due to changes in the primary power system and the increasingly unconventional operation of utility networks. Investments in the UK transmission network in particular aim to enable the delivery of significant renewables capacity through the introduction of more series compensation, HVDC links and quadrature booster transformers [1]. Furthermore, these assets provide the flexibility in system operation which alleviates stress from a highly constrained system. These changes to the network come with their own set of challenges in terms of maintaining acceptable protection performance and indeed the selection of appropriate settings.

Adaptive power system protection is seen to address some of the performance issues with existing protection schemes. Both utilities and manufacturers are discussing this topic more openly as a means of coping with and enabling the changes in power system operation. Despite offering a compelling technical advantage over conventional protection practices, the lack of adaptive protection testing methodologies remains one of the main barriers to adopting such a protection strategy. To this end, this paper discusses the difficulties associated with adaptive protection testing. It then follows on by defining fundamental functional and performance requirements, which provide a stepping stone to enable effective testing. The functional requirements are emphasised through an architecture that was proposed previously in [2]. Defining a rigorous architecture is arguably an essential prerequisite to achieve effective adaptive protection testing.

The paper focuses on two aspects of adaptive protection testing. The first aspect is the verification of adaptive protection logic based on functional design. The absence of adaptive protection testing standards means that the verification exercise must resort, in the first instance, to formal methods that ascertain the possibility of violating the adaptive scheme design. This also includes determining the appropriate settings or setting ranges allowed during the adaptation process. Secondly, the validation of overall adaptive protection schemes is discussed. In this case, industry standards (e.g. IEC 60255) still hold. However, tests defined in these standards must be complemented by application driven testing scenarios that lead to the stimulation of the adaptive logic as appropriate. Validation platforms and tools are also investigated while communications testing is given particular attention. The scope of the testing covered in this paper is restricted to those tests carried out prior to placing the scheme in service. Therefore, commissioning tests are not discussed in detail. Furthermore, hardware or platform testing is also not discussed as the main concern with adaptive protection testing is the validity of its

[1] iabdulhadi@eee.strath.ac.uk

behaviour as opposed to the reliability of the hardware or its compliance to relevant standards which are considered trivial relative to the behaviour validation challenge.
Adaptive distance and overcurrent protection schemes were prototyped and tested in line with the methodologies discussed in this paper. Results for these tests are presented and comments are made on the issues that remain to be tackled.

KEYWORDS

Power System Protection - Adaptive Protection - System Requirements - System Validation and Verification - Scheme Life Cycle - Real Time Simulation.

1. EXISTING PROTECTION SCHEME PERFORMANCE AND THE NEED FOR ADAPTIVE PROTECTION

Recent power system blackouts that were characterised by protection scheme mal-operation highlight the less than satisfactory performance some existing protection schemes are offering especially under stressed conditions [3]. Investments to alleviate network constraints are at the top of the agendas for network operators [1]. This is especially the case where increased renewable generation is to be connected at transmission level. Planned FACTS and HVDC installations are at the core of these network improvements.
There is no doubt that some of these network technologies can negatively impact the performance of installed protection systems. For instance, the use of thyristor controlled series compensation (TCSC) can result in distance protection reach errors as well as polarisation issues due to current inversion [4], [5]. Furthermore, inadequate TCSC control can give rise to sub-synchronous resonance (SSR) [6]. Coordinated control of quadrature booster (QB) transformers used to manage steady state power flows can also result in distance protection reach errors [7]. When such devices are used dynamically, fixed protection settings may not be adequate and the cited works show evidence that there is a real risk of protection mal-operation or failure to operate. Finally, wide-area disturbances have resulted in their fair share of protection mal-operations with sometimes devastating effects as was the case in the 2003 blackouts [8]. Similar issues are faced at the distribution level, which are mainly caused by increased levels of distributed energy resources (DER) [9].
The common denominator in most of the cases and others omitted is inadequacy of active protection settings for given situations. In the case of TCSC, knowledge of the device's operational mode can be directly translated into a more suitable setting that is dynamically selected as appropriate to minimise distance reach errors. Moreover, dynamically blocking the operation of the distance protection third zone during over-load conditions can mitigate unwanted line tripping. Dynamic settings changes can be achieved through adaptive protection logic. Such logic can monitor the state of the primary system including primary plant status and alter the settings of the protection system as appropriate. Before delving into the main subject of the paper – that is adaptive protection verification and validation, the concept of adaptive protection and approaches to achieving it will be discussed.

2. APPROACHES TO ADAPTIVE PROTECTION

A definition of adaptive protection adopted by the IEEE can be found in [10]. This states that "adaptive protection is a protection philosophy that permits and seeks to make adjustments automatically in various protection functions to make them more attuned to prevailing power system conditions". This definition indicates that the main objective of adaptive protection is to maintain acceptable protection scheme performance under different power system conditions through automatic re-configuration of the protection IED. It is assumed that an IED is required as it is not feasible to automatically change the protection configuration with older generation protection relays. The protection reconfiguration can be approached in two distinct ways. The first method involves selecting an active setting from a number of pre-configured protection settings as deemed appropriate for the prevailing power system conditions. An example of this is the use of different settings groups. Each can cater for a specific mode a FACTS device may operate at within a protected line. The use of pre-

calculated protection settings groups (SG_1, SG_2, … , SG_n) limits the uncertainty of possible active protection settings at any given time. The calculation of these settings groups is subject to system studies that are carried out on a case by case basis. A settings group is identified for each set of foreseen primary system states. The activation of a particular settings group takes the form of a one to one mapping between a primary system state and a corresponding settings group. Figure 1 shows a functional diagram where adaptive logic activates the appropriate settings group based on primary system conditions. The primary system conditions can be obtained from status indications of circuit breakers or FACTS devices in addition to conventional system measurements.

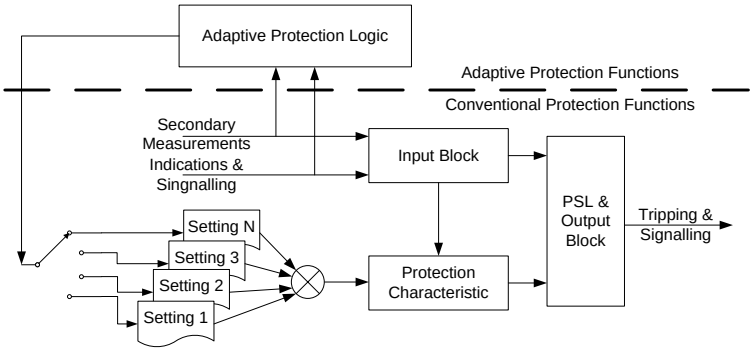

Figure 1 Adaptive protection logic used to activate a suitable settings group

The second method involves calculating new protection settings on the fly in response to a change in system conditions. For instance, the re-grading of IDMT protection along a ring distribution feeder may be necessary should the network topology change [11]. In this case, the network fault level has a direct impact on tripping times. Therefore, the calculation of optimised settings by considering the network fault level is more favourable to the use of pre-determined settings groups. In contrast to settings groups, calculated settings lead to more uncertainty in the knowledge of active settings at any given time. This can be rectified by placing hard limits on the allowed range of settings. These limits can be determined through network studies under different operational states (e.g. topology changes, DG penetration levels).

3. ADAPTIVE PROTECTION REQUIREMENTS AND ARCHITECTURE

A standard bay solution specification by a utility will contain typical functional and performance requirements. Furthermore, the manufacturer will reflect these requirements in their protection offerings as well as producing capable relaying platforms. These requirements are influenced by the different life cycle stages a scheme goes through. From an adaptive protection scheme point of view, the elicitation of scheme requirements is at the core of this lifecycle. Table 1 lists a number of requirements that are not specific for a particular scheme.

Table 1 Requirements for adaptive protection schemes

User Requirements	Functional Requirements	Performance Requirements
Utilisation of existing functions and equipment	System event detection and qualification	Application/network/scheme dependent
Standard function interfaces	Protection performance evaluation	Maintain existing specified performance levels
Definition of conditions which sanction adaptive protection actions	Online verification of adaptive protection actions	Implementation/platform dependent

Facilitating substation integration is a major user (utility) requirement. Achieving adaptive protection functionality should make use of the existing substation infrastructure and indeed existing protection devices. Additional investment into information and communications technology (ICT) systems may

be necessary, however standard interfaces and data models must be used to facilitate the integration of the adaptive functions and at later stage their replacement when necessary.
The functional requirements of an adaptive protection scheme revolve around the valid selection of new protection settings in response to system events specified by the user. This necessitates developing self verification functions which evaluate the performance of standard protection elements at the active setting and then sanction setting changes when necessary. Additional verification functionality is also necessary to check whether the new protection settings were correctly applied in the target devices. The performance requirements are twofold – those specific to the scheme functionality and those related to the adaptive scheme implementation. Standard scheme performance requirements defined by utilities and international standards remain applicable in this case. For instance, a reach of around 150% for distance protection second zone should not be affected by the addition of adaptive functionality. In fact, the adaptive protection functions must ensure that this reach is maintained should it be affected by the presence of a FACTS device for instance. Conversely, the adaptive scheme implementation has a great bearing on the performance requirements. For example, if the adaptive functionality requires a communication link to interrogate plant status information, the link requirements (e.g. latency, availability) must be specified on an application basis. Once these requirements have been identified, they will serve as a reference point for testing procedures discussed in the following sections.
Defining a structural model is a powerful means of capturing the different scheme requirements. The architecture proposed by the authors in [2] provides this desired structural rigor. Since the architecture is functionally abstract and defines the interfaces between its constituent elements, the process of integrating these elements is facilitated. Moreover, the architecture acts as a starting point for modelling, developing and implementing the required adaptive functionality through a model based design (MBD) approach. Consequently, efficient sub component and overall system testing can be achieved [12]. The architecture of [2] is shown in Figure 2. In this instance, it illustrates a couple of functional verification units that encompass a number of scheme sub components under test.

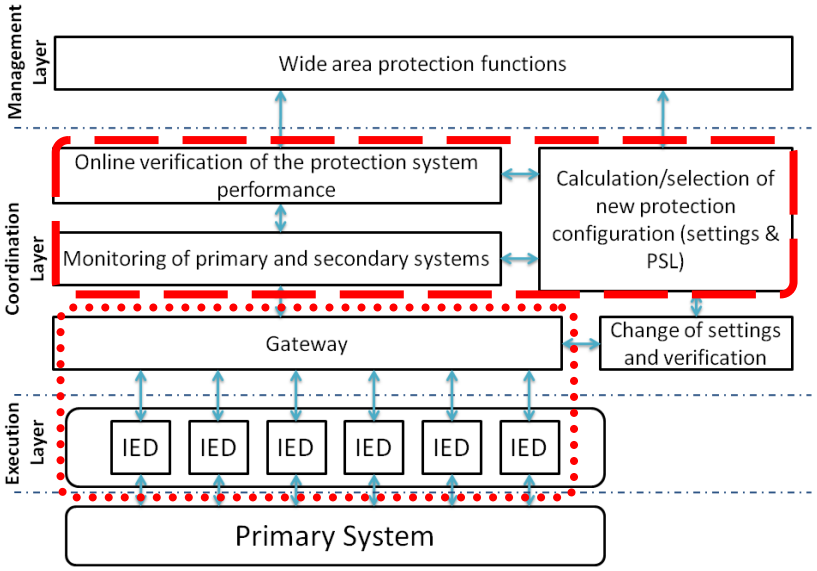

Figure 2 Adaptive protection architecture illustrating verification units

The dotted region in Figure 2 indicates a testing unit boundary. This particular functional unit requires verifying the correct exchange of information between the IEDs and the adaptive functions contained within the coordination layer through the communications gateway. Furthermore, the dashed region outlines the unit within which the correct setting selection in response to primary system events can be verified. Eventually, a validation of the overall system is necessary to ensure correct behaviour and that any integration issues are identified. A detailed account on how this verification may be achieved is described in the following section.

4. VERIFYING THE PERFORMANCE OF ADAPTIVE FUNCTIONS

Protection schemes designed with a fixed setting rely on being robust against a well understood set of power system operating conditions. However, a shift in these operating conditions, as discussed earlier, can cause deterioration in their performance. By adopting an adaptive protection strategy it can become difficult to create a direct relation between power system conditions and adaptive setting selection/calculation. Therefore, one of the main challenges of adopting an adaptive protection philosophy is verifying its functionality to remove potential uncertainty in its behaviour. The problem of verifying the performance of the adaptive functions entails two main tasks:

- Functional verification: at design stage, adaptive setting selection/calculation algorithms' output must be defined in relation to primary system states. When the adaptive functions are developed their outputs are continually tested in response to simulated primary system stimuli. This usually results in iterative modifications to ensure that functional requirements are met.
- Software verification: in addition to ironing out software bugs, it is important to provide sufficient code execution coverage while testing adaptive setting selection/functions. The fact that power system states leading to a change in settings can be variable in range and nature means that a representative set of testing scenarios is required to ensure that the software meets specifications.

Figure 3 illustrates how the process of adaptive logic functional verification can be achieved. The main objective of this verification procedure is to determine the correct setting selection in relation to the primary system state. This is done in isolation of the protection functions, as this process is a pre-requisite to the overall protection scheme validation. The primary system state inputs include the relevant information required by the adaptive logic, especially status indications of primary plant. The setting selection corresponding to each system input is recorded and verified against the logic design.

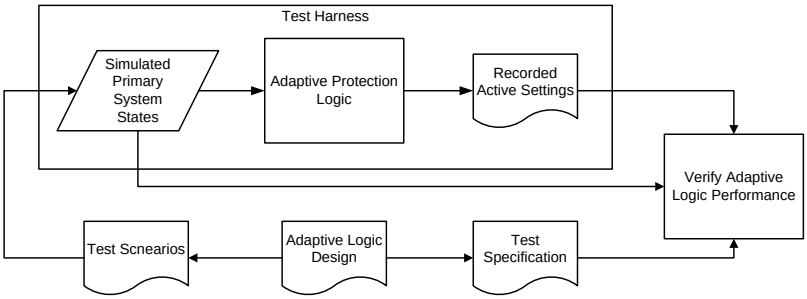

Figure 3 Unit testing of adaptive logic to verify its performance

The verification procedure illustrated in Figure 3 is simulation based. Formal verification methods can also be used. These refer to methods which examine certain properties of the system under test and qualify their performance through rigorous formulation. Such properties include the stability and determinism of the adaptive logic. Stability of the adaptive logic relates to setting changes in response to system events. When an event occurs in the power system, then the adaptive protection functions can respond to this event in the form of a setting change if necessary. The adaptive setting selection should be stable against perturbations in the power system that do not warrant changes in protection configuration. This logic stability requirement places the burden on the functions which determine the power system state based on measurements. Determinism from the point of view of the adaptive logic means that if the current state of a protection scheme is known, then its behaviour is known for any power system input. Achieving a deterministic adaptive protection scheme is important to ensure that the setting changing behaviour is well understood in relation to varying power system conditions.
Performing formal verification on the adaptive functionality requires an accurate representation of the behaviour of the adaptive system. This means that a form of transfer function must be formulated for this purpose. Adaptive scheme states can then be determined with the knowledge of primary system states. The model of the adaptive protection logic at earlier development stages can be used to derive this relationship by observing its behaviour during simulation.

5. VALIDATION OF ADAPTIVE PROTECTION SCHEMES

5.1. SCHEME FUNCTIONAL VALIDATION

The process of validating the performance of an adaptive protection schemes involves two stages – offline scheme validation and on-site scheme validation. The former can be considered as a form of factory acceptance test (FAT) of the full scheme while the latter is comparable in scope to site commissioning tests (SCT). The on-site validation may encompass a trial period of successful operation of the protection scheme before being connected into full service and rolled out onto other parts of the system. For wide area adaptive protection schemes there may be difficulties in obtaining outages for all the circuits needed so offline testing is more important in these situations provided that an appropriate primary system model is used to capture the wide-area phenomenon under question. As indicated earlier, the on-site testing is not discussed further as it is out with the scope of this paper. A scheme functional validation aims to test the overall functionality of all the scheme components – that is the adaptive logic in addition to the protection IEDs and supporting infrastructure. Assuming that the individual elements have been functionally verified, the functional validation is effectively a black-box type of test where the operation of the scheme in response to system events must be established in relation to the test specification.

The use of protection test sets or real-time hardware in the loop (HIL) simulation are common protection scheme validation methods [13]. These methods remain valid for adaptive protection testing. However, it is necessary to expand the typical set of fault testing scenarios to include changing primary system conditions such as changes to primary system plant status, topology changes, wide-area disturbances, etc. HIL testing is most effective when code generated from the original functional model of the adaptive functions is used as part of the testing loop. Tools such as Simulink can be used to achieve this and bridge the gap between the functional model and prototype/device under test.

Appropriate tools are necessary to perform the testing procedures as well as to collect and analyse the outcomes of the results. As the complexity of the protection scheme increases, the amount of testing and nature of tests can produce high volumes of data that are difficult to cope with manually. Testing engineers, especially from the utilities' point of view do not necessarily need visibility of the underlying low level testing procedures.

5.2. COMMUNICATIONS TESTING

As adaptive protection functions rely on communications to gather system information and activate new protection settings, it is important to assess the impact of communications or lack of on the performance of the adaptive protection scheme. Moreover, a fall back strategy should be built into the adaptive logic such that the occurrence of a communications failure mode does not result in complete scheme failure or mal-operation (i.e. the scheme should degrade gracefully). Therefore, the adaptive schemes ability (by design) to cope with communication failure must also be verified.

Inaccurate assumptions are usually made when incorporating communications into protection scheme models and testing procedures. For instance, a point to point communications topology is assumed or a fixed time delay is used to represent communications interactions between multi-device schemes. This may be sufficient when testing a simple two ended scheme over a deterministic communication channel. However, when adaptive protection functions rely on multiple sources of information to calculate settings in addition to communicating the outcome to multiple protection IEDs, the impact of communication failure becomes all the more important to understand. This requires more accurate communication models that reflect substation arrangements and protocols. This can be achieved using communications systems emulation. Open source emulators or otherwise can be used to introduce communications channel delays, data corruption and packet loss. Some communication standards have built in test modes such as IEC 61850 test flags which facilitate the testing of logical node operation [14]. Where multivendor IEDs are used in adaptive protection schemes and peer to peer messages between IEDs are used, the system integrator and tester must learn how to use all the configuration and testing tools provided by each manufacturer. This imposes a significant burden and may have a negative impact on the quality of the protection system and quality of testing. Standardisation of configuration and testing tools is important in the future to enhance the testing of such schemes.

6. TEST CASES

6.1. ADAPTIVE DISTANCE PROTECTION FOR TRANMISSION LINES WITH QUADRATURE BOOSTER (QB) TRANSFORMERS

QBs have an impact on the reach of distance protection relays upstream of the transformer [7]. One way of addressing this issue is to dynamically extend distance zone reaches in order to compensate for the under reach. The approach used in this case relies on two settings groups where SG_1 is the default case and SG_2 covers for the worst case scenario when the QB is energised. Switching to the second SG is determined by the state of the QB and tap position. This adaptive logic was presented by the authors in [2], [7].

The adaptive protection logic was modelled in Simulink and a test harness was also developed in Simulink around the adaptive logic in order to verify its behaviour in line with the functional design. Furthermore, automatic code generation was used for direct implementation into the target (in this case an industrial PC). This eliminates errors introduced by manual coding and maintains code consistency by enforcing variable types and standard function structures. The test harness is similar to that shown in Figure 3. It essentially forms a functional test unit of the adaptive protection code. Eventually, the behaviour of the adaptive scheme implementation can be validated against that of the original Simulink model. The adaptive protection logic requires knowledge of the QB status in order to select an appropriate settings group. Therefore the verification procedure involves stimulating the adaptive logic through changing the QB state in an attempt to affect the reach of the distance protection. In order to provide sufficient testing coverage, a pseudo-random binary sequence (PRBS) with appropriate limits was used to represent the QB status indications fed to the adaptive logic. Generating this signal is readily available using the signal generator block in Simulink. Using a PRBS not only offers an exhaustive means of testing scenario generation, but is also repeatable with knowledge of the initial state and sequence seed [15]. Line loading and circuit topology information were also used to identify instances of load encroachment and mis-coordination. To better visualise the performance of the adaptive logic, a number of protection 'performance states' were defined: (1) Over/under reach – this is caused by the failure of the adaptive logic to reflect the state of the QB through an appropriate settings group; (2) Load encroachment – occurs when extending zone reaches during circuit overloads. If no load blinders are present, the zone extension is blocked until circuit loading is reduced; (3) Mis-coordination – extending the second distance zone must be executed while taking into account adjacent short lines to avoid mis-coordination.

Figure 4 illustrates a testing iteration. The different performance states are shown in a binary or enumerated fashion. Changes in QB mode can result in a temporary error in protection reach. This is due to the finite time required to change to the correct setting. In this case the time delay is a single simulation time step. Therefore, not only performance state information is required to verify the design, but the time spent in each of these states is also required. The experience of developing the test harness underlined the importance of the adaptive functions information exchange. Adopting a unified information model throughout scheme modelling, prototyping and testing reduces the overhead in the adaptive scheme lifecycle. It also streamlines the process of testing since additional information handling/conversion interfaces are redundant.

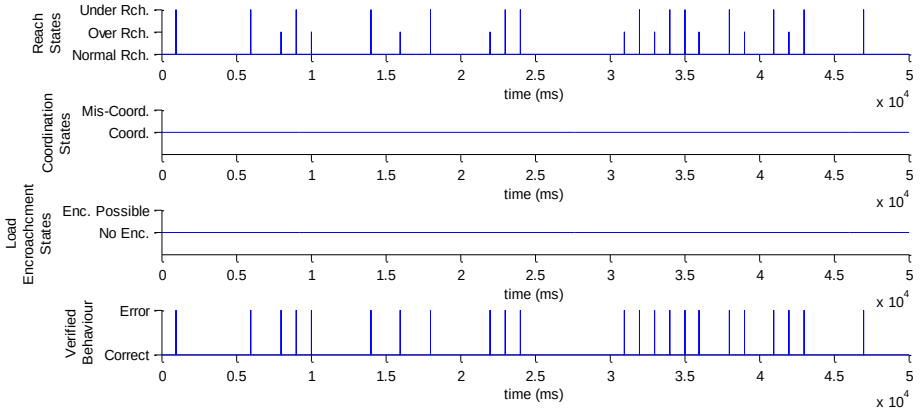

Figure 4 Protection performance states and verified behaviour indications

6.2. ADAPTIVE OVERCURRENT PROTECTION FOR DISTRIBUTION NETWORKS WITH AUTOMATIC LOAD RESTORATION

Distribution network topology changes, such as those resulting from automatic load restoration, have an impact on the overcurrent protection performance [11]. A particular issue is related to the loss of discrimination between adjacent relays on either side of a normally open point (NOP) in a ring distribution feeder when the NOP is automatically moved for load restoration purposes following a fault. Adaptive logic was developed to re-grade the overcurrent protection on the ring and ensure correct discrimination between relays in series.
HIL simulation was used to validate the whole scheme. This involved running a number of topology and fault scenarios to comprehensively test the adaptive logic's ability to correctly calculate the new settings based on the new network topology. Figure 5 illustrates a scheme monitor that logs testing scenarios which includes the status of the simulated network and the resulting response of the adaptive logic. The objective of the test is to validate the functionality of the overcurrent scheme in accordance with typical requirements specified by international standards (e.g. IEC 60255). In this case, the tests are only valid when the adaptive logic is stimulated through changing the primary system state (i.e. topology changes) in addition to typical fault scenarios.

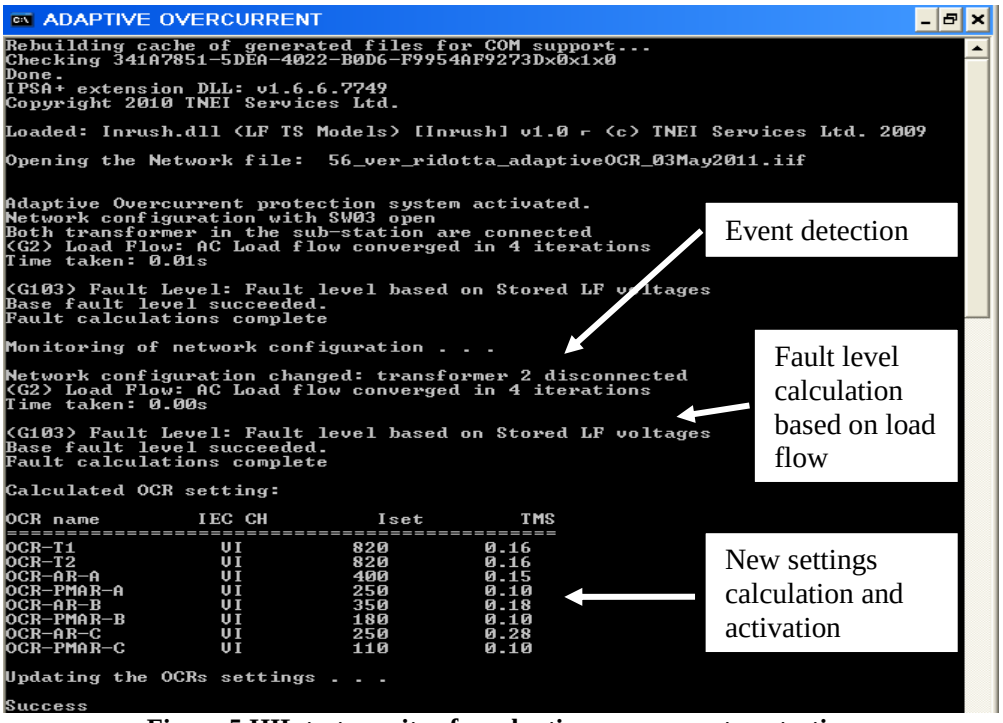

Figure 5 HIL test monitor for adaptive overcurrent protection

One of the main issues that arise from the validation tests is the potentially large amount of data contained within the test log. This requires post processing to determine the correct response of the adaptive protection scheme to network events. It may then be necessary to employ automated data analysis which compares the obtained protection behaviour with the expected one in light of the network events. It is unlikely that advanced knowledge discovery (e.g. data mining) is necessary to ascertain anomalies in the scheme performance from the testing log – the verification process discussed earlier attempts to address these potential issues especially those stemming from adaptive logic behaviour uncertainty.

CONCLUSIONS

This paper underlines the importance of adaptive protection testing. Although existing testing practices are still valid for fulfilling parts of the tests, it is necessary to complement them with tests that specifically target the adaptive functionality. Achieving adaptive logic verification relies on

stimulating the logic inputs and observing its behaviour against the functional design. As the observed logic behaviour may not be binary in nature, it may be necessary to create an abstraction of the behaviour which reflects the performance metrics being verified. Incorporating the conventional protection functions and communications infrastructure within the adaptive scheme requires an efficient means of validation. White box testing already used is resource consuming with multifunctional IEDs. Therefore, the validation of the full scheme must be approached in light of the pre-verified adaptive logic. This means that targeted black-box fault scenarios coupled with network changes that stimulate the adaptive logic should be conducted. The measured protection performance can then be directly compared with utility requirements which are usually aligned with international standards.

One of the immediate steps that can be taken to facilitate the testing of adaptive protection, is to adopt a model based design approach to model and develop the adaptive functions. Using common tools such as Simulink enables efficient design, simulation and automatic code generation. This approach greatly reduces verification testing time as well as code debugging time. Furthermore, work is necessary to find ways of porting new testing methodologies into usable tools that can be readily integrated within utility and manufacturer verification and validation procedures. These tools should also include automated post-testing results analysis.

BIBLIOGRAPHY

[1] ENSG "Our Electricity Transmission Network: A Vision for 2020."2009.

[2] I. Abdulhadi, F. Coffele, A. Dysko, C. Booth, and G. Burt, "Adaptive Protection Architecture for the Smart Grid," in Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2011 IEEE PES, 2011.

[3] J. De La Ree, Y. Liu, L. Mili, A. G. Phadke, and L. DaSilva, "Catastrophic Failures in Power Systems: Causes, Analyses, and Countermeasures," Proceedings of the IEEE, vol. 93, no. 5, pp. 956–964, May 2005.

[4] M. Khederzadeh and T. S. Sidhu, "Impact of TCSC on the protection of transmission lines," Power Delivery, IEEE Transactions on, vol. 21, no. 1, pp. 80–87, 2006.

[5] H. J. Altuve, J. B. Mooney, and G. E. Alexander, "Advances in series-compensated line protection," in Protective Relay Engineers, 2009 62nd Annual Conference for, 2009, pp. 263–275.

[6] R. A. Castro and H. A. Pineda, "Protection System Considerations for 400 kV Series Compensated Transmission Lines of the Central Western Network in Venezuela," in Transmission & Distribution Conference and Exposition: Latin America, 2006. TDC '06. IEEE/PES, 2006, pp. 1–5.

[7] I. F. Abdulhadi, G. M. Burt, A. Dysko, R. Zhang, and J. Fitch, "The evaluation of distance protection performance in the presence of Quadrature Boosters in support of a coordinated control strategy," in Developments in Power System Protection (DPSP 2010). Managing the Change, 10th IET International Conference on, 2010, pp. 1–5.

[8] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," 2004.

[9] K. L. Butler-Purry and M. Marotti, "Impact of Distributed Generators on Protective Devices in Radial Distribution Systems," in Transmission and Distribution Conference and Exhibition, 2005/2006 IEEE PES, 2006, pp. 87 –88.

[10] IEEE, "IEEE Std. C37.113-1999: IEEE Guide for Protective Relay Applications to Transmission Lines," IEEE, 2000.

[11] F. Coffele, C. Booth, G. Burt, C. McTaggart, and T. Spearing, "Detailed Analysis of the Impact of Distributed Generation and Active Network Management n Network Protection Systems," 2011.

[12] B. Kirby, L. Zou, J. Cao, and I. Kamwa, "Development of a predictive out of step relay using model based design," presented at the Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2011 IEEE PES, 2011.

[13] P. Forsyth, T. Maguire, and R. Kuffel, "Real time digital simulation for control and protection system testing," in Power Electronics Specialists Conference, 2004. PESC 04. 2004 IEEE 35th Annual, 2004, vol. 1, pp. 329–335 Vol.1.

[14] D. S. Ouellette, M. D. Desjardine, and P. A. Forsyth, "Using a real time digital simulator to affect the quality of IEC 61850 GOOSE and sampled value data," in Managing the Change, 10th IET International Conference on Developments in Power System Protection (DPSP 2010), 2010, pp. 1–5.

[15] M. G. Bartley, D. Galpin, and T. Blackmore, "A comparison of three verification techniques," 2002, p. 819.