Reachability Analysis for the Verification of Adaptive Protection Setting Selection Logic

Ibrahim Abdulhadi, *Member, IEEE,* Adam Dyśko, *Member, IEEE,* Graeme Burt, *Member, IEEE*

***Abstract*--The testing of adaptive protection schemes is a problem that remains largely unaddressed. These schemes can be characterized by uncertainty in behavior due to the dynamic changes in their configuration to suit prevailing network conditions. This paper proposes a novel approach to formalizing this behavior using hybrid systems modeling. This unlocks the ability to verify the safety performance of the schemes using reachability analysis. In this paper, an adaptive setting selection logic for distance protection is verified for its safety, using reachability analysis, during changes in network conditions.**

***Index Terms*--Adaptive relaying, distance protection, hybrid systems, reachability analysis, performance verification**

I. Introduction

RECENT blackouts mainly caused by protection mal-operation [1, 2] have given impetus to the revision of transmission network operator policies and practices when it comes to the application and setting of protection schemes [3]. A direct result of these is the interest in wide-area monitoring, protection and control systems (WAMPAC) and system integrity protection systems (SIPS) which can potentially aid in mitigating such events [4, 5]. In addition, adaptive protection is seen as one of the promising approaches to delivering the required protection performance under these changing network conditions [6, 7]. By dynamically selecting protection settings or re-configuring the scheme logic, adaptive protection schemes can effectively respond to varied operational conditions while maintaining required performance levels. By adapting the protection behavior in line with the primary system changes, specified minimum performance objectives are ensured. However, it is perceived that such behavior introduces uncertainty in the correct choice of new configurations. Furthermore, changes in a particular scheme may have knock-on effects resulting in an overall un-coordinated secondary system.

Despite a number of adaptive protection schemes being proposed in the literature for different applications, limited attention was given to methods of verifying the scheme performance [8]. This is particularly critical as moving away from a fixed setting operational paradigm poses difficulties in the management of the protection settings and indeed a barrier to adopting such schemes on a wider scale. Performance verification can be tackled through a simulation-based approach where targeted functional tests of the adaptive protection logic can reveal faults in design or implementation. This would be an extension of existing closed loop protection testing practices [9, 10] which involve creating a set of test scenarios and comparing expected and measured performance. However, devising a comprehensive set of test scenarios may be difficult to fully verify a scheme and oversight may occur. Alternatively, more formal methods of verification can be used to examine specific properties of the adaptive protection behavior in response to defined stimuli. For instance, the possibility of the scheme choosing an incorrect setting for a specific primary system condition could be evaluated using reachability analysis which is explored in this paper. These two approaches to performance verification need not be mutually exclusive. But can be used as a set of complementary procedures to achieve greater confidence in adaptive protection behavior [8].

Reachability analysis has been proposed to verify the safety of power system control and protection actions to maintain its stability. For instance, [11] verifies the safety of fault release control – a form of operational tripping scheme. If generator disconnection occurs, certain transmission lines are tripped in order to avoid angular instability of other generators in the network. Generator angular stability limits are used as criteria to determine the safe operating region of the power system within the state space. Violating these limits results in loss of synchronism. In [12], reachability analysis is used to determine whether voltage instability occurs as a consequence of transmission circuit disconnection. This takes into account the automatic voltage control of the generator along with the discrete transitions caused by the disconnection of the lines. The critical value of the bus voltages determines the safe operating region. Voltage stability is also examined in [13] where reachability analysis is used to determine the onset of voltage instability. Moreover, the paper proposes supervisory control to mitigate its effects by issuing a combination of voltage control measures as appropriate. At the core of this analysis is a hybrid dynamical model which formulates the behavior of systems under study using a set of discrete abstractions of the system's state space [14]. The resulting abstraction is then studied to determine whether the system reaches unsafe states which reflect unacceptable performance [15].

This research was supported by the UK Research Councils' Energy Program as part of the Supergen FlexNet consortium grant no. EP/E04011X/1.

The authors are with the Institute for Energy and Environment, Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow, G1 1XW, UK (e-mail: ibrahim.f.abdulhadi@strath.ac.uk).

The example applications discussed above focus on studying the direct impact of protection or control performance on the performance of the primary system (e.g. impact on stability). Furthermore, the examples are based on conventional approaches to protection and control. To this end, this paper will examine the use of reachability analysis with adaptive approaches to protection to verify the safety property of their setting selection logic – an application not considered in the literature. So this paper focuses on the interactions, between the primary and secondary systems, which trigger adaptation in protection behavior. While examining the effectiveness of this approach to adaptive protection scheme verification, the following contributions are made:

- Extension of the standard hybrid abstraction necessary to encompass adaptive protection logic behavior.
- Novel application of reachability analysis based on the mapping between 'operational' and 'performance' invariant sets of the hybrid state space.

Section II introduces hybrid systems modeling and establishes the necessary relations to formulate a working behavioral model for adaptive protection applications. Section III applies the principles of hybrid modeling to an example adaptive distance protection scheme, while defining the safety states necessary to perform reachability analysis. Section IV demonstrates the use of the developed behavioral model and the application of reachability analysis to the adaptive scheme.

II. Hybrid Modeling of Power Systems And Protection Schemes

Key to performing effective adaptive scheme verification is the understanding of the dynamic behavior of the adaptive protection scheme. This involves interactions between the primary system, protection relays and overarching adaptive protection logic. Describing these interactions is possible through hybrid system modeling which describes the relationship between the continuous and discrete dynamics of a system simultaneously [16, 17]. Continuous dynamics in the power system are related to the changes in loading conditions, generator outputs, etc. While discrete dynamics are attributed to switching events such as circuit breaker operation and transformer tap changes. Circuit breaker operation is mainly controlled by the applied protection or automation schemes which play a major role in the discrete dynamics. By examining a protection relay closely, it can also be seen that the relay itself exhibits continuous dynamics in the form of the protection characteristics. For example, the onset of a short circuit condition results in a continuous change in the measured current. When this is viewed in conjunction with an overcurrent protection characteristic for instance, the relay will eventually reach a trip decision in line with the continuous evolution of the current. This trip can be thought of as a discrete jump (transition) to a new point in the state space.

A hybrid system H takes the form of an automaton that describes the different states of the system and at the same time captures the discrete events through state transitions. This is formulated in (1) [14]:

$$H = (Q, X, In, Init, f, Dom, E, G, R) \tag{1}$$

Where, $Q = \{q_0, q_1, \dots, q_n\}, n \in \mathbb{N}$ is the set of discrete states, $X \subseteq \mathbb{R}^n$ is the set of continuous states within the set of discrete state, In is the set of control and disturbance inputs that influence the dynamic changes in x, $Init \subseteq Q \times X$ is the set of initial states, $f(q,x): Q \times X \to \mathbb{R}^n$ is the continuous vector field (this defines how the continuous state x dynamically changes over time), $Dom(q): Q \to 2^x$ is the discrete state domain, $E \subseteq Q \times Q$ is the set of edges or transition maps (this defines the original state and destination state of a transition between two discrete states, $G(x): E \to 2^x$ is the set of transition guard conditions (this defines the conditions that must be satisfied before a discrete state transition occurs), and $R(q,x): Q \times X \to 2^X$ is the continuous vector field reset relation (this defines the new value of the continuous state x within a new discrete state q after a discrete transition).

A. Primary System Model

To apply the automaton of (1) in a power system context, the general model can be adjusted to deal with the specific system being analyzed. In the case of power system stability, for instance, the field vector can represent the angular or voltage stability dynamics and examples of their formulation can be found in [11] and [12] respectively. [18, 19] illustrate the transitions between discrete states describing the states of a transmission line as a result of protection operation as well as the transition between power system operational states. While [20] incorporates the action of tap changer into the primary system model and its effect on the system voltage profile. In this paper, the primary system part of the hybrid system model will reflect the mode of operation of a quadrature booster transformer (QB). This builds on previous work that evaluates the performance impact of QB on distance protection and adaptive protection strategies to mitigate this impact [21].

B. Adaptive Protection System Model

Modeling the interactions between the primary system and underlying protection schemes for dynamic analysis was first introduced in [22] through the modification of the power system admittance matrix as a result of protection action. As shown in Figure 1, protection relays encompass a number of core elements that deliver the desired functionality. The adaptive protection logic illustrated in Figure 1 has direct control over the active protection settings by making an appropriate selection depending on the primary system conditions that are being monitored. Each block can be detailed in terms of constituent components (e.g. timers, comparators), these have been described in literature [23] and mostly have no bearing on the context of this paper. In this paper, the main area of concern, in terms of adaptive protection, is that the dynamic setting selection based on changes in primary system state is 'safe'.

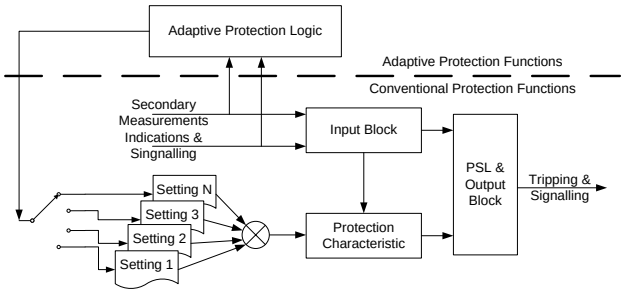

Figure 1 Adaptive protection scheme elements

This translates to whether a suitable setting group is selected for a given power system condition. In order to verify the safety property of this dynamic behavior, reachability analysis must be applied. Consequently, the remainder of this section develops a working hybrid model for this purpose. The influence of the active settings on the output of the protection scheme can be described as in (2).

$$Y = f(U, S_n, L) \tag{2}$$

Where Y is the tripping or signaling output of the protection scheme based on the active setting S_n, implemented scheme logic L and scheme input U (in the form of measured or derived secondary analogues and/or remote signaling or binary indications). The adaptive protection logic effectively alters the active settings dynamically as in (3).

$$S_n = \delta(U) \tag{3}$$

Where the adaptive protection operator δ acts on the input U to activate the appropriate protection setting S_n. Thus δ can simply take the form of one to one mapping between a subset of $U_n \subseteq 2^U$ and a predetermined settings group $SG \subseteq S_n$ (i.e. $\delta(U): U_n \rightarrow S_n$). Alternatively, the adaptive logic may choose an optimum S_n setting based on a calculation algorithm that seeks to coordinate multiple protection relays (e.g. automatic grading of protection based on established grading methods or more advanced methods involving optimization techniques [24]). In this paper the focus is on a one to one mapping between system states and predetermined settings groups. It is clear so far that an adaptive protection scheme involves interactions between discrete and continuous dynamics that require a formal definition. To achieve this definition, the paper proposes to extend the abstraction of these interactions based on previous hybrid systems modeling literature.

C. Discrete Event System Abstraction

The interactions between the continuous and discrete elements of a hybrid dynamical system can be understood by abstracting the continuous dynamics to an equivalent discrete system through a discrete event system (DES) abstraction [16, 25]. This is achieved by introducing interface elements between the abstracted continuous system and discrete controller usually known as event and action generators. These handle information exchanges between the two interacting dynamics. In a simple process feedback control system, the event generator is representative of the analogue to digital converter that samples the plant's controlled quantity and passes it on to the controller for processing. The action generator is the digital to analogue converter used to apply set points to the controlled plant. A standard DES abstraction is depicted by the solid blocks and arrows of Figure 2 (DES1).

However, an adaptive protection scheme exhibits a hierarchical structure where the adaptive protection logic oversees the conventional protection functions based on the primary system state. At the same time, the conventional protection scheme operates on the primary system based on its state that is being monitored by the instrument transformers (or protection signaling). This in effect results in two concurrent control loops with different operating time scales and simultaneous continuous and discrete state transitions at different levels in the hierarchy. The adaptive protection logic also requires information from the conventional protection in addition to the information from the continuous plant (power system). It is important to note that the hierarchy need not be physical. This is because the purpose of the abstraction is to expose the adaptive logic behavior for verification. Due to these factors, existing approaches to the DES abstraction are inadequate. To this end, the DES abstraction should be extended to encompass the adaptive protection logic as shown in Figure 2 by the dashed arrows and blocks (DES2).

The conventional protection systems will monitor continuous primary system quantities $x_1'(t)$. A discrete event $\tilde{x}_1[n]$ is generated should these quantities exhibit excursions in relation to a certain threshold. In response, the protection system produces a trip command $\tilde{r}_1[n]$ if the event is in line with the active protection setting S_n. The associated circuit breaker then trips in response to the trip command $r_1(t)$. Similarly, the adaptive protection logic monitors both the states of the protection system $x_2(t)$ and the state of the primary system (or specified components of it) $x_1''(t)$. Based on pre-set thresholds, the events $x_2[n]$ and $x_2''[n]$ are generated for use by the logic. The adaptive logic then determines an appropriate setting $\tilde{r}_2[n]$ accordingly and activates it in the target relay by means of $r_2(t)$. This developed DES abstraction will be applied to an example adaptive distance protection scheme in the following section.

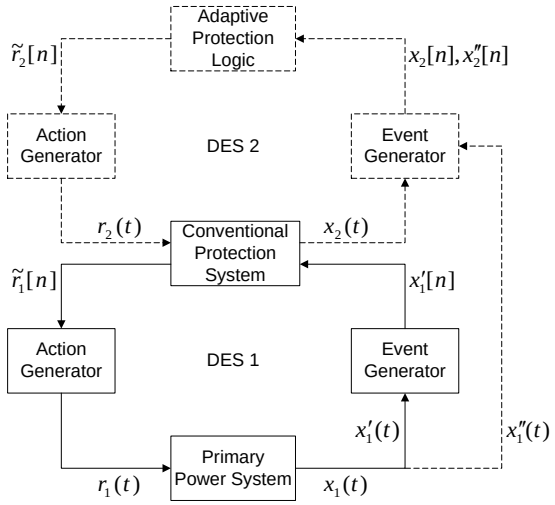

Figure 2 DES abstraction for an adaptive protection scheme

III. Applying the Hybrid Model to Adaptive Distance Protection

In this section, the hybrid systems fundamentals presented thus far will be used to model an example adaptive distance protection scheme. This example is based on the previous work published in [7, 21]. In [21], it has been shown that an under reach of protection zones may occur when a quadrature booster (QB) transformer is operating in buck or boost modes while default distance zone settings are used. An adaptive protection strategy has also been presented in [21] to correct for this reach error by selecting from pre-determined settings groups. This adaptive protection algorithm has been experimentally implemented and validated using hardware in the loop testing as presented in [7]. The purpose of the treatment in this paper is to verify whether the adaptive protection used to select between settings groups may operate in an unsafe manner. Safety in this context will be defined more formally later on and reachability analysis will be the means through which this safety property is verified. To model the adaptive distance scheme behavior, consider its constituent components summarized in Table I. This is in line with the developed DES abstraction in Figure 2. The performance of the adaptive logic can be determined by creating a mapping between the operating states of the listed primary and secondary system components. This mapping represents the interaction between these subsystems.

Table I
Summary of hybrid dynamics of studied adaptive distance protection

DES abstraction block	Associated system component(s)	Nature of component dynamics	Role within the system
Adaptive protection logic	Setting selection logic	Discrete	Activation of new settings group
Conventional protection system	Distance protection elements	Continuous	Fault detection according to active settings group
	Programmable scheme logic	Discrete	Issue trip command after time delay
Primary power system	QB controller	Discrete	Control and reporting of QB mode and tap position
	Transmission circuit	Continuous	Line loading status
	Transmission circuit breaker	Discrete	Line connection status obtained from breaker status

It is then proposed that the overall hybrid system is partitioned into two invariant discrete sets Q_{pps} and Q_{cps} which represent the primary power system (pps) and conventional protection system (cps) respectively. Invariant sets are those where if $x(t) \in Q$ then $x(\tau) \in Q \ \forall \ \tau \geq t$. This applies to all $x(t)$ and $x[n]$ defined in the DES abstraction of Figure 2. This means that all primary system continuous states $x_1(t)$ and conventional protection system continuous states $x_2(t)$ are strictly bound by their respective discrete domains $\mathrm{Dom}(q_{pps}) \subseteq Q_{pps} \times X_1$ and $\mathrm{Dom}(q_{cps}) \subseteq Q_{cps} \times X_2$. Thus, the discrete states Q_{pps} and Q_{cps} are mutually exclusive.

A. Defining safety states in the hybrid model

Prior to performing reachability analysis on the adaptive protection logic to verify it safety property, it is necessary to define the unsafe states that the logic can potentially reach. This will be achieved using the DES abstraction and invariant states defined earlier. The partitioning of the hybrid state space according to the invariant sets Q_{pps} and Q_{cps} can be illustrated in Figure 3.

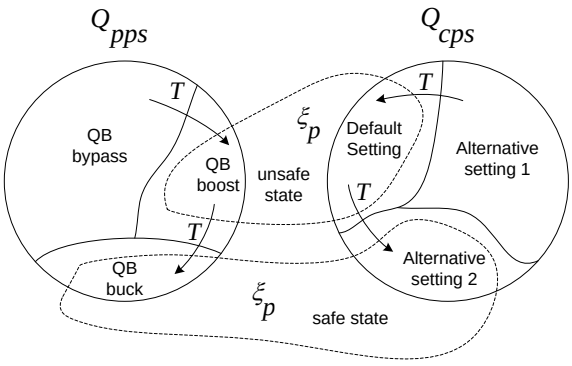

Figure 3 Partitioning of the hybrid state space into invariant sets

It can be seen that Q_{pps} represents the different primary system states related to the operation of the QB. Also, Q_{cps} reflects the different operational modes of a conventional protection relay as dictated by its settings. Q_{pps} and Q_{cps} will thereafter be referred to as 'operational states'. Discrete transitions between the sub-states $q_{pps} \subseteq Q_{pps}$ and $q_{cps} \subseteq Q_{cps}$ are indicated by T. These sub-states must also be, by definition, mutually exclusive to ensure that defined safe states are unique. Thus, these sub-states also become invariant sets.

In addition to the operational states, it is now proposed that new invariant discrete sets ξ_p are created and denoted 'performance states'. These performance states represent unique groupings of operational sub-states. In other words, no two sub-states belonging to an operational state share the same performance state grouping. For instance, the performance state that groups 'QB buck' and 'Alternative setting 2' sub-states shall not include 'Default setting' or 'QB bypass' under the same grouping.

The invariant performance sets ξ_p defined are used to identify these unsafe states $\overline{G} \subseteq \xi_p$. Where $\overline{G}$ denotes an unsafe state. In Figure 3, the performance state combining the 'default setting' and 'QB boost' states is considered unsafe since this particular combination results in distance protection under reach [21]. As mentioned previously, invariant sets are mutually exclusive. Thus, the boundaries of the performance states can be clearly defined in the hybrid state space. Ultimately, this will result in a clear (binary) indication of whether a particular state can be considered safe or not. It is important to note that the safety examination in this paper is restricted to the correct behaviour of the adaptive logic. As such, the implications on unsafe behaviour on the primary system (e.g. power system instability) are out with the scope of the paper. So, the system should either never exist in an unsafe state $\overline{G}$, expressed as:

$$\square((q,x) \notin \overline{G}) \quad (4)$$

Where □ (square) is the 'always' logical operator, or alternatively, the system should eventually always exit the unsafe state:

$$\Diamond\square((q,x) \notin \overline{G}) \quad (5)$$

Where ◊ (diamond) is the 'eventually' logical operator. This temporal aspect reflects the finite amount of time required to exit an unsafe state through adaptive protection setting changes. For a detailed examination of this temporal dimension from a hybrid system perspective, timed hybrid automata can be considered. However, this is out with the scope of the paper.

B. Implementation of the DES abstraction with adaptive distance protection

The adaptive protection logic (excluding distance protection elements) is developed in Simulink and the overall scheme response was validated in a previous publication using a hardware in the loop testing configuration [7]. Simulink Stateflow toolbox was used to implement the operational states defined above. Additional logic is created to map between operational and performance states based on the safety definitions for this particular adaptive scheme. Two primary system components were considered in this study, the QB transformer and the protected transmission line. Their respective operational states are shown in Figure 4. The active states of the primary system components are determined through status indications from the QB controller and circuit breakers associated with the line. These status indications reflect the $x_2''[n], x_2[n]$ signals of the DES abstraction. The loading of the line is used to determine the impact of potential load encroachment on the behavior of the adaptive protection logic. Heavily loaded lines are more likely to cause load encroachment related mal-operation of distance protection. Thus, the adaptive logic must take this into account. Other phenomena such as power swings are not considered as this is dealt with by dedicated distance protection functionality (power swing blocking) and does not trigger any setting changes by the adaptive logic nor is impacted by zone reach, thus it is not being verified here.

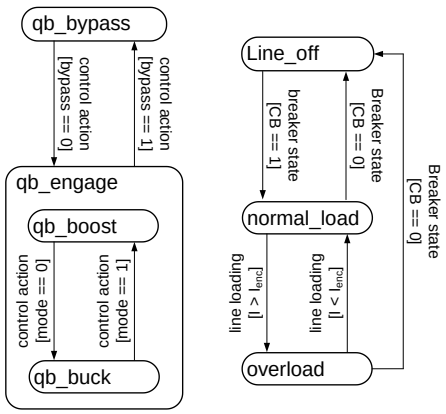

Figure 4 QB and protected line operational states

IV. Applying Reachability Analysis to Adaptive Distance Protection

In this section, the reachability analysis methodology is described and demonstrated for an example adaptive distance protection scheme previously developed in [7, 26]. As explained earlier, the reachability analysis aims to uncover erroneous behavior in the adaptive setting selection logic. This is achieved by ascertaining whether the adaptive scheme that is modeled in a hybrid state space reaches an unsafe state during its operation. A particular example of this is the potential under reach in distance protection zones if a QB is installed in the circuit and operated in boost or buck modes. If the adaptive logic was 'error free' then this under reach can be mitigated by dynamically extending the zone reach. Dynamic extension of zone reach is realized by selecting a different setting group with the desired zone reach setting. Given the initial conditions $Init$ for a hybrid system H, the reach of the hybrid system can be described as:

$$Reach(H) = \{\overline{G}\ \forall\ Init \subseteq (q,x) \exists\ T_{\overline{G}}, s.t. \overline{G} \subseteq \xi_p\} \quad (6)$$

This implies that should the system reach an unsafe state from a certain $Init$, then it is possible to identify the backwards trajectory obtained from the unsafe transition $T_{\overline{G}}$. This can be used to identify faults in the adaptive logic, by observing the scheme inputs and the resulting adaptive logic state transitions leading to the unsafe state entry. The performance states that represent the unsafe states $\overline{\mathrm{G}} \subseteq \xi_{\mathrm{p}}$ are summarised in Table II. This shows the condition for entry in to and exit from unsafe states. These conditions are qualified by $x_2''[n], x_2[n]$ of the DES abstraction. In Table II, QB_{bk}, QB_{bt} and QB_{bp} represent QB buck, boost and bypass modes respectively which are also operational invariant sets in the developed DES abstraction. Also, SG_1 to SG_4 represent the used settings group 1 to 4 respectively (these are summarized in Table III along with selection criteria). The zone reaches are expressed in the percentage of the protected line length.

As discussed earlier, the potential for load encroachment is taken in to account. Under stressed conditions, the protection should be geared towards security as opposed to dependability, thus the adaptive logic temporarily inhibits zone extension under heavy loading conditions. The level of line current at which load encroachment is likely is indicted by I_{enc} in Table II. This threshold is determined by simulation and varies with the power system under consideration. The '|' operator indicates AND logic, and the '¯' operator indicates the complement of a state.

Table II
Safety conditions for adaptive logic under test

$\overline{G}$	Entry conditions	Exit Conditions
Under-reach	$QB_{bk}\|SG_1$	$QB_{bp}\|SG_3$
Under-reach	$QB_{bt}\|SG_1$	$QB_{bp}\|SG_4$
Over-reach	$QB_{bp}\|SG_1$	$QB_{bt}\|QB_{bk}\|SG_1$
Load-encroachment	$I_{enc}\|\overline{SG}_1$	$\overline{I}_{enc}\|SG_1$

Table III
Setting group assignment

SG	Reach Settings	Selection criteria
SG1	Zone 1 = 80%, Zone 2 = 150%, Zone 3 = 220%	QB_{bp}, I_{enc}
SG2	Not used	-
SG3	Zone 1 = 80%, Zone 2 = 160%, Zone 3 = 230%	$QB_{bt}, \overline{I}_{enc}$
SG4	Zone 1 = 80%, Zone 2 = 170%, Zone 3 = 250%	$QB_{bk}, \overline{I}_{enc}$

In light of this, a safety performance verification procedure based on reachability analysis is proposed and is shown in Figure 5. As shown in the figure, the hybrid system state space is determined including the definition of the safety criteria. The adaptive logic must then be stimulated by changing the state of the primary system components of interest. In this case, the QB state must be changed as this has a direct impact on the adaptive setting selection logic behavior being verified. The performance states are then directly obtained to determine whether an unsafe state has been reached. If an unsafe state is reached, then it can be concluded that an error is present in the logic which can be diagnosed by monitoring the trajectory $T_{\overline{G}}$ leading to the unsafe state. This trajectory will infer the conditions $x_2''[n], x_2[n]$ that led to the unsafe state entry.

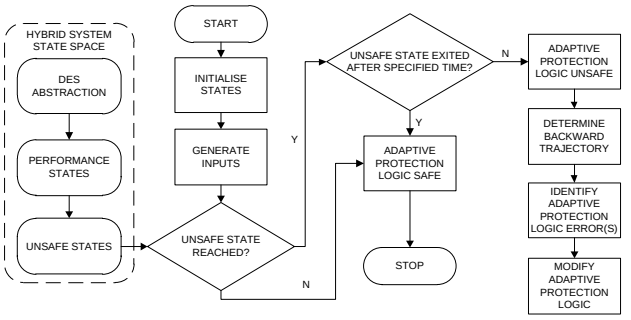

Figure 5 Reachability analysis procedure

Once the DES abstraction has been developed, the discrete transitions between the system states in the hybrid system can be determined without incorporating the primary system continuous states. This is because $x_2''[n], x_2[n]$ are known for each QB and circuit loading state. In other words, the primary system model continuous dynamics become redundant in the reachability analysis. As such, computational resources are saved. This is an important differentiator between the reachability analysis approach proposed in this paper compared to the literature referred to earlier.

V. Test Setup and Simulation Results

The hybrid models reachability analysis methodology developed in the previous section will be used to verify the performance of adaptive distance protection applied to transmission lines with quadrature booster transformers (QBs) installed. The overall test setup is shown in Figure 6. Inputs to the adaptive protection logic include signals representing QB states and protected line loading. Both inputs and adaptive logic response (i.e. setting group selection) are monitored to verify the logic safety. Note that no distance protection elements are implemented, as the verification focuses on the adaptive logic behavior that governs new setting selection.

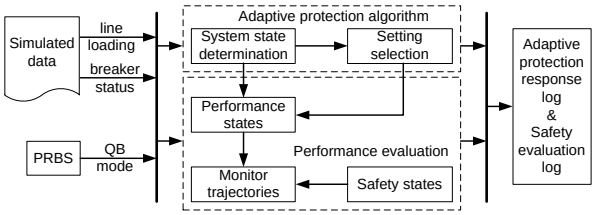

Figure 6 Reachability analysis test setup

A. Primary System Model

The power system under consideration is shown in Figure 7 (model data is shown in Table IV). It consists of four 400kV circuits of 200km each. The purpose of the model is to generate line loading data as inputs to the test. The distance protection scheme (including adaptive logic) under examination is located at A in Figure 7 (denoted by ANSI 21). There are two operating conditions that are of interest from the adaptive logic point of view that result in reaching an unsafe state – the impact of the QB status on the distance protection reach and the possibility of load encroachment while zone 3 is extended by the adaptive logic.

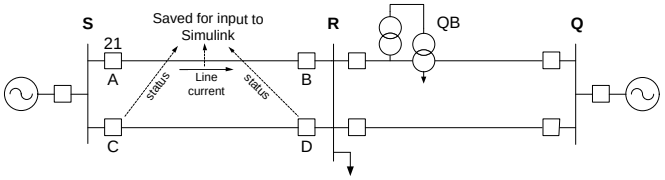

Figure 7 Primary system under test

Table IV
Power System Model Data

Line Impedances (primary ohms)	Line Configuration	CT, VT Ratios
Z1 = 0.027+j0.296 Ω/km	Four single circuit segments	CT ratio = 1000:1A
Z0 = 0.1+j0.439 Ω/km	Segment length = 200km	VT ratio = 400k:110V

B. Adaptive Protection Strategy

The function of the adaptive distance protection logic is to choose an appropriate zone reach from predetermined settings groups in response to changes in the QB mode. This also takes into account the loading of the line. The adaptive logic refrains from extending the zone reach should load encroachment become a potential issue due to circuit overloading. Figure 8 shows how load encroachment can occur if line CD in the test model is disconnected. Adaptive extension of the third zone to compensate for the presence of the QB under this circumstance would be undesirable. In this case, the scheme defaults to the original settings group as a best compromise. The line current leading to this situation is captured from the simulation and fed into the Simulink model as an input to the adaptive logic. The adaptive protection algorithm is detailed by the authors in [7, 21]. The settings groups used have been presented in Table III.

C. Verification of Adaptive Logic Safety

The QB state inputs to the logic were in the form of pseudo-random binary sequence (PRBS) representing different QB operating modes.

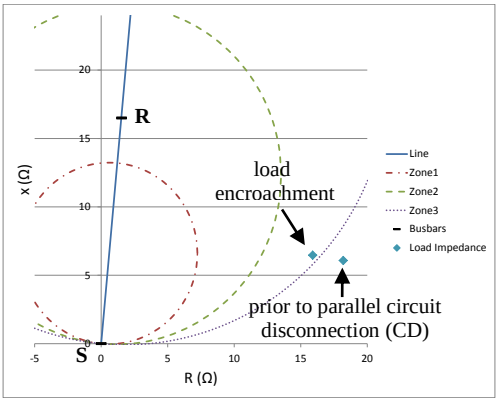

Figure 8 Load impedance prior and post load encroachment (secondary ohms)

This is shown in Figure 9 as 'QB connection' and 'QB mode'. The PRBS is obtained from the signal generator block in Simulink. The use of the PRBS is considered as an effective means of providing exhaustive coverage for possible system executions and repeatability of testing conditions [27]. Furthermore, hysteresis in the logic can be discovered when using this approach. An increase in line current (secondary value) occurs at 25s in the simulation to reflect the load encroachment scenario (i.e. disconnection of line CD).

The different performance states ξ_p that the adaptive scheme resides in after subjecting the logic to the inputs are also shown in Figure 9. These are the 'reach states' and the 'load encroachment states'. These performance states are enumerated as 'under reach', 'over reach' and 'normal reach' for the former and 'encroachment possible' and 'no encroachment' for the latter. The bottom trace in Figure 9 is set to unsafe if any of the above performance states satisfies the conditions for an unsafe state (defined in Table II) and vice versa.

It can be seen from the bottom trace in Figure 9 that the adaptive logic alternates between safe and unsafe states. However, it only resides in an unsafe state for a short period of time. This corresponds to the simulation time step (1ms) which is the maximum amount of time necessary to reach a setting selection decision. In reality, this time delay will increase depending on the scheme implementation. Between 25-50s, the increased line current value results in the logic reverting to the default setting (SG1) regardless of the QB mode. This is because the logic recognizes that the increase in line loading beyond the I_{enc} threshold will result in load encroachment, so dynamically extending zone 3 is inhibited. This situation remains the same regardless of the QB state until the end of the simulation time. Thus, inhibiting zone extension during heavy line loading conditions is deemed safe.

An intentional logic error was then introduced to the adaptive logic to disable its load encroachment related response, and the same inputs were used to stimulate the logic. This means that the logic would not inhibit zone extension even under heavy line loading conditions. The purpose of this test is to determine whether the reachability analysis would identify a genuine unsafe state (i.e. not a temporary one while awaiting setting change). The related analysis results are shown in Figure 10. The increase in load current through the

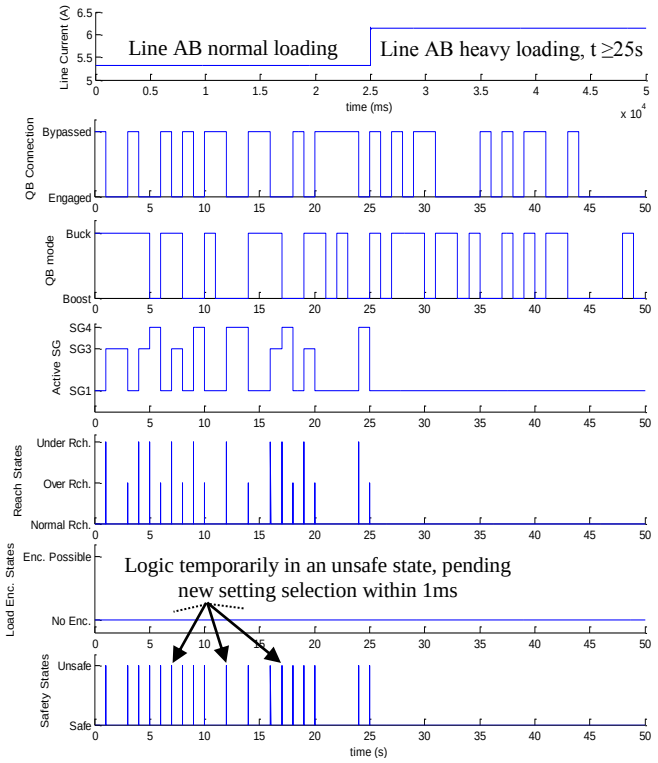

Figure 9 Inputs and performance of adaptive logic indicated by safe states

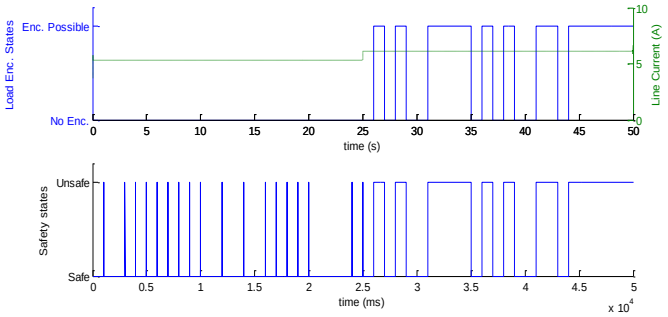

Figure 10 Error introduced in the adaptive logic results in unsafe zone extension

protected line AB, combined with zone extensions prompted by the QB mode changes result in an unsafe state entry. This is indicated in Figure 10 at several occurrences after 25s where the logic dwells in an unsafe state for longer than a simulation time step (the maximum amount of time required to select a new setting group). In this case, the logic error is known because it was intentionally introduced for testing purposes. In practical situations, unsafe state indications would be used by the testing engineer to diagnose the erroneous logic by determining the conditions that led to the unsafe state entry.

D. Discussion of reachability analysis in light of results

So long as the power system state can be inferred from a set of discrete transitions, then explicit continuous space computations will not be necessary. However, this assumes that the evolution of the continuous primary system state is not influenced by the outcome of the logic decision. Given the scope of the verification, this assumption is valid. This is because the verification is being conducted to determine whether logic actions are safe based on the consequences of an

unsafe outcome. And these unsafe outcomes have been determined using the performance states ξ_p. The temporal dimension of reachability analysis is also of relevance. It is necessary to identify the maximum time period that an adaptive protection scheme requires to provide a decision. Otherwise the scheme may become vulnerable to mal-operation if changes in the primary system occur during this time period. Thus, further work is necessary to incorporate the temporal dimension into the hybrid model and consequent reachability analysis.

Finally, the verification approach has proven to be flexible as it does not require the inclusion of conventional protection behavior and is independent of logic implementation. Indeed, the same analysis can be integrated in hardware in the loop validation procedure for overall scheme testing. This is only true if the invariant performance sets and associated safety states are defined based on the hybrid system interactions that trigger the adaptation of settings, as well as an understanding of the impact of adaptive setting changes on the performance of protection elements.

E. Application of safety verification to other adaptive protection schemes

The approach to safety verification in essence requires the identification of unsafe states – a subset of the performance states developed in this paper. These states are determined based on the defined continuous and discrete interactions between constituent components of the scheme. It can then be said that a foundation has been laid for applying the safety verification (reachability analysis) technique to other types of adaptive protection schemes. Unfortunately, implementing and testing of other schemes is out with the scope of this paper. Nevertheless, the following points can be made as guidelines for conducting reachability analysis under such circumstances:

- The distance protection considered in this paper is based on a mho characteristic. Should a different characteristic be used (e.g. quadrilateral), then determining the required alterations to the characteristic to minimize the impact of reach errors should be considered when designing the pool of settings. Verification of the setting selection logic should then follow the same procedure presented thus far.
- There have been numerous examples of adaptive distance protection schemes proposed in the literature to deal with different performance issues. Some of which are not based on dynamically changing settings, but on less deterministic approaches such as fuzzy logic [28]. In such cases, reachability analysis may still be applicable provided that a relationship between the input and output of the logic can be determined. Moreover, such schemes are only tested using a large set of fault scenarios – an approach whose drawbacks have been discussed in the introduction of this paper. Thus, reachability analysis can be a powerful complementary approach to the verification of such scheme's performance.

VI. CONCLUSION

This paper presented and demonstrated a novel application of reachability analysis to verify the performance of adaptive distance protection setting selection logic. A redefined discrete abstraction of the hybrid system which represents the interactions between the primary system and adaptive protection was formulated. This modification was necessary to capture the full control hierarchy introduced by the measurements and actions of adaptive logic. By partitioning the hybrid system state space into invariant operational and performance sets, it was possible to exclude the continuous dynamics from the analysis while clearly defining the boundaries of the safety states of the system.

The practical utilization of the safety verification would be of interest to manufacturers and utilities dealing with adaptive protection. Although protection scheme developers can directly apply such verification methodologies on their adaptive algorithms, utility commissioning engineers require meaningful performance metrics without delving into the intricacies of system behavioral modeling. As such, it is important to migrate such methodologies into tools and processes that meet usability requirements of end users.

REFERENCES

[1] A. Atputharajah and T. K. Saha, "Power system blackouts - literature review," in *Industrial and Information Systems (ICIIS), 2009 International Conference on*, 2009, pp. 460-465.

[2] S. H. Horowitz and A. G. Phadke, "Blackouts and relaying considerations - Relaying philosophies and the future of relay systems," *Power and Energy Magazine, IEEE,* vol. 4, pp. 60-67, 2006.

[3] US-Canada Power System Outage Task Force, "Final Report on the August 14th Blackout in the United States and Canada," 2004.

[4] V. Terzija, G. Valverde, C. Deyu, P. Regulski, V. Madani, J. Fitch, *et al.*, "Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks," *Proceedings of the IEEE,* vol. 99, pp. 80-93, 2011.

[5] M. Begovic, V. Madani, and D. Novosel, "System Integrity Protection Schemes (SIPS)," in *2007 iREP Symposium - Bulk Power System Dynamics and Control - VII. Revitalizing Operational Reliability*, 2007, pp. 1-6.

[6] D. Tholomier and A. Apostolov, "Adaptive protection of transmission lines during wide area disturbances," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, 2009, pp. 1-7.

[7] I. Abdulhadi, F. Coffele, A. Dysko, C. Booth, and G. Burt, "Adaptive protection architecture for the smart grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, 2011, pp. 1-8.

[8] I. Abdulhadi, F. Coffele, A. Dysko, C. Booth, G. Burt, G. Lloyd, *et al.*, "Performance Verification and Scheme Validation of Adaptive Protection Schemes," in *2012 CIGRÉ Session (44th Edition)*, 2012.

[9] Alstom, *Network Protection and Automation Guide - Protective Relays, Measurement and Control*, 2011.

[10] IEEE, "IEEE Std C37.233-2009: IEEE Guide for Power System Protection Testing," pp. 1-112, 2009.

[11] Y. Susuki, T. Sakiyama, T. Ochi, T. Uemura, and T. Hikihara, "Verifying fault release control of power system via hybrid system reachability," in *Power Symposium, 2008. NAPS '08. 40th North American*, 2008, pp. 1-6.

[12] Y. Susuki and T. Hikihara, "Predicting Voltage Instability of Power System via Hybrid System Reachability Analysis," in *American Control Conference, 2007. ACC '07*, 2007, pp. 4166-4171.

[13] R. R. Negenborn, A. G. Beccuti, T. Demiray, S. Leirens, G. Damm, B. De Schutter, *et al.*, "Supervisory hybrid model predictive control for voltage stability of power networks," in

American Control Conference, 2007. ACC '07, 2007, pp. 5444-5449.
[14] E. M. Navarro-López and R. Carter, "Hybrid automata: an insight into the discrete abstraction of discontinuous systems," *International Journal of Systems Science*, pp. 1-16, 2010.
[15] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi, "Computational techniques for the verification of hybrid systems," *Proceedings of the IEEE*, vol. 91, pp. 986-1001, 2003.
[16] X. D. Koutsoukos, P. J. Antsaklis, J. A. Stiver, and M. D. Lemmon, "Supervisory control of hybrid systems," *Proceedings of the IEEE*, vol. 88, pp. 1026-1049, 2000.
[17] Y. Susuki, T. J. Koo, H. Ebina, T. Yamazaki, T. Ochi, T. Uemura, *et al.*, "A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance," *Proceedings of the IEEE*, vol. 100, pp. 225-239, 2012.
[18] G. K. Fourlas, K. J. Kyriakopoulos, and C. D. Vournas, "Hybrid systems modeling for power systems," *Circuits and Systems Magazine, IEEE*, vol. 4, pp. 16-23, 2004.
[19] G. K. Fourlas, "Modeling of an electrical power transmission system using hybrid systems," in *Control Applications, 2005. CCA 2005. Proceedings of 2005 IEEE Conference on*, 2005, pp. 1516-1521.
[20] I. A. Hiskens and M. A. Pai, "Hybrid systems view of power system modelling," in *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, 2000, pp. 228-231 vol.2.
[21] 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.
[22] L. G. Perez, A. J. Flechsig, and V. Venkatasubramanian, "Modeling the protective system for power system dynamic analysis," *Power Systems, IEEE Transactions on*, vol. 9, pp. 1963-1973, 1994.
[23] A. Dysko, J. R. McDonald, G. M. Burt, J. Goody, and B. Gwyn, "Integrated Modelling Environment: a platform for dynamic protection modelling and advanced functionality," in *1999 IEEE Transmission and Distribution Conference*, 1999, pp. 406-411 vol.1.
[24] P. P. Bedekar, S. R. Bhide, and V. S. Kale, "Optimum coordination of overcurrent relays in distribution system using genetic algorithm," in *International Conference on Power Systems, 2009. ICPS '09*, 2009, pp. 1-6.
[25] M. Yasar, A. Beytin, G. Bajpai, and H. G. Kwatny, "Integrated Electric Power System supervision for reconfiguration and damage mitigation," in *IEEE Electric Ship Technologies Symposium, 2009. ESTS 2009*, 2009, pp. 345-352.
[26] J. Kincaid, I. Abdulhadi, A. S. Emhemed, and G. M. Burt, "Evaluating the Impact of Superconducting Fault Current Limiters on Distribution Network Protection Schemes," in *Universities' Power Engineering Conference (UPEC), Proceedings of 2011 46th International*, 2011, pp. 1-5.
[27] M. G. Bartley, D. Galpin, and T. Blackmore, "A comparison of three verification techniques," 2002.
[28] M. Sanaye-Pasand and P. Jafarian, "An Adaptive Decision Logic to Enhance Distance Protection of Transmission Lines," *IEEE Transactions on Power Delivery*, vol. 26, pp. 2134-2144, 2011.

Ibrahim Abdulhadi (S'08, M'11) received the M.Eng. and PhD degrees in electronic and electrical engineering from the University of Strathclyde, UK, in 2007 and 2013. He is currently a Research Associate within the university's Institute for Energy and Environment. He has experience working for UK distribution and transmission network operators. His research interests include power system protection, real-time power system simulation, hardware in the loop testing and communications applications in smart grids.

Adam Dyśko (M'06) received the M.Sc. degree from the Technical University of Łódź, Poland, in 1990, and the PhD degree from the University of Strathclyde, Glasgow, U.K., in 1998. Currently, he is a Lecturer in the Department of Electronic and Electrical Engineering, University of Strathclyde. His main research interest areas are power system modeling and simulation, power system protection and power quality.

Graeme Burt (M'95) received the B.Eng. and PhD degrees from the University of Strathclyde, Glasgow, U.K. He is a professor within the Department of Electronic and Electrical Engineering at the University of Strathclyde, where he co-directs the Institute for Energy and Environment and he is the director of the Rolls-Royce University Technology Centre in Electrical Power Systems. His international activities include serving on the board of the Association of European Distributed Energy Resources Laboratories (DERlab e.V.), and collaborating in EU programs including the Distributed Energy Resources Research Infrastructure (DERri), and the European Energy Research Alliance (EERA) in Smart Grids.