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

C2-201

CIGRE 2012

System Integrity Protection Schemes – Increasing operational security and system capacity

E. HILLBERG[1], F. TRENGEREID[2], Ø. BREIDABLIK[2], K. UHLEN[1], G. KJØLLE[1], S. LØVLUND[2], J.O. GJERDE[2]
[1)] Norwegian University of Science and Technology, [2)] Statnett Norway

SUMMARY

System Integrity Protection Schemes (SIPS) are increasingly utilised in power systems worldwide to provide additional power transfer capacity and enhanced operational security. The implementation of Phasor Measurement Units (PMU) and Wide Area Monitoring Systems (WAMS) provide opportunities to improve the conventional system integrity protections. These improvements can increase the protection schemes' awareness of the system state, providing robustness towards unforeseen disturbances and enhanced operational security to extraordinary events.

In this paper, a technique of how to assess the security to extraordinary events is described, where the concept of a secure operating region is extended to involve multiple contingencies, referred to as *the $N-k$ secure operating region*. This paper also includes an overview of the SIPS in the Norwegian power system, and a security assessment study performed on the IEEE Reliability Test System 1996. The study includes conventional and WAMS based SIPS solutions, and demonstrates the importance of incorporating dynamic contingency analysis when assessing the security of a power system.

KEYWORDS

System Integrity Protection Schemes – Operational security – Power transfer capacity – Extraordinary events – $N-k$ security assessment – IEEE Reliability Test System

Emil.Hillberg@ntnu.no

1. INTRODUCTION

Power transfer capacity limits are set in order to maintain a reliable operation of the power system. Typically, power transfer capacities between areas, or sub-systems of an interconnected power system, are defined by limitations on one or several power transfer corridors (PTC). A PTC can be identified as a set of transmission circuits that form an interface in a power system, which may impose a bottleneck in the system during a specific operating scenario. Limitations are often related to the thermal capacities of transmission lines and other equipment; however, the stability of the power system may as well constitute limiting factors. In the Continental European power system, main limitations are typically on thermal capacities, while stability limiting factors are of high concern in the less densely interconnected Nordic power system, [1, 2].

Maintaining a reliable operation of the power system implies that the system should be both adequate and secure. The adequacy of the power system can be defined as the existence of sufficient facilities in the system to satisfy its demand [3], referring mainly to the level of available generation and transmission capacity. Power system security reflects a systems ability to withstand disturbances, [3], where a contingency during insecure operation could result in instability. Extraordinary events (large disturbances or blackouts) are often caused by system instability, where the degraded system collapses after stability limits are violated, [4]. Since many power systems are operated according to the $N-1$ security criterion, stability limits are rarely violated by a single contingency. This further implies that the security to extraordinary events can be expressed as the security to multiple contingencies, i.e. $N-k$ security.

System Integrity Protection Schemes (SIPS) are implemented in many power systems worldwide. According to [5], approximately half of the globally installed SIPS can be classified as applications related to increasing the transfer capacity, while the other half is classified as increasing the operational security. SIPS are, in contrast to common component protection, designed to preserve the power system integrity during abnormal conditions. Another possible classification of SIPS is on the type of activation signal, which can be either event-based (detecting of predefined events, such as breaker tripping signals) or response-based (measuring electrical parameters, e.g. frequency or voltage), [6]. Most SIPS tend to be of the event-based type, [5], and are characterised by taking predefined actions to predefined events. Event-based SIPS are fast acting and designed to improve transient rotor angle stability and short-term voltage stability, they are, however, without protection against unforeseen events and consequence of SIPS action might be hard to anticipate for all operating scenarios. An example of commonly used response-based SIPS is the under-frequency load-shedding scheme (UFSL), which often is implemented on a system wide basis in order to prevent the collapse of a system due to frequency instability. Approximately 75% of all SIPS are intended to prevent instability, and corrective actions are in more than 50% of the cases related to load shedding or generation tripping, [5].

This paper is organised as follows:
Section 2 holds a description of SIPS in the Norwegian power system. Section 3 describes a technique for assessing the security to extraordinary events, and a security assessment analysis is included in section 4. Discussion and conclusions are provided in section 5.

2. SYSTEM INTEGRITY PROTECTION SCHEMES IN NORWAY

2.1 Background

The Norwegian transmission system is normally operated according to the $N-1$ security criterion. However, this criterion can not always be fulfilled and therefore a minimum acceptable operational security level has been defined, where: *a contingency should not have consequences beyond the disconnection of 200 MW load with duration up to 1 hour during normal operation, or 500 MW up to 2 hours during maintenance,* [7]. In such cases, the sub-system is referred to as being $N-0$ or $N-½$ secure, depending on the consequences of a probable contingency:

- $N-0$ secure operation refers to cases where a single outage leads to uncontrolled loss of load, e.g. in the case of radial operation in the transmission network
- $N-½$ secure operation reflects the mitigating impact by armed SIPS. In this way, the consequences of an event can be limited to a controlled load shedding, as described by [8]. This does, however, not automatically imply that an islanded system will be able to continue in stable operation, even though local load and generation are in balance after the SIPS action.

There are around twenty different SIPS installed in the Norwegian power system, affecting over 6 GW of production (approximately 20% of the total installed production) and more than 1.3 GW of load (approximately 5% of the maximum peak load). On top of this, there is an under-frequency load shedding scheme implemented in the Nordic system, which in Norway is activated when the frequency reaches below 48.7 Hz, affecting up to 7 GW of load.

The SIPS are utilised to increase transfer capacities of almost 20 different PTCs during normal operation and to improve the operational security during strained situations. In this section, the functionality and experience of some of these schemes are described.

2.2 Classification, objective & functionality

The installed SIPS in the Norwegian power system can, based on the nature of their corrective actions, be structured into four categories: generation tripping, load shedding, system separation, and HVDC emergency power. Both event-based and response-based activation signals are used, varying from local measurements of frequency, voltage, or power oscillation, to trip signals from remote breaker protection and over-current relays.

In many cases, SIPS are utilised to increase power transfer capacities, either to enhance system utilisation during normal operation or in scenarios with high load or insufficient local production. SIPS are also used to increase the security in situations with strained operation, e.g. during maintenance of an important transmission line, with the purpose to limit consequences of contingencies while sustaining a sufficient transmission capacity. All of the SIPS are manually armed by the transmission system operator (TSO), with the decision based on analyses made during the operation planning phase. Actual outcome of mitigating actions of armed SIPS is continuously updated in the control centre, based on state estimator data.

2.3 Operation experience & future trends

Since the 1980s, Statnett (the Norwegian TSO) has employed an increased number of SIPS in the power system, implying a more demanding operation of the system in terms of both utilisation and complexity.

Statistics collected from the national control centre, describing the initiation of SIPS in Norway, limited to generation tripping schemes, are displayed in the figures below. Figure 1 shows the annual number of SIPS initiations together with the amount of disconnected generation. The number of affected units, together with the cost (including both annual unit participation fees as well as activation fees), are shown in Figure 2 . The economical gain from utilisation of SIPS have note been included here, due to the difficulty in acquiring quantifiable data such as: earnings from increased energy exchange, savings from mitigated cost of energy not supplied, value of delayed investments, etc.

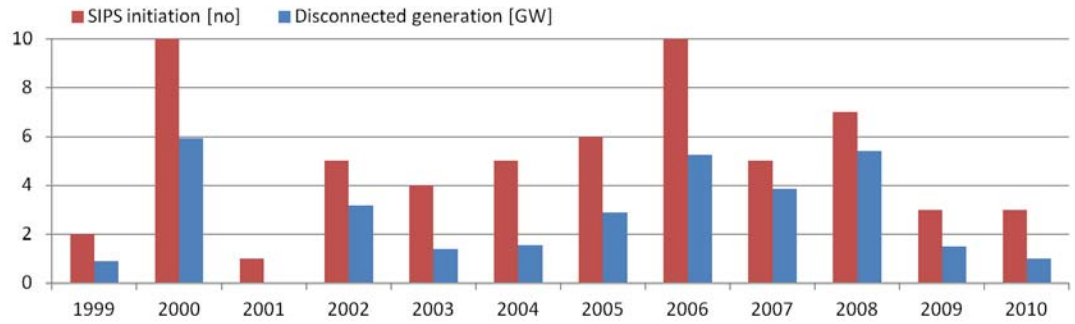

Figure 1: Annual number of SIPS initiations and resulting disconnected generation in Norway.

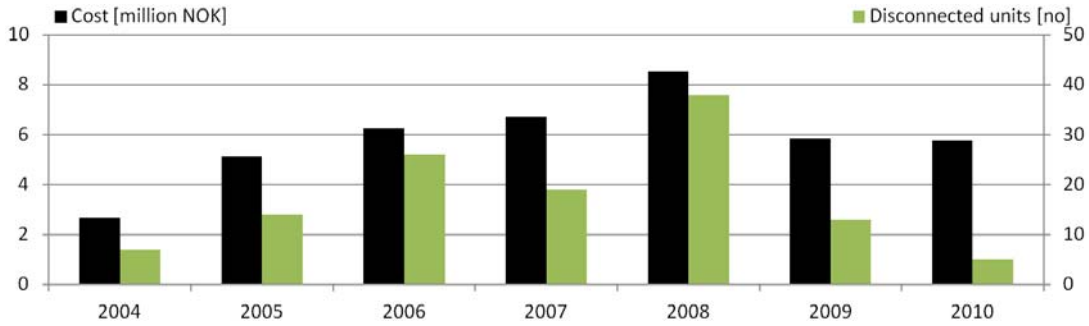

Figure 2: Annual cost and number of disconnected units by SIPS initiation in Norway.

There are some negative operational experiences reported, and an example is described in [9]. The report describes an event where the delayed operation of one SIPS initiated a system separation, leading to approximately 2 GW of production deficit in the main Nordic system. Automatic production increase led to overload and the triggering of another SIPS, which, however, failed to operate. The missed operation actually prevented a production disconnection, which likely would have led to an unstable scenario. This example shows the high complexity of SIPS control and operation, as well as the difficulty in designing protections against unforeseen event. It is therefore important to consider the risks involved when the operating scenarios largely rely on the performance of a number of SIPS.

According to [7], no further load shedding schemes[1] will be employed, stating that investments in new transmission capacity are imperative to increase future transfer capacity while maintaining a satisfactory level of operational security.

[1] Several other schemes (generation tripping and HVDC emergency power) are, however, planned to be installed in the near future.

3. SECURITY TO EXTRAORDINARY EVENTS

3.1 Background

Many historical blackouts have been the result of the progression of cascaded events, followed by system separation and instability, [4]. The system operators' lack of situational awareness has been identified as one of the root causes, as well as the system's insufficiency to regain stable operation in the post-contingency state, [10, 11]. In this section, improved security to extraordinary events is proposed through enhanced awareness by means of visualisation of the secure operating region related to single and multiple contingencies as well as the arming of SIPS.

3.2 N – 1 secure operating region

The $N-1$ secure operation, limited by aspects described in the introduction, can be assessed through contingency analysis. In some power systems it is possible to identify power transfer corridors with critical influence on the available secure transfer capacity. Such PTC could be utilised to visualise a region defining the secure operation, as suggested by [3, 12] and exemplified in Figure 3-I. Since a secure operation is of a multi dimensional nature, it is important to identify relevant quantities when visualising the secure region. In a power system with several critical PTCs, it might be reasonable to visualise several regions defined by different PTCs. In Figure 3-I, the secure operating region is visualised, together with the actual operating point, using the $N-1$ secure power transfer capacity of PTC_I relative to the capacity of PTC_{II}. The size and shape of the secure region will vary for different operating scenarios, since modifications of the network topology and other aspects influence the security of the power system.

3.3 N – k secure operating region

Similarly as suggested in the previous sub-section, the secure operating region related to multiple contingencies can be visualised as exemplified in Figure 3-II. Assessing the $N-1$ to $N-k$ secure operating region can be done by contingency analysis to the k^{th} subsequent contingency level. Such contingency analysis can be very tedious, and screening techniques might be necessary to identify contingencies which affect the critical PTC. Representation of a multiple contingency security region can be beneficial to assess the operating scenarios' vulnerability to extraordinary events. This may be further improved by explicit monitoring of vulnerability indices, where an example is the k_{min}-*index*. This index describes a distance to the stability limits of a system, determined by the minimum number of subsequent contingencies that lead to instability. A continuously updated estimation of the k_{min}-*index,* quantifying the vulnerability of the actual operating scenario, can improve the situational awareness of the operator when considered in relation with a historical perspective.

3.4 SIPS security enhanced operating region

The effects of arming a specific SIPS can be visualised as exemplified in Figure 3-III. The figure shows how arming of a SIPS enhances the security around the actual operating point. In cases where the desired operating point is outside the $N-1$ secure region, the SIPS can be used to provide an acceptable level of security. Utilising the secure operating region related to multiple contingencies, the efficiency of specific SIPS can be assessed regarding the improvement of the system's resilience to extraordinary events.

Showing the full region of secure operation, i.e. not limiting to the first quadrant as in Figure 3, will display both positive and negative effects of armed SIPS. In this way, the decision procedures may be influenced to reduce the number of simultaneously armed SIPS. Such reduction may also decrease the risk of adverse effects in case of events unforeseen when designing the SIPS.

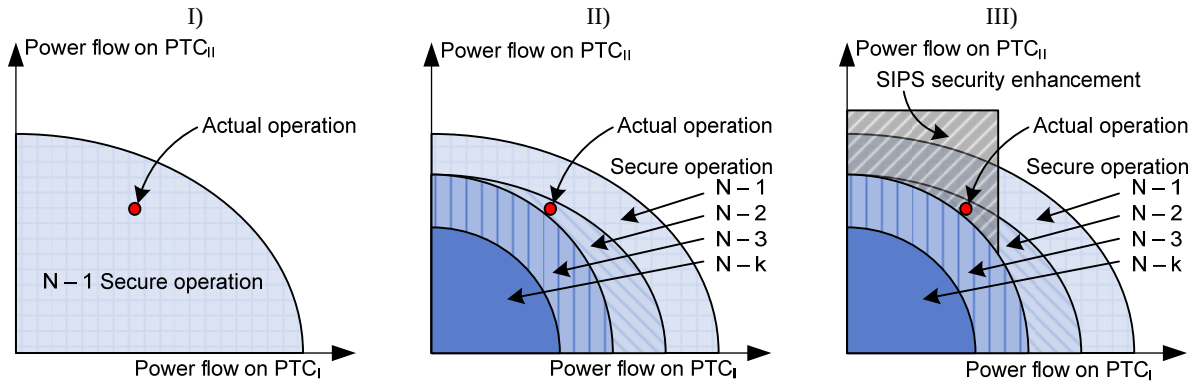

Figure 3: Visualising actual operating point and the secure region of operation[2] for a specific operating scenario, using the power flow on PTC_I relative to the flow on PTC_{II}: I) $N-1$ secure operation, II) $N-1$ to $N-k$ secure operation, II) SIPS security enhancement

4. SECURITY ASSESSMENT ANALYSIS

This section describes a security assessment of the transmission capacity across specific interfaces of a power system. The study is performed on the IEEE Reliability Test System 1996, which is a benchmark model for reliability assessment studies.

4.1 Study model

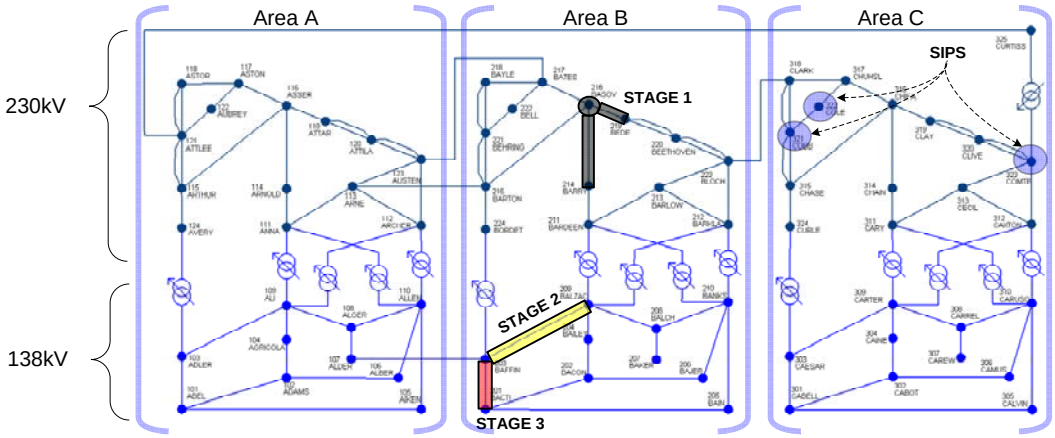

Figure 4: Single line diagram describing the IEEE Reliability Test System 1996, the dimensions does not reflect the line lengths. The markings *STAGES* and *SIPS* relate to the studies described in subsections 4.3 and 4.4, respectively.

The IEEE Reliability Test System 1996, defined in [13], consists of 73 buses in three equally designed areas, as shown in Figure 4. Each area has approximately 3.4 GW of installed

[2] In order to simplify the interpretation of the figures, the complexity is reduced with respect to the shapes in Figure 3; the more realistic shapes of a secure operating region is highly irregular.

production and a peak load of 2.8 GW. The areas are interconnected by five tie-lines, here referred to as the A-B, A-C, and B-C tie-lines, forming the inter-area power transfer corridors: PTC_{AB}, PTC_{AC}, and PTC_{BC}, respectively. In the analysed model, the optional DC-link is excluded, synchronous condensers are exchanged to SVCs, and the dynamic models suggested in [14] are used to represent the synchronous generators.
The studied operating scenario is a low load scenario, corresponding to a total system demand of approximately 50 % of the peak demand. Two cases of power exchange are studied, with power transfer between areas listed in Table I. In both cases, area A is a region with a low level of power interchange, while areas B and C are import and export regions, respectively.

Table I: Inter-area power exchange of the studied operating scenarios

	Case 1	Case 2
PTC_{AB} Power flow(MW) (rating: 175 + 2×500 MVA[3])	220	255
PTC_{AC} (MW) (rating: 500 MVA[3])	240	150
PTC_{BC} (MW) (rating: 500 MVA[3])	420	365
Area A Power export (MW)	15	-105
Area B Power export (MW)	-640	-620
Area C Power export (MW)	655	515

4.2 N – 1 security assessment

The $N-1$ security of both cases is assessed through dynamic contingency analysis, studying faults on transmission lines, transformers, and generators, where a 3-phase short-circuit is applied for 100 ms followed by disconnection of the affected unit.

Case 1 is identified to be insecure for the following contingencies: fault and trip of either of the A-C and B-C tie-lines (PTC_{AC}, PTC_{BC}). Since the desired power export from area C (655 MW) is well above the short term $N-1$ thermal rating of the tie-lines to area C, tripping one of these lines would result in an excessive overload of the remaining line. The dynamic analyses indicate that tripping PTC_{AC} results in rotor angle instability, which might lead to a large disturbance[4]. Hence, Case 1 can not be considered secure, from an $N-1$ perspective. Some of the results from the $N-1$ contingency analysis are shown in Figure 5. Parts I and IV describe the power flow on PTC_{BC} and PTC_{AC}: P_{BC} and P_{AC}, for all stable contingencies. Parts II-III and V-VI include the voltage angle and frequency difference over the same PTCs: $\Delta\delta_{BC}$, Δf_{BC} and $\Delta\delta_{AC}$, Δf_{AC}, for all studied contingencies (except when the PTC itself is tripped). The analysis includes contingencies with the short-circuit applied on either end of a line, hence two cases where A-C and B-C tie-line trips can be seen in the figure. The dashed red curves represent contingencies where the short-circuit is on the C-side of the line. These contingencies have a significantly higher impact on the system than contingencies where the short-circuit is on the other side of the line, as can be seen in parts II and III of the figure.

[3] The thermal overload capabilities of all lines are 120 % for 24 hours and 125 % for 15 minutes.

[4] It should be noted that in a power flow simulation, the disconnection of PTC_{AC} resulted in a stable solution, although with approximately 135 % overload of PTC_{BC}. Assuming the PTC_{BC} would trip, the system separates into two islands which could remain in stable operation depending on islanding control and the level of reserves available in each island. These results demonstrate an important difference between dynamic and power flow simulations, where the latter disregards the transient phenomena and therefore may not be able to identify the criticality of the contingency.

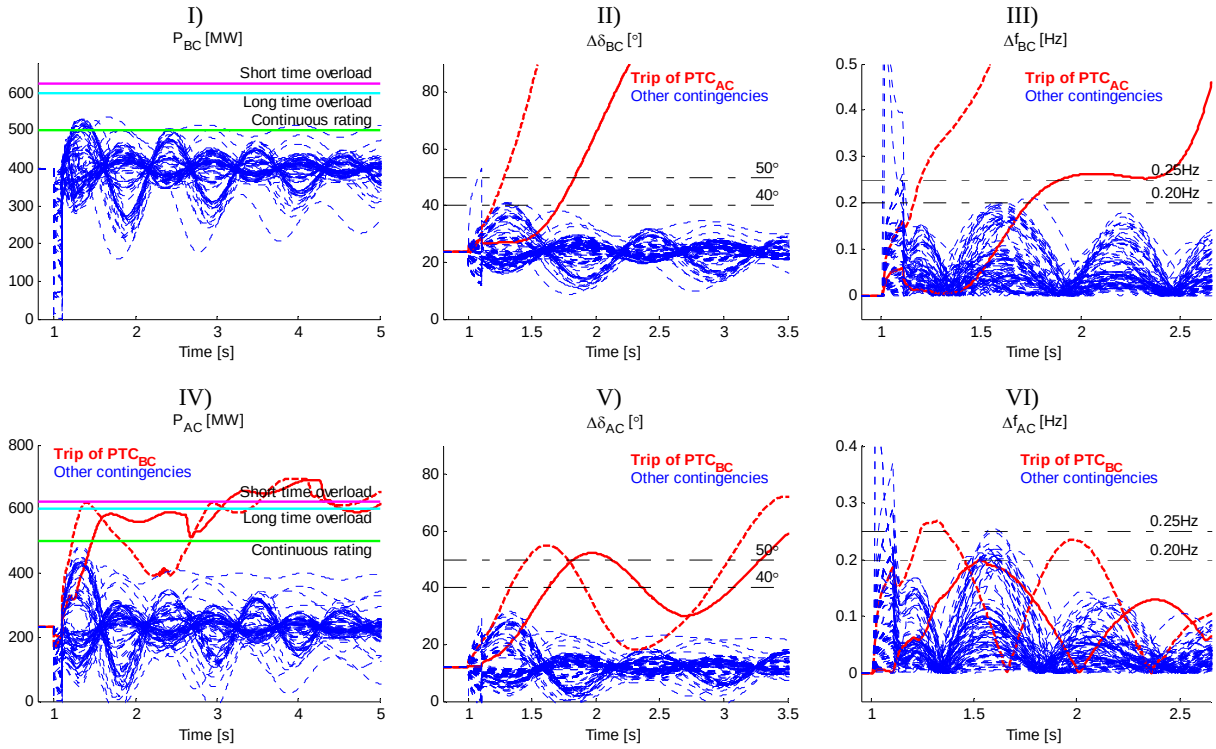

Figure 5: Results from the $N-1$ contingency analysis of Case 1, showing power flow, angle difference and frequency difference of PTC_{BC} (I-III) and PTC_{AC} (IV-VI)

Case 2 has been found secure for all the analysed contingencies, even though the desired power export from area C (520 MW) is above the continuous $N-1$ thermal rating of the tie-lines from area C, it is well below their long term overload capability.

4.3 N – k security assessment

The $N-k$ security of Case 2 has been assessed through both an $N-k$ contingency analysis and an analysis of common cause failures.

The $N-k$ contingency analysis is performed with consecutive contingencies, where the subsequent contingency occurs after the system has reached a steady state, but before any generation re-dispatch has taken place. A set of contingencies including the largest generation unit in area B (located on bus 221, see Figure 4) and PTC_{BC} is identified to cause instability. Independently of which contingency is occurring first, the system cannot regain stable operation after the second contingency. This suggests that Case 2 can be considered $N-1$ secure, but $N-2$ insecure[5].

Common cause failures, where the failure of a single item leads to the disconnection of several components, are not always a part of an ordinary $N-1$ contingency analysis. The consequences of such failure may have high impact on the system, and an example of this is described here.
The breaker-and-a-half configuration shown in Figure 6, describes the layout of substation 216, where a failure of the midsection breaker results in the disconnection of the outgoing lines to buses 214 and 219.

[5] Other contingency sets leading to instability can be identified through a more extensive $N-k$ contingency analysis, however, the number of subsequent contingencies will be minimum two.

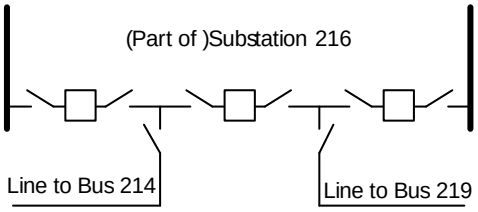

Figure 6: Single line diagram describing substation 216, with breaker-and-a-half configuration feeding lines to buses 214 and 219, according to [13].

In both Case 1 and 2, such failure leads to thermal overload of lines, followed by a thermal cascade, resulting in instability. The first part of the event can be separated in three stages, as marked in Figure 4:

- Stage 1 includes the failure at bus 216 and the trip of lines 216-214 and 216-219
- Stage 2 represents the overload and trip of line 203-209
- Stage 3 represents the overload and trip of line 203-201.

The thermal capacity of each of the lines in stages 2 and 3 is 175 MVA[6].

In Case 2, the overload in Stage 2 (124%) is just below the short-term emergency rating of the line, implying that there might be time to implement manual remedial actions before any protection disconnects the line. If such actions are not taken, or if the actions are insufficient, the line is likely tripped. In Stage 3, the line load (153 %) is far beyond its short-term emergency rating, which might lead to a fast protective disconnection of this line. If the line is tripped, the main part of area B is fed only through PTC_{BC}, and the system experiences instability. Case 2 can thus be considered $N-1$ secure, but $N-1$ inadequate when considering common cause failures.

This study reveals both the importance in identifying failures to include in the contingency analysis of a security assessment study, and that insufficient remedial actions, to mitigate the overload of a line which might seem to be of minor importance to the system state, may cause instability.

4.4 SIPS security enhancement

It is possible to design System Integrity Protection Schemes to improve the security of the analysed cases. Here, a study is made of a generator tripping scheme in area C and its influence on the $N-1$ security of Case 1. The efficiency of three different types of arming and activation/triggering signals is assessed:

I. Event-based, monitoring the trip signal of circuit breakers in PTC_{AC}: $SIPS_{CB}$
II. Response-based, monitoring the voltage angle differences over PTC_{BC}: $SIPS_{\delta}$
III. Response-based, monitoring the bus frequency at both sides of PTC_{BC}: $SIPS_{f}$

A manual (or automatic) arming is assumed to limit the operating scenarios where the SIPS can be triggered, and that, e.g., the level of inter-area power transfer is used to identify an appropriate level of generation tripping in each scenario. The mitigating action studied here, is acting on sources in the production dense 230 kV region of area C, as marked in Figure 4.
A thorough assessment of the arming procedures and activation signals is necessary to limit the risk of inappropriate SIPS actions. Arming procedures can be designed through identification of the operating criteria that defines the secure operating area, while an

[6] The thermal overload capabilities of all lines are 120 % for 24 hours and 125 % for 15 minutes.

extensive dynamic analysis is needed to identify appropriate activation signals and their magnitude. Here, the analysis is limited to the cases and contingencies described previously.

From Figure 5, the unstable contingencies are easily distinguishable in both $\Delta\delta_{BC}$ and Δf_{BC}, supporting their potential as SIPS activation signals. It is suggested that an internal arming is used together with a time delay, to prevent unwanted SIPS action during switching events. Based on the results of the dynamic contingency analysis, the suggested arming and activation signal magnitudes, as marked in Figure 5, are:

$\Delta\delta_{BC}$ - arming: 40° for 200ms, activation: 50°

Δf_{BC} - arming: 0.2Hz for 200ms, activation: 0.25Hz

δ and f measurements are considered to be available, from e.g. a WAMS, and the total delay between measurement and the implementation of mitigating action is assumed to be no longer than 100 ms.

Figure 7 describes the response, after the trip of PTC_{AC}, with and without the suggested SIPS, including the power flow, angle, and frequency difference over PTC_{BC}. The dashed curves in part II represent the fault with the short-circuit occurring at the C-side of the line. The system response of this contingency is too rapid for the $SIPS_{\delta}$ and $SIPS_{f}$ solutions to act before the system becomes unstable, and only $SIPS_{CB}$ results in a stable solution. All other curves in the figure represent the fault with the short-circuit occurring at the A-side of the line. For this fault, all the studied SIPS solutions results in a stable post-fault system, however, the event-based $SIPS_{CB}$ scheme shows lower levels of oscillations due to the more rapid activation than the response-based schemes.

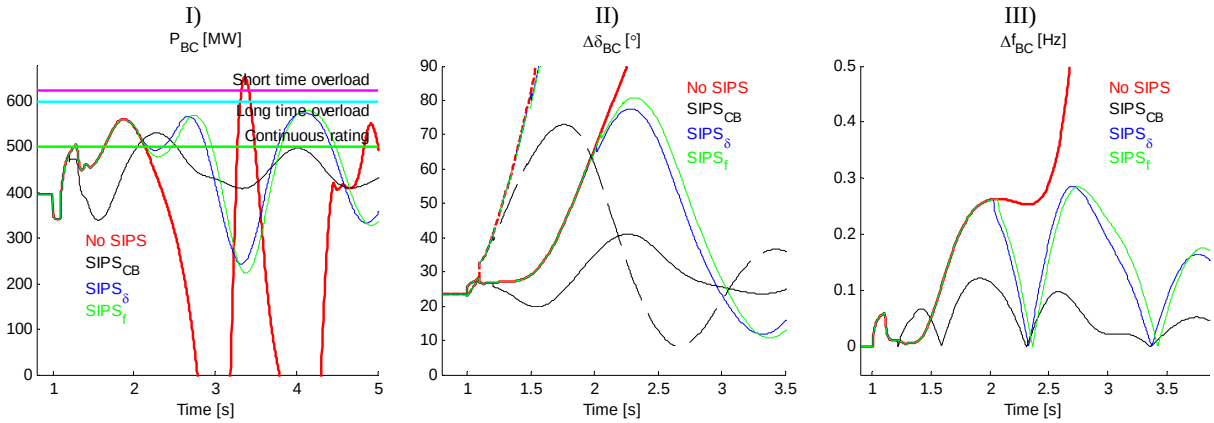

Figure 7: Results for different SIPS activation signals after trip of PTC_{AC}, in Case 1: I) P_{BC}, II) $\Delta\delta_{BC}$, III) Δf_{BC}

In Figure 8, the characteristics of PTC_{BC} are included in the form of the power-voltage, the power-angle, and the rotor motion curves. According to the equal-area criterion, passing the unstable equilibrium point, here approximated by (P_S, $\Delta\delta_U$), would result in instability since the decelerating torque was not able to sufficiently decelerate the machine before it starts to accelerate out of synchronism. This behaviour is seen in the scenario without SIPS, where the angle increases beyond $\Delta\delta_U$. For the scenarios with SIPS, the maximum angles ($\Delta\delta_{CBmax}$ and $\Delta\delta_{\delta fmax}$) are lower than $\Delta\delta_U$ and the system stabilises at a post-contingency stable equilibrium point (represented by V_S, P_S, and $\Delta\delta_S$). It is, however, complex to identify the actual unstable equilibrium point, since: the mechanical power is not constant but depending on the response of the governor controller, and the voltage dependency of loads will affect the electrical power flow. Through simulations with increased delay in SIPS mitigating actions, the actual $\Delta\delta_U$ is approximated to 110degrees for the studied scenario.

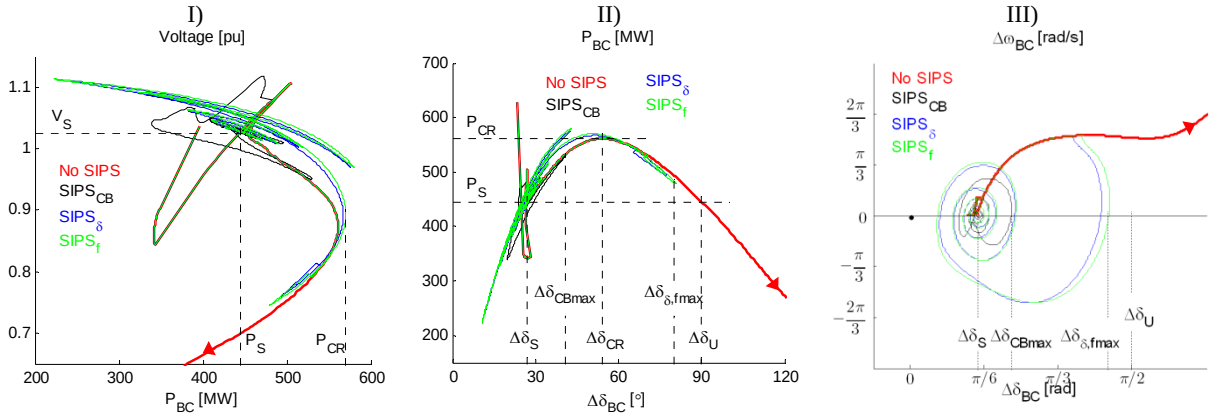

Figure 8: Results for different SIPS activation signals after trip of PTC_{AC}, in Case 1: I) Power-voltage (nose) curve, II) Power-angle characteristics, III) Rotor motion trajectory

5. DISCUSSION AND CONCLUSIONS

This study gives examples of SIPS solutions utilising monitoring parameters provided by a WAMS. The studied SIPS solutions are not the optimal ones, and other schemes can further improve the $N-1$ security of the studied cases. Response-based solutions, as the suggested $SIPS_\delta$ and $SIPS_f$ will not be as fast as event-based SIPS, but they will be able to provide increased protection against multiple or unforeseen contingencies that event-based protections can not. Improvements in SIPS activation can be done using adaptive response, providing optimal protection in each operating scenario. The sufficient amount of mitigating actions depends on the required actions for the system to remain stable. In the case of generation tripping, factors such as the level of spinning reserves and reactive power capabilities available after the SIPS action are needed to be considered. It is also possible to select the mitigating actions through a sensitivity analysis, assessing the stabilising effects of each component.

This study also demonstrates that thermal overloading of a line, which seems to be of minor importance to the system state, can cause instability if mitigated actions are not implemented. Furthermore, it is shown that power flow simulations might not be able to identify critical contingencies, since transient phenomena are disregarded. These findings underline the importance of performing dynamic contingency analysis during a security assessment study, also in power systems where thermal capacities is the normal limitation on the power transfer capacity.

The described visualisation of an $N-k$ secure operating region, together with a continuous monitoring of the *k-index*, could provide improved awareness of the power system's vulnerability to extraordinary events. This does however imply the need of continuously performed $N-k$ contingency analysis to properly identify the vulnerabilities as the operating scenario of the system changes.

6. ACKNOWLEDGEMENT

The authors would like to thank PhD candidate J. Lamponen and Professor L. Haarla, both at Aalto University School of Electrical Engineering, Espoo, Finland, for the cooperation in developing the concept of dynamic $N-k$ vulnerability assessment and in the work of modelling and simulation of the IEEE Reliability Test System 1996.

The support provided by T. Toftevaag at SINTEF Energy Research, related to power system dynamic phenomena, is gratefully acknowledged.

BIBLIOGRAPHY

[1] Nordel, *The Nordic Grid Code*. 2007; Available from: www.entsoe.eu/

[2] IAEW, CONSENTEC, *Analysis of Electricity Network Capacities and Identification of Congestion, Final Report*. 2001; Available from: ec.europa.eu

[3] CIGRE Task Force 38.03.12, *Power system security assessment: A position paper*, ELECTRA, no. 175, Dec., 1997

[4] IEEE Task Force on Blackout Experiences, Mitigation, and Role of New Technologies, *Blackout Experiences and Lessons Best Practices for System Dynamic Performance, and the Role of New Technologies*, Special Publication 07TP190, 2007

[5] Madani, V., Novosel, D., Horowitz, S., Adamiak, M., Amantegui, J., Karlsson, D., Imai, S., Apostolov, A., *IEEE PSRC Report on Global Industry Experiences With System Integrity Protection Schemes (SIPS)*, IEEE Transactions on Power Delivery, 2010, Vol. 25, p. 2143-2155

[6] CIGRE Task Force 38.02.19, *System Protection Schemes in Power Networks*, Technical Brochure 187, 2001

[7] Statnett, *Nettutviklingsplan 2010. Nasjonal plan for neste generasjon kraftnett (in Norwegian)*. 2010; Available from: www.statnett.no

[8] Breidablik, Ø., Giæver, F., Glende, I. *Innovative Measures to Increase the Utilization of Norwegian Transmission*, IEEE Power Tech Conference, 2003, Bologna, Italy

[9] Walseth, J.Å., Eskedal, J., Breidablik, Ø., *Analysis of Misoperations of Protection Schemes in the Nordic Grid - 1st of December 2005*, Protection, Automation & Control World, 2010,

[10] Johansson, E., Uhlen, K., Nybø, A., Kjølle, G., Gjerde, O. *Extraordinary events: Understanding sequence, causes, and remedies*, European Safety & Reliability Conference, 2010, Rhodes, Greece

[11] CIGRE Study Committee 39, *The Control of Power Systems During Disturbed and Emergency Conditions*, Technical Brochure 36, 1989

[12] Uhlen, K., Pálsson, M., Time, T.R., Kirkeluten, Ø., Gjerde, J.O. *Raising stability limits in the Nordic power transmission system*, 14th Power Systems Computation Conference, 2002, Sevilla, Spain

[13] Reliability Test System Task Force, *The IEEE reliability test system - 1996*, IEEE Transactions on Power Systems, Vol. 14, No.3, 1999

[14] Johansson, E., Uhlen, K., Kjølle, G., Toftevaag, T. *Reliability evaluation of wide area monitoring applications and extreme contingencies*, Power Systems Computation Conference, 2011, Stockholm, Sweden