Impact of the reliability of ICT systems on power systems with system integrity protection schemes

Frédéric Sabot, Pierre Henneaux, Pierre-Etienne Labeau, Jean-Michel Dricot

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Impact of the reliability of ICT systems on power systems with system integrity protection schemes

Impact de la fiabilité du réseau de communication sur l'efficacité des actions correctives automatiques effectuées sur les réseaux électriques

Frédéric Sabot
BEAMS – Electrical Energy
Université libre de Bruxelles
Brussels, Belgium
frederic.sabot@ulb.be

Pierre Henneaux
BEAMS – Electrical Energy
Université libre de Bruxelles
Brussels, Belgium
pierre.henneaux@ulb.be

Pierre-Etienne Labeau
Service de Métrologie Nucléaire
Université libre de Bruxelles
Brussels, Belgium
pierre.etienne.labeau@ulb.be

Jean-Michel Dricot
Cybersecurity Research Center
Université libre de Bruxelles
Brussels, Belgium
jean-michel.dricot@ulb.be

***Résumé*—La transition énergétique conduit à l'installation de sources distribuées dont la production est fortement variable et qui imposent donc de nouvelles contraintes au réseau électrique. Les possibilités de renforcement du réseau étant limitées à court terme, opérer le réseau en utilisant les critères traditionnels de sécurité préventive limiterait la flexibilité du réseau. Aussi, une telle manière d'opérer s'éloigne de plus en plus de l'optimum économique. Utiliser des moyens de sécurité corrective permet de diminuer les coûts mais introduit de nouveaux modes de défaillances. En effet, les actions correctives nécessaires doivent être appliquées rapidement et de manière fiable. Un exemple de sécurité corrective est l'utilisation de systèmes de protection de l'intégrité du réseau (SIPS an anglais). Le SIPS considéré dans cette communication consiste en (i) des Phasor Measurement Units (PMUs) qui mesurent des valeurs locales de tension et courant avec un taux d'échantillonnage de 25-120 Hz, (ii) un Centre de Contrôle (CC) qui détermine l'état du système à partir de ces mesures et décide des mesures correctives nécessaires, (iii) un réseau de communication qui fait le lien entre les PMUs et le CC. Cette communication étudie l'impact d'un mauvais fonctionnement du réseau de communication sur la stabilité d'un réseau électrique équipé d'un tel SIPS.**

***Keywords*—schémas de protection de l'intégrité du système, théorie des files d'attente, fiabilité des réseaux de télécommunication, systèmes cyber-physiques, cyber-attaques**

This work has been prepared with the support of the Belgian Energy Transition Fund, project CYPRESS (https://cypress-project.be).

***Abstract*—With the energy transition, the share of distributed renewable energy resources, whose production is highly variable, is increasing in the grid. As reinforcements are not always desirable (costly), relying solely on preventive security might strongly limit the grid flexibility, thus leading to non-optimal operations. Corrective security appears as an attractive alternative, but it introduces new failure modes as corrective actions have to be performed timely and reliably. An application of corrective security is the use of System Integrity Protection Schemes (SIPSs). The SIPS considered in this work consist in (i) Phasor Measurement Units (PMUs) that perform local measurement of electrical values with a sampling rate of 25-120Hz (ii) a Control Centre (CC) that estimates the state of the system from the measures of the PMUs and automatically takes necessary corrective actions (iii) a communication infrastructure that links the PMUs to the CC. This paper studies the impact of imperfect communications on power systems equipped with this kind of SIPS.**

***Keywords*—system integrity protection schemes, queuing theory, telecommunication network reliability, cyber-physical systems, cyber-attacks**

I. Introduction

Due to the increase in the share of renewable energy sources and the difficulties to build new transmission infrastructure, dynamic stability issues are becoming more common in power systems throughout the world. System integrity protection schemes (SIPS) are a cost-effective way to mitigate those

issues and are thus being installed by many Transmission System Operators (TSOs) [1]–[4]. The integration of SIPSs is usually done in two phases. In the first phase, the TSO designs a SIPS to mitigate a specific problem in the system. This SIPS requires data from only a few buses to detect this specific problem and has a small set of possible actions. In this phase, the SIPS usually has a dedicated ICT infrastructure [2]. In the second phase, the TSO starts to rely on SIPSs to mitigate various issues. In this case, a more scalable design consists in a centralised Control Centre (CC) that has access to measurements from most buses in the system. Then, a dedicated ICT infrastructure makes less sense. The SIPS thus uses the existing ICT infrastructure used for traditional operations [3], [4]. Beyond scalability, an advantage of the second type of SIPS is that they can make use of classical state estimation algorithms to compute the most likely state of the whole system even with partial information.

Most of the literature on SIPS reliability focuses on the first kind of SIPS, see e.g. [5] and the references therein. For this kind of SIPS, the dedicated infrastructure and small number of elements implies that bandwidth issues do not exist. These systems can thus be modelled with classical reliability techniques (Markov chains, reliability block diagrams, etc.). For the second kind of SIPS, this is no longer true. Most of the papers studying those SIPSs thus use (co-)simulations to predict the behaviour of the ICT infrastructure [6]–[8]. In this work, we propose to use queuing theory instead. The advantage of queuing theory is that it gives an analytical formulation for the delays in the ICT system. It thus allows to have a better understanding of the system and to explore the impact of disturbances more easily.

Section II describes the physical part of the considered test case as well as how it is operated. Section III describes the cyber part and how to design it using queuing theory. Section III also explains how to monitor the performance of the ICT infrastructure. Section IV and section V respectively analyse the impact of ICT failures and the impact of traffic-based cyber-attacks on the performance of the considered power system equipped with a SIPS. Section VI concludes with a summary and perspectives.

II. Physical system

The physical part of the case study considered in this work is a modified version of the Roy Billinton Test System (RBTS) [9]. It is shown in Fig. 1. This system is similar to the transmission grids of Canada and Nordic countries. Indeed, it has hydro generators in the north (bus 1), connected with long lines (L2, L3 and L7) to the load centres in the south (mainly buses 3 and 4). It also has coal (as the RBTS was designed in 1989) generators closer to the loads (bus 1). The peak load of the RBTS is 185 MW.

These systems usually have issues with angle stability, which can be alleviated using a SIPS. (Rotor) angle stability is the capability of (synchronous) generators to remain synchronised after disturbances. In other words, it refers to their capacity to maintain or restore the equilibrium between

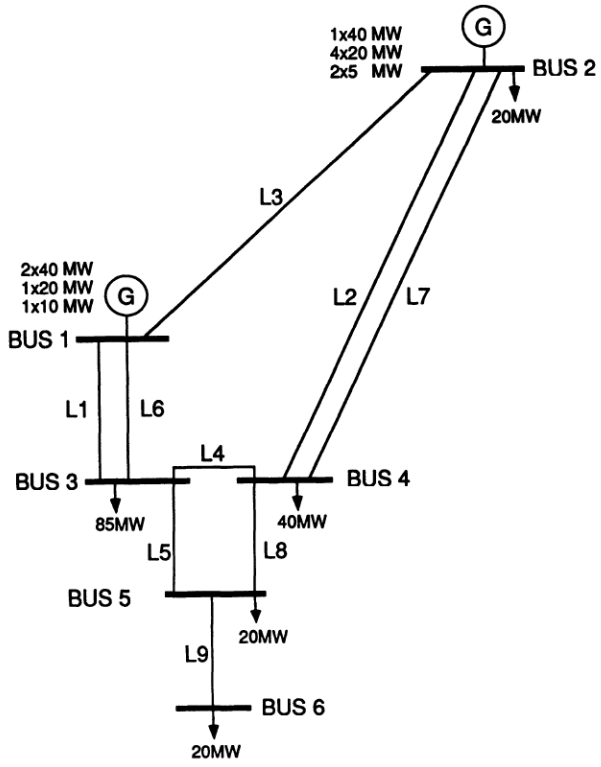

Figure 1. RBTS single line diagram. Adapted from [9]

the electromagnetic and mechanical torque that are applied by the grid and the turbine respectively. A more complete introduction to angle stability can be found in [10]. It is important to note that while transient stability issues have historically been mostly observed in countries with very long lines, the increasing share of renewable generation and the difficulties to build additional infrastructures are expected to lead to increasing transient stability concerns in all countries. A SIPS has recently been installed in Belgium [2].

To increase the likelihood of angle stability issues in the RBTS, the line lengths have been doubled. Also, no dynamic data was available for this system, and they have been added in this work. The full data set used is available on [1]. The power system simulator Dynaωo has been used [11]. The load is assumed to vary between 100 and 185 MW depending on the time of day and of the year. The distribution of the load between the different buses is assumed constant. The loading order of the generators is in increasing order of marginal costs, i.e. hydro units have priority, then the coal units are activated in decreasing order of capacity. A minimum spinning reserve of 40 MW is also assumed.

If operated this way, the system encounters angle stability issues when the load is in the 140 to 160 MW range. This corresponds to operation close to maximum hydro capacity, and relatively low coal production. This results in high power flows from bus 2 to the rest of the system. This worst single

[1] https://github.com/FredericSabot/dynawo/tree/6_LambdaMu2022

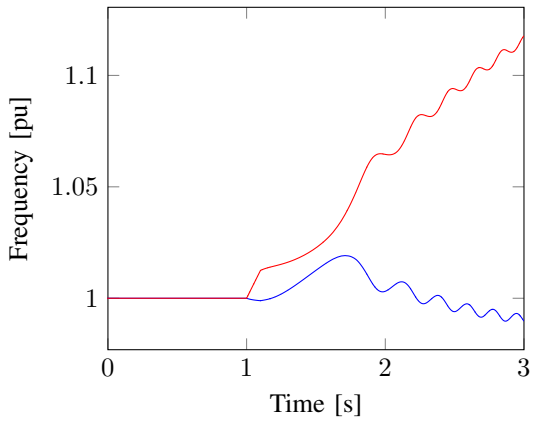

Figure 2. Evolution of the frequency at bus 1 (blue) and 2 (red) after a short circuit fault at t = 1 s on line 3 near bus 2. Total load is 160 MW

Table I
MAXIMUM ALLOWABLE DELAYS FOR EACH OF THE RELEVANT GENERATOR DISCONNECTIONS DEPENDING ON THE TOTAL LOAD

Load [MW]	**Disconnection of X at bus 2**	
	20 MW	**2x20 MW**
100-130	N/A	N/A
140	252 ms	352 ms
160	173 ms	302 ms
185	N/A	N/A

contingency that can occur on this system is a short-circuit fault on line 3 near bus 2 (assumed to be cleared in 100 ms by opening the line). Fig. 2 shows the evolution of the frequency at buses 1 and 2 after this contingency. As can be seen from the figure, generators at bus 2 are not able to evacuate enough electrical power after the fault. They thus accelerate and quickly lose synchronism.

A preventive solution to this issue would be to limit to hydro generation (bus 2). However, this would have to be compensated by an increase of the coal generation (bus 1) that has higher marginal cost and emits more CO_2. This is unwanted, especially knowing that the fault has a low frequency of occurrence. A more cost-effective solution is to use a SIPS that will only act after the occurrence of a fault. The SIPS can take several actions to keep the system stable after a fault. The traditional solution is to disconnect one or two generators at bus 2 to reduce the power flows in lines 2, 3 and 7. This must be done in a timely manner to avoid loss of synchronism. Table I lists the maximum time delay between the occurrence of the fault and the disconnection of generator(s) at bus 2. It can be noted that if two generators are disconnected instead of one, higher delays can be allowed. This however causes a larger drop in frequency that causes some load to be disconnected by under-frequency load shedding protections. The possible actions of the SIPS are thus in decreasing order of preference: fast disconnection of a generator (no consequences), slower disconnection of two generators (some load shedding), no actions (loss of synchronism possibly leading to a blackout).

Table II
MINIMUM LOAD REDUCTION AT BUS 3 AFTER A FAULT ONE LINE 3 NEAR BUS 2

Total load [MW]	**Load 3 [MW]**	**Minimum load reduction at bus 3 if applied in**		
		100 ms	**200 ms**	**300 ms**
140	64.3	10.7 MW	13.2 MW	19 MW
160	73.5	15.7 MW	19.7 MW	28.2 MW

Here, we also propose a second more futuristic type of action based on demand response. It consists in quickly reducing the load at bus 3 (the load bus that is the closest to bus 1) after the fault. This causes an increase of the frequency of the generators at bus 1 which makes them stay synchronised with generators at bus 2. Table II shows the magnitude of the load reduction necessary to keep the system stable. Similarly to the first case, a faster activation of the SIPS leads to less severe corrective actions. An advantage of this method compared to the first one is that the system can then be brought faster back to normal operation. Indeed, the loads can be restored to their initial values after a dozen seconds. While in the first case, the disconnected generators must be shut down and restarted before being reconnected. This method is however more complex as it requires to have communication with numerous individual customers. Indeed, we only want to disconnect loads that are willing to be disconnected for a dozen of seconds (e.g. heaters, fridges, batteries), but not entire feeders. This has implications that are discussed more in details in next section.

III. CYBER SYSTEM

This section describes the design of the ICT infrastructure that is necessary for the SIPS to work. In particular, section III-A describes how to size the infrastructure using queuing theory. And, section III-B explains how to monitor in real-time the performance of the ICT infrastructure.

A. *Infrastructure sizing*

As briefly described in the introduction, we consider a centralised SIPS. More precisely, we consider that every bus is equipped with a Phasor Measurement Unit (PMU) that sends measurements (voltage, currents, frequency, and possibly breakers status for newer PMUs [1]) to a CC. Usually, Phasor Data Concentrators (PDCs) are placed between the PMUs and the CC to aggregate the PMU traffic. Due to the small size of our test system but without loss of generality, we however do not consider them here.

It is thus necessary to have a communication infrastructure to link the PMUs to the CC. TSOs can either have their own infrastructure, this is e.g. the case in the UK [12, p110] and in Germany [13, p42] where OPtical Ground Wires (OPGWs) are installed on top of most transmission lines, or rent it from an Internet Service Provider (ISP). In the second case, the design of the infrastructure is outsourced to the ISP. We will thus focus on the first one. Also, we consider that a single OPGW is installed in parallel to every transmission line

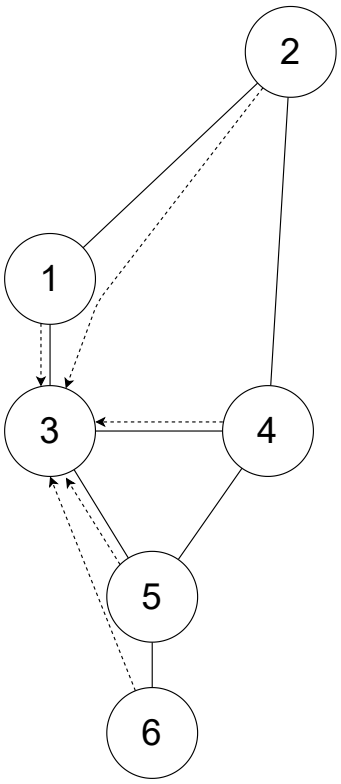

Figure 3. Communication network in parallel to the RBTS. Plain lines represent communication links, and dashed arrows represent PMU traffic flows in normal operation

(including the double lines). The topology of the considered ICT infrastructure is shown in Fig. 3.

TSOs usually only use a fraction of the bandwidth provided by the OPGWs. They thus often choose to rent part of this bandwidth to ISPs [12, p110]. The traffic used for the SIPS should however not be in competition with the ISPs' traffic. This is achieved using Quality of Service (QoS) mechanisms such as weighted fair queuing. These mechanisms allow to guarantee a given amount of bandwidth for the SIPS. Below, we show how to use queuing theory to determine the minimum bandwidth to reserve for the SIPS to stay under a maximum delay.

The most common assumption in communication network traffic engineering is to consider that the distribution of arrivals is Poissonian [14]. In other words, it means that packets arrive with a constant mean rate and independently of the time elapsed since the last event. This assumption is very often valid in ISP networks due to the large number of independent inbound traffic sources. Then, we define the traffic load (or traffic intensity) of an element (router, firewall, etc.) as:

$$\rho = \lambda/\mu \tag{1}$$

where λ is the arrival rate of packets in the element [packets/s], and μ is the processing rate of the element [packets/s]. Then, from the Poisson assumption, a well-known result from

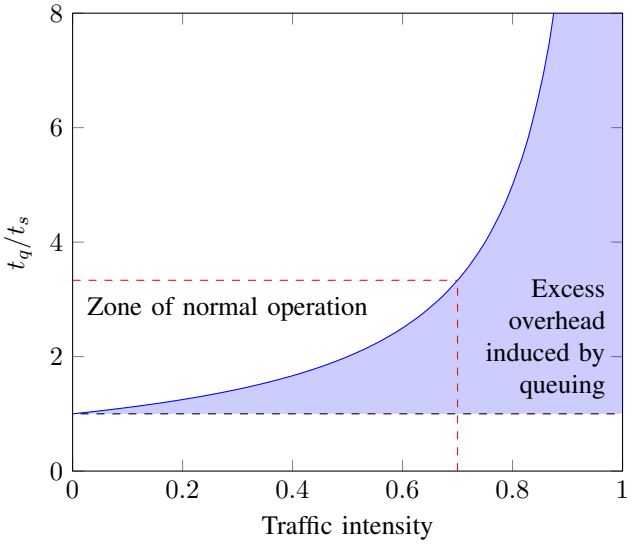

Figure 4. Communication delays as a function of congestion

queuing theory [14] is that the average number of packets in the queue of the element is given by[2]:

$$N = \frac{\rho}{1-\rho} \tag{2}$$

We can then use Little's law [15] that states that the average queuing time t_q [s] spent by a packet in a system is given by:

$$t_q = N/\lambda \tag{3}$$

(Little's law is valid for any stationary system, e.g. a single queue or a complex network.) It is also interesting to decompose t_q into the waiting time t_w and the processing time $t_s = \frac{1}{\mu}$. For this, we simply observe that when a packet arrives in a queue, it must wait for the average N packets already present to be processed. So,

$$t_w = N t_s \tag{4}$$

From (3) and (4), we deduce that,

$$t_w = \frac{\rho}{1-\rho} t_s \tag{5}$$

and,

$$t_q = \frac{1}{1-\rho} t_s \tag{6}$$

Equation (6) is plotted in Fig 4. This figure illustrates clearly the impact of congestion on delays. From this figure, we can also observe that, in order to limit the waiting delay (and its derivative with respect to ρ), we need to operate the network such that ρ is lower than 0.7 or even 0.5.

Now, we illustrate this methodology by applying it on the RBTS. For this, we consider that each PMU generates 120 kbps of traffic (packets of 300 bytes [16] sent at 50 Hz), that 300 kbps is reserved in each link for the SIPS, and that

[2]Assuming a steady-state system, infinite buffer size, and $\rho \leq 1$

Table III
COMPUTATION OF THE AVERAGE TIME SPENT BY A PACKET IN A GIVEN LINK FOR A RESERVED BANDWIDTH OF 300 KBPS

Link	Traffic	ρ	N	t_q [ms]
2-1	120 kbps	0.4	0.67	13.3
1-3	240 kbps	0.8	4	40
4-3	120 kbps	0.4	0.67	13.3
5-3	240 kbps	0.8	4	40
6-5	120 kbps	0.4	0.67	13.3

Table IV
AVERAGE COMMUNICATION DELAYS BETWEEN EACH PMU AND THE CC

PMU #	t_q (ms)
1	40
2	53.3
4	13.3
5	40
6	53.3

packets are routed to the shortest path as shown in Fig. 3. Also, we consider that the processing time of routers is limited by the bandwidth of links, i.e. is equal to the packet size divided by the bandwidth, so 8 ms. We can compute the average queuing time in each router[3] as shown in Table III. Then, the average communication delay between a given PMU and the CC is simply given by the sum of the delays in the path between this PMU and the CC. Those delays are shown in Table IV.

These delays can be compared with the allowable delays for generator tripping (Table I). The smallest allowable delay is 173 ms. From this delay, we have to remove the constant delays. We consider 5 ms and 10 ms for the processing times in the PMUs and CC respectively [6], 20 ms worst-case delay due to the sampling rate of 50 Hz, and 60 ms for the circuit breaker of the generator [17]. We also consider 8 ms communication delay between the CC and the generator (i.e. the processing time in one router, the message to the generator goes in the opposite direction compared to the PMU traffic and is thus not affected by congestion). We neglect the propagation delays (1 ms per 200 km for a refractive index of the communication medium of 1.5). There is thus 70 ms remaining for the communication delays between the PMUs and the CC. We can then verify than the average delays in Table IV are lower than 70 ms. It is also possible to compute the probability of the delays being lower than 70 ms. This is however more complex, and we refer to [14] for more information.

The computations above have been made assuming a Poisson distribution of arrivals. The PMUs however send packets at a deterministic and constant rate. The developments above are still useful because the merging of several influxes in larger network tends to produce Poisson distributions. Also, the above method will very often lead to conservative results. In our particular case, simulations in ns-3 [18] resulted in communications delays of 8 ms (the processing time in one router) for PMUs 1, 4 and 5, and 16 ms (twice the above value) for PMUs 2 and 6. Finally, due to the small amount of traffic needed by the SIPS (and its critical nature), it is inexpensive to have large margins. This is true even for large networks. For example, even if we consider than all 2700 substations operated by the french TSO (mostly at 225 and 400 kV level) [19] send PMU packets (300 bytes [16]) at a sampling rate of 50 Hz, it only results in a total of 360 Mbps[4]

If the SIPS makes use of demand response, it is also necessary to have a communication infrastructure between the CC (and/or the individual buses) and end-users. Due to high geographical dispersion of end-users, it is completely unrealistic for the TSO to build its own ICT infrastructure for this purpose. The TSO thus has to make service level agreements (SLAs) with distribution system operators (DSOs) or ISPs. The TSO defines the amount of necessary bandwidth and maximum delay, and the DSO or ISP then has to make sure that those constraints are satisfied (e.g. using queuing theory, QoS, etc.).

B. Monitoring of delays

Even if the ICT infrastructure has been appropriately sized, it is still useful to monitor its performance and to verify that the delays are under a given bound. Indeed, delays could increase following failures, bugs, attacks, increase of the traffic, etc. When high delays are detected, the SIPS should arm schemes that are less time critical (i.e. disconnection additional generators or loads), or send an alarm to the operators such that they take preventive actions (e.g. reduction of the production at bus 2).

Monitoring the communication delays between the PMUs and the CC is direct since the packets sent by PMUs are precisely time-tagged (PMUs' clock are synchronised via GPS). For communication with end-users, this is not possible. An alternative is to estimate communication delays from Round Trip Time (RTT) measurements. In other words, when the TSO sends a message to a given end-user, it measures the time that passed between sending the message and receiving the acknowledgement message from the end-user. Assuming a symmetric network, the one-way delay is half the RTT. Since the TSO might not always need to communicate with end-users, it is necessary to use so-called keep-alive messages to have a continuous monitoring of the RTT. RTT measurements are used very often in ICT networks. We present below a RTT-based mechanism used by TCP as defined by the Internet Engineering Task Force standard [20]. There are similar mechanisms in other communication protocols such as RTP (Real-Time Protocol).

In TCP, when an application sends a messages, it expects to receive an acknowledgement from the recipient. If it does not receive one, it resends the message. The Retransmission

[3]For routers where multiple PMU influxes are merged, we can still assume a Poisson distribution of arrivals due to the additivity of the Poisson distribution. Thanks to this additivity property, queuing theory can easily be applied in large networks.

[4]In the future, the size of the packets might increase slightly due to the transition to IPv6 (20 bytes), additional information regarding substation equipment being included in the PMU traffic (a few dozens of bytes), and longer cryptographic headers (a few dozens of bytes).

TimeOut (RTO) is defined as the maximum time after which a sender considers that if it did not receive an acknowledgement signal, then its message was lost and must thus be resent. The RTO can thus be seen as an upper bound (with a good probability) of the RTT. As the RTT can vary in time (due to variability of the traffic, seasonal effects, attacks, etc.), a "smoothed" RTT is defined. Each time a new measurement R' of the RTT is made, the smoothed RTT is updated according to:

$$\text{SRTT} = (1 - \alpha) \times \text{SRTT} + \alpha \times \text{R'} \quad (7)$$

where α is a parameter often set to 0.125. To compute the RTO, a safety margin is added to the SRTT. This margin is higher when there are higher variations of the RTT. Mathematically, we compute the variation of the RTT with:

$$\text{RTTVAR} = (1 - \beta) \times \text{RTTVAR} + \beta \times |\text{R'} - \text{SRTT}| \quad (8)$$

and the RTO as:

$$\text{RTO} = \text{SRTT} + 4 \times \text{RTTVAR} \quad (9)$$

The recommended value for β is 0.25.

IV. Impact of cyber failures

The impact of cyber failures is studied differently if the ICT infrastructure is owned by the TSO or by an ISP. In the first case, the TSO can simply perform the same analysis as in section III but considering that some of the links are failed. For example, after a failure of link 3-4, traffic from the PMU 4 will be redirected through path 4-5, 3-5 which will increase the occupancy rate and queuing delays along this path. A higher bandwidth will thus be necessary to stay under the target delay. Additionally, if simultaneous failures of communication links and power lines are considered (due to a common mode failure), an additional delay has to be considered for the rerouting of the traffic.

In the second case, cyber failures will usually have a lower impact. This is because ICP's networks are usually more meshed than TSO's grids. For example, Fig. 5 shows the core network of BT (formerly British Telecom). It consists of 8 inner core nodes that are fully linked to each other, and 12 outer nodes that are each connected to at least 3 core nodes.

Also, in this case, it is the ISP and not the TSO that has to make sure the cyber failures have a limited impact on the performance of the ICT infrastructure. The SLA should define to what level of reliability the ICT performance should be guaranteed. Carrier-grade lines are often leased with a reliability level of 99.999% (i.e. 5 minutes of total downtime per year).

V. Impact of traffic-based cyber-attacks

The impact of cyber-attacks is usually classified into three categories: confidentiality, integrity and availability. Loss of confidentiality has no direct impact on the power system. It must be addressed through the use of classical cryptography. Attacks on integrity (i.e. attacks that modify the data that is exchanged between different nodes) can cause wrong control

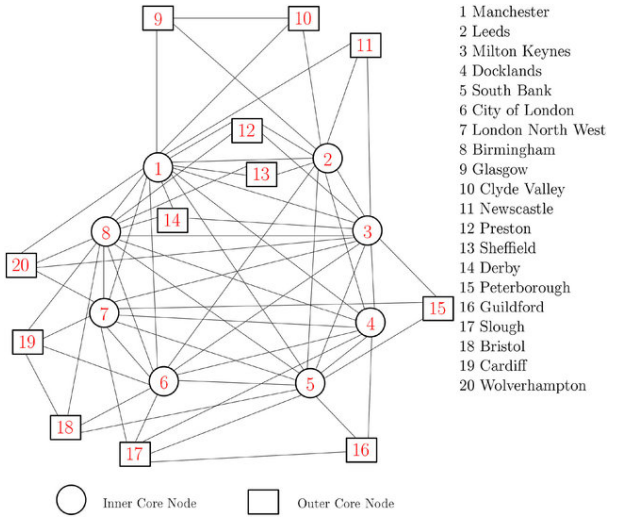

Figure 5. BT 21st Century Network [21]

actions either by modifying directly control messages, or by modifying the measurements that are necessary to perform control actions. One advantage of using a state-estimation-based SIPS is that it makes False Data Injection Attacks (FDIAs) more difficult. This is because the state estimator is based on a least square method. Measurements that have a high residual can thus be disregarded. This reduces the size of the set of possible successful attacks. There is a large body of literature on FDIAs (see e.g. the review papers [22], [23]). Specific cryptography techniques can also be used to protect integrity of the data (e.g. keyed hashing, authenticated encryption). We thus focus on availability attacks in this paper.

The most straightforward example of availability attack is the Denial of Service (DoS) attack. It is a volumetric attack that consists in simply exhausting computer resources by sending large amounts of redundant packets. The effect can intuitively be seen as a shift to the right in Fig. 4. When small to medium amounts of traffic (compared to the available processing capacity of the system[5]) are injected, it results in an increase of delays. When the total arrival rate is larger than the processing capacity of the system, then most packets are dropped; this is the most common case. QoS mechanisms can defend against DoS attacks, but they have to not only reserve bandwidth but also buffers.

The high amount of traffic caused by DoS attacks makes them easy to detect. They can thus often be mitigated automatically and relatively quickly. An attacker might thus prefer to use more "subtle" attacks to be less easily detected but still have an impact on the performance of the SIPS. For example, if an attacker is able to take control of a router, he can then drop arbitrary packets instead of sending them to their original destination. This will have a different impact depending on the protocols that are used. In this work, we follow the IEEE C37.118.2 recommendations, and consider that the traffic from

[5]We focus on link bandwidth in this work, but the processing capacity of the CC could also be a limiting factor. The effect is however the same.

PMUs uses UDP and the control traffic (from the CC) uses TCP [16].

If the attacker is unable to decrypt the packets going through the router he hijacked, he might choose to simply drops half the packets he receives. Since we consider no retransmission for monitoring packets, it means that half the data will no longer reach the CC. For example, if the router 1 (from Fig. 3) is attacked, then measurements from either bus 1 or 2 will be unavailable. In this case, we only lose one measurement. The state estimation algorithm can thus still compute the state of the whole system. However, in a real-scale system, individual routers (especially those near the CC) would see more measurements. It is thus possible to lose observability on part of the grid (standard methods for observability analysis can be used, e.g. [24]). Control messages on the other hand should never be completely missed, but they might need to be sent several times before being actually received. This introduce additional delays, and it would thus be useful to use a lower retransmission time than what is defined in [20].

If the attacker is able to decrypt the packets, he can cause more harm by dropping specific packets. For the SIPS that does not use demand response, the attacker can drop all the disconnection messages that are sent to the generators. This means that the SIPS is basically out of service and that a blackout could thus occur in case an action of the SIPS is needed. The SIPS considered in this work only has to operate for faults on lines 2, 3 and 7 (and only for some system configurations), so about once per year. The risk caused by such attacks is thus limited. For larger systems that heavily rely on SIPS for many different types of faults (e.g. ref. [4] reported 4 operations of its SIPS for the first 11 days of 2016), the risk would be higher. It is worth noting that the attacker does not necessarily need to decrypt the packets. A lot of information can be deduced from the non-encrypted headers of the packets (e.g. from the source, destination, and protocol used).

For the SIPS that uses demand response, the attacker could drop part of the acknowledgement messages. The SIPS would then think that less demand response is available and potentially trigger preventive actions.

VI. Conclusion

In this work, we studied the impact of imperfect communications on the stability of a power system equipped with a PMU-based SIPS. First, we designed a classical SIPS that uses generator rejection to mitigate angle stability issues. We then extended the SIPS to make it able to also leverage demand response. This extension implied the need for an ICT infrastructure on the distribution side. This meant that the TSO would not own this infrastructure but would have to rent it through a SLA. We thus focused on the ICT infrastructure on the transmission side. For this, we first reminded that traffic used for time-critical applications such as a SIPS should be isolated from background traffic using QoS mechanisms. We then used traffic engineering to estimate (in a conservative way) how much bandwidth should be reserved for the SIPS application.

We then showed how to use RTT measurements to assess the performance of the ICT infrastructure in real-time. We explained how to use queuing theory to study ICT failures. Finally, we discussed the impact of DDoS and router hijacking attacks. This work focused on a SIPS designed to mitigate a specific issue in a power system. In future work, we will study the reliability of a more complex SIPS designed to mitigate cascading outages.

References

[1] I. Ivanković, D. Brnobić, S. Skok, I. Šturlić, and R. Rubeša, "Time delay aspect for basic line protection functions with synchrophasor in WAMPAC system," in *2018 IEEE International Energy Conference (ENERGYCON)*, Nicosia, Cyprus, 2018.

[2] R. Hanuise, M. Malichkar, and E. Alcázar, "Ensuring the stability of the Belgian grid with a special protection system," in *47th Annual Western Protective Relay Conference*, Virtual conference, 2020.

[3] J. Malcón, R. R. Syed, and S. K. Raghupathula, "Implementing a country-wide modular remedial action scheme in Uruguay," in *3rd Annual PAC World Americas Conference*, Glasgow, Scotland, 2015.

[4] D. Dolezilek and D. Rodas, "Upgrading from a successful emergency control system to a wide-area monitoring, protection, automation, and control system for the country of Georgia power system," in *7th Annual Protection, Automation and Control World Conference*, 2016, accessed on 2022.06.08. [Online]. Available: https://cms-cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6760_UpgradingSuccessful_DD_20160429_Web2.pdf?v=20171206-212309

[5] N. Liu, "Reliability assessment of a system integrity protection scheme for transmission networks," Ph.D. dissertation, Department of Electrical & Electronic Engineering, University of Manchester, 2017.

[6] S. Canevese, E. Ciapessoni, D. Cirio, A. Pitto, and M. Rapizza, "Wide area system protection scheme design with an artificial intelligence approach considering communication constraints," in *2016 IEEE International Energy Conference (ENERGYCON)*, 2016.

[7] W. Yu, Y. Xue, J. Luo, M. Ni, H. Tong, and T. Huang, "An UHV grid security and stability defense system: Considering the risk of power system communication," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 491–500, 2016.

[8] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all-PMU state estimator – A case study on co-simulation platform GECO," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Taiwan City, Taiwan, 2012.

[9] R. Allan, R. Billinton, I. Sjarief, L. Goel, and K. So, "A reliability test system for educational purposes - basic distribution system data and results," *IEEE Transactions on Power Systems*, vol. 6, no. 2, pp. 813–820, 1991.

[10] P. Kundur and N. Balu, *Power System Stability and Control*, ser. EPRI power system engineering series. McGraw-Hill, 1994.

[11] A. Guironnet, M. Saugier, S. Petitrenaud, F. Xavier, and P. Panciatici, "Towards an open-source solution using Modelica for time-domain simulation of power systems," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, oct 2018.

[12] U. Knight, *Power Systems in Emergencies: From Contingency Planning to Crisis Management*. Wiley, 2013.

[13] H. Georg, "Co-simulation based performance evaluation of ICT infrastructures for smart grids," Ph.D. dissertation, Facultät für Elecktrotechnik und Informationtechnik, Techischen Universität Dortmund, 2015.

[14] N. Mir, *Computer and Communication Networks*. Prentice Hall, 2015, accessed on 2022.06.08. [Online]. Available: https://flylib.com/books/en/2.959.1.96/1/

[15] J. D. Little, "A proof for the queuing formula: $L = \lambda W$," *Operations research*, vol. 9, no. 3, pp. 383–387, 1961.

[16] "IEEE standard for synchrophasor data transfer for power systems," *IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1–53, 2011.

[17] National Grid, "Technical specifications 3.02.01: circuit-breakers," 2018, accessed on 2022.06.08. [Online]. Available: https://www.nationalgrideso.com/document/33141/download

[18] T. R. Henderson, M. Lacage, G. F. Riley, C. Dowell, and J. Kopena, "Network simulations with the ns-3 simulator," *SIGCOMM demonstration*, vol. 14, no. 14, p. 527, 2008.

[19] RTE. Maintaining and making adjustments to the grid. Accessed on 2022.06.08. [Online]. Available: https://www.rte-france.com/en/uninterrupted-flow-current/maintaining-and-making-to-the-grid

[20] M. Sargent, J. Chu, D. V. Paxson, and M. Allman, "Computing TCP's retransmission timer," RFC 6298, Jun. 2011, accessed on 2022.06.08. [Online]. Available: https://www.rfc-editor.org/info/rfc6298

[21] E. Ekomwenrenren, H. Alharbi, T. Elgorashi, J. Elmirghani, and P. Aristidou, "Stabilising control strategy for cyber-physical power systems," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 265–275, 2019.

[22] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[23] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021.

[24] A. Gómez-Expósito and A. Abur, *Electric Energy Systems*. Florida: Taylor & Francis Group, LLC, 2009, ch. State estimation.