Chapter 3

Power system protections

As mentioned in the previous chapters, protections play a key role during cascading outages. Protections are usually designed to protect a given element against faults and abnormal conditions. The stability of the system as a whole plays a secondary (but still important) role in the design of protection systems. So, history has shown that even a protection operates "as designed", it can sometimes contribute to the propagation of a cascade and sometimes prevent its propagation [42]. Another point to consider is that, as the system operates in a (potentially very) degraded state during cascading outages, protection misoperations (either unwanted or missing trips) can become likely and impact the propagation of the cascade.

Section 3.1 briefly reminds the basic protection principles. Then, section 3.2 discusses the scope of considered protections in this thesis. Section 3.3 reviews the most important (from a system reliability perspective) protection misoperations that can occur during/due to cascading outages. And section 3.4 concludes with a list of the protection models considered in this thesis.

3.1 Power system protection basics

This section briefly introduces protections systems used in power systems. For a more complete overview, the reader is referred to textbooks on the subject. The book [43] has been used as a basis for this section.

3.1.1 Components

Protections systems usually consist of three main elements.

- Transducers (i.e. voltage transformers (VTs) and current transformers (CTs)) that reduce the magnitude of electrical quantities to values that are easier to work with (e.g. voltages from 400 kV to 110 V and currents from 1000 A to 1 A.).
- A relay that measures those electrical quantities and applies some predetermined logic to decide when to trip.
- A circuit breaker (CB) that disconnects the protected element. Note that for elements connected to more than one terminal (e.g. lines), a protection system (including transducers, a relay and a circuit breaker) is placed at each terminal.

3.1.2 Reliability, dependability and security

The reliability of protection systems is decomposed into two concepts: dependability and security. Dependability is the measure of certainty that a protection will operate for all faults for which they are designed to operate (e.g. always trip when there is a fault on the protected line). Security (of a protection system, not to be confused with security of a power system) is the measure of certainty that a protection will not operate for faults other than the ones for which it is designed (e.g. never trip for faults on nearby lines). Most protection systems are designed for high dependability. This is because allowing sustained (e.g. short-circuit) faults can cause important physical damage and even deaths. On

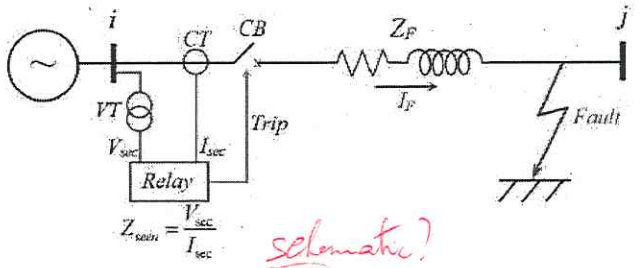


Figure 3.1: Working principle of distance protection [44]

the other hand, an isolated security issue (i.e. a protection incorrectly trips during normal operation) should have no consequences in a N-1 secure system. Security issues can however threaten the system stability when they occur following a fault or during a cascading outage. Balancing dependability and security is the most challenging aspect of protection system design.

3.1.3 Most common line protection schemes

The most common line protection schemes are reviewed below. Other types of elements (generators, transformers, etc.) can also use those schemes, but also other schemes. The latter are reviewed in the reference book.

- Distance protection: the basic idea behind distance protection is that during a metallic short-circuit fault of a line. The working principle of distance protections is shown in figure 3.1. It is based on the fact that during a metallic short-circuit of a line, the ratio between the voltage and the current (called apparent impedance) measured by the relay is equal to the impedance of the portion of the line between the relay and the fault. If this measured impedance is smaller than the impedance of the entire line, it means that the fault is on the line and that the relay should open the line. In practice, uncertainties[1] imply that the presence of a fault can only be guaranteed when the apparent impedance is lower than 80 to 90% of the line impedance. Multiple "zones" are thus necessary to protect a line. The most common zones definition is as follow: Zone 1 protects 80-90% of the line and operates "instantaneously" (i.e. with no intentional time delay). Zone 2 protects 110-120% of the line (i.e. the full line with some margin) and operates with some time delay (e.g. 300 ms) to coordinate with the zone 1 of adjacent line(s). Together, zone 1 and zone 2 protect the full line. Using telecommunications, it is possible to have instantaneous operation for the full line. Additionally, a zone 3 is often used as a backup protection for the adjacent line(s). It thus covers the full line plus the longest adjacent line plus some margin. It operates with a larger time delay than zone 2 (e.g. 600 ms to 2 s). Distance protection is the main protection in transmission systems.
- Differential protection: the working principle is that the sum of ingoing and outgoing currents in a given protected zone should equal to zero according to Kirchhoff's law. A sum that is (significantly) different from zero indicates the presence of a fault and the necessity to trip. Due to the geographical expansions of line (dozens to hundreds of kilometres), it is necessary to have communication between both end of a line to use differential protections. Differential protection is thus mostly used for extra high-voltage (EHV) lines (400 kV in Europe).
- Overcurrent protection: as the name indicates, overcurrent protection disconnect the protected line when it is subject to high currents. It can either be definite-time (trips when the current is higher than a threshold for a given duration) or inverse-time (trips faster for more severe overcurrents). Overcurrent protection is only used a backup protection in transmission systems.

[1] Infeed from other side of the fault, variation of line parameters due to variable sag, etc.

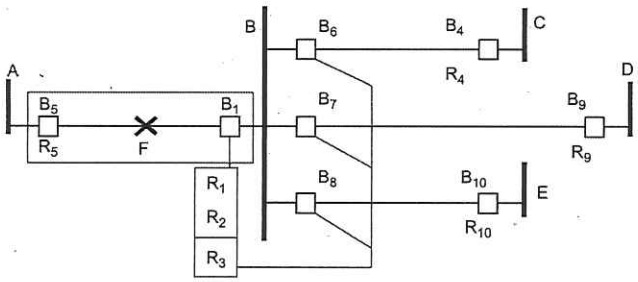


Figure 3.2: Duplicate primary, local backup, and remote backup protection [43]

3.1.4 Redundancy

As for all critical systems, redundancy is used to increase the reliability of protection systems. This is especially true at higher voltage levels where higher levels of redundancy are used. The example in Fig. 3.2 demonstrates the different kinds of backups used. In this example, there is a fault on line AB. The primary protection is the relay R_1 that sends a tripping signal to breaker B_1. R_2 is the duplicate primary protection. It can be identical to R_1 or use a different scheme. The transducers and battery power supply can also be duplicated. The breaker is usually not duplicated due to its higher cost. R_3 is the local backup or breaker failure protection. If R_1 or R_2 send a tripping signal but B_1 does not open, it will send a trip signal to B_6, B_7 and B_8.Breaker failure protection operates with a larger time delay than the primary protection. R_4, R_9 and R_{10} act as remote backup protection. Remote backup protection is often performed by zone 3 relays.

Note: in its final version, this thesis will include a paragraph on substation configurations, the generic configuration(s) used in the test systems and statistical data on failure rates. More information on substation configurations can be found in [45]

3.2 Note on the protection models used in this thesis

The main objective of this thesis is to design a methodology for probabilistic dynamic security assessment of power systems. While probabilistic dynamic security assessment could be useful to help protection design, it is not ~~the not~~ the main objective as a satisfactory security assessment methodology has to be designed first. The protection models used in this thesis were thus chosen to satisfy two criteria. The models should lead to a relatively accurate estimation of the risk[2] and realistic cascading outage scenarios[3] such that (i) the added value of the method compared to QSS methodologies can be shown, (ii) variance reduction techniques used in the probabilistic methodology have similar performance than with more elaborated models. To explain the second criteria, it is necessary to briefly introduce probabilistic methods. Probabilistic methods often use Monte Carlo (MC) methods to handle uncertainties. The issue with basic MC is that, as power system are very reliable, most MC simulations lead to scenarios with no consequences which waste computational resources. Techniques that increase the likelihood of sampling more "interesting" scenarios (i.e. scenarios that contribute more to the total risk) are thus necessary. Those techniques can loosely be referred to as variance reduction techniques. The two criteria are quite abstract, but the main idea is to focus on protections that have the highest impact on the risk. This can be done through study of past cascading outages and experience.

It is difficult to obtain data regarding the exact protection design used by TSOs. Also, this data does

[2]It should be noted that, even if using more complex models, the exact value of the risk (in MWh/y or €/y) is of low significance. What is important is to be able to compare the risk associated with different scenarios and to be able to identify actions that most effectively reduce the risk.

[3]The IEEE CFWG also recommends verifying that the methodology leads to cascading outage sizes that follow a power law [46]. The validation of the methodology is discussed in more details in chapter 6.

not exist for academic test systems. It is thus necessary to use generic protection settings. If a TSO apply the methodology, he should have access to its database of protection settings. On the other hand, he initially might not have all protection models in its dynamic simulator, nor the interface necessary to automatically bring the protection settings to the simulator. He will thus likely also use the methodology with generic protection models. The methodology will then show what settings to modify to reduce the risk of cascading outages. It can then be a good exercise to compare those settings (obtained in a greenfield environment with a focus on system security) and the ones designed by protection engineers (in brownfield, with a focus on dependability, and with additional concerns regarding resistive faults, different types of fault, etc.).

3.3 Protection performance during system disturbances

As power system are drawn far from normal operation during cascading outages, protections are more likely to misoperate. Possible misoperations have been reported by the IEEE Power System Relaying and Control Committee (PSRC) in a report [42], its summary [47] and in previous works [48]. However, as mentioned above, only the misoperations that contributed most to the risk in previous blackouts are considered. The misoperations considered are more similar to the smaller list of misoperations given in [49, ch3] (that is itself based on [42], [47], [48]).

On top of those misoperations that are linked with the system degraded state, the possibility of a relay not operating simply because the relay (or its transducers, power supply or CB) is failed has to be considered.

Note: in its final version, this thesis will include more details on the misoperations that are not considered and the reasons for not considering them.

3.3.1 Distance protection

Distance protection misoperations are the most common type of misoperations. The zone 3 is the one that cause the most issues. This is because zone 3 has to overreach in order to provide backup for adjacent lines. During large disturbances, this zone is thus susceptible to trip even in the absence of fault. The three main causes for unwanted operations of zone 3 relays are listed below.

- High demand: higher line currents imply that the apparent impedance measured by relays decreases (if voltage is roughly constant). In some extreme cases, this can cause the apparent impedance to enter zone 3 or even zone 2. To avoid this issue, a load blinder must be used as shown in Fig. 3.3. According to NERC's (North American Electric Reliability Council) requirements, the distance protection must not trip for currents 1.5 times the maximum current line rating (considering dynamic line rating) at 85% of nominal voltage and for a power factor of 30 degrees [42]. Such a load blinder is thus used in our model.

- Power swings: large (potentially stable) power swing can cause distance relay to misoperate. To illustrate this, consider the following example. A test system consist of two synchronous generators connected by a single line. During a stable system swing, the angle difference between the two generators can be up to 180 degrees[4]. The voltage at the electrical centre of the network (here the middle of the line) is then 0 (sum of the voltages of the two generators assuming the magnitude of the voltages are equal). From the relay point of view, this is equivalent to a metallic three-phase fault. The difference is that power swings develop on longer time scales than short-circuits. Relays can thus use a power swing blocking (PSB) function to distinguish between faults and swings. The model of PSB used in this thesis is still to be defined.

- Voltage instability: during voltage collapses, voltages decrease and loads tend to draw more current to partially maintain a constant power. For relays, this causes a reduction of the apparent impedance and potentially trips in zone 3 or zone 2. Similarly to power swing, the difference compared to actual fault is that voltage instabilities develop slower. However, there is no standard method to distinguish between voltage instabilities and power swings. PSB can thus be used for both. As PSB typically reset after 2 s, the voltage collapse should be stopped faster to avoid tripping

[4]According to the basic equal area criterion model.

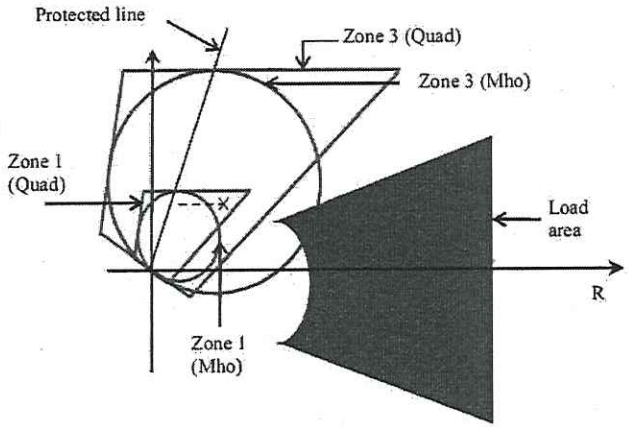


Figure 3.3: Load encroachment. The green zones are quadrilateral zones used by modern numerical relays. The red zones are mho characteristics used by old electromechanical relays [50]

of distance relays. It should be noted that while tripping due to a voltage instability is usually unwanted, it can in some case limit the propagation of the cascade by isolating the zone where the voltage instability take place.

Some other types of misoperations are given in [42] but not considered in this thesis. For example, currently installed numerical relays use methods like discrete Fourier transform (DFT) to evaluate phasor quantities (voltage and currents) used in the protection logic. This introduces inaccuracies during frequency deviations. However, those inaccuracies are relatively minor (up to 10% during very large frequency deviations) and affect all relays in the same way as the frequency is usually uniform in the whole system (or in a given island is the system is split). Those inaccuracies thus cannot significantly change the order of operations of protections. It is thus expected that neglecting this effect should not have a high impact on the possible cascading scenarios nor on their consequences.

Distance protection of multiterminal lines (lines with three or more connections) requires additional considerations. However, as academic test systems do not include such lines, those issues are not considered here.

3.3.2 Overcurrent protection

Line overcurrent protection is only ever used as a backup protection. It is thus expected to have little impact during cascading outages [42]. Ref. [42] mentions possible misoperation of the ground overcurrent element for untransposed lines (those lines are unbalanced and thus generate zero (and negative) sequences currents even when only positive sequence voltages are present). With numerical relays, it is however possible to solve this issue by restraining the ground element by a fraction (e.g. 10%) of the positive sequence current. This issue is thus not considered.

Overcurrent protection is sometimes installed on transformers to backup the differential protection and to protect the transformer against overcurrents (that reduce its lifetime). Typical settings for overcurrent protection of transformers is to trip for 130-200% of the transformer rating [49].

3.3.3 Differential protection

Due to its design, differential protection is mostly insensitive to system disturbances. The main reasons it is not the only type of protection used is the need for a communication medium (in the case of lines) and inability to act as a backup for elements outside of the protected zone. Some possible misoperations are given in [42] but are not considered here.

3.4 Summary of protection models used

The generic protection models used in this thesis are listed below. These models include the considerations given in section 3.3 as well as relatively standard protection models used in other (probabilistic or even deterministic) dynamic security assessment studies. Note that, by default, all protections that are said to operate instantaneously (or with no intentional time delay) are supposed to operate in 100 ms (this corresponds roughly to 20 ms for the relay to take the decision and 80 ms for the CB opening)[5].

3.4.1 Line protection

Lines are supposed to be protected by a distance and a differential relay. Actually, since no misoperations of differential relay are considered, differential relays are not explicitly modelled in the power system simulator. The differential protection only implies that faults will be cleared instantaneously for the whole line, not only the part that is covered by zone 1. Also, it reduces the likelihood of missing trip (discussed in more detailed in the final version of the thesis, pilot distance protection will also be discussed).

Zone 1 protects 80% of the line and operates instantaneously. Zone 2 protects 120% of the line and operates with a 300 ms delay (including CB opening time[6]). Zone 3 setting is more complex due to infeed effects. It still has to be defined. Load encroachment of 150% of the maximum line current at 85% of the voltage with a 30 degrees power factor is also included. Finally, a PSB function is also added (exact model to be defined).

Since only three-phase faults are considered (use of a RMS simulator), auto-reclosing of lines is not considered.

3.4.2 Generator protection

Generators must be protected against undervoltage (that cause degraded performance of auxiliaries), over- and underfrequency, overexcitation and out-of-step conditions. Thus the following protections are used:

- Undervoltage protection: this is especially critical for nuclear generators. For those, an instantaneous undervoltage protection set at 0.9 pu is used. For other types of generators, a less strict protection can be used.
- Under- and overfrequency: past blackouts (e.g. the 2003 Italy blackout) have shown that distributed generators tend to unexpectedly disconnect during frequency excursions. In this thesis, it is assumed that generators connected on the transmission side strictly follow ENTSO-E requirements for continental Europe [51]. So, instantaneous protection is used for frequencies outside of the range 47.5-51.5 Hz. According to [42], hydro units can operate in a large band of frequency. Generators connected to the distribution side are discussed in more details in chapter 5.
- Overexcitation: Volt-per-Hertz protection is used. The settings are still to be defined.
- Out-of-step: a simple model of out-of-step protection is used. The generator trips instantaneously when the angle difference between the generator and the centre of mass of the system (or the island if the system is split) is larger than 180 degrees.

Under- and overexcitations limiters are also considered although they are not stricto sensu protections.

[5] The probability distribution of this time must still be defined
[6] To be confirmed.

3.4.3 System protection

Undervoltage load shedding (UVLS) is not used by all TSOs and is thus not considered in this thesis. Underfrequency load shedding (UFLS) is used following ENTSO-E standards [52]. More precisely, UFLS instantaneously disconnects load by steps between 49 and 48 Hz. The number and size of steps is still to be defined.

Special protection schemes (SPSs) can also be considered. However, since they are designed to mitigate a specific weakness of a given system, it is not possible to define a generic model of a SPS. SPSs are discussed in chapter 4.

3.4.4 Transformer protection

An instantaneous overcurrent protection set at 150% of the rating of the transformer is used. No inverse-time protection is used. To be confirmed.

3.4.5 Protections on the distribution side

This is discussed in more details in chapter 5. Generator and motor protections are considered, but not line protections.

Chapter 4

Special protection schemes

This chapter is based on the following publication:

- F. Sabot, P. Henneaux, P.-E. Labeau and J.-M. Dricot, 'Impact of the reliability of ICT systems on power systems with system integrity protection schemes', in *23e congrès de Maîtrise des risques et de Sûreté de Fonctionnement (Lambda Mu 23)*, 2022. DOI: `ToBeAddedAfterPublication`

As discussed previously, dynamic stability issues are becoming prevalent in many power systems due to various causes such as market liberalisation, intermittent energy sources, increase of static limits (thanks to better conductors and dynamic line rating), etc. There are three main general solutions to mitigate dynamic issues:

- Installation of new transmission infrastructure and upgrade of existing installations (lines, transformers, etc.): this solution is potentially the most effective but it has the drawback of high lead times (up to ten years) and costs. Also, due to public and regulatory pressure, TSOs have to give more and more justifications to choose this option.
- Redispatching: redispatch actions such as curtailment of renewable generation can also mitigate dynamic issues. However, these actions drive the system away from the economical optimum. These actions can be judged cost-prohibitive as they have to be performed each time a (plausible) disturbance threatens the stability of the system while the probability of the disturbance actually occurring can be very low. (Line switching is a low-cost redispatching action, but it cannot alleviate all issues on its own.)
- Special protection schemes (SPSs): SPSs are schemes that automatically perform corrective actions upon detection of a disturbance. These schemes lead to lower operating costs since corrective actions only have to be performed after a disturbance actually occurs. They are also significantly less expensive and quicker to install than transmission infrastructure. SPSs have to act quickly to be effective, usually in dozens of milliseconds to a few seconds. Possible actions that can be taken by a SPS include: generation rejection, turbine fast valving, braking resistor, fast unit start-up, governor setpoint change, load shedding, shunt switching, HVDC fast power change, on-load tap changer (OLTC) blocking, quick increase of synchronous condenser and FACTS voltage setpoint, and system splitting [53].

Case-specific solutions (e.g. fast frequency response to mitigate frequency instability, OLTC blocking to mitigate voltage instability, etc.) are also important but are too numerous to be discussed here. This chapter focuses on SPSs and in particular how to consider them in a probabilistic dynamic security assessment. In particular, section 4.1 discusses reliability considerations regarding SPSs and section 4.2 discusses the communication infrastructure necessary to use SPSs as well as potential threats linked to communications. Finally, section 4.3 concludes with perspectives of future work regarding SPSs.

In the literature, various definitions of SPSs exist. In this thesis, the following definitions are used. A system integrity protection scheme (SIPS) is a protection scheme whose primary objective is to protect the integrity of the whole power system. This contrasts with classical protection schemes whose primary objective is to protect a given element against unacceptable conditions (including sustained faults). A

SPS is any SIPS that is not a local under-frequency load shedding (UFLS) or under-voltage load shedding (UVLS) scheme. The term defence plan is also used in the literature. SIPSs are often the main elements of a defence plan, although other (slower) mitigation measures are also included [49], [53]. This term is however not used in the remaining of this thesis.

4.1 Reliability considerations

The integration of SPSs is usually done in two phases. In the first phase, the TSO designs a SPS to mitigate a specific problem in the system. This SPS requires data from only a few buses to detect this specific problem and has a small set of possible actions. In this phase, the SPS usually has a dedicated ICT infrastructure [54]. In the second phase, the TSO starts to rely on SPSs 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 SPS thus uses the existing ICT infrastructure used for traditional operations [55], [56]. Beyond scalability, an advantage of the second type of SPS 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.

The reliability of the two types of SPSs has to be evaluated with different methodologies. The first type of SPS usually has a dedicated communication infrastructure and requires a limited number of remote measurements. The reliability of this kind of SPS can thus be modelled using standard reliability analysis such as reliability block diagrams and fault trees. An example of such approach can be found in [57] and the references therein. It should however be noted that due to their relative low cost and critical nature, those SPSs are usually designed with a very high level of reliability (both selectivity and dependability). For example, the SPS presented in [54] determines the state of each line end using a 2-out-of-4 voting scheme. It also has two redundant communication infrastructures, and it has been extensively tested prior installation. It might thus not be necessary to include the possible misoperation (nor unwanted nor missing operations) in a probabilistic security assessment. It can be considered in a more possibilistic approach, but this is out of scope of this thesis.

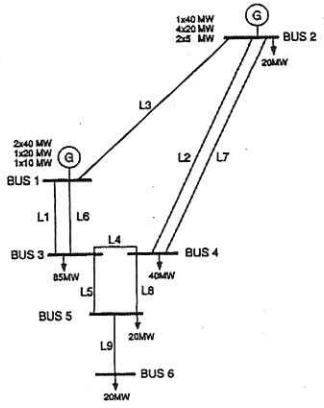
The reliability analysis of the second type of SPS can be decomposed into three parts: state estimation, communication and control actions. Estimating the state of the system requires to have a sufficiently large (and diverse) set of measurements. Observability analysis can be used to determine if a given set is appropriate. It should be noted that the (relatively recent) large-scale installation of phasor measurement units (PMUs) implies that the random loss of a few measurements should have very limited impact on the state estimation performed by the SPS. It is thus mostly inadequate performance of the communication infrastructure that can potentially lead to poor state estimation. The performance of the communication infrastructure is discussed in section 4.2. Once the SPS has evaluated the state of the system, identified a disturbance and successfully sent a control action to one or several actuators, those actuators have to actually implement the corrective action. The performance of the actuators can again be evaluated using standard reliability methods (fault trees, etc.).

4.2 ICT infrastructure

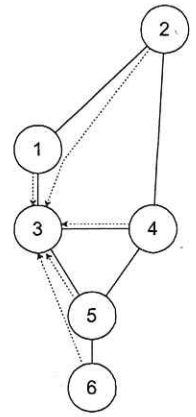
The first type of SPS has a very simple communication infrastructure and is thus no longer considered in the remaining of this chapter. Most of the literature on (the second type of) SPSs simulate the ICT infrastructure by simulating it with network[1] simulators such as ns-3, OMNeT++ or OPNET [58]. Some even use co-simulations, i.e. interface power system and network simulators and make them run together [59], [60]. Co-simulation is discussed in more details in appendix A. In this thesis however, it is preferred to use basic queuing theory. This approach allows to have 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.

So, queuing theory is introduced and used to size the ICT infrastructure in section 4.2.1. Then, it is used to study the impact of failures in section 4.2.2. A simple method to monitor the communication performance in real-time is then proposed in section 4.2.3. Finally, the impact of different types of cyber-attacks is discussed in section 4.2.4.

[1] In this thesis, network is short for communication network, and grid is short for electrical grid.



(a) Physical part. Adapted from [63]



(b) Communication infrastructure. Plain lines represent communication links, and dashed arrows represent PMU traffic flows in normal operation

Figure 4.1: Cyber-physical Roy Billinton test system (RBTS)

4.2.1 Infrastructure sizing

The test case considered in this section is the Roy Billinton test system (shown in Fig. 4.1a) equipped with a centralised SPS. The SPS consists in PMUs that are installed at each bus and send measurements (voltage, current, frequency and possible breaker status) to a control centre (CC) located near bus 3. The ICT infrastructure is shown in Fig. 4.1b. In real networks, phasor data concentrators (PDCs) are placed between the PMUs and the CC to aggregate the PMU traffic. This is is not the case here due to the small size of the system considered. The methods presented below can however easily be adapted to consider those PDCs.

It is 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 [61, p110] and in Germany [62, 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[2]. The focus is thus placed on the first case. However, ISPs use a similar methodology to what is described below. Also, for the sake of simplicity, it is assumed that a single OPGW is installed in parallel to every transmission line (including the double lines).

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 [61, p110]. The traffic used for the SPS 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 SPS. Below, queuing theory is used to determine the minimum bandwidth to reserve for the SPS 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 [64]. In other words, it means that packets arrive with a constant

[2] There is a tendency of operators of geographically-extended systems (e.g. railroads) to install fibre optic cables in parallel to their infrastructure and to sell them to ISPs. Part of the capacity of the cables is then rented back to the utility. There are two main causes to this trend. First, the bandwidth of modern cables often vastly exceeds the needs of utilities. Second, ISPs have more experience in managing communication infrastructures. A concern that this introduces is that critical communication infrastructures (electricity, railroad, etc.) get connected to the global internet. However, it has been shown many times that and "air gap" is not an effective cyber-security measure.

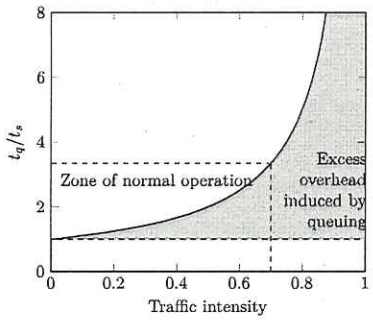


Figure 4.2: Communication delays as a function of congestion

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[3]. Then, traffic load (or traffic intensity) of an element (router, firewall, etc.) is defined as:

$$\rho = \lambda/\mu \tag{4.1}$$

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 queuing theory [64] is that the average number of packets in the queue of the element is given by[4]:

$$N = \frac{\rho}{1-\rho} \tag{4.2}$$

We can then use Little's law [65] that states that the average queuing time t_q [s] spent by a packet in a system is given by:

$$t_q = N/\lambda \tag{4.3}$$

(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, one can simply observe that when a packet arrives in a queue, it must wait for the average N packets already present to be processed. So,

$$t_w = N t_s \tag{4.4}$$

Eq. (4.3) and (4.4) imply that,

$$t_w = \frac{\rho}{1-\rho} t_s \tag{4.5}$$

and,

$$t_q = \frac{1}{1-\rho} t_s \tag{4.6}$$

Eq. (4.6) is plotted in Fig 4.2. This figure illustrates clearly the impact of congestion on delays. This figure shows that, in order to limit the waiting delay (and its derivative with respect to ρ), the network should be operated such that ρ is lower than 0.7 or even 0.5.

This methodology is now illustrated on the RBTS. For this, it is assumed that each PMU generates 120 kbps of traffic (packets of 300 bytes [66] sent at 50 Hz), that 300 kbps is reserved in each link for the SPS, and that packets are routed to the shortest path as shown in Fig. 4.1b. Also, the processing time of routers is assumed to be limited by the bandwidth of links, i.e. is equal to the packet size divided

[3]The validity of this hypothesis in the communication network of an SPS is discussed later in this section.

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

Table 4.1: 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 4.2: 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

by the bandwidth, so 8 ms. The traffic in each link is simply the sum of all traffics going through this link[5]. From this traffic, one can compute the traffic intensity and the average queuing time as done in Table 4.1. 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 given in Table 4.2.

These delays can be compared with the maximum delay allowable for the SPS's actions. In this case, the SPS protects the system against angle stability issues by disconnecting a 20 MW generator at bus 2 when either line 2, 3 or 7 is lost. In [6], I showed that for this particular system, the generator should be disconnected at most 173 ms after the line loss. To determine the maximum communication delay that satisfy this constraint, the other (constant) delays have to be subtracted from those 173 ms. The processing times in the PMUs and CC is taken as 5 and 10 ms respectively [58]. A 20 ms worst-case delay due to the sampling rate of 50 Hz is also considered. The circuit breaker of the generator is supposed to open in 60 ms [67]. A constant 8 ms delay is considered for communication between the CC and the generator[6]. The propagation delays (1 ms per 200 km for a refractive index of the communication medium of 1.5) are neglected. There is thus 70 ms remaining for the communication delays between the PMUs and the CC. One can then verify than the average delays in Table 4.2 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 discussed in traffic engineering textbooks [64].

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 this particular case, simulations in ns-3 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 SPS (and its critical nature), it is inexpensive to have large margins. This is true even for large networks. For example, even if all 2700 substations operated by the french TSO (mostly at 225 and 400 kV level) [68] send PMU packets (300 bytes [66]) at a sampling rate of 50 Hz, it only results in a total of 360 Mbps[7].

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

[6]Queuing theory could also be used to compute this delay, however as messages from the CC to the generator travel in the opposite direction as messages from PMUs to the CC, they do not affect each other (assuming full duplex links).

[7]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).