Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network

A. Bobbio d, G. Bonanni a, E. Ciancamerla a, R. Clemente b, A. Iacomini c, M. Minichino a,*, A. Scarlatti c, R. Terruggia d, E. Zendri c

* Corresponding author.
E-mail address: minichino@casaccia.enea.it (M. Minichino).

A general framework that shows the typical and common interdependencies between a power CI and a Telco CI is reported in Fig. 1. Interactions among hardware, software and human operators are difficult to capture and to model and adequate formalisms and granularity for CI models have to appropriately addressed. Furthermore, convenient indicators and performance measures of CI interdependencies have to be properly defined. The exploration of suitable modelling approaches for interdependent CIs has been the object of many research lines in the recent literature [2,3,17,18]. A network topology analysis takes inspiration by the works of Watts and Strogatz [5] and Albert and Barabasi [6]. Albert and Barabasi [6] underline how a given topological network asset may improve network resilience in response to an accidental failure, but may expose the network to high vulnerabilities in the presence of malicious attacks.

A service oriented risk analysis, is investigated in [18], while in [9], Event driven process chains are used to model the branched chains of reactions after an incident happens.

Simulative analysis is a possible alternative. In [7,26] a federation of multiple domain-specific simulators are explored and in [8] the development of specific tools for the simulation of interdependent infrastructures, in the presence of scenarios that include different typologies of infrastructures, are proposed.

A general framework that shows the typical and common interdependencies between a power CI and a Telco CI is reported in Fig. 1.

1. Introduction

Power grids and Telco networks have a large impact on everyday life and are typically referred to as critical infrastructures (CIs) since their correct operation is essential for the everyday life of our modern society. CIs share, in general, (b)directional dependent relationships and mutual influences so that they are interdependent. Interdependency is especially true because CIs are more and more reliant on information and communication technology and, largely through this reliance, they have become more and more interdependent. The successful delivery of any essential CI service depends upon the operating status not only of the CI which is intended to deliver such a service but also on the operating status of any interdependent CI. Initial disturbances in (or even destruction of) parts of one CI, may result in cascading effects in the infrastructure itself and/or in the other interdependent CIs [1]. There is a growing interest in developing models and tools for CI interdependency analysis, as witnessed by various research programs in EU [19–21] and USA, but practical and methodological difficulties are immense.
The upper part of the figure shows the power CI, which is composed by the electrical grid and the Telco of the electrical grid. Telco of electrical grid provides the communication facilities needed to control the electrical grid and may be partly operated by the power operator and partly by the Telco operator.

The lower part of Fig. 1 shows the Telco CI which consists of several networks that provide different Telco services (voice, mobile voice, data, mobile data, etc.). In addition Telco networks require a reliable power supply that is provided by the power CI (power to Telco services). However, it is rather common that Telco offices (or at least the most important ones) have their own emergency power supply system, for backup reasons in case of outages of the main power supply. The set of emergency power supplies is owned and managed by the Telco operator (lower left part of Fig. 1).

The power distribution grid is managed and controlled through a supervisory control and data acquisition (SCADA) system that constitutes the nervous system of a power grid. The operation and control of SCADA relies on communication links among SCADA nodes, partly dependent on the public Telco network and, for such a reason SCADA systems represent one of the major channels of mutual propagation of disturbances and adverse events between power grids and Telco networks. Many power grid services, like supply of critical users/large urban areas, grid reconfiguration after failures and telemetry, are increasingly depending upon the adequate functionality of their SCADA system whose correct operation strictly depends on the adequate functionality of Telco network. On the other hand both SCADA system and Telco network need to be fed by power grid.

To guarantee adequate reliability and performance for the transmission bandwidth, SCADA communication links typically rely on a main, usually proprietary, communication network and on a redundant Telco network. However, due to different reasons, including market deregulation, in electrical and in Telco infrastructures, part of SCADA communication links could rely on a public Telco network, as in the present case study. This fact introduces a number of potential failure points that previously did not exist.

The present paper investigates a risk based modelling methodology, which aims to predict stochastic indicators of services delivered by interdependent CI, say a Telco network and a power distribution grid [16,24]. To this end, the paper proposes a multi-formalism and multi-solution stochastic approach [4,23], in which different modelling frameworks and solution techniques are applied to different parts of the interconnected networks in order to realize a good trade-off between modelling power and analytical tractability, and to confine the application of more intensive computational techniques to those parts of the networks, only, that actually require it.

The proposed approach is intended to be a valuable quantitative methodological support for failure scenarios involving interdependent CIs. For the sake of clarity, our approach is applied to an actual failure scenario occurred on January 2, 2004 and initiated with the outage of a Point of Presence (PoP) of the Italian telecommunication backbone, located in Rome. Examining the dynamic of the failure scenario, it appeared evident the criticality of two SCADA communication links, provided by a public Telco company and essential for the observability and the control of a large part of the power distribution grid. The availability of the two SCADA links relies on three interconnected networks: (a) Telco network, which directly supports the two communication links throughout a single pair high speed digital subscriber line (SHDSL) connection; (b) power distribution grid which provides the main power supply at the Telco sites. (c) Telco emergency power supply, which feeds the Telco network in the case of loss of the main power supply. The paper is organized as follows. Section 2 examines the dynamics of the failure scenario under study in order to identify the dependencies and criticalities in the interconnected CIs. Section 3 proposes a service oriented approach to quantify the behaviour of the interconnected CIs in the examined reference scenario. Section 4 enlightens the proposed multi-formalism technique and shows how different formalisms have been applied to different CIs. Finally Section 5 shows and discusses quantitative results.

2. Failure scenario of the case study

A failure scenario consists in the identification of the sequence of adverse events that have produced an anomalous and undesirable behaviour in the interconnected CIs, the identification of services that have been impaired (in terms of continuity, readiness, performances, response time) during the sequence of adverse events and the set of interconnected networks that support such services and have contributed to their degradation. In this paper, we concentrate our attention on an actual failure scenario, occurred on January 2, 2004 and initiated with the flooding of a major node of the Italian Telco network, located in Rome [19]. A breakage of a metallic pipe, carrying cooling water of the air-conditioning plant, caused the flooding of the floor under which cables of Telco devices were located. The rooms were flooded up to the height of 10 cm and several boards/devices of transit exchange (TeX) and of point of presence (PoP) of the national backbone (PoP-BBN), located on the floor, were flooded and went out of service for short circuit. Main power supply to the Telco node, provided by the power distribution grid, went out of service, as well. Diesel generators of Telco emergency power supply failed to start due to the presence of water; at this stage, only batteries provided power supply to the still working boards/devices. After a while, batteries also dropped, being over their capacity, and the node went out of service completely. As a consequence of the node outage, part of wired and wireless Telco services in Rome tilted, causing problems and delays in different infrastructures. For what specifically concerns the present case study, the node outage caused the complete unavailability of two redundant communication links, which connected two SCADA
control centres of the power distribution grid of Rome, through the flooded PoP. The sequence of adverse events and of the involved CIs is traced with the help of the system overview given in Fig. 2.

2.1. Power distribution grid

The power distribution grid of Rome is, nowadays, operated by a single operator, but consisted of two autonomous grids, previously operated by two different operators. Originally, each one of the two autonomous grids had its own SCADA system, with its manned control centre.

After the unification, the two power grids were kept as they were while the two SCADA systems have been integrated, so that now there is a unique SCADA system but with two control centres. The left control centre in Fig. 2, called main SCADA control (MSC), is manned, while the right control centre, called disaster recovery SCADA (DRS) is unmanned. They are linked by means of two redundant communication links provided by a public Telco network. Each control centre has a direct observability of the portion of the grid to which it is devoted and an indirect observability of the complementary portion of the grid through the two redundant communication links. The whole grid operability is supervised by the human operator located in the manned MSC. As a consequence of the Telco node outage caused by the flooding, the two communication links went out of service and the operator completely lost the observability of the portion of the grid gathered by the DRS control centre (Fig. 2), that become completely inoperable. A major grid blackout was avoided due to the concomitant absence of any grid failures, and the presence of good weather conditions, which did not require any grid reconfiguration.

Fig. 3 enlarges the left part of Fig. 2 and shows the portion of the power distribution grid, directly controlled by the manned MCS control centre. The grid includes a portion of the high voltage (HV) grid at 150 kV, and the backbone of medium voltage (MV) grid at 20 kV, which feeds the flooded node of the Italian Telco network. In Fig. 3, nodes Pi (large rectangles) represent HV substations while nodes Mi (small rectangles) represent MV substations. Nodes Ei represent the substations of the Italian power transmission grid that interface and feed the power distribution grid. The physical link between any two nodes is an electrical trunk. A trunk may be a homogenous or a heterogeneous trunk. In the first case, the physical properties of the trunk, including its age, failure rate, electrical properties, are constant along its length. In the second case, the trunk is constituted by a series of two or more homogeneous trunks. Fig. 4 reports a view of the properties and values of some electrical trunks (type: aerial/underground, material, dimension: section and length, reactance, impedance and failure rate for years and unit of length). The MV substations named M5, M6 and M7, provide the main power supply to the flooded Telco node. A similar portion of the power distribution grid is controlled by the SCADA unmanned control centre (right part of Fig. 2).

2.2. SCADA system

Fig. 5 shows the SCADA system and its mapping on the power distribution grid. The SCADA is constituted by two control centres MSC and DRS and by a set of remote terminal units (RTUs) that interface the SCADA with the power distribution grid at high voltage (HV) (Pi boxes) and medium voltage (MV) (Mi boxes) substations. The links among electrical substations do not represent electrical trunks as in Fig. 3 but data communication links. The main SCADA control centre (MSC) directly observes and controls the portion of the power grid of Fig. 3 (shown on the left portion of Figs. 2 and 5).

The disaster recovery SCADA control centre (DRS) directly observes the complementary portion of the power distribution grid (shown in the right part of Figs. 2 and 5) and sends the observed parameters to the MSC for control. Hence, MSC controls and supervises the whole power grid, directly and through the DRS, while DRS assumes the control and the supervision of all the grid, in case of MSC failure. MSC and DRS are connected, via firewalls, by two public, redundant, high speed Telco links.

Information and data (i.e. power flows, voltages, frequencies, loads, breakers positions and power transformers status) are transmitted from any RTU to its control centres, while commands (i.e. the remote control of switchgears for energizing/de-energizing power transformers and distribution feeders under normal/disturbance/fault conditions) are transmitted from the control centres to RTUs by means of communication links.

SCADA system can be decomposed in three subnets (Fig. 5).

(i) The default proprietary network (DPN) serially connects the SCADA control centres to HV RTUs. The DPN nodes (HV RTUs) are depicted as rectangles labelled Pi (i=1, 44). To increase the connectivity and the reliability of the SCADA system, DPN
nodes can also communicate each other through a redundant public switched telephone network (PSTN) subnetwork via transit exchange (TeX) nodes.

(ii) The PSTN network composes the backup public Telco network. PSTN nodes are numbered on the graph from 55 to 61 and from 63 to 66 and are connected via dotted lines. PSTN nodes cannot communicate each other through the DPN nodes. For reliability purposes, the PSTN network provides a redundant connection of each HV RTUs to MSC and DRS. Furthermore, two virtual private networks (VPN) are established between the two SCADA control centres MSC (node 63) and DRS (node 64), via two single pair high speed digital subscriber line (SHDSL) connections, throughout two routers located in two point of presence (PoP), named PoP1 (node 65) and PoP2 (node 66). The actual Telco network supporting the two SHDSL connections is detailed in next section, since it has been recognized as a critical point in the failure scenario.

(iii) MV RTUs, differently from HV RTUs, are connected to SCADA centres by means of public global system mobile (GSM) connections (point/dashed lines). Particularly, MV_RTU are connected to their SCADA control centre throughout a base
trans-receiver sub-system (BTS–node 62) and a transit exchange (TeX). MV_RTU nodes, labelled from M1 to M10, are terminal nodes that can be reached through the PSTN subnetwork.

2.3. Telco network

The bandwidth required between the MSC and the DRS of SCADA system in Fig. 5 is of 2 Mbit/s and is realized by a bidirectional single pair high speed digital subscriber line (SHDSL) Telco connection, whose scheme is detailed in Fig. 6.

Here, we consider an IP (Internet Protocol) 2 Mbit/s bidirectional connectivity, mapped into a SHDSL connection and offered over the same platform, that provides asymmetric DSL (ADSL) services to residential customers. Moreover we consider that the DSL platform is based on asynchronous transfer mode (ATM) digital subscriber line access multiplexer (DSLAM). The SHDSL signal is carried over a copper twisted pair from the MSC/DRS location to a DSLAM in the closest local Telco site. Here, the signal is multiplied by the DSLAM, with other customer signals, into a 155 Mbit/s ATM virtual path, that is carried over the synchronous digital hierarchy (SDH) network to an ATM switch. SDH network aggregates data flows at different bit rates and re-transmits them over long distances. SDH relies on optical rings constituted by add drop multiplexer (ADM) and bidirectional optical cables. ADMs perform signal multiplication (they gather many tributary signals and multiplex them into one signal at higher rate), transmission over optical fibres and protection rerouting over the SDH ring in case of a single failure. In main Telco sites, digital cross-connects (DXCs) allow the automatic cross connection of the SDH circuit. DXCs are used to increase the flexibility of the SDH transmission network. The ATM switch is then connected to a provider edge (PE) router that is responsible to establish a virtual private network (VPN) between the two SCADA control centres. This VPN is actually established via two SHDSL connections, respectively, from the MCS site and the DRS site to the same PE router located into a main Telco site. In order to increase the reliability of the connection between the MSC and DRS sites, two equivalent VPNs are configured on the Telco Network. To protect the connections from common cause failures, the two VPNs follow two different geographical paths. However, during the Telco outage, due to a previous maintenance operation, both VPNs were traversing the same flooded node (the main Telco site in Fig. 6).

2.4. Telco emergency power supply

Telco sites are protected against the loss of the main power supply by means of an emergency power supply, typically constituted by a composition of benches of batteries and diesel generators. Fig. 7 shows the configuration of a typical power supply of a main Telco site. It consists of a DC supply at low voltage and AC supply at 380 V. The power distribution grid provides 20 kV medium voltage (MV), converted to 380 V low voltage (LV) passing through the block constituted by MV–LV transformers. Diesel generators provide energy at 380 V on the loss of the main power supply. Uninterruptable power supply (UPS), is mainly constituted by a rectifier, an inverter and batteries. The rectifier converts the AC into DC to supply batteries, while the inverter converts the DC into AC.

Since a diesel motor takes a few minutes to activate the alternator after a main power interruption, the batteries should guarantee the emergency power supply during this interval. Diesel generators and batteries are typically dimensioned to provide power to the whole set of Telco devices in a Telco office. In particular batteries are dimensioned to cope with short interruptions (in the range of tenth of minutes), while diesel
generators should cope with long-lasting (some hours) power interruptions. Note that small and local Telco offices may have reduced emergency power supply capabilities.

2.5. (Inter) dependencies within the failure scenario

The PoP node outage caused operability problems and delays in the Telco network, in the power grid and in different infrastructures of Rome. Limiting our attention to the Telco network and the power grid, there is a number of major (inter)dependencies that can be identified within the failure scenario. Inside the Telco network, the cooling/air-conditioning plant, the diesel generators and the batteries share a possible geographical dependence since they are, usually, situated relatively close to each other. Furthermore, there is a cycle of interdependencies between the MSC control centre and the flooded Telco node, because the substations of the power grid are controlled through the flooded Telco node and, conversely, the Telco area, where the flooded node is located, is powered via MV substations (nodes M5, M6 and M7 in Fig. 3), controlled by the MSC.
The MSC and DRS control centres share a common dependence on the Telco network through the two links, affected by the Telco power outage. On failure of such links, the operator completely loses the observability of the portion of the grid gathered by the unmanned control centre DRS (Fig. 2). As a consequence, SCADA services performed by the operator (such as grid reconfiguration, when required by a grid failure) on the portion of the grid gathered by the unmanned control centre becomes completely unavailable, exposing the power grid to the occurrence of uncontrollable blackouts.

3. Service availability of interconnected networks

A natural way to deal with the complexity of the performance and reliability analysis of interconnected CIs is to follow a service oriented approach. By this we mean that the different services provided by the interdependent CIs are isolated and analysed separately. As a unifying measure to characterize the delivery of an appropriate service level, we propose the service availability defined as the probability that a specific service delivered by interconnected networks is operational at time t, accounting for the availabilities of all the interconnected networks required for delivering such a service.

A service oriented approach is, at the same time, customer oriented since CIs deliver services according to a Service Level Agreement, in case of Telco CI, or to the regulation of the National Energy Authority, in case of power CI. Services delivered to customers can be a single one as in case of power grid (i.e. power supply) or multiple ones as in case of Telco networks, where a variety of services like, voice, mobile voice, data, mobile data, are offered. The focus on the availability of services in interconnected networks is a natural extension of the QoS indicators in each CI single domain.

The modelling/evaluation process is an iterative exercise, as sketched in Fig. 8, that requires the cooperation of the modellers and the CI operators and consists in successive definition/implementation/refinement steps starting from the identification of the failure scenario, and passing through methodology, tools and models. The identification of a failure scenario requires a deep brainstorming between CI operators and modellers aimed at understanding the structure, interdependency and operation of CIs, the services delivered and the CIs involved. This preliminary effort is the initial basis to proceed at the exploration of (inter)dependencies and possible critical or adverse natural/random/cascading events, following a risk and decision analysis methods as those proposed in [14,18].

Interconnected networks are then decomposed [19] in terms of elements, segments and connections, according to the use case of the service under consideration (different use cases rely on different network elements, segments and connections) and by means of the identification of failure and repair mechanisms of each network. At the state of the art, we believe that no single technique has the modelling and the analytical power to cope with the quantitative evaluation of the service availability of large interconnected networks as power grids and Telco networks at regional/national level. For this reason, we propose to represent each network by a convenient stochastic modelling technique, able to capture the main network technological issues and realistic assumptions about the failure and recovery mechanisms. The decomposition approach, combined with a strategy of successive refinements, allows us to identify and apply to each subnetwork the most convenient modelling formalism, with respect to accuracy and analytical tractability.

The selection of the appropriate technique depends upon different factors including the dimension of the network, the network topological and technological features (in terms of dependencies among network elements and network configuration), realistic assumptions on network failure and recovery mechanisms, the granularity of network models. Once the suitable modelling technique has been selected for each part of the networks, each model can be considered in isolation to study the contribution of each part to the availability of that particular service. Then, all models can be combined hierarchically to evaluate the influences of the interdependencies.

3.1. Failure scenario of the case study

Referring to the actual case study, the analysis of the failure scenario has identified the service availability of the two SHDSL connections between the two SCADA control centres MSC and DRS (Figs. 2, 5 and 6) as the most critical point. The connections traverse the flooded node at the main Telco site (Fig. 6) that contains many transmission and routing devices, including the ones which support the SHDSL connection. Telco nodes, as the one under consideration, are powered by the power distribution grid and by an emergency power supply, like the one reported in Fig. 7.

As a consequence, the following interconnected networks have been included in the analysis:

- **Telco network**, which supports the two redundant SHDSL connections between MSC and DRS (Fig. 6). SHDSL connection carries only data over IP (Internet Protocol) and supports voice over IP (VoIP). Data are needed between RTUs and the two control centres of the SCADA system. Moreover, VoIP may be needed to exchange information between operators located at RTUs and at the control centres.

- **Power distribution grid**, including a portion of the HV network at 150 kV and the backbone of MV network at 20 kV, which powers the flooded Telco node (Fig. 2, MV substations M5, M6, M7).

- **Telco emergency power supply** which provides energy to the Telco node in case of outage of the power grid. The layout of the power emergency node under consideration is given in Fig. 7.

The critical SHDSL connection between MSC and DRS has been expanded in Fig. 6 in its main constituent blocks. At the granularity level of Fig. 6 and considering the optical nature of the connections among the Telco devices it may be assumed, quite realistically, that a failure of a constituent device will not affect the failure of other network devices. Hence, the SHDSL connections can be represented as a series configuration of complex blocks and thus can be analysed by resorting to the reliability block diagram (RBD) method. The RBD method has been implemented by resorting to the commercial tool ITEM software [13].

To model the correct sequence of operations of an emergency power supply, we need to represent a sequence of successive timed operations, initiated by the interruption of the main power supply.
supply: the starting on demand of batteries and generator, their operation, with possible failures and repairs. Such times and events are dependent on each other so that a modelling approach must be based on the state space generation. The stochastic activity networks [10] have been selected in this case, since they are supported by a very flexible software tool Möbius.

To represent the reliability and connectivity properties of the power distribution grid depicted in Fig. 3 we resort to the tool NRA (network reliability analyser), a prototype academic tool, which implements network reliability analysis based on binary decision diagrams, a powerful formalism to manipulate Boolean expressions [11].

In the following we briefly present and discuss the main characteristics and differences of the above formalisms.

3.2. Reliability block diagrams

Many systems can be regarded as composed by interconnected subsystems and can be modelled and analysed using the reliability block diagram (RBD) method as combinations of blocks arranged in various configurations, usually series and/or parallel [22]. The structure of the RBD defines the logical effect of a failure on the system operation. The quantitative system reliability evaluation using RBD requires that blocks are considered statistically independent. A RBD should only contain one input and one output node and the logical flow starts from the input and ends to the output node. A series connection requires that all blocks are operating for the system to be operating, while a parallel connection is used to model redundancy. A system can contain combination of series and parallel connections to make up the network. In the presence of more complex structure methods based on network reliability analysis are more appropriate.

3.3. Stochastic activity networks

Stochastic activity networks (SANs) are a powerful and flexible stochastic generalization of petri nets (PNs) [15]. Different aspects of distributed real-time systems can be modelled and analysed by these models: concurrency, timeliness, fault-tolerance and degradable performance. Similar to other classical extensions of petri nets, SANs have some limitations for modelling large scale systems due to the state space explosion. SANs are defined as a tuple of four primitives: place, activity, input gate and output gate. A place is an extension of NRA. Two algorithms have been implemented [11,12]; the first one is based on the exhaustive search for the minimal paths between source and destination using the classical Dijkstra’s algorithm, the second one constructs the BDD of the connectivity function directly, by means of a depth-first search on the graph. The construction and manipulation of the BDD’s is managed through the library developed at the Carnegie Mellon University. The complete list of the minpaths and mincuts may be optionally displayed. In the analysis of the present failure scenario, the NRA tool has been extended to cope with the connectivity of networks with multiple sources and multiple destination nodes.

4. Models of interconnected networks

According to the analysis of the case study considered in Section 2, we first build the appropriate stochastic model for each one of the CIs that have been involved in the failure scenario, as specified in the following:

(i) The public Telco network and its influence on the SHDSL connection between the two SCADA control centres MSC and DRS. The appropriate model is RDB.
(ii) The power distribution grid and its influence in the supply of electrical energy to the Telco network. The appropriate model is an extension of NRA.
(iii) The Telco emergency power supply and its influence on providing electrical power upon unavailability of the main grid. The appropriate model is SAN.

Finally, the results of each model are hierarchically combined to provide the service availability of the SHDSL connection in the presence of interdependent failure phenomena.

4.1. RBD model of the Telco network

Fig. 9 reports the RBD of the SHDSL connection provided by Telco network (Fig. 6), excluding the last mile (the last trunk which
connects each control centre to the DSLAM). For clarity the blocks in Fig. 9 are ordered in the same sequence as in Fig. 6 and consist in the following devices: DSLAM, SDH rings (SDH STM-16 and SDH STM-64), DXC, ATM switch and PE router. Each block of the RBD of Fig. 9 is, in turn, hierarchically decomposed in a succession of series/parallel RBD sub models, according to the functional characteristics of the devices to be represented, until the basic components, for which failure and repair rates may be known, are reached.

As an example, Fig. 10 shows a functional scheme of the SDH-STM16 ring of Fig. 9. A SDH ring is constituted of ADM elements and transmission sections (the fiber optical cables between the ADMs). The ring assures the protection of any transmission section against single failure. One-way rings use two fibres, one for working traffic and the other one for protection facility. During the normal operation, the synchronous transport module (STM) flow is carried out by each ADM on clockwise working traffic. If some failure occurs in one of the transmission sections or in an ADM, the working flow is deviated counter clockwise on the protection fiber (Fig. 10).

The functional analysis of the ring of Fig. 10 shows that in normal operation data flows clockwise on fibres a, b, c; in case of single failure, data flows counter clockwise on fiber d. This behaviour corresponds to the RBD of Fig. 11. The length of each transmission section of the ring, which impacts on its failure rate, is assumed to be about 10 km.

4.2. SAN model of the Telco emergency power supply

Main power supply loss, starting, running and duration ending of diesel generators and batteries (Fig. 7) are events that occur sequentially in time. When the main power supply fails, generators start with some probability and may fail during operation. Batteries provide backup emergency power for a certain maximum number of hours or until they fail during operation.

To represent the described relationships among events and duration times, we build the SAN model, shown in Fig. 12, whose main features are the following. On failure of the main power supply (a token in place Power_down), Telco emergency power supply is activated (a token in place emergency), then both batteries and diesel generators are demanded to start to supply emergency power (a token in the place battery_start_up and a token in the place diesel_start_up). Main power supply may be recovered at any time (firing of the timed transition mu_pp). In such a case, all the emergency activities are stopped (a token in the place stop_start). Batteries are ready to operate with a certain probability (case transition battery_ready and may fail or may become exhausted (transition lambda_b), reaching their failure state (token in place battery_down) from which a recovery action may occur (transition mu_b). Differently from batteries, diesel generators do not provide power instantaneously. After a starting duration time, diesel may be running (a token in the place diesel_up) with a certain probability (timed case transition t_start). Diesel failure (a token in the place diesel_down may occur in two modes: (a) failure to start (either manually or automatically); (b) failure to run (failure of the generator during operation given that started successfully).

4.3. NRA model of the power distribution grid

The portion of the power distribution grid, represented in Fig. 3, has been modelled and analysed via NRA. The NRA tool requires in input the network topology and the failure/repair rates of its elements ( derivable from the knowledge of the trunk electrical properties reported in Fig. 4). The goal of this part of the overall analysis is to investigate the probability that the MV substations M5, M6 and M7, that provide energy to the Telco network, are powered from substations E1, E2 and E3. We are in the presence of a multiple source, multiple destination problem that requires an extension of the usual node to node two terminal reliability analysis.

Let \( C(E_i, M_j) \) be the Boolean connectivity functions between any combination of a node \( E_i \) (i = 1, 2, 3) with a node \( M_j \) (j = 5, 6, 7). In a multiple destination problem it may be requested to evaluate the probability that all destinations are powered, or at least one of them, or \( k \) out of \( n \) \((k:n)\). The connectivity functions \( C(E_i, M_j) \) are not mutually statistically independent since they may share common trunks or paths in the network, and, hence, the standard rules for the reliability analysis of independent blocks, like in RBD,
cannot be applied in this case. However, in NRA the functions $C(E_i, M_j)$ are represented by BDDs and we can first combine the BDDs to get the desired representation of the combined connectivity function, and then compute the probability on the so obtained combined BDD.

In the model of the power distribution grid, it is assumed that the electrical trunks, represented by dashed lines in Fig. 3, cannot provide backup in case of failure of any trunk of the grid.

5. Results and discussion

This section presents and discusses the quantitative results obtained by applying the explained multi-formalism hierarchical approach. Results represent a first refinement of the iterative modelling process between modellers and CI operators shown in Fig. 8.

Quantitative analysis requires quantitative data about the failure and repair characteristics of the elementary blocks and components appearing in the models. As it is well known, getting reliable data may be difficult or even impossible, also because they are considered highly confidential by CI managers. In our case, data came mainly from technical meetings with CI operators and partly from the literature, but further improvements and refinements are possible.

Fig. 13 shows the unavailability of the pure SHDSL connection between the two SCADA control centres MSC and DRS, computed from the RBD model of Fig. 9. Each block of Fig. 9 is usually expanded in a chain of RDBs as, for instance, the STH-STM16 block in Fig. 11. Table 1 shows the first 8 out of 32 minimal cut sets (mcs) of the SHDSL connection, ordered by decreasing unavailability. It is noteworthy to observe that the major source of unavailability is constituted by the failure of the optical fibres. The 3 most unavailable mcs are of order 2 and refer to the contemporary failures of the fibres in the working flow and in the recovery circuit in the STM-16 rings (see Fig. 11).
The following 3 most unavailable mcs refer to a similar combination of failures in the STM-64 rings. The last two mcs are of order one, and refer to the single failure of the common part and output interface of ATM.

The reliability of the portion of the power distribution grid of Fig. 3 has been computed by NRA. The failure rates of the various trunks have been derived from the data of Fig. 4 and range between a maximum of $\lambda_{MAX}=0.148$ y$^{-1}$ and a minimum of $\lambda_{MIN}=0.00529$ y$^{-1}$. According to Section 4.3 we denote by $C(E_i,M_j)$ the Boolean connectivity functions of a node $E_i$ ($i=1, 2, 3$) with a node $M_j$ ($j=5, 6, 7$). As a consequence, the usual measure of the point to point reliability may be defined as the probability that this connection is working

$$R_{E_iM_j} = \Pr[C(E_i,M_j)]$$  \hspace{1cm} (1)

In order to analyse the probability that the Telco node involved in the failure scenario is correctly fed by the power grid we have investigated the following cases:

(a) Point to point reliability between a node $E_i$ and a node $M_j$, using (1).

(b) Probability that all the nodes $M_j$ are fed by a source $E_i$. To this end the individual point to point connectivity functions are combined in AND as in

$$R_{AND} = \Pr[C(E_i,M_5) \land C(E_i,M_6) \land C(E_i,M_7)]$$  \hspace{1cm} (2)

(c) Probability that at least one $M$ node is fed by a source $E_i$. To this end the individual point to point connectivity functions are combined in OR as in

$$R_{OR} = \Pr[C(E_i,M_5) \lor C(E_i,M_6) \lor C(E_i,M_7)]$$  \hspace{1cm} (3)

(d) Probability that at least two out of three nodes $M_j$ are fed by a source $E_i$:

$$R_{2:3} = \Pr_{2:3}(C(E_i,M_5),C(E_i,M_6),C(E_i,M_7))$$  \hspace{1cm} (4)

It is usually recognized that the unreliability is more expressive than the reliability. Hence, Fig. 14 reports the unreliability functions computed from the previous formulas, assuming as a source node, node $E_1$.

Curves denoted by $M_5$, $M_6$ and $M_7$ report the point to point unreliability (Eq. (1)), curve denoted AND the unreliability computed from Eq. (2), the curve denoted OR the unreliability computed from Eq. (3), and, finally, the curve denoted 2:3 the unreliability computed from Eq. (4). As expected the configuration denoted AND is the most reliable, while the configuration OR is the most reliable. The inset in Fig. 14 shows an enlargement of the curves to put in evidence the different behaviours. Assuming as a pessimistic upper bound for the out of service time of each trunk of the network the value of about one week, corresponding to a repair rate $\mu=50$ y$^{-1}$ we obtain, for the same configurations of Fig. 14, the unavailability curves reported in Fig. 15.

To gain insight on the weakest points of the network we can examine the list of the mcs, whose total number is displayed in Table 2 for the examined configurations.

For all the examined configurations, the two most critical mcs are of order two and they are listed in Table 3 together with their steady state unavailabilities.

Inspection of Fig. 3, shows that the weakest mcs $(P26–M10\land P13–M1)$ and $(P26–M10\land M3–M2)$, correspond to the interruption of the trunks that feed the series of MV stations. This observation suggests a possible design improvement in the configuration of the grid by modifying the connection of the MV stations M1–M10 to nodes P26 and P13 in parallel instead of in series as in the actual structure of Fig. 3. The analysis of this new parallel connection shows a remarkable improvement in the computed unreliability and unavailability functions, as reported in Figs. 16 and 17, respectively, where the new curves are marked with $\ast$ and the old ones (from Figs. 14 and 15) are reported for comparison.

Fig. 14. Unreliability of various configurations between E1 and M5, M6 and M7.

![Unreliability of various configurations between E1 and M5, M6 and M7.](image)

![Unavailability of various configurations between E1 and M5, M6 and M7.](image)

<table>
<thead>
<tr>
<th>Source node</th>
<th>M5</th>
<th>AND</th>
<th>OR</th>
<th>2:3</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>134</td>
<td>168</td>
<td>106</td>
<td>142</td>
</tr>
</tbody>
</table>

Table 2

<table>
<thead>
<tr>
<th>Source node</th>
<th>M5</th>
<th>AND</th>
<th>OR</th>
<th>2:3</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>134</td>
<td>168</td>
<td>106</td>
<td>142</td>
</tr>
</tbody>
</table>

Table 3

<table>
<thead>
<tr>
<th>Unavailability</th>
<th>mcs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>P26–M10\land P13–M1</td>
</tr>
<tr>
<td>2</td>
<td>P26–M10\land M3–M2</td>
</tr>
</tbody>
</table>

Inspection of Fig. 3, shows that the weakest mcs $(P26–M10\land P13–M1)$ and $(P26–M10\land M3–M2)$, correspond to the interruption of the trunks that feed the series of MV stations. This observation suggests a possible design improvement in the configuration of the grid by modifying the connection of the MV stations M1–M10 to nodes P26 and P13 in parallel instead of in series as in the actual structure of Fig. 3. The analysis of this new parallel connection shows a remarkable improvement in the computed unreliability and unavailability functions, as reported in Figs. 16 and 17, respectively, where the new curves are marked with $\ast$ and the old ones (from Figs. 14 and 15) are reported for comparison.
Notice that Fig. 17 is in logarithmic scale to enhance the differences in the two technological configurations. Modifying the structure may improve the unavailability by an order of magnitude.

The two most critical mcs are now changed and they are listed in Table 4 together with their steady state unavailabilities.

The coupled analysis of the interdependencies between the Telco network and the power supply has been investigated under various assumptions about the configuration of the interconnections. The unreliability of the SHSDL connection has been plotted in Fig. 18 under the examined cases.

Case I: is the base case. The pure Telco network is examined in isolation, without considering the connection with power supply provided by main power supply and emergency power supply.

Case A: is the base case. The pure Telco network is powered by a non-repairable main power supply, with no Telco emergency power supply.

Case B: The Telco network is powered by a non-repairable main power supply; the Telco emergency power supply is just constituted by batteries that are considered as non-repairable.

Case C: The Telco network is powered by a non-repairable main power supply; the Telco emergency power supply is constituted by batteries and Diesel generators that are considered as non-repairable.

Case D: The Telco network is powered by a repairable main power supply with a non-repairable emergency power supply constituted by batteries and diesel generators. Two subcases are examined:

Case D1: A short outage time of the main power supply; correct operation is restored in 3 min.

Case D2: A medium outage time of the main power supply; correct operation is restored in 6 h.

The labels of the curves of Fig. 18 correspond to the examined modelling assumptions. The unreliability of the pure SHDSL connection (curve I) is lower than the unreliability of the connections with any powering solution. Case A is the worst case since the main power supply is considered as non-repairable and with no Telco emergency power supply. The other powering cases (curves B, C, D1, D2) provide intermediate results.

Novelty in this paper is to demonstrate, by means of an actual case study, that the analysis techniques and performance indicators well acquainted in risk analysis of single CIs may be extended to interdependent CIs. CI operators, like power grid operators, are very motivated in understanding how availability indicators of services delivered by their CIs (such as customer average interruption duration (CAIDI)), depend upon the availability of SCADA services and in turn on the availability of the interconnected Telco CI.

6. Conclusions

In previous studies aimed at investigating the interdependencies between power and Telco networks, the SCADA system was not explicitly, or very roughly, modelled. On the contrary, we have demonstrated here how an actual failure scenario is affected by the availability of two critical public communication links between two SCADA control centres. Furthermore, we have shown that quantitative analysis is a valuable way to identify weak points in the networks and to suggest design improvements.
In a continuation of this research [21], we intend to investigate degradation and loss of services observed by an operator of SCADA system under various possible failure scenarios. Heterogeneous models (stochastic versus deterministic, agent based, dynamic simulation) are under development to perform short term predictions of quality of services performed by a SCADA operator versus quality of power supply delivered to customers. The final aim is to propose a real-time alerting system to support decisions of SCADA operators in preventing degradation and loss of power to customers caused by events occurring in the interconnected Telco infrastructure.

Acknowledgements

This research is originated by the participation in the EU projects IRRIIS (http://www.irriis.org/) and MICIE (http://micie.eu/) and the Italian MIUR project Cresco (http://www.cresco.enea.it/). The authors wish to thank G. Rapanotti for fruitful discussions on some technological aspects and D. Lefevre.

References

[26] DIESIS EU Project (http://www.diesis-project.eu/).