Chapter 14

Securing CEI “By-Design”

By Nikolaus Wirtz, Alberto Dognini, Abhinav Sadu, Antonello Monti, Guilherme Brito, Giovanni di Orio, Pedro Maló and Cosmin-Septimiu Nechifor

DOI: 10.1561/9781680836875.ch14

Published in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures* by John Soldatos, James Philpot and Gabriele Giunta (eds.). 2020. ISBN 978-1-68083-686-8. E-ISBN 978-1-68083-687-5.

Suggested citation: Nikolaus Wirtz *et al.* 2020. “Securing CEI “By-Design”” in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Edited by John Soldatos, James Philpot and Gabriele Giunta. pp. 245–274. Now Publishers. DOI: 10.1561/9781680836875.ch14.

now
the essence of knowledge

14.1 Resilience and Vulnerability of CEI

Critical Energy Infrastructures (CEI) do not only consist of the power grid and electrical equipment, but also of the communication infrastructure, measurement devices, and control functionalities, which are networks in different domains and at different scale. Dependencies between these networks include power supply of communication infrastructure by the power grid and the dependence of components in the power grid on Control Centre commands. In combination, the networks and their interdependencies form a complex system where a small initial set of component failures has the potential to cause cascading failures leading to partial or complete breakdown of the system. Consequently, for a comprehensive analysis of the vulnerability and resilience of such a system, all the relevant domains and their interdependencies must be included and modeled.

For distributed systems with many components, such as the transmission or distribution grids, a graph-theoretic approach can be applied to perform an analysis of potential cascading in the system. A graph $G = \langle V, E \rangle$ is a mathematical object formed by a set of vertices V and a set of edges E, where each edge $e = \langle u, v \rangle$ is connecting two vertices u and v. We are using simple graphs to represent the network’s topology and directed graphs to represent the dependency between components. Simple graphs do not allow self-loops (edges that are connected to the same vertex) and duplicate edges (multiple edges that are connected to the same vertices) and its edges are bidirectional. Self-loops are not required for the modeling, while duplicate edges could be used to represent redundant lines, cables, or links. However, redundancy can also be expressed as an attribute of an edge in a simple graph. In general, power grids and communication networks allow the flow of energy and data in both directions of a line or link, making a simple graph a suitable representation of the network. Directed graphs, however, as described in [41], consist of arcs as unidirectional edges, which point from one vertex to another. The dependency graph represents components as vertices of the graph and arcs as a dependency, pointing from the dependent component to the supporting component.

14.1.1 Example of use Case and Implementation

The system investigated in this sample use case is based on a generic distribution grid segment [20], which has been extended by a physical and a logical communication network and a measurement and control network as described in Figure 14.1.

The **power grid** consists of multiple loads at the LV level, supplied by four different substations in a radial configuration. Since the grid is meshed, different paths are available to supply the loads under normal operating conditions. This redundancy is utilized for network reconfiguration in case of a fault. For the vulnerability analysis, we simplified the network by aggregating the loads of each section; since in case of a fault in the grid, we expect either all the load nodes of a section to function or none of them.

The real physical communication equipment is not known, and we assume that an **optical communication network** is used to support measurement and control of the power grid. The optical cables are parallel to power lines, thus connecting the same vertices of the graphs; and there is a communication node at each load node of the power grid.

The **logical communication network** uses the optical network’s infrastructure to exchange data between nodes. Each link of this network connects two logical

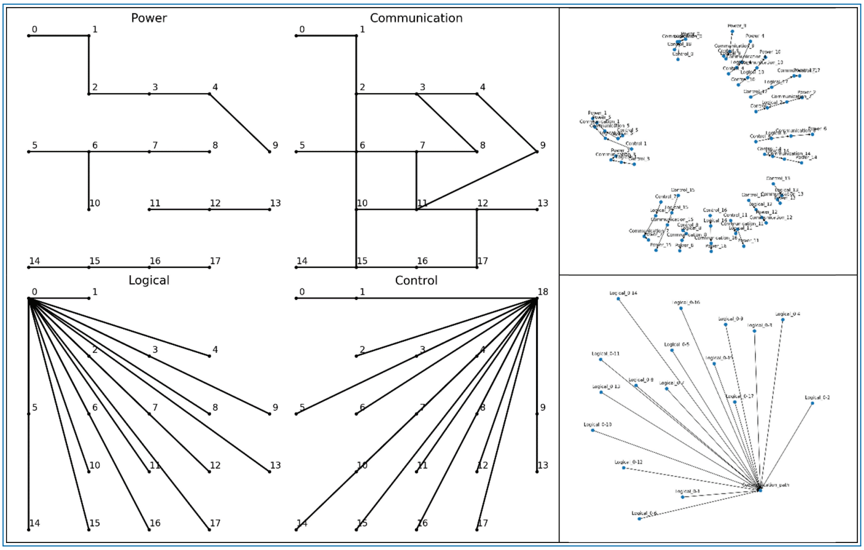


Figure 14.1. Network topologies and node and edge dependency graphs for the example use case.

communication nodes and requires a path in the optical network between the respective physical communication nodes.

The grid operation uses a **measurement and control network** with a central control node (the control center node), which gathers measurement data, processes it, and provides control functionality. This control center node is connected to each of the measurement and control nodes, representing the nodes in the power grid that are equipped with measurement devices and switching equipment that can be remote-controlled.

To model the **interdependencies**, we assume that each node of the power grid supplies the local communication node with power, which in turn supports the local node of the logical communication network. Each node in the logical communication network finally supports one or multiple nodes of the measurement and control network. All the dependencies between nodes are represented in a node dependency graph, which is shown in Figure 14.1 for the default configuration of the scenario. Every link in the logical communication network is dependent on the availability of a path between the respective nodes in the optical communication network. If there is no path available, the link fails, as data can no longer be exchanged.

In addition to the interdependencies, there are domain-specific **intradependencies** in each of the networks. For the power grid, we assume each subgraph must include at least one load node as energy consumer and one substation node as energy provider. If this is not the case, all nodes of the subgraph fail. For the optical and logical communication networks, we assume that isolate nodes fail, since they are no longer able to send or receive data and thus cannot fulfill their purpose. For the measurement and control network, we assume each subgraph must include at least one control center node as measurement data consumer and control command provider and one measurement node as measurement data provider and control command consumer.

In this example scenario, four different configurations of the system are evaluated and compared:

- A **default configuration,** where no by-design measures are implemented
- The **DV configuration,** where Double Virtualization is applied to virtualize part of the functionality of the measurement and control network and thus make it independent from the actual hardware. In this configuration, the control functionality is virtualized, and we assume that it can be hosted by any of the communication nodes at the power grid substations. This is represented in the model by adding dependencies, as "Control_18" is now depending on "Logical_5," "Logical_13" and "Logical_14" in addition to the dependence on "Logical_0." Consequently, additional logical communication links are added, to connect any of the logical communication nodes located at loads to any of the nodes located at substations.
- The **SR configuration,** where a network reconfiguration algorithm provides service restoration by design for the power grid, to resupply lost loads after a failure in the grid. This is represented in the model by adding edges to the power network, representing the lines with switches that are normally open and can be used to provide redundant paths. These additional lines are only used in the reconfiguration after a fault happened, therefore depending on a control command from the control center. In case the control command cannot be received, the switches cannot close, and the line will not be put in operation.
- The **DV_SR configuration,** where both by-design measures are applied.

To evaluate the performance of the complete system after a fault has occurred, we choose two performance indicators:

- The **number of supplied loads,** as a measure of the service level to energy consumers, is maintained.
- The **number of loads that are controllable,** as a measure of the reliability of the final configuration after the cascading sequence has ended. For loads that

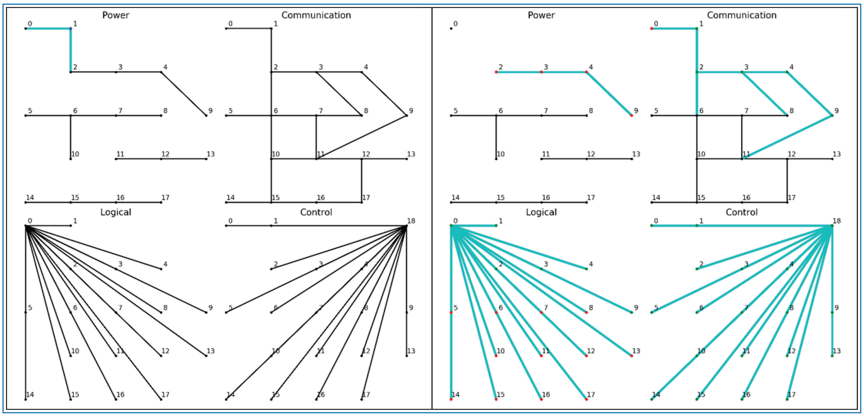


Figure 14.2. Initial and cascading failures of the example use case.

are not controllable, measurements are not available, and targeted reconfiguration is not possible. If the number of controllable loads is smaller than the number of supplied loads, the capability to react to load changes or additional failures is impaired.

14.1.2 Results and Conclusion

The results for a failure at load node 1 are explained in detail to show how the failure is cascading through the system. Initially, as shown in Figure 14.2, load node 1 is failing, causing the edges to the neighboring nodes to fail. Since nodes 2, 3, 4, and 9 are no longer connected to a substation, they are unsupplied and fail. The respective communication nodes are no longer supplied and fail, too, isolating physical communication node 0 and causing it to fail. The cascade proceeds to the logical and the measurement and control networks, causing in both cases the failure of some nodes (including the node that supports or provides control, respectively), then causing all links to fail, and finally also the isolated nodes. In the final state, a large part of the power grid is still supplied, but the controllability has been lost completely and the remaining grid can no longer be monitored.

For a comparison of the different by-design measures, the failure scenario described above has been repeated for each of the nodes in the power grid, representing a single fault happening in different parts of the grid. For each fault, the final state of all networks has been determined via the cascading analysis. The result is shown as boxplots in Figure 14.3, where the box is marking the upper and lower quartile and the orange line marking the median, while the whiskers mark the minimum and maximum.

Even in the default scenario, most of the loads remained supplied no matter where the initial fault happened. However, as presented in the example, the

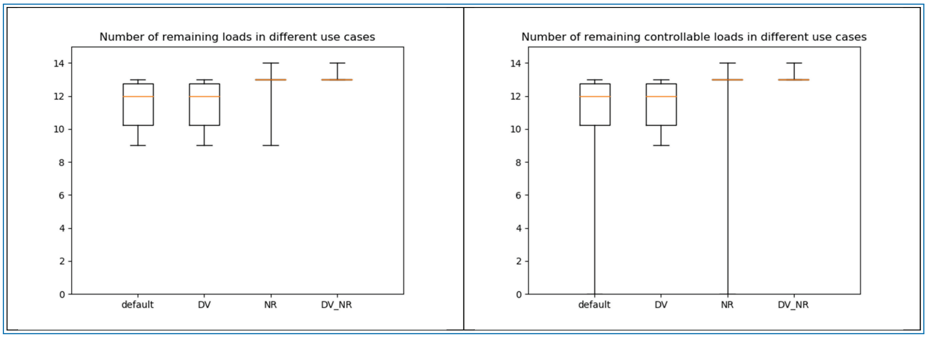


Figure 14.3. Assessment of cascading for different scenarios of the example use case.

capability to monitor and control the remaining part of the power grid is lost completely, if the substation hosting the control center is affected by the initial fault.

The DV configuration manages to solve this issue, enabling the other substations to provide redundancy for supporting the control center functionality. In effect, the remaining part of the power grid remains controllable due to the DV application. Yet, it must be noted that DV does not improve the number of supplied loads. Since a reconfiguration of the power grid is not considered here, it is likely that the initial fault causes additional load nodes of the subgraph to fail. Due to the radial topology of the grid, the closer the fault is to the substation, the more load nodes are failing.

The SR configuration greatly improves this situation and enables more supplied loads in the final state. Due to the meshed topology of the grid that can be utilized for reconfiguration, only the initially failed load is lost in the final state, if the initial fault occurs at a load node. If it occurs at a substation node, there may not be a load node failure at all. However, if the substation hosting the control center functionality fails, the ability to reconfigure the grid is lost and the final state of the system is as in the default configuration.

Only the combination of both by-design measures provides complete containment of a fault independent from its location. If a load node fails initially, only this node is failed in the final state. If a substation node fails initially, the power supply of all load nodes can be maintained. Finally, the capability of monitoring and control of the grid is secured.

The above results show how the impact on the power supply can be minimized effectively by applying by-design measures. While each of the investigated measures improved the resilience of the grid, the combination of both measures provided additional synergies and can avoid the worst case of a failure at the substation hosting the control center. Containing initial failures and reducing cascading to a minimum independent from the location of the initial failure is of increased importance in case of targeted attacks on the most critical components of the system, to stop attackers exploiting vulnerabilities of the system.

14.2 Double Virtualization

Recently, critical infrastructures have been evolving into more complex networks of Cyber-physical Systems (CPS), creating several challenges in the monitoring and controlling of these systems [24]. Double Virtualization (DV) is a specific strategy capable of addressing this, by providing a solution based on the cloud computing paradigm, while enabling a certain degree of decentralization.

For realizing DV, it works on two logical layers: the **Functional Layer** which abstracts the computational resources for management, control, and monitoring functionalities of an asset, and the **Data Layer,** where the logic and features of the deployed applications, such as connectivity and computational operation, are virtually represented. The former offers the remote connectivity, leveraging the control features of the device (while possibly including self-awareness features), while the latter encompasses, in the virtualization process, the set of applications running of the given devices (e.g., logic and configuration for acquiring data, pre-processing, and database query).

By keeping the Functional and the Data Layers decoupled from one another, but acquiring their virtualizations, the DV opens the path on installed devices in a given network to enable real-time reconfiguration and to control running applications and move them from one device to another. This is particularly useful to facilitate the monitoring and control of the Critical Energy Infrastructures (CEI) domain, which comprises a wide variety of dispersed and heterogeneous assets. As matter of fact, in modern power system, the challenge of these types of systems has moved from networking and hardware (such as connection protocols, CPU power and consumption, etc.) to how to connect this amount of different data sources into the specific demands of the hosting platforms and applications. In this context, virtualizations of physical assets—such as the ones offered by DV—and their delivery as services over the network ensure the separation of the functionalities from the specific runtime, protocols, and communication in order to construct highly dynamic, extensible, and flexible environments, as confirmed in [25–28].

The control and monitoring of CEIs deeply rely on the evolvement of the smart grid concept, which incorporates technologies to enhance and provide a better “awareness” of the grid state [29], such as *Advanced Metering Infrastructure* (AMI) or *Wide-Area Monitoring, Protection and Control* (WAMPAC) systems based on *Phasor Measurement Units* (PMU) and *Phasor Data Concentrators* (PDC), aiming at the provision of the guidelines for collecting, transport, and use of data generated on

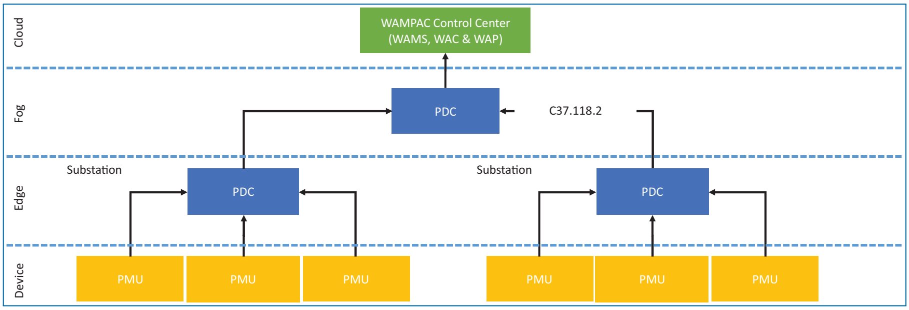


Figure 14.4. Typical WAMPAC system architecture.

the grid. However, these technologies heavily rely on Information & Communication Technologies (ICT), thus exposing the smart grid to a wide range of possible cyberattacks [30].

In this sense, the DV applied to the dedicated computational units of the WAMPAC architecture, as exemplified in Figure 14.4, represents an alternative solution to mitigate cyberattacks that can possibly jeopardize the complete smart grid. To this aim, the DV separates the logical control from the hosting computational hardware into another device and efforts on performing early detection of cyber-physical attacks while enabling mechanisms that provide a continuous operation of the CEI by reallocation of application logic into another asset.

14.2.1 Double Virtualization System Model

For accomplishing DV in a system, it is necessary to adopt the relevant set of assets—DV Assets—with the necessary logic, by either transforming the already existing and/or adding new devices. Additionally, DV demands the inclusion of control, monitoring, and management methodology of these DV Assets, which implies the addition of extra devices in the system—DV Administration & Management (DVA&M). Although in an ideal implementation, DVA&M should be also considered a DV Asset (whose running applications are exclusively for managing and monitoring); in the current implementation, this is not mandatory, since we focus primarily on the already existing devices of the WAMPAC system for demonstrating the concept. Considering all this, and taking the WAMPAC architecture as application model, the system’s transformation is depicted in Figure 14.5.

14.2.2 Double Virtualization Assets

In this type of component, the implemented mechanisms related to the DV provide the ability to gather the necessary information about its resources and functionalities: virtualize the resources/applications running (e.g., bash/Python scripts and

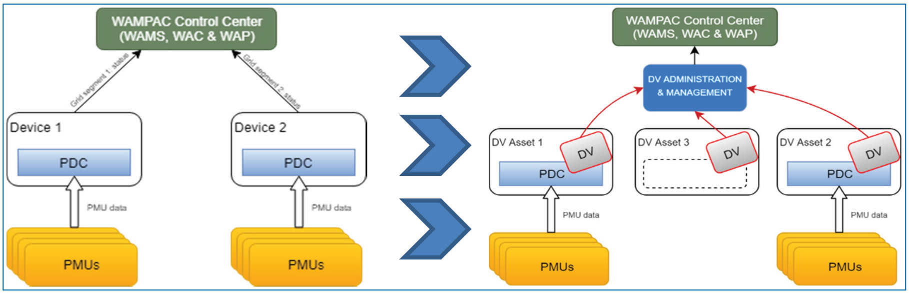


Figure 14.5. Simple grid-monitor model using PMU measurements and equivalent model with double virtualization integration.

their network connections configuration), in a structured data format that may be moved and interpreted on other devices; remote access points that enable the DVA&M devices to access over an internet connection for performing the DV monitoring/administration.

The DV Asset must then be provided, among others, with the following specifications and features:

- **Virtualization:** the DV logic included in the DV Assets must be capable of representing the device and its logical applications in a defined data format.
- **Connectivity:** server and client endpoints must be present, in order to interact with the DVA&M for sending and receiving information, as is the virtualization of the applications or control commands.
- **Monitoring:** the DV Asset must include the necessary services that enable its monitoring by the DVA&M. Furthermore, it may contain self-awareness features that track inner changes that may be also relevant and is able to forward them to the DVA&M.

14.2.3 Double Virtualization Administration and Management

The pivot point of development of the DVA&M component is the ability to execute the monitoring and administration of a set of DV Assets which are connected to it over the network. In this sense, taking in consideration the requirements of the overall system, the chosen approach envisions the use of diverse software patterns, as for example, Service Oriented Architecture (SOA) for addressing communication between devices and Service Orchestration in the optic of management of these same machines, and which was inspired in previously researches, such as presented in [31]. Moreover, the DVA&M is structured taking as base the Observe-Orient-Decide-Act (OODA) pattern, introduced by John Boyd and firstly drafted in [32], in order to achieve the desired logic. Assisted by the OODA loop, the

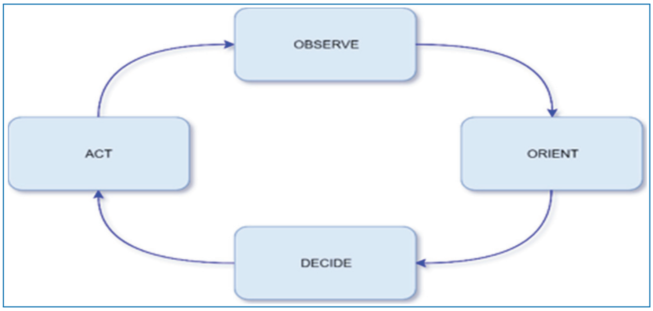


Figure 14.6. Simple OODA loop.

DVA&M entity gathers the abilities to lightly anticipate harmful situations through the continuous monitoring of the several assets behaviors, making use of incoming sensing information, and use it to perform decisions and actions to mitigate detected failures.

The four steps of the OODA loop (Figure 14.6) are described as:

- **Observe:** acquisition of information data, incoming from the detection modules of the system. This information about the DV Assets and can be obtained from internal logic or from an external source.
- **Orient:** in this stage, the received control data is provided with meaning, so that analyses mechanisms can be applied. For example, matching the data to the respective DV Asset and respective previous samples for tracking relevant changes.
- **Decide:** this is where the gathered data is analyzed with the provided algorithms for discovering or handling the detected failures, and furthermore to decide what is the next action. That is to say, if and in what terms the system shall react to the attack detection. This step also provides all output necessary for enforcing the reaction, such as is the case of a migration, where the virtualized logic of an attacked DV Asset needs to be moved into another one.
- **Act:** when this step is activated, it uses all the gathered information to trigger and complete all the mitigation process, while handling the involved DV Assets, in any way possible, through the established connections implemented specifically for administration purposes.

The DVA&M must then be implemented in accordance with the following specifications and features:

- **Database/Registry:** necessary for storage of the relevant information of the DV Assets, like the specifications of the device and the respective virtualizations.

- **Connectivity:** The DVA&M provides the necessary server and client endpoints in order to receive and send information to the other components (DV Assets, external detectors, …).
- **Monitoring:** the DVA&M hosts simple monitoring mechanisms (Acknowledge and Heartbeat/Watchdog techniques) dedicated to the connectivity status of DV Assets, yet it shall also be able to handle incoming information from external detectors and forward it into the decision algorithms.
- **Decision:** the DVA&M must be able to filter the incoming information from the multiple DV Assets and decide whether any action shall be activated, and in that case, handle all the consequent process
- **Mitigation:** the mechanisms to autonomously interact with the faulty DV Assets, while performing the necessary control commands and exchanging the necessary information.

14.3 Example use Case and Implementation

14.3.1 Technological Details

Node-Red framework has been selected as the development and deployment tool for the DV system. Node-Red offers a browser editor for development and deployment and runs over Node.js runtime environment, which stands as one of the prevailing software for development of applications under the Internet of Things (IoT) scope. Moreover, Node-Red applications are constructed on a flow-based semantics, by wiring nodes, and allow an easy creation and setup of computational resources that provide functions, APIs, and online services supported by a wide number of protocols usage. Node-Red also enables the creation and integration of custom nodes (provided by a highly active community), extending its potential for connectivity to, for example, legacy systems.

Another important highlight is the fact that Node.js is supported by a variety of operating systems and processor architectures, such as ARM processors used in single board computers like Raspberry Pi or Odroid. This leverages the cross-platform implementation and widens the number of possible resources to use.

With respect to the interoperability among the DV components in use, the created endpoints that are related to DV functionalities follow the REST pattern, while most of the inherent data is represented in JSON format.

Regarding the security mechanisms, several options are available, including the standard authorization schemes for HTTP. However, while adopting the use of certificates to enable HTTPS for encryption, client certificate authorization, which is built in the HTTPS handshake, was tested and subsequently included, while being optionally customized.

14.3.2 Internal Detectors

The implemented DVA&M comprises built-in detection methods oriented to evaluate connectivity status of the DV Assets. Even if not necessarily the lost connection of a device is caused by some sort of attack, either physical or cyber, it is still plausible to assume it. Moreover, to ensure the resilience of the system, the detection of such failure is used by the DV to trigger the migration of the faulty DV Asset into an available one, as a mitigation strategy.

For both Acknowledge and Heartbeat techniques, the DVA&M has a specified timeout, in which the DV Asset must report to the DVA&M that it is available. The difference is that in the Acknowledge technique, the DV&AM makes a request and the timeout refers to the response time, while in the Heartbeat/Watchdog technique, the DV Asset itself periodically sends acknowledge messages and the timeout is used within the Watchdog. It must be considered that, in both cases, the period of the acknowledge messages and the timeout value must be set so that there is no overlap within the sequence, making it susceptible to induce false failure detections.

14.3.3 External Detectors

Event detection represents the activity of detecting relevant events in (near) real-time from the stream of raw data observations. Most event detection systems are generic, where the user must deploy a set of processing rules at design time, which are used to push observations at run time. The result of the processing is delivered back to the application in form of events.

The event detection engines can be evaluated according to the following categories:

- Development platform, representing the programming language used for event detection applications development
- Event detection language, the operators which can be used to define event extraction rules
- Development model, representing the flexibility used for defining event detection patterns
- Advertised event rate
- Out of the box deployment possibilities
- Integration/compatibility with other technologies
- Licensing.

The network and the communication infrastructure represent an important commodity of an IT system, including the Smart Grid ones. For such a system, it is important to detect as early as possible any attempt of unauthorized access/usage of the network. The network monitoring module has the scope to detect any abnormal behavior of the network.

Regardless of the network assets (routers, switches), the monitoring can be done using the Remote Network Monitoring (RMON) Protocol [40]. The RMON protocol can be used to extract real-time information about the device, such as bandwidth or ports connected/disconnected. Depending of the device type, the processing logic can be embedded into the switch (if it has enough processing power) or a field device (like a Raspberry PI) can be located in the nearby area to execute this activity. In most of the cases, a centralized solution will overload the network. The list of switch operating parameters can include:

- Network utilization (per each port or overall);
- Error Rate;
- Port connectivity.

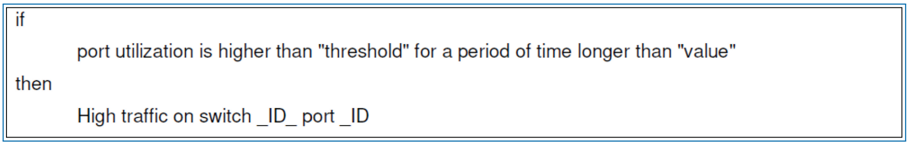
In general, the various components of a system generate log data which is used for monitoring the component status and for debugging. Depending on the architecture, each component can have its own log file or the system can have a centralized logging infrastructure. In most of the cases, when one component is affected by a perturbation, several components might report the abnormal behavior in their log file.

External detectors can be plugged into the DVA&M, by accessing specific endpoints (REST) created for the effect. In the DV case study, this was tested with the log data pattern matcher implemented by SIEMENS, offering the following features:

- Merge multiple log files considering the log event timestamp
- Define domain specific log data patterns (at design time)
- Apply the log data pattern on the streams of log events (at run time).

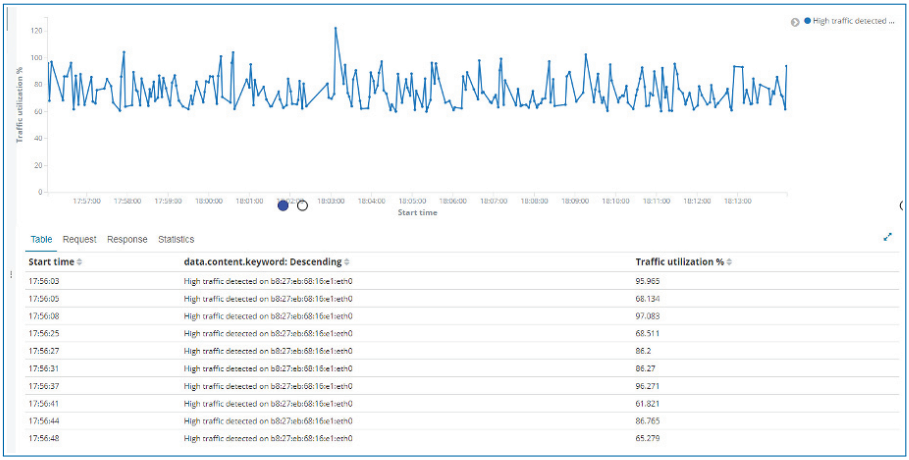
The following example is relevant for high traffic on device interface observation. The logic of observation pattern is depicted in Figure 14.7.

The observed behavior in case of an attack in the context of this use case is presented in Figure 14.8.



```
if
        port utilization is higher than "threshold" for a period of time longer than "value"
then
        High traffic on switch _ID_ port _ID
```

Figure 14.7. Observation pattern logic.



Start time ⇕	data.content.keyword: Descending ⇕	Traffic utilization % ⇕
17:56:03	High traffic detected on b8:27:eb:68:16:e1:eth0	95.965
17:56:05	High traffic detected on b8:27:eb:68:16:e1:eth0	68.134
17:56:08	High traffic detected on b8:27:eb:68:16:e1:eth0	97.083
17:56:25	High traffic detected on b8:27:eb:68:16:e1:eth0	68.511
17:56:27	High traffic detected on b8:27:eb:68:16:e1:eth0	86.2
17:56:31	High traffic detected on b8:27:eb:68:16:e1:eth0	86.27
17:56:37	High traffic detected on b8:27:eb:68:16:e1:eth0	96.271
17:56:41	High traffic detected on b8:27:eb:68:16:e1:eth0	61.821
17:56:44	High traffic detected on b8:27:eb:68:16:e1:eth0	86.765
17:56:48	High traffic detected on b8:27:eb:68:16:e1:eth0	65.279

Figure 14.8. Observed behavior of the log data pattern matcher in case of an attack.

The messages received from external detectors may lead the DVA&M to take some decision and possibly trigger some mitigation action, like trying to reconfigure some DV Asset or perform a migration. In the case of the log data pattern matcher, the approach is to evaluate if a determined number of warnings related to a given DV Asset is received during a time window, thus inducing the DVA&M to activate the mitigation process for the faulty device.

Also, by including this and other detectors that provide a wider panoply of parameters of the DV Assets (e.g., network interfaces traffic information, CPU loads, temperatures of the CPUs, response time of the APIs and services, etc.), the decision algorithms can evolve to more accurate results, like in the case of an occurring migration, where the DVA&M should decide which is the more adequate DV Asset to receive and start running a new set of applications.

14.3.4 Use Case

For demonstrating the DV functionality, the use-case scenario is based on the previously shown WAMPAC system, where PDCs are wired up to PMUs for collecting data. Besides this, a spare development of the PDC consists in hosting small preprocessing algorithms. These PDCs were adopted with the DV logic, and furthermore, its applications were virtualized in compliance with the DV specifications.

Finally, in order to gather the necessary results, a connection failure was induced in one PDC, by unplugging the ethernet cable. When doing this, the DVA&M is able to detect that the unplugged PDC is no longer responding, triggering the migration process, and consequently, the set of application is launched on another

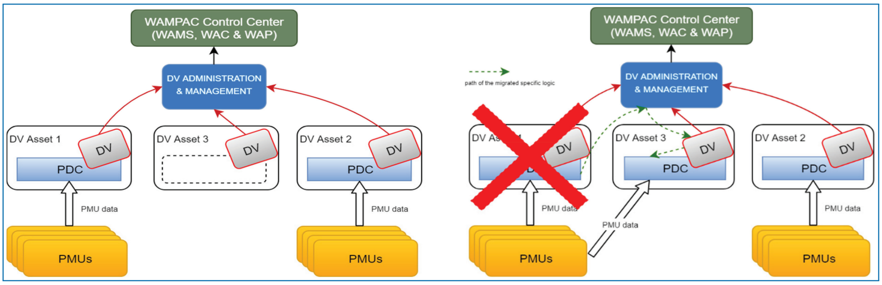

WAMPAC Control Center (WAMS, WAC & WAP)
DV ADMINISTRATION & MANAGEMENT
DV Asset 1
DV Asset 3
DV Asset 2
DV
PDC
PMU data
PMUs
path of the migrated specific logic
WAMPAC Control Center (WAMS, WAC & WAP)
DV ADMINISTRATION & MANAGEMENT
DV Asset 3
DV Asset 2
DV
PDC
PMU data
PMUs

Figure 14.9. System state before and after the detection of lost connectivity of a DV asset and migration strategy applied as mitigation strategy.

PDC which was chosen during the decision algorithm of the DVA&M, as depicted in Figure 14.9.

The context of the use case is as described below.

The Fault Detection Algorithm (FDA) plays an important role in power grid observability and is also the first functionality of a self-healing grid. Depending upon the different grounding schemes of the different grids, the impacts of the fault currents in the grid varies [33]. Furthermore, with the availability of high accuracy and high frequency of measurements from PMUs, advanced FDA schemes, based on PMU data, are being designed [34, 35]. The FDA is deployed in a dedicated hardware that receives continuously the stream of PMU data corresponding to the voltages at different nodes and currents flowing through specific branches in the network. The PMU data is parsed into the FDA after proper protocol translation. The parsed PMU data is then processed by the FDA which detects the occurrence of faults based on the changes in the zero sequence components. Given that the reporting frequency of PMU can be as high as 50 frames per second or more for power networks with nominal frequency of 50 Hz, the fault inception moment can be captured with delay of 20 ms at maximum. Since the timestamp of an event is critical information for correct evaluation of fault location, it is of paramount importance to ensure the uninterrupted operation of FDA. With introduction of DV, the availability of FDA can be substantially increased when fault in communication network or cyberattack occurs, and therefore, the robustness of the fault detection scheme is ensured.

14.3.5 Conclusion

The DV model implemented in the use-case scenarios have, in general, fulfilled the stipulated outcomes in terms of functionality and proof of concept. More specifically, the defined mitigation strategy—migration—was achieved, once a connectivity failure was detected, by completing the transaction of the running application from the faulty device into the best suitable device.

It can also be stated that the main requirements were accomplished: the virtualization process of the assets functional and application layers; communication system for supporting the data transaction inherent to the DV, using REST endpoints; implementation and integration of, respectively, internal and external detectors and corresponding monitoring mechanisms; decision algorithms that can be shaped according to the monitoring parameters in use; and the processing/management of the mitigation actions by either DV Assets and DVA&M components of the system.

In this sense, the DV is a viable solution to augment the resilience of the system. However, taking in consideration that the DV application is still in an early stage, several items that shall be developed and/or improved in the future implementations have been already identified.

For instance, in such scenarios as the Fault Detection described in the previous section, where it is of such crucial importance to minimize the downtime caused by the network failure, some technical choices can be made towards this improvement, such as minimizing the routes of the network connections (number of intermediary routers, not using VPN, etc.), opt for a faster alternative to using client certificate authorization (which takes some time for validation during the HTTPS handshake) and also refining the detection, decision, and action processes of the DV itself.

Another improvement to be considered, for a more proactive solution, is to pre-setup DV Assets with one another's logic, for minimizing the amount of data to be passed to trigger the mitigation and, consequently, the time of the process. Of course, this comes at the cost of more storage and CPU load, but depending on the use case, it may be profitable.

Regarding the critical Single Point of Failure (SPoF) paradigm, the current DV system is not yet completely capable to solve this thematic. In a more close-up glance, it can be noticed that the SPoF was removed from the "functional" area of the system (where DV Assets co-exist); however, the introduction of DVA&M device results in a new SPoF. One possible solution that was put on the table is to create a cluster of DVA&M devices in the system and apply also the DV solution to them, with the respective nuances. For example, in order to avoid the hierarchical structure that induces SPoFs, one can adopt monitoring patterns such as the circular pattern. Furthermore, the Blockchain technology may directly offer a solution for decentralization, but from the performed investigation, we found that the requirements for implementing Blockchain (e.g., high-performance CPUs, big data storage) for very demanding time requirements, this may be a challenge and other instances of Distributed Ledger Technology may be required in these demanding scenarios.

14.4 Service Restoration

The basic functionality of a self-healing power grid is to restore the loads that were de-energized either due to natural disasters or targeted attacks on the grid. There are two kinds of events that create outages in the grid. One that occurs frequently but have lower magnitude of outage, like tripping of lines due to faults in the lines due to ageing of the cables. The other type of events are the ones that have High Impact but occur with Low Probability (HILP events). A HILP event introduces severe and rapidly changing circumstances that may have never been experienced before, causing multiple outages in the network and creating large de-energized sections [1].

A typical Service Restoration (SR) scheme for distribution grids, after successful fault detection and isolation, should be able to perform the following:

- Restore as much out-of-service customers as possible in a minimum time, by providing a sequence of operations to the switches. Preference in use of tele-controlled switches in re-powering process should be given, to reduce the restoration time.
- Consider the priority of the loads and restore the most crucial customers (hospitals, devices controlling the gas network pumps, cellular base stations, and other critical infrastructures) first.
- Preserve radiality of the grid with every switching operation prescribed in the sequence.
- Maintain the voltage of the grid as per the limits imposed in the grid codes of the specific country.
- Satisfy loading constraints of the lines and substation loading.

For the outages caused by the non-HILP events, different approaches are proposed in the literature for optimal selection of the tie switches (normally open switches, generally connecting different feeders or segments of the same feeder) to be closed. These can be classified into expert systems [3–5], Multi-Objective Evolutionary Algorithm (MOEA) [6–8], heuristic-based systems [9–12], meta-heuristics and mathematical programming based [2]. Though the MOEA methods and heuristic methods for SR are popular, they have longer running times and are sensitive to the accuracy of generating the feasible topologies, from which the optimal solution would be deduced. Furthermore, Mixed Integer Programming (MIP)-based methods have also been proposed [13–15]. The mathematical programming methods, especially the MIP based, prove to be computationally expensive.

Hence, they would not be suitable for real-time application with stringent time constraints. One of the major challenges in designing a service restoration scheme to cope with the HILP events is that, in addition to the aforementioned attributes, the SR scheme should also react to rapidly changing system condition. It should be able to consider, in real time, the uncertainties in the power generation and load demand so that possible network congestion is avoided while grid restoration. Furthermore, it should adapt to changes in grid topology as subsequent multiple faults may occur due to the propagation of the HILP events. Unlike the heuristic, meta-heuristic, and mathematical programming-based SR schemes, the rule-based algorithms have been found better suited for real-time applications. They can provide sub-optimal, interim solutions to cater to emergency situations [5], due to their lower computational complexity. Nevertheless, the Rule Based Service Restoration Algorithm (RB-SRA) should also incorporate distribution grid operator preferences in selecting the optimal service restoration option. This is vital as grid operators in different countries have to follow different operational norms and adhere to specific grid codes. Thus, for designing a universal service restoration, the RB-SRA has to be extended with a Multi-Criteria Decision Making (MCDM) algorithm. The MCDM approach facilitates optimal selection of solution from the set of possible solutions considering the dynamic preferences of the decision-maker [16–18]. In this case, the set of solutions are the choice of optimal restoration sequence considering the preferences of the network operator. It should be noted that the MCDM enabled RB-SRA would not be the most optimal service restoration (considering the cost of operation, power losses, etc.) but would be a best effort solution catering to dynamic outages caused by propagation of the HILP events.

14.4.1 MCDM-Enabled Rule-Based Service Restoration Algorithm (RB-SRA)

The MCDM-enabled RB-SRA has 4 major sequential steps, Namely:

(1) Identification of loads to be restored;
(2) Determination of alternative reconfigurable paths;
(3) Network security assessment with state estimation;
(4) MCDM-based selection of optimal restoration path.

Identification of loads to be restored

When multiple faults occur or the continuous load growth is not promptly combined with substation reinforcement, the reconnection of all de-energized loads cannot be achieved [36]. Hence, it is necessary to identify the most critical load and quickly restore it. The RB-SRA selects, among the de-energized nodes that are outside the fault-zone, the one with the highest priority index. This parameter is an independent characteristic of each load, assigned by the grid operator to indicate its criticality. If multiple loads have the same index, the algorithm selects the one consuming (or generating) the highest active power. The chosen node is taken as target for the restoration plan.

Determination of alternative reconfigurable paths

Once the load to be restored, named $\boldsymbol{b}$, has been identified as described above, the best reconfiguration topology to re-energize it has to be computed. Firstly, the proposed algorithm inspects all the $\boldsymbol{n}$ primary substations present in the network. For each substation, it determines the most suitable path towards the load by using Dijkstra's algorithm. Considering two nodes $\boldsymbol{a}$ and $\boldsymbol{b}$ in a weighted graph G, Dijkstra's algorithm calculates the shortest path that connects them, named $G'_{a,b}$. In this case, $\boldsymbol{a}$ is the selected substation, $\boldsymbol{b}$ is the load to be restored, and the weight of each edge is the series impedance of the line. Hence, considering $|\overline{Z}_{x,y}|$ as the magnitude of complex series impedance $|\overline{Z}_{x,y}| = R_{x,y} + jX_{x,y}$ between adjacent nodes $\boldsymbol{x}$ and $\boldsymbol{y}$ of the graph, the shortest path $G'_{a,b}$ has a total impedance Z_a^b such that $Z_a^b = \min \sum_{x,y \in G'_{a,b}} |\overline{Z}_{x,y}|$. With respect to total impedances of other paths that can connect $\boldsymbol{a}$ to $\boldsymbol{b}$, Z_a^b has the minimum value for graph $G'_{a,b}$. If the shortest path exists, it includes at least one bus tie which is currently open and, by closing it, allows to energize load $\boldsymbol{b}$ from substation $\boldsymbol{a}$. With the switches now closed and the path made electrically continuous, the whole network topology has changed, represented by the graph $G_{a,b}$ for which $G'_{a,b} \subset G_{a,b}$ ($G'_{a,b}$ is a subset of $G_{a,b}$). This procedure is repeated for each substation present in the grid. If multiple faults occur or the continuous load growth is not promptly combined with substation reinforcement, the reconnection of all de-energized loads could not be achieved [36].

Network security assessment with state estimation

Each network configuration proposed by the RB-SRA is to be checked versus line congestion and voltage security limits via State Estimation (SE) [37]. Many methods are available for SE but among them the Weighted Least Square (WLS) approach is most popular [37, 38]. It is based on the minimization of the square of the measurement residual vector. With input as the set of measurements, the uncertainty class of the measurement devices, network topology and its parameters, the WLS based SE is able to provide the estimate of the state of the grid that may be magnitude and angle of node voltage (for node voltage-based SE) or the magnitude and angle of the branch current (for branch current-based SE). Furthermore, from the estimated states all the power flows in the grid, loading of the network lines, and the power losses can be calculated.

For each proposed grid topology, represented with graph $G_{a,b}$, the following constraints should be respected:

- Radiality of the network: if a path exists between nodes a and b, the closing of the tie switches in this restoration scheme must maintain each substation electrically disconnected from the others.
- Voltage limits: at each node of the grid, the voltage magnitude must remain in the range of ±10% of the nominal value [39].
- Respect of loading limits: the current flowing in each edge must comply with the cable/conductor or substation transformer specification $|\overline{I}_{x,y}| \pm 3\mu_{|\overline{I}_{x,y}|} < I_{max_{x,y}}$.

Where $|\overline{I}_{x,y}|$ is the line current magnitude at the generic edge $(\boldsymbol{x}, \boldsymbol{y})$ and its uncertainty $\mu_{|\overline{I}_{x,y}|}$; $I_{max_{x,y}}$ indicates the continuous current carrying capacity of the line or the overcurrent limit of the transformer at the primary substation, and in emergency situation, a certain percentage of overloading is acceptable for limited amount of time. If the proposed configuration $G_{a,b}$ does not fulfill the requirements, it is discarded and the restoration of load $\boldsymbol{b}$ cannot be achieved by the substation $\boldsymbol{a}$.

MCDM-based selection of optimal restoration path

Once the set of secure reconfiguration paths has been determined, the optimal solution has to be identified. To do this, the proposed algorithm combines two criteria dependent upon settings predefined by the user, namely the power losses and the utilization of the lines, as described below.

- *Total power losses in the network* ($P_{x,y}$): The power loss $P_{x,y}$, between two generic nodes $\boldsymbol{x}$ and $\boldsymbol{y}$, is estimated by the following formula, using the estimated line-to-ground node voltages by the SE algorithm and the electrical lines are modeled as the π equivalent circuit.

$$P_{x,y} = 3\,\mathfrak{R}\left[\overline{V}_x\left(\overline{V}_x\frac{G_+ + jB_+}{2}\right) + \overline{V}_y\left(\overline{V}_y\frac{G_+ + jB_+}{2}\right) + \left((\overline{V}_x - \overline{V}_y)\left(\frac{(\overline{V}_x - \overline{V}_y)}{R_+ + jX_+}\right)\right)\right]$$

Where R_+, X_+, G_+, B_+ are the positive sequence line resistance, reactance, conductance, and susceptance, respectively. The power losses are added for each line of the network (edges of graph $G_{a,b}$) to obtain the total power loss P^a of the candidate topology restored through substation $\boldsymbol{a}$.

- *The utilization of electrical lines* ($\theta_{x,y}$): It is a measure of overloading of the lines in the grid. The different service restoration options can be ranked on the basis of their relative network loading. The higher the value of $\theta_{x,y}$, the better is the distribution of power flow in the specific network configuration

$$\theta_{x,y} = \frac{I_{max_{x,y}} - |\overline{I}_{x,y}|}{I_{max_{x,y}}} \tag{14.1}$$

Where $\boldsymbol{x}$, $\boldsymbol{y}$ are two nodes between which the current $\overline{I}_{x,y}$ flows and the line connecting the nodes $\boldsymbol{x}$ and $\boldsymbol{y}$ has the maximum current carrying capacity of $I_{max_{x,y}}$. For each network topology that is analyzed, three minimum values of $\theta_{x,y}$ are recorded in descending order. In the case of graph $G_{a,b}$, they are indicated as θ_1^a (the minimum one), θ_2^a & θ_3^a, for which θ_1^a is related to the electrical line having the current most close to its specific ampacity. The selection of the optimal solution requires the combination of these two aspects, summarized as the four criteria $P^a, \theta_1^a, \theta_2^a, \theta_3^a$. Then, using the MCDM technique, the optimal restoration path is selected. The MCDM technique is a two-step algorithm. In the first step depending upon the relative pairwise weight of the criteria, an absolute weight for each criterion is deduced. In the second step, these weights are used to determine the relative closeness of the available solution to the ideal solution. For the first step, the Analytical Hierarchical Process (AHP) is implemented to determine the absolute weights of criteria with the pairwise weights of the criteria. The pairwise weights are assumed to be provided by the network operator. The comparison matrix Γ is calculated using the pairwise weights provided by the operator [22].

$$\Gamma = \begin{bmatrix} 1 & \omega_{P\theta_1} & \omega_{P\theta_2} & \omega_{P3} \\ 1/\omega_{P\theta_1} & 1 & \omega_{\theta_1\theta_2} & \omega_{\theta_1\theta_3} \\ 1/\omega_{P\theta_2} & 1/\omega_{\theta_1\theta_2} & 1 & \omega_{\theta_2\theta_3} \\ 1/\omega_{P\theta_3} & 1/\omega_{\theta_1\theta_3} & 1/\omega_{\theta_2\theta_3} & 1 \end{bmatrix} \tag{14.2}$$

In which ω is the comparison value between the attributes indicated by the subscripts, which ranges from 1/9 (attribute of second subscript is extremely important with respect to the first one) to 9 (attribute of first subscript is extremely important with respect to second one) according to the AHP scale. A detailed possible AHP weights and their interpretation is provided in Table 14.1. The subscripts

Table 14.1. AHP weight interpretation.

Intensity of Importance ($\omega_{P\theta}$)	1	3	5	7	9	2, 4, 6, 8
Interpretation	P, θ are of equal importance	P is slightly more important than θ	P is strongly more important than θ	P is very strongly more important than θ	P is extremely more important than θ	Intermediate importance between two adjacent judgment

$P^a, \theta_1^a, \theta_2^a, \theta_3^a$ represent the power losses and the line utilization of the three most consumed lines, respectively. The priority vector is obtained, which ranks the four criteria and shows relative weights among them. The approximate calculation of the priority vector (PV) can be done as shown in equations:

$$PV_j = \frac{\sum_{l=1}^{m} \overline{p}_{jl}}{m} \quad \text{where } \overline{p}_{jk} = \frac{\Gamma(j,k)}{\sum_{l=1}^{m} \Gamma(l,k)} \quad \text{and } m\text{: number of criteria} \tag{14.3}$$

Then, these relative weights are combined with the power losses and line utilizations of each feasible solutions, indicated by the different values of a as reference substation, according to the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) [23]. A generic set of equations that govern the TOPSIS-based ranking of the alternatives are given below. For $\boldsymbol{t}$ alternatives and $\boldsymbol{m}$ number of criteria, the decision matrix $\boldsymbol{D}$ can be created as shown below in Equation (14.4):

$$D = \begin{bmatrix} d_{11} & \dots & d_{1m} \\ \vdots & \dots & \vdots \\ d_{t1} & \dots & d_{tm} \end{bmatrix} \tag{14.4}$$

The weighted normalized decision matrix integrating the Priority Vector calculated in Equation (14.3) can then be derived as in Equation (14.5):

$$v_{ij} = PV_j \, r_{ij} \quad \text{where } r_{ij} = \frac{d_{ij}}{\sqrt{\sum_{i=1}^{m} d_{ij}^2}} \tag{14.5}$$

The next step in the TOPSIS-based ranking is to calculate the positive ideal solution ($\boldsymbol{A}^+$) and the negative ideal solution ($\boldsymbol{A}^-$) where B is a set of Benefit criteria and C is a set of Cost criteria:

$$\boldsymbol{A}^{+} = \{v_1^{+}, \ldots v_m^{+}\} \quad \text{where } v_j^{+} = \{\max(v_{ij}) \text{ if } j \in B; \min(v_{ij}) \text{ if } j \in C\} \tag{14.6}$$

$$\boldsymbol{A}^{-} = \{v_1^{-}, \ldots v_m^{-}\} \quad \text{where } v_j^{-} = \{\min(v_{ij}) \text{ if } j \in B; \max(v_{ij}) \text{ if } j \in C\} \tag{14.7}$$

The purpose to calculate the $\boldsymbol{A}^{+}$ and $\boldsymbol{A}^{-}$ is to measure the distance of the alternatives from the positive ideal solution and negative ideal solution. The best alternative would be the one that is as close to the positive ideal solution and as far as from the negative ideal solution. In order to rank the alternatives, the relative closeness is then calculated as in Equation (14.8):

$$C_t^{+} = \frac{S_t^{+}}{S_t^{+} + S_t^{-}} \quad \text{where } S_t^{+} = \sqrt{\sum_{i=1}^{m} (v_{ij} - v_j^{+})^2} \quad \text{and}$$

$$S_t^{-} = \sqrt{\sum_{i=1}^{m} (v_{ij} - v_j^{-})^2} \tag{14.8}$$

For the service restoration process, the TOPSIS allows us to compute the closeness of each candidate solution to the ideal one, which is composed by the minimum power loss P^a and maximum reserve line capacity $\theta_1^a, \theta_2^a, \theta_3^a$. Among the possible solutions, indicated by the different values of $\boldsymbol{a}$ as reference substation, the one having the highest closeness ${C_a}^{+}$ is chosen to reconnect the load $\boldsymbol{b}$. Then, a closing signal is sent to the open tie switch related to this configuration.

The selected optimal solution is, then, a trade-off between the minimization of power losses in the line and the avoidance of lines having the current close to its limit. The comparison parameters ω are defined by the grid operator before the service restoration is started; they are set depending on whether more importance is assigned to power losses or line utilization aspect. For example, in case of aged cables, one can place greater emphasis on line utilization (by decreasing $\omega_{P\theta_1}$, $\omega_{P\theta_2}$ and $\omega_{P\theta_3}$) in order to avoid the excessive worsening of line condition.

Test case

The test grid used to validate the MCDM-based RB-SRA is a medium voltage distribution grid at 13.8 kV with four primary substations. Figure 14.3 represents its single line diagram and includes the elements naming used below [20]. Its 37 nodes connect loads that range from 100 kW to 1 MW; the length of the electrical lines varies from 800 m to 2200 m. Nodes I2 and L1 host DERs of 200 kW and 250 kW, respectively. Complete data of the grid can be found in [21]. The black

Table 14.2. AHP pairwise priorities.

Pair of criteria	$\omega_{P\theta_1}$	$\omega_{P\theta_2}$	$\omega_{P\theta_3}$	$\omega_{\theta_1\theta_2}$	$\omega_{\theta_1\theta_3}$	$\omega_{\theta_2\theta_3}$
AHP pairwise weights	7	8	9	2	2	2

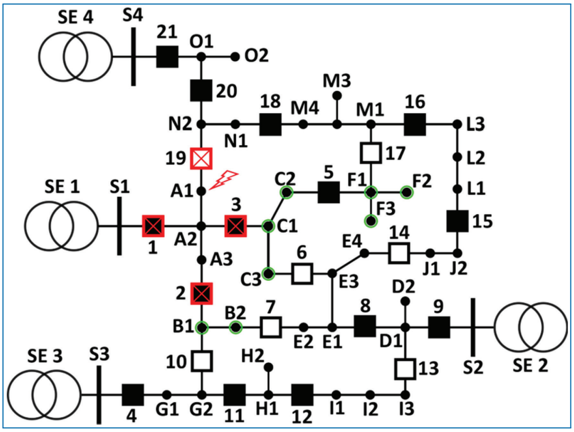


Figure 14.10. Location of the fault for test case.

squares indicate the normally closed switches, whereas the normally open ones are shown with white squares.

This scenario inspects the occurrence of a single fault and the presence of multiple loads having the same priority index, for which the nominal active power is considered to determine the restoration target. In this test case, the most important criterion of the service restoration is the minimization of the power losses, with marginal relevance of lines utilization in the decision process. The comparison parameters ω are reported in Table 14.2.

The single electrical fault occurs at node A1; the protection system opens the upstream circuit breaker indicated by number 1 and, in order to isolate the fault area, the downstream circuit breakers 2, 3, and 19 (which is already open). These four switches, indicated with red frames in Figure 14.10, remain in a tripped condition and cannot be reclosed until the fault has been repaired.

The MCDM-enabled RB-SRA receives the status of the tripped breakers, and it first identifies the faulty zone; hence, it excludes the nodes A1, A2, and A3 from the restoration process.

The de-energized loads are downstream of the switches 2 and 3; they are marked with green circles in Figure 14.8, whereas their priority indexes and nominal active power are reported in Table 14.3. Both the loads B2 and C2 have the highest priority index; since the nominal active power of B2 is higher, it is selected as target for the restoration process.

Table 14.3. De-energized Loads and their critical index.

Loads	B1	B2	C1	C2	C3	F1	F2	F3
Priority Index	3	1	4	1	2	4	3	4
Active Power [MW]	0.37	0.70	0.27	0.46	0.17	0.27	0.22	0.35

Table 14.4. Computational performance of MCDM-enabled RB-SRA.

Test Case	Test Case 1
Loads	B2 C2
Min (Seconds)	2.15 2.97
Average (Seconds)	2.29 3.16
Max (Seconds)	2.97 3.84

In the next step, the algorithm evaluates the possible reconfiguration paths associated to each substation. The substation SE 1 is not suitable, since the switches in the fault zone cannot be operated. Moreover, SE 4 is excluded too, because the radial topology cannot be maintained (SE 4 and SE 2 would be electrically connected). The power loss related to SE 2 is 4.5% larger (corresponding to 30.7 kW) than SE 3, making SE 3 solution the closest to the ideal one ($C^+_{SE2} = 0$ and $C^+_{SE3} = 1$). Hence, the closing command to switch 10 is sent. Once the database updates the switch status and the closing command is sent to field device, the SR algorithm restarts; the loads B1 and B2 are now energized by SE 3; hence, the algorithm evaluates the restoration of the loads in the branch downstream of switch 3, selecting the node C2 as first target. Only SE 2 or SE 4 could restore the selected load (and, consequently, all the nodes in the same branch) by maintaining the radial structure. The restoration is achieved by closing the switch 6, for which P^{SE2} is smaller of 36% than P^{SE4} making the closenesses to ideal solution $C^+_{SE2} = 0.82$ and $C^+_{SE4} = 0.18$. All the de-energized loads outside the fault zone are reconnected; then, the algorithm is concluded. The algorithm always checks for the real-time switch position data before it closes the tie switch to reenergize the loads, by doing so it detects if a subsequent fault had occurred that triggered other switches/circuit breaker position. If it detects a change, then it stops the current operation and reruns the complete MCDM-enabled RB-SRA for the new topology of the grid and lost load configuration. This functionality helps in handling multiple sequential failures introduced by the HILP events.

The performance of the MCDM-enabled RB-SRA is tabulated in Table 14.4. The restoration of grid for the same fault locations have been performed 100 times for a stochastic evaluation.

Conclusion

Self-healing or automated service restoration of the power grids is one of the important functionalities of resilient smart grids. With increasing frequency of occurrence of natural disasters and targeted cyber-physical attacks on the power grids, the automated service restoration becomes a vital functionality of the electrical energy infrastructure. Furthermore, with higher dependence on the Information and Communication Technology (ICT) infrastructure for the operation of the power grid, the automatic service restoration becomes a complex problem as the ICT infrastructure might also fail due to power network failures thus jeopardizing the automatic service restoration procedure. Therefore, in addition to the aforementioned algorithm for emergency service restoration, mechanisms should also be included to optimally restore the grid considering the availability of ICT infrastructure. The proposed methodology enables to restore the grid considering the criticality of the load and the preferences of the network operator for single and multiple faults. However, it should also be extended to also optimize the life of each switch or circuit breaker thus making sure that switches and breakers are not stressed by extremely high number of switching made during the restoration process over a period of time.

14.5 Conclusion of the Chapter

In the first part of this chapter, we have shown that applying by-design measures, the resilience of CEI can be increased. Utilizing additional redundancies and enabling the physical and communication and control networks to autonomously adapt in case of incidents enables the infrastructure to self-heal and to either minimize the impact or recover from it. While applying by-design measures individually can already improve the service level, combining different by-design measures (including different domains as power, communication and control) provides synergies since this approach recognizes the interdependencies between different domains of CEI.

Double Virtualization has been introduced as by-design measure to avoid single points of failure in the functional layer of grid monitoring and control, represented by centralized monitoring and control functionalities that are dependent on a specific device. Virtualizing these functionalities enables utilization of redundancies provided by the availability of various devices in the infrastructure that are able to host respective functionalities. DV has been applied to Fault Detection Algorithm as example use case to showcase the principle. Restrictions and recommendation for applying DV as well as the potential for future improvements of the principle have been given in the conclusions.

Service Restoration has been introduced as by-design measure to reconfigure the electrical grid after occurrence of one or multiple faults. It has been described how a multi-criteria approach can be implemented with the help of MCDM and TOPSIS, enabling distribution system operators to configure the reconfiguration strategy based on predefined priorities assigned to a set of criteria as restoration of power supply to critical loads as well as complying to voltage limitations of the grid. The principle has been demonstrated based on test cases covering faults in test grid that represents a part of a distribution system. Based on relevant criteria, the priorities for restoring the grid after faults can be refined and a suitable reconfiguration strategy can be derived.

Although the comparison of cascading effects in a test system indicates that resilience can be increased by applying by-design measures as DV and SR, requirements of a specific CEI must be considered before implementing the proposed or other by-design measures. Applicability of DV, for example, might depend on requirements of the functionality, which is to be virtualized. Applicability of SR might depend on the capability of the electrical equipment to perform flexible reconfiguration as well as regulatory constraints for system operation.

References

[1] M. Panteli and P. Mancarella. The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. IEEE Power and Energy Magazine, 13(3):58–66.

[2] C. Liu, S.J. Lee, and S.S. Venkata. An expert system operational aid for restoration and loss reduction of distribution systems. IEEE Transactions on Power Systems, 3(2):619–626, May 1988.

[3] C.-S. Chen, C.-H. Lin, and H.-Y. Tsai. A rule-based expert system with colored petri net models for distribution system service restoration. IEEE Transactions on Power Systems, 17(4):1073–1080, Nov. 2002.

[4] T. Ananthapadmanabha, A.D. Kulakarni, A.S.G. Rao, J.G. Char, K.R. Rao, and K. Parthasarathy. Knowledge-based methodology for intelligent sequence switching, fault identification and service restoration of distribution system. International Journal of Electrical Power & Energy Systems, 19(2):119–124, 1997.

[5] Y. Kumar, B. Das, and J. Sharma. Multiobjective, multiconstraint service restoration of electric power distribution system with priority customers. IEEE Transactions on Power Delivery, 23(1):261–270, Jan. 2008.

[6] R. Srinivasa Rao, S. V. L. Narasimham, M. Ramalinga Raju, and A. Srinivasa Rao. Optimal network reconfiguration of large-scale distribution system using harmony search algorithm. IEEE Transactions on Power Systems, 26(3):1080–1088, Aug. 2011.

[7] D.S. Sanches, J.B.A. London, A.C.B. Delbem, R.S. Prado, F.G. Guimaraes, O.M. Neto, and T.W. de Lima. Multiobjective evolutionary algorithm with a discrete differential mutation operator developed for service restoration in distribution systems. International Journal of Electrical Power & Energy Systems, 62:700–711, 2014.

[8] S. K. Goswami and S. K. Basu. A new algorithm for the reconfiguration of distribution feeders for loss minimization. IEEE Transactions on Power Delivery, 7(3):1484–1491, July 1992.

[9] S. Dimitrijevic and N. Rajakovic. Service restoration of distribution networks considering switching operation costs and actual status of the switching equipment. IEEE Transactions on Smart Grid, 6(3):1227–1232, May 2015.

[10] M. Gholami, J. Moshtagh, and L. Rashidi. Service restoration for unbalanced distribution networks using a combination two heuristic methods. International Journal of Electrical Power & Energy Systems, 67:222–229, 2015.

[11] M. E. Baran and F. F. Wu. Network reconfiguration in distribution systems for loss reduction and load balancing. IEEE Transactions on Power Delivery, 4(2):1401–1407, April 1989.

[12] C. Lee, C. Liu, S. Mehrotra, and Z. Bie. Robust distribution network reconfiguration. IEEE Transactions on Smart Grid, 6(2):836–842, March 2015.

[13] B. Chen, C. Chen, J. Wang, and K. L. Butler-Purry. Sequential service restoration for unbalanced distribution systems and microgrids. IEEE Transactions on Power Systems, 33(2):1507–1520, March 2018.

[14] T.T. Borges, S. Carneiro, P.A.N. Garcia, and J.L.R. Pereira. A new opf based distribution system restoration method. International Journal of Electrical Power & Energy Systems, 80:297–305, 2016.

[15] N.R.M. Fontenele, L.S. Melo, R.P.S. Leao, and R.F. Sampaio. Application of multi-objective evolutionary algorithms in automatic restoration of radial power distribution systems. In 2016 IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS), pages 33–40, May 2016.

[16] A. Kumar, B. Sah, A. R. Singh, Y. Deng, X. He, P. Kumar, and R.C. Bansal. A review of multi criteria decision making (MCDM) towards sustainable renewable energy development, Renewable and Sustainable Energy Reviews, vol. 69, 2017.

[17] R. R. Yager, "Modeling prioritized multicriteria decision making," in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 34, no. 6, pp. 2396–2404, Dec. 2004.

[18] P. Espie, G. W. Ault, G. M. Burt and J. R. McDonald, “Multiple criteria decision making techniques applied to electricity distribution system planning,” in IEE Proceedings – Generation, Transmission and Distribution, vol. 150, no. 5, pp. 527–535, 15 Sept. 2003.

[19] A. Angioni, A. Kulmala, D.D. Giustina, M. Mirz, A. Mutanen, A. Dede’, F. Ponci, L. Shengye, G. Massa, A. Repo S. Monti, (2017, April). Design and implementation of a substation automation unit. IEEE Transactions on Power Delivery, vol. 32, no. 2, pp. 1133–1142.

[20] N. R. M. Fontenele, L. S. Melo, R. P. S. Leao, and R. F. Sampaio. Application of multi-objective evolutionary algorithms in automatic restoration of radial power distribution systems. In 2016 IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS), pages 33–40, May 2016.

[21] A. Dognini and A. Sadu. Networkdata_MV_FLISR_use_case.pdf. https://www.fein-aachen.org/en/projects/rbosr/ accessed on 11th September 2019.

[22] A. Jaiswal and R. B. Mishra. “Cloud Service Selection Using TOPSIS and Fuzzy TOPSIS with AHP and ANP.” In: Proceedings of the 2017 International Conference on Machine Learning and Soft Computing. ICMLSC ’17. Ho Chi Minh City, Vietnam: ACM, 2017, pp. 136–142. isbn: 978-1-4503-4828-7. doi: 10.1145/3036290.3036312. url: http://doi.acm.org/10.1145/3036290.3036312.

[23] G.H. Tzeng and J.J. Huang. *Multiple Attribute Decision Making: Methods and Applications*. A Chapman & Hall book. Taylor & Francis.

[24] Q. Zhu and T. Başar, “Robust and resilient control design for cyber-physical systems with an application to power systems,” in 2011 50th IEEE Conference on Decision and Control and European Control Conference, 2011, pp. 4066–4071.

[25] A. Rocha *et al.*, “An agent based framework to support plug and produce,” in 2014 12th IEEE International Conference on Industrial Informatics (INDIN), 2014, pp. 504–510.

[26] G. Di Orio, A. Rocha, L. Ribeiro, and J. Barata, “The PRIME Semantic Language: Plug and Produce in Standard- based Manufacturing Production Systems,” presented at The International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2015), Wolverhampton, UK, 23–26 June 2015, 2015.

[27] J. Soldatos, S. Gusmeroli, P. Malo, and G. Di Orio, “Internet of Things Applications in Future Manufacturing,” in *Digitising Industry – Internet of Things Connecting the Physical, Digital and Virtual Worlds*, River Publishers, 2016.

[28] G. D. Orio, P. Maló, J. Barata, M. Albano, and L. L. Ferreira, "Towards a Framework for Interoperable and Interconnected CPS-populated Systems for Proactive Maintenance," in 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), 2018, pp. 146–151.

[29] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment," *J. Adv. Res.*, vol. 5, no. 4, pp. 481–489, Jul. 2014.

[30] S. Majumder, A. Mathur, and A. Y. Javaid, "Cyber-Physical System Security Controls: A Review," in Cyber-Physical Systems: Architecture, Security and Application, S. Guo and D. Zeng, Eds. Cham: Springer International Publishing, 2019, pp. 187–240.

[31] G. Brito, G. Di Orio, and J. Barata, "Orchestrating loosely coupled and distributed components for product/process servitization," presented at the 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), 2017, pp. 1199–1204.

[32] J. R. Boyd, "The essence of winning and losing," *Unpubl. Lect. Notes*, vol. 12, no. 23, pp. 123–125, 1996.

[33] A. Zidan *et al.*, "Fault Detection, Isolation, and Service Restoration in Distribution Systems: State-of-the-Art and Future Trends," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2170–2185, Sept. 2017.

[34] S. Barman and B. K. S. Roy, "Detection and location of faults in large transmission networks using minimum number of phasor measurement units," in IET Generation, Transmission & Distribution, vol. 12, no. 8, pp. 1941–1950, 30 4 2018.

[35] M. A. Ebrahim, F. Wadie and M. A. Abd-Allah, "Integrated fault detection algorithm for transmission, distribution, and microgrid networks," in IET Energy Systems Integration, vol. 1, no. 2, pp. 104–113, 6 2019.

[36] James Northcote-Green and Robert Wilson. *Control and Automation of Electrical Power Distribution Systems*. CRC Press, 2007.

[37] A. Abur and A.G. Exposito. *Power System State Estimation: Theory and Implementation*. CRC Press, March 2004.

[38] R.F. Stengel. *Optimal Control and Estimation*. Dover Books on Mathematics. Dover Publications, 2012.

[39] EN 50160:2010. Voltage characteristics of electricity supplied by public electricity networks. Standard, CENELEC, July 2010.

[40] S. Waldbusser, C. Kalbfleisch, D. Romascanu, "Introduction to the Remote Monitoring (RMON) Family of MIB Modules," Network Working Group, Standard, https://tools.ietf.org/html/rfc3577

[41] van Steen, Maarten: Graph theory and complex networks. An introduction. 2010.