

INTERDEPENDENCIES BETWEEN AN ELECTRIC POWER INFRASTRUCTURE WITH DISTRIBUTED CONTROL, AND THE UNDERLYING ICT INFRASTRUCTURE

Tom Rigole, Koen Vanthournout, Geert Deconinck

Electrical Engineering Department, K.U.Leuven¹

Keywords: Infrastructure Interdependencies, Agents, Modeling and Simulation, Distributed Generation, Autonomous Electricity Networks

Abstract

The electric power grid is evolving from a centrally controlled grid with only a handful of regulated monopolies to an open liberalized electricity market. Also, more and more small scale dispersed generators are being deployed in the distribution net. This puts extra stress on the power grid in an era where electricity is one of the most important commodities for economical, industrial and everyday activities. Therefore new control strategies are being proposed to maintain the desired degree of availability. These control strategies are often based on ICT infrastructures, rendering new or amplifying old dependencies. The possible impact of these interdependencies on dependability of the power system should be thoroughly investigated. In this paper, we first give a quick overview of a possible design to cope with these changes and present a scheme for distributed control of dispersed generators in a power distribution net. Based on a thorough investigation of this scheme, we try to underline the importance of understanding the interdependencies between the power grid and the ICT infrastructure controlling it.

1 Introduction

Recent years, the electrical power grid has changed dramatically ([1],[2]). Due to the deregulation of the grid it has evolved from a vertically integrated grid with only a handful of regulated monopolies to a liberalized open market with various competing market players. However, these changes put extra stress on the grid. First of all, trading power between areas with different power costs has lead to an increasing amount of power transfers over the grid. Also, control and supervision of the grid has become more difficult due to the new structure of generation, transmission and distribution of electrical power. Whereas these instances used to be vertically integrated and monopolistic, nowadays these are composed of various distinct, competing instances. Privacy constraints and a more complex structure have complicated the information flow between various parties controlling the grid.

Furthermore, the total power demand is gradually increasing, while the capacity of the power infrastructure has grown only at a much slower rate. Next to budgetary reasons, this is mainly because of regulatory and environmental impediments.

There is also an increasing trend to deploy small scale dispersed generators in the distribution net, also referred to as *Distributed Generation* (DG) (an overview is given in [1]). This radically changes the traditional transmission topology, where we have large power plants generating electricity, which is transported over the high voltage transmission grid to local substations. These substations connect the high voltage grid to the radial low voltage

¹ Katholieke Universiteit Leuven (Catholic University of Leuven)
ESAT/ELECTA, Kasteelpark Arenberg 10, 3001 Heverlee, Belgium. Tom.Rigole@esat.kuleuven.be

distribution net. Within such a local distribution net, power is supplied by a single substation (and mostly one backup substation) that connects it to the transmission grid.

There are several reasons for the deployment of distributed generators in low voltage nets; Power generation can be brought closer to consumption, reducing transmission losses. A significant amount of distributed generation in a low voltage distribution net can lower its (peak) demand, reducing the load on the transmission net supplying it. Also, DG allows for participation in the power market without the tremendous initial investment costs of a traditional large facility. Finally, many generators using renewable energy sources, such as wind or solar energy, are typically deployed as small dispersed generators in the distribution grid.

All these changes and evolutions put extra stress on the power grid in an era where electricity is one of the most important commodities for economical, industrial and everyday activities. Therefore new control strategies are being proposed to maintain the desired degree of dependability ([10],[3],[4]). These control strategies are often based on new ICT technologies, such as cheap open networks (e.g. the *Internet*), wireless networking, low cost small Intelligent Electronic Devices (IED), etc. Also the use of standard off-the-shelf components (hardware/software/communication) may increase flexibility and efficiency in building the control architectures. But next to providing a tremendous amount of new possibilities, these technologies can introduce new vulnerabilities in the system. In communication networks security issues might be of concern, especially in open and wireless networks. Commercial Off-The-Shelf components may reduce the level of control of the designer over the system, blinding him for certain vulnerabilities. Internet platforms for trading power or transmission capacity are a potential target for hackers. Also, the ICT infrastructures controlling the power grid may depend on the power provided by the very grid they control. Such vulnerabilities can render new or amplify old dependencies and interdependencies. The possible impact of these interdependencies on dependability of the power system should be thoroughly investigated.

The remainder of this paper is structured as follows. In the second section, we describe how traditional control systems for the power grid are built. The third section discusses how a general agent based control approach can boost the robustness of the grid. Section four presents a design and implementation of such an agent based approach controlling distributed generators in an autonomous electricity network. The fifth section discusses how the interconnection of infrastructures such as the power grid and communication networks may lead to new vulnerabilities and interdependencies; typical faults and problems are presented, and possible remedies are proposed. Finally, some risk assessment methods, using modelling and simulation, are discussed.

2 Traditional Control Systems

Current control systems for the power grid are designed to meet the demands of the traditional grid, and are based on two layers of control: local protection and control systems, and a centralized hierarchical control system.

Local protection systems are fast acting systems without any global knowledge of their environment, typically used to break circuits in case of short-circuits in transmission lines, such as circuit breakers and reclosers. The protection offered by these systems thus consists of the isolation of a faulted grid segment from the rest of grid. These systems have no need for communications to perform their primary task, though it is useful for grid operators and supervisory systems to know what circuit breakers and reclosers are activated, so they can take corrective actions. Protective systems are a critical part of the grid, since a malfunction may lead to unnecessary high load on certain power lines, and grid sections blacking out.

Another type of local control is the *droop control* used in large centralized generation facilities. Droop control, also called *primary control*, is used to balance both active and

reactive power, based on *frequency* measured locally. This kind of control has no need for communications.

Central control systems (Supervisory Control And Data Acquisition) are mainly built upon the traditional vertically integrated transmission system. The underlying communication infrastructure does not provide any information flow other than to the central control centres, which manage the huge amount of data received from various grid entities. The burden of inferring corrective measures or generating control data within certain time bounds is imposed on this relatively small number of control stations.

SCADA systems rely upon communications for various tasks; for example the control of generators to maintain rated frequency and scheduled power flows (*secondary control*), or to optimize generation for economic criteria (*tertiary control*). Some other examples are: remote control of sectionalizing switches or transformer tap settings, remote load shedding, data gathering on system states and device parameters, etc. Communication requirements (*quality of service*) for all these control signals are different, some critical signals have to be delivered within a bounded time (*real time constraints*, e.g. for controlling sectionalizing switches), while other signals may be omitted without bringing the system at risk (e.g. for economic optimization).

As mentioned before, the increasing use of distributed generation radically changes the traditional hierarchical generation and transmission topology (see [1] for an extensive overview). This shift also imposes a change in the control infrastructures of the distribution net. The amount of small scale generators explodes almost exponentially, where in the traditional system only a limited number of power plants and substations had to be accounted for. Central control becomes infeasible in this scenario, due to the enormous processing and high communication bandwidth requirements for the vast amount of components.

Most DGs nowadays are installed and controlled locally as passive elements, merely providing power to the net; when the strong grid they are connected to fails, or large voltage dips occur, these devices just disconnect themselves from the grid. However, DG could provide services to improve system service quality, reliability and security. Extra functionality and flexibility in their control could make them able to function without a connection to a strong grid providing voltage and frequency stability, or let them ride through short voltage dips. Also, using power electronic equipment, most distributed generators can be used as VAR compensators for local voltage support.

3 Agents Controlling the Grid

The evolutions in the electricity grid have convinced us to design an intelligent, distributed control scheme ([2],[10]). In this scheme distributed generators and control equipment, such as circuit breakers, are equipped with an autonomous control entity or *agent*, implemented on some kind of Intelligent Electronic Device. Such a control entity can supervise the component at hand, fetching state parameters of the component from various sensors. The agent interprets these parameters and aggregates this into a higher level conclusion on the current state of the component. This avoids the need to send many low-level parameters of the component over communication channels, reducing communication network loads. Agents within a low voltage distribution net set up a virtual communication network (*overlay network*, often referred to as peer-to-peer network) that connects the agents in that low voltage segment. In this way agents can exchange important state information, so an agent is not only aware of the state of its own component, but also has a notion of the global environment in which it is operating. From this environmental knowledge an agent can deduce the best action to be taken to deal with sudden changes or failures in the local distribution net. Networks used for communication may comprise open networks, such as the Internet, or dedicated communication lines, or a combination of these.

Besides allowing for distributed control, this scheme fits well in the intrinsic hierarchical topology of the electricity grid by the so called '*holistic approach*' ([5]). One level up from

the local distribution net we find the medium voltage grid. On this level every single low voltage net can be represented as a super-agent that aggregates all agents in that distribution net. This way, a different agent society can be built at every level of the grid, or those super-agents could interact with the traditional central control facility.

This approach allows for fast reaction speed compared to the traditional central control (as claimed in [2]), since failure mitigation and optimization actions are executed locally. Also, the intelligent agents have detailed knowledge about the state of the component and its environment, where a central control system can only estimate that state and act upon that estimation due to bandwidth limitations.

[19] even claims critical infrastructures will remain vulnerable to a variety of attacks, unless neighbourhoods are able to fend for themselves. So local critical infrastructures, and their underlying control infrastructures, have to become self-controlling and self-healing. They reason no infrastructure can be build with enough security and redundancy (control centers, communication lines, power lines, etc.) to survive the impact of coordinated terrorist attacks, warfare, hurricanes, earthquakes, etc. as a whole. Eliminating typical weaknesses in hierarchical control infrastructures (central control stations form single points of failure) by use of distributed control with autonomous agents could give a tremendous boost to the infrastructure's robustness. Distributed generation can also reduce the dependence of a low voltage grid segment on the transmission grid and central generation facilities.

Various applications of agent based control schemes for the grid (also referred to as '*smart grid*') have been proposed in literature. Here we give a short overview of some noteworthy examples.

- Intelligent circuit breakers ([20]): According to [21] malfunctioning or wrongful switching of protection systems are at the basis of 63% of all major system disturbances. Therefore a scheme was presented to control these circuit breakers by intelligent agents, using fuzzy logic and communication with other agents to decide the best action when a near short circuit current is observed.
- Agents in electronic markets: Multi-agent technology can be used for real-time online power markets. Agents buy and/or sell power trying to minimize the costs and/or maximizing income while meeting the demand of their master (e.g. generation facility, factory, household, etc.).
- Supply-demand matching ([22]): Intelligent forecasting of demand and generation (e.g. for solar cells or wind turbines) and matching these by adjusting generator output or intelligent loads, may reduce regulating needs and costs.
- Intelligent load shedding: Intelligent loads may be switched off when network load is high, according to some priorities. Heating or air conditioning may be switched off temporary without anyone noticing, while hospitals or traffic signals may only be shed when there are no other options.
- Autonomous Electricity Network (AEN) ([10],[13]): An AEN is low voltage net with a decent amount of DG installed, that is self-regulating and possibly able to continue operating, if necessary in a degraded way, when it is disconnected from the grid. In the next section we will discuss our design and its implementation for a distributed control scheme for such an AEN.

4 An Autonomous Electricity Network: Design and Implementation

In this section a distributed, agent based control scheme of DG in a low voltage net will be presented. Such a control scheme should be able to boost DG solutions to their full potential. Recapitulating the definition of an agent as "*An autonomous system (software and/or hardware), that is situated in an environment (possibly containing other agents) and acts on it, based on inputs from that environment or from other agents, in order to pursue its own goals, and is often able to learn from previous experiences.*", we recognize following components in our AEN:

- Agent: Entity controlling the active and reactive power output of a distributed generator in order to pursue grid stability, high power quality and economic optimization.
- Environnement: Low voltage distribution net.
- Inputs from environment: Local measurements of frequency and voltage level.
- Inputs from other agents: Communication over a (possibly open) network between agents exchanging state information.

In the description of this control scheme, we will first describe the communication among agents and then how power output is controlled by the agents based on local measurements and global knowledge of the LV segment ([3],[4],[13]).

4.1 Agent Communication

An important factor for the successful deployment of DG is the cost, so the underlying communication infrastructure should be as inexpensive as possible. Nowadays, open packet switched networks, such as the Internet, are widely available and cheap (compared to dedicated links). That is why our communication scheme is constructed in such a way it can deal with this dynamic, unreliable environment with limited bandwidth and unbounded latency.

Agents in a power distribution net set up an *overlay network* (or *virtual network*) on an underlying network, forming *peer-to-peer* (P2P) connections between agents (comparable to systems such as Gnutella or Napster²) ([11],[12]). This is done in a fully distributed way; no server listing of its members is needed. An agent joining the overlay network must know only one current member, which it will contact. This member will pass on other members with whom the new agent can form a limited number of peer-to-peer connections. The choice of which members to connect to is based on a semantic distance metric, based on descriptive XML files of the agents. An agent will tend to connect to similar agents. Additionally some connections will be made to agents with a much larger semantic distance, as to avoid the P2P network splitting up in clusters of similar agents and to limit its diameter (maximal number of hops to go from one agent to another). Finally, to improve robustness of the overlay network, an agent keeps a list of former neighbours, which can be used as access points after the agent has been disconnected from the network. This overlay network forms an ideal structure for communication over unreliable packet switched networks; agents can join, leave and re-enter at will, there is no need for central coordination and scalability is high. An example of such an overlay network connecting generators in an electricity distribution net is shown in Figure 1.

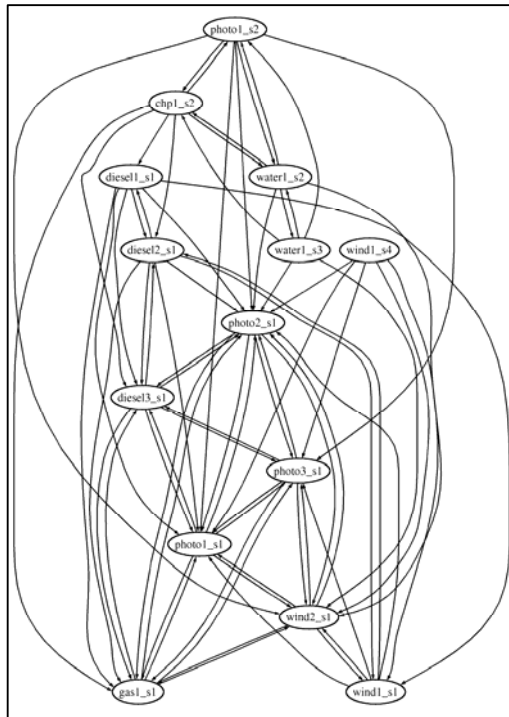


Figure 1: example of an overlay network formed in a power distribution net containing various generators (diesel engines, photovoltaic cells, wind turbines...)

² The Napster peer-to-peer network is not constructed in a distributed way; central servers are needed listing possible members and keeping databases of their shared files.

For the exchange of information over such an overlay network, there are multiple options. Flooding³ or multicasting⁴ of messages could be used. The former has quite high network demands, while the latter is not supported over the Internet. The method we use here is called *gossiping*; every agent exchanges information at fixed time intervals with one of his neighbours (chosen randomly). If that neighbour exchanges this new information with one of his neighbours (and so forth...), the news spreads in the network. This also explains its name; the way information is spread is very similar to how gossips are spread in a society from person to person.

4.2 Controlling Power Output

We will briefly comment on the various levels of control for both active and passive power output by generators in our AEN. Three levels of control (primary, secondary and tertiary), which are also used for controlling power output of generators in high voltage transmission grids, have been adapted for use in a distribution net communicating over unreliable communication networks.

Primary control regulates active and reactive power outputs based on local measurement of frequency and voltage, using droop curves as shown in Figure 2. For a thorough discussion on how droop control is adapted to function in a resistive distribution net, instead of an inductive high voltage grid, see [13]. Primary control doesn't maintain rated frequency and voltage, but it balances power without communication needs.

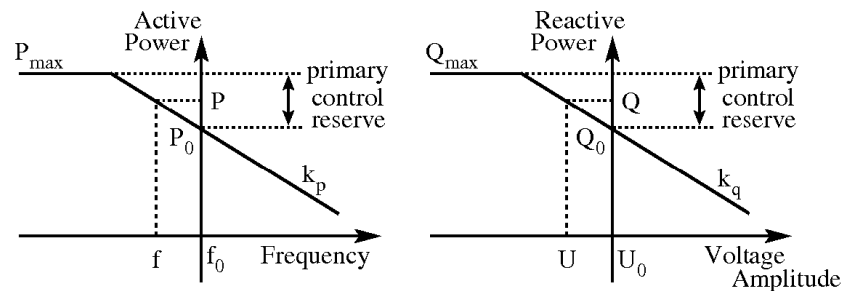


Figure 2: Droop control curves; active and reactive power output of a generator are regulated by measurement of respectively frequency and voltage levels (situation for an inductive grid).

Secondary control is mainly responsible for maintaining rated system frequency and scheduled power transfers. Tertiary control optimizes generator output for economic criteria. Secondary and tertiary control both require some form of coordination, traditionally performed by a central control entity communicating with generator controllers. For secondary control the frequency and power flows on tie-lines of the controlled section are sent to the central controller. This controller calculates new settings for the droop control of generators in his section as to bring frequency and power transfers to their rated values. For tertiary control, the central controller has an aggregation of the *marginal cost* (MC) curves of all generators in the system. Based on these curves, settings for all generators are calculated to minimize costs, and dispatched to the generators in the field.

In our control scheme however, both secondary and tertiary control are performed in a distributed way ([10]). Agents controlling generators communicate only with their direct neighbours, exchanging their marginal cost curves. Next, the two gossiping generators will adjust their power output as to make their MCs equal, while total power production remains constant. Continuing this gossiping process will ultimately lead to the point where all

³ Every new message received by an agent is forwarded to all its neighbours, except to the neighbour from which it received it.

⁴ Method to send a single IP-package to a group of receivers, this routing method can however only be used over LANs since not all routers in the Internet support multicast-routing.

generators in the distribution net produce power at the same marginal costs. A similar gossiping process can be used for secondary control.

5 Faults, Problems and Possible Solutions

The agent based control systems described in this paper all have one thing in common: their control algorithms for the power grid rely on an underlying ICT infrastructure. Moreover, the ICT infrastructure itself relies on the very power grid it controls. These facts show there might be important interdependencies between the two infrastructures that might lead to catastrophic failures if these are not taken into account when designing and building control systems.

Next, we describe some typical faults and problems occurring in, on the one hand power grids, and on the other hand ICT infrastructures. We will have a look at how our autonomous electricity network deals with these faults, or what could be done to mitigate possible consequences. In designing strategies to mitigate consequences of faults or remedy the vulnerability responsible for that fault, the *risk*⁵ introduced by that vulnerability has to be carefully weighted against the cost for the remedy.

5.1 Problems and faults in power grids

5.1.1 Power Quality

Power Quality (PQ) covers a broad range of power issues; voltage profile dips, voltage swells and harmonic distortion are some of the most important ones. Voltage dips are mostly caused by short circuits or high loads, such as electrical motors or electrical heating, switching on. Voltage swells (though less common) are caused by high loads switching off. Harmonic distortion is pollution of the 50Hz electrical signal by high frequencies, mostly caused by electronic devices.

In our AEN, because of the close distance of fast reacting distributed generators to the loads, the impact of voltage dips can be decreased. Also, because of the secondary control mechanism, the voltage will at all times be kept as close as possible to its nominal value at every point in the distribution net.

The agent population dispersed over the distribution net can monitor PQ in the net. This information could be used to identify loads responsible for deterioration of the power quality or pinpoint locations where actions should be taken to improve PQ.

5.1.2 Grid Disconnection

The distribution net may be disconnected from the transmission grid by various causes. The most likely cause might be the outage of multiple transmission lines (e.g. weather conditions might cause such simultaneous failures), cutting off a segment of the grid from any power supply.

Our system has been build to be able to form an energy island or microgrid, operating within nominal ranges and balancing power when it has been disconnected from the grid. Since we are using open networks, there might be a chance that these communications fail due to the same reasons that caused the islanding of the grid section. Therefore our AEN can function without any kind of communication, although frequency and voltage profiles might not remain at their nominal values, and no economical optimisation will occur.

5.1.3 High Peak Demands

Power demand is in no way a constant, it is changing continuously with high peak demands. These demands determine the power line, transformer and generation capacities, and thus the

⁵ Risk could be measured as: (probability of occurrence of fault) * (cost of the consequences). Cost may be interpreted as 'severity', such as damage inflicted on a companies reputation or loss of human life, more than a purely economical term.

infrastructural cost. Lowering these peaks would have both economic and ecologic advantages.

In our system we try to optimize costs using marginal cost curves. If the transformer connecting the distribution net to the grid also has a marginal cost curve, then its cost can be set high when the lines feeding the transformer are highly loaded. This would have as a result that local distributed generators increase their power outputs, and thus lowering peak demands as seen from the viewpoint of the transmission grid. This is a typical example of how collaboration in a multi agent system, with agents pursuing their own, simple objectives (minimising cost), leads to high level emergent behaviour (lowering peak demand).

5.2 Faults and Problems in an ICT Infrastructure

5.2.1 Delays in Open, Packet-Switched Networks

A packet switched network, such as the Internet, typically only has a best effort to deliver packets. Communication latency can't be predicted and packages can be lost. Luckily transport layer protocols such as TCP can abstract this low level handling of jitter, latencies and packet losses; nevertheless, real time behaviour can never be guaranteed. This has as a consequence that this kind of network may not be used for time critical control data.

Our AEN has been constructed in a way that no communication of critical control data is needed; communication is only used for optimization, so latencies in the network can only influence the time it takes to converge to an optimal working point of the generators. Deviations in power quality and non-optimal economic behaviour could be weighted against the cost of a dedicated communication network with guaranteed bandwidth and predictable timing behaviour.

Though, it is not unthinkable that some agent based control applications might require real time behaviour, and thus a certain level of *Quality of Service* (QoS), while still desiring the flexibility, low cost and general accessibility of a public network. It might be worth mentioning that many methods have been described in literature to guarantee a certain level of QoS over a packet switched network. This is mainly because of the growing use of streaming media over the Internet. One type of proposed methods is based on priority queuing of packets in routers, and bandwidth reservation per priority category (see RFC⁶ 2474, 2475, 2597, 3246, and others); standard IP packets (IPv4) even have an 8-bit *type of service* header entry indicating a priority level, although this entry is not used by routers on the Internet. Another type of QoS implementation over the Internet is described in RFC 2205-2210 (and some others); the most important protocol of this kind is the *Resource reSerVation Protocol* (RSVP). RVSP is used to reserve resources for a certain stream of packages from sender to receiver (a 'channel' is created). Due to this reservation of resources, congestion is eliminated and the QoS level can be guaranteed. Notice this protocol behaves more like a circuit based (like ATM networks) than a packet switched network.

5.2.2 Reliability of Open Networks

Also, the internal structure of an open communication network and its dependency on the power grid is not known to the designers of the control system. Therefore it is very hard to determine its reliability and availability. There is a big chance that such communication infrastructures go (partially) down the very moment the power grid is in a critical state (e.g. partial blackout), so control systems using public networks will have to function in absence of these communications.

The overlay network constructed by the agents in our AEN has some intrinsic fault tolerance, which deals with the dynamically changing topology of the underlying network to avoid overlay network partitioning and enables re-entering of nodes after disconnection from the network.

⁶ Request For Comments; documents proposing and/or describing algorithms used over the Internet. See: <http://www.ietf.org/rfc.html>

If a distributed control application would be designed requiring high reliability and availability of communication channels, while still preferring a cheap open network, backup channels have to be provided. A second ISP, a dial-in modem or a cellular phone (GPRS, UMTS) are some possible options for relatively cheap backup connectivity.

5.2.3 Reliability of Components off the Shelf (e.g. desktop computers)

Use of standard components in control applications may lead to unexpected behaviour of the application, because the designer of the application has only limited knowledge of the exact design of these components; he merely sees it as a black box that in most of the cases performs its expected functions. In our AEN for example, general purpose desktop computers running on Linux are used; these computers might be a source of unexpected failures and behaviour of the overall application. Intrusions by viruses, worms and Trojans are not unlikely, especially when the computer is connected to the Internet. Also, general purpose Operating Systems (OS) tend to crash, maybe not so often (depending on the OS) but it has to be accounted for. Crashes are especially likely to happen when computers are used for other applications next to the control application. Distributed control systems have the pleasant property of not having single points of failures in their design, therefore infrequent and isolated failures of nodes due to crashes or viruses don't pose a big threat to the system. However, one must be aware of the possibility of common cause failures in these systems. A worm might for example lead to a common cause failure for the majority of controlling computers, leading to a system wide failure. Next to standard defences such as firewalls and virus detectors, diversity in hardware and software can make the system more resilient against these types of system wide failures.

5.2.4 Security issues in ICT infrastructures

When using open networks for communication of control data, security becomes a serious issue. People may try to hack into these systems for various reasons: inflicting damage (e.g. terrorists, warfare), personal profit (e.g. in real time markets), revenge (e.g. on a company after being fired), or just for fun. There are many different kinds of security breaches, some of which are described next.

Confidentiality: Sending data over an open network makes it vulnerable to eavesdropping. In control applications such a passive attack may not seem harmful, and in most cases isn't. But one must be careful that leakage of some control commands, state information or for trade orders in a real time market can't be abused for pinpointing weak spots in the systems, making profit in an illegal way or simply endangering the privacy of certain companies or individuals. An effective defence against this kind of attack may be done through encryption of sensitive data using standard cryptographic protocols (DES, AES, RSA).

Denial of Service: A more active, though relatively simple attack is a denial of service attack. Despite its simplicity to conduct, it is very hard to defend against. Someone might find a way to overload the network with useless data packets, occupying all available bandwidth so no control data can be sent. Also, servers may be constantly bombarded with fake requests, denying them of performing their designated tasks.

Integrity: Imagine if someone was able to alter control messages that are sent over the communication network. Modifying control signals could possibly knock down the whole system, or impostors could change pricing information in a real time market for personal profit. Several algorithms exist to enforce integrity of messages, and should be implemented if necessary.

Authentication: The same arguments as for data integrity can be made for authentication. Imagine an attacker could masquerade himself as a power generator forging false state signals, or as a system operator sending false control signals. Again, appropriate authentication protocols should be implemented where needed. Public key certificates could prove a person's or a company's identity; though there is still the question of which person or company is to be trusted. The most obvious way is letting central instances, such as

governmental institutions or independent system operators, hand out and revoke licences. Other models, such as distributed trust models, seem to fit more in our distributed agent based approach; though these have disadvantages of their own.

Insider Threat: A very difficult problem to tackle in security is the insider threat, people that have rightful access to a system, but use it for illegal purposes. The best way to mitigate such problems is limiting access rights of people as much as possible. Logging the actions of people can be useful both for detecting such abuses and as evidence for suing the offender afterwards. This approach can be used for individual systems, though in a distributed control environment things are quite different. Here, a central controller could monitor agents in the system, or a distributed approach could be implemented where agents monitor each others actions. The latter could go hand in hand with a distributed trust model (cfr. supra).

Physical Security of Control Systems: An aspect of security of ICT systems that is mostly underestimated is the physical security of the system. Once a malicious person has physical access to a computer system, most security measures fail. A typical example is that of company with firewalls, intrusion detection systems, VPNs, etc. installed to protect their confidential files, but no questions are asked when a repair guy walks out carrying a computer. Although this is more a social and organisational problem than an IT related one, it is surely worth mentioning.

6 Assessing Risk of Interdependencies: modelling and simulation

When trying to assess the risk involved with certain vulnerabilities and dependencies, there are two aspects of risk that have to be determined:

1. *Probability* of a certain failure of happening (caused by faults, made possible by some vulnerabilities).
2. *Impact* of that failure: can be measured in terms of availability of the system, power quality, economical cost, ecological impact, impact on a company's reputation, etc., or some combination of these.

Then risk is determined as the multiplication of this probability by the impact.

In this section we will discuss some methods for assessing the risk of vulnerabilities in such dynamic and adaptive interconnected systems. These might also be used for testing new control paradigms or discovering new vulnerabilities.

6.1 Reliability Engineering Approach

In reliability engineering some great methods exist to assess the reliability of complex systems composed of many interdependent parts. Typical examples of these are fault trees, reliability block diagrams, Petri-nets or Markov chains. These methods are used in fields requiring high reliability such as PCB design, medical equipment, aeronautics or nuclear plants. Though, these methods are quite procedural and it is hard to describe dynamic and adaptive behaviour of multi agent systems with these. Therefore, though maybe useful to model low level behaviour of underlying equipment (failure probabilities of DSPs, inverters, generators, communication lines, routers, etc...) or even agent behaviour (agent state transitions modelled with Petri-nets or Markov chains), other methods are needed to describe the behaviour on system wide levels.

6.2 Multi Agent Based Modelling and Simulation

Recent years, the multi agent based paradigm has also spread to the world of modelling and simulation of complex systems, in the form of *Multi Agent Simulators* (MAS) ([6],[7],[8],[16],[17],[18]). Mostly, such simulations have been performed in biosciences, to study the behaviour of ant colonies, swarms of bees, schools of fish, etc. Economics research, for example influences of certain incentives on behaviour of market players, is also a typical field for MAS. It has been proposed to use MAS for simulation of complex adaptive interconnected infrastructures ([7],[8],[14],[15]). Different complicated components of the infrastructures can be broken up in more simple parts, which can be modelled by an agent with

presents its typical behaviour. This behaviour can be modelled using typical reliability engineering techniques or some logic; the complexity of this low level behaviour can of course be tuned to the needs of the simulation at hand. It is also nice to see how easily an adaptive agent in a distributed control scheme can be modelled in MAS, since it follows exactly the same paradigm.

In Figure 3 high level example of a MAS model for our AEN is presented. A nice property of this modelling approach is the modularity of its various components. For example, communication infrastructure agents (access points) only have a certain interface by which they are addressed. Agents using the communication infrastructure don't know the underlying complexity or structure of the network. The communication network may represent the Internet, where some statistical distribution is used for delay of messages, or the communication network may be represented using lower level router agents, or it could be a dedicated network with fixed timing constraints, etc. The same argument holds for the power grid representation. The complexity of representation will depend on the type of simulation one wants to perform, as will be shown in some short example cases.

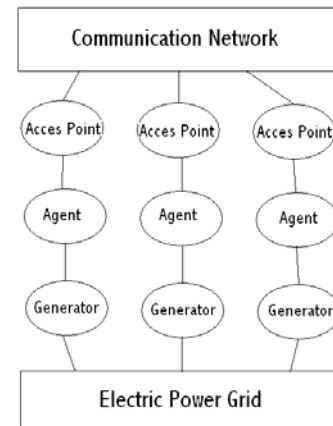


Figure 3: modular construction of multi agent based simulation.

Next, some short examples of possible multi agent simulations, with different time frames and complexity of various infrastructures and components, are presented. These examples are based on our AEN implementation.

- **Impact of Delays in Open Networks:** What is the difference in operating cost due to a slower convergence of economical optimization in agent based approach communicating over an open network with delays in comparison to a central server based approach with dedicated communication? This simulation needs good network models, but the underlying power grid model is less important.
- **Risk of Security Breaches:** How can a hacker sending false state messages to generators influence grid stability? This simulation needs a very good power grid simulator, but only basic communication models.
- **Influence of Trust Models:** Using a central institution for handing out licenses and controlling agents, or applying a distributed approach with distributed trust and agents monitoring each other. What is the influence on security of these trust models? This simulation could be done even without communication and power grid models, and results of the 'Risk of Security Breaches' simulation could be used to apply results to our AEN.
- **Impact of AENs on Electricity Market:** What are long term impacts on electricity markets when such AENs with possibilities for real time markets are installed in great numbers?

General frameworks and rules for designing this kind multi agent based models and simulations are yet to be developed, but much research has been done, and undoubtedly will be done in the near future, into this field.

Conclusions

In this paper we have shown how new control paradigms, based on distributed agent based systems, are being designed to deal with the changing power grid. It is believed that decentralised control may lead to a more robust and more open power grid. We have presented a practical implementation of such an agent based control scheme for distributed generators in a low voltage distribution net. We have shown how these new control paradigms create new or amplify old dependencies between the critical infrastructures of the power grid and communication networks. The risks introduced by these interdependencies have to be

studied thoroughly, using common sense in the first place, but also by the use of traditional reliability assessment tools and newly developed multi agent based models and simulators.

References

- [1] J. Cardell, M. Ilić, R. D. Tabors, "Integrating Small Scale Distributed Generation into a Deregulated Market: Control Strategies and Price Feedback", *MIT Energy Laboratory Technical Report, MITEL-98-001, April, 1998*.
- [2] S. Massoud Amin, B. F. Wollenberg, "Toward a Smart Grid", *IEEE Power & Energy Magazine, Vol. 3, number 5, September/October 2005, p. 34-41*.
- [3] M. N. Marwali, J.-W. Jung, and A. Keyhani, "Control of Distributed Generation Systems — Part II: Load Sharing Control", *IEEE Transaction on Power Electronics, Vol. 19, No. 6, November 2004*.
- [4] M. C. Chandorkar, D.M. Divan, R. Adapa. "Control of parallel connected inverters in standalone ac supply systems", *IEEE Trans. on Industry Applications, 29(1):136–143, Jan 1993*.
- [5] A. Koestler, "Ghost in the Machine", 1967.
- [6] M. Heller, "Interdependencies in Civil Infrastructure Systems", <http://www.nae.edu/nae/bridgecom.nsf/weblinks/KGRG-573PLA?OpenDocument>.
- [7] Rinaldi, "Modeling and Simulating Critical Infrastructure and Their Interdependencies", In *Proceedings of the 37th Annual Hawaii International Conference on System Sciences 2004*.
- [8] Tolone, Wilson, Raja, Xiang, Hao, Phelps and W. Johnson, "Critical Infrastructure Integration Modeling and Simulation", In *Proceedings of 2nd Symposium in Intelligence and Security Informatics Tucson, Arizona, June 2004*.
- [9] D. Bakken, A. Bose, C. Dyreson, S. Bhowmik, I. Dionysiou, H. Gjermundrod, L. Xu, "Impediments to Survivability of the Electric Power Grid and Some Collaborative EE-CS Research Issues to Solve Them", *Fourth Information Survivability Workshop (ISW-2001/2002) "Impediments to Achieving Survivable Systems"*.
- [10] K. Vanthournout, G. Deconinck, R. Belmans, "Agora: Distributed Tertiary Control of Distributed Resources", *15th Power Systems Computation Conference, 2005, Liege, Belgium*.
- [11] K. Vanthournout, G. Deconinck, R. Belmans, "A Small World Overlay Network for Resource Discovery", In *M.Danelutto, D.Laforenza & M.Vanneschi, editors, 10th Int. Euro-Par Conference(Euro- Par 2004), Lecture notes in Computer Science Vol.3149, Springer, Berlin, Pisa, Italy, Aug/Sept., 2004; pp. 1068-1075*.
- [12] K. Vanthournout, G. Deconinck, R. Belmans, "Building Dependable Peer-to-Peer Systems", *Supplemental volume of international conference on dependable systems and networks (DSN-200), Florence, Italy, June, 2004; pp. 297-301*.
- [13] K. De Brabandere, B. Bolsens, J. Van den Keybus, A.Woyte, J. Driesen, and R. Belmans. "A voltage and frequency droop control method for parallel inverters". In *Proceedings of the IEEE Power Electronics Specialists Conf. (PESC-2004), pages 2501–2507, Aachen, Germany, Jun 2004*.
- [14] Tolone, Xiang, W. Johnson, "Applying Cougaar to Integrated Critical Infrastructure Modeling and Simulation", In *Proceedings of First Open Cougaar Conference New York City, July 2004*.
- [15] Dudenhoefter, Perman, Sussman, "A Parallel Simulation Framework for Infrastructure Modeling and Analysis", In *Proceedings of the 2002 Winter Simulation Conference*.
- [16] A. Helsingier, M. Thome, T. Wright, "Cougaar: A Scalable, Distributed Multi-Agent Architecture", *SMC 2004 - IEEE Conference on Systems, Man and Cybernetics*.
- [17] Repast Agent Simulation Toolkit, <http://repast.sourceforge.net/>.
- [18] System for Parallel Agent Discrete Event Simulation (SPADES), <http://spades-sim.sourceforge.net/>.
- [19] E.E. Balkovich, R.H. Anderson, "Critical Infrastructures will Remain Vulnerable; Neighbourhoods must fend for themselves", In *International Journal of Critical Infrastructures, Vol. 1, No. 1, 2004, pp. 8-19*.
- [20] J. Huang, S.S. Venkata, "Wide Area Adaptive Protection: Architecture, Algorithms and Communications", In *Proceedings of Power Systems and Communications Infrastructures for the Future, Beijing, September 2002*.
- [21] Disturbances Analysis Working Group, "Review of Selected Electric System Disturbances in North America", NERC, Princeton, New Jersey 08540-5731, 1979-1995.
- [22] PowerMatcher, <http://www.powermatcher.net/>.

Author Biographies

Tom Rigole is a PhD candidate at the Katholieke Universiteit Leuven (K.U.Leuven), Belgium, since 2005. He is a research assistant of the research group ELECTA (Electrical Energy and Computing Architectures) of the Department of Electrical Engineering (ESAT). He received his M.Sc. in Computer Science from the K.U.Leuven, Belgium in 2005. His research focuses mainly on critical infrastructures, dependable electric power and ICT infrastructures, and multi agent systems.

Koen Vanthournout received a M.Eng. degree in electrical engineering from the Groep T Industriële Hogeschool of Leuven, Belgium in 1999 and the M.Sc. degree in Artificial Intelligence from the Katholieke Universiteit

Leuven, Belgium in 2000, where he is currently pursuing a Ph.D. degree in Engineering Sciences. His research interests include automation, distributed systems and the electricity grid.

Geert Deconinck is associate professor at the Katholieke Universiteit Leuven (K.U.Leuven), Belgium, since 2003. He is a staff member of the research group ELECTA (Electrical Energy and Computing Architectures) of the Department of Electrical Engineering (ESAT). His research focuses on dependability aspects of ICT systems embedded in industrial applications.