# Microgrid Cyber-Security

Subjects: Engineering, Electrical & Electronic
Contributor: Djaffar Ould Abdeslam

The study examines the existing approaches to address cyber-physical security from a microgrid perspective. the work on the smart grid application, in general, lacks approach intersections and is still being dealt with from separate domains in the research world. Using the microgrid model to carry out experiments on the cyber-physical security has plenty of practical justifications attributed to the important role it plays in paving the way towards smart grids, the microgrid's context was mainly consulted owing to the relative simplicity in capturing and recording the interventions, either as an injected attack or control modification. Cybersecurity measures for energy systems still come as accessories and not as a built-in function. In particular, for most of the part, the electricity-related equipment that gets evolved at an exponential rate makes it extremely difficult for cyber defenses' mechanisms to keep pace with this development in the absence of up-to-date standards and common market trends.

Keywords: Cyber-physical security ; microgrid ; cyber-attacks ; Transport protocol ; State estimation ; Blockchain

## 1. Industrial Cybersecurity Incidents Emergence

The 21st century witnessed the initiation of various cyber incidents affecting sensitive infrastructures. The discovered complexity of cyber-attacks on Industrial Control Systems (ICS) revealed the dexterity level of the attackers in Industrial Con [1].

The smart grid internet interconnection subjects the grid to different forms of hazards, particularly with regard to Advanced Persistent Threats (APT), Distributed-Denial-of-Service (DDoS), botnets, and zero-days. Stuxnet, Duqu, Red October, or Black Energy are only a few examples of the advent mayhems touching industrial security since 2010 [2].

Stuxnet, the worm that caused the first reported cyber-physical incident, was discovered by a senior researcher at Kaspersky Lab, Roel Schouwenberg, in June 2010. With a purpose that was beyond stealing, erasing or modifying data, Stuxnet endeavored to cause material sabotage in the supervisory control and data acquisition (SCADA) system as a physical industrial control system. It was regarded as the first cyber-warfare weapon to encompass a complex piece of malware that has infected an estimated 50,000 to 100,000 computers mostly found in Iran, Indonesia, India, and Azerbaijan [3].

Duqu and Flame, another two worms intended towards industrial control systems, were observed more than a year after Stuxnet. Despite the similarities in code source with Stuxnet, they had different objectives. Duqu was designed to track and gather useful information that would help to compromise the opted industrial control set. Flame or Flamer was a more sophisticated malware, especially developed for cyber espionage on these networks. Spotted cases were mainly located in Iran and other countries of the Middle East [4].

In December 2015, a cyber-attack on Ukraine's power system has procured a wide-area outage, affecting around 225,000 customers. The attack was associated with a new variant of Black Energy Trojan named Disakil [2]. According to reports issued by power companies, the SANS institute and Electricity Information Sharing and the Analysis Center (E-ISAC), the problem started several months before the actual attack by installing the malware through phishing emails. At this period, the hackers only monitored and collected valuable information about the system operation during what is usually called the reconnaissance phase. On the day of the incident, the attackers took control over the Human–Machine Interface (HMI) and cut the power by opening a certain number of breakers. In order to intercept the service restoration, a denial of service (DoS) attack on the communication network, additionally to the classic telephone lines, was employed to prevent the clients from reporting the problem. Even applications that determined the outage extent were blocked by the malware that was able to recognize the system softwares [5][6].

One year earlier, the same threat agents were identified by the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) during an attempt to penetrate the U.S. electric sector. Despite the fact that the attack, in this case, never happened, it definitely attracted attention on the future potentials of the cyber threats on a sector of

utmost vitality [3].

## 2. Overview

### 2.1. Cyber-Physical Security

The IEA (International Energy Agency) defines energy security as “the uninterrupted availability of energy sources at an affordable price”. Traditionally, security used to be achieved on two fundamental levels; short-term security that deals with the stability of the demand-supply procurers, and the dynamism that enables the energy system to adapt as quickly as possible to sudden changes in the grid loads. Moreover, long-term security focuses on investments that support economic and sustainable development requirements.

Recently, with the arrival of smart grids which are essentially defined according to IEEE 2030-2011 standard, as a composition of three interoperability infrastructures, as set forth in Figure 1. This suggested interdependency has led the security problem to grow in complex imposing supplementary challenges threatening of introducing easier ways of causing damage to the fundamental security concerns, all along with creating new ones.

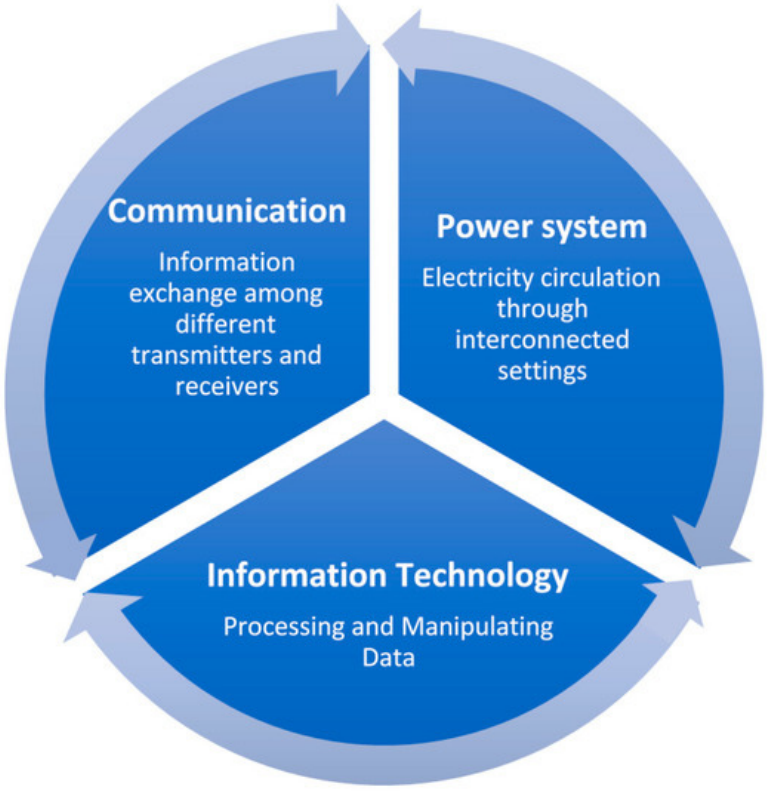


**Figure 1.** Smart grid architecture in compliance with IEEE 2030.

Consequently, recent security assessment has focused on identifying the potential vulnerabilities introduced by the cyber layer and analyzes the possible impacts on energy systems, which has given birth to a brand new research area called cyber-physical security. A cyber-physical system is co-engineered collaborating domains of physical and computational counterparts, in which the crucial system tasks are basically handled with its physical part, while informatically enhanced processes- normally referred to as cyber- are responsible for maximizing the exploration of intelligent devices and application [7].

The reason why academia recently chose to add the term “physical” to the equation is to shed light over the emerging threats imposed by connecting these two fundamentally different infrastructures together, which practically may lead to problems that do not particularly belong to a failure of either systems [8]. In light of these assumptions, further investigation is still needed to either confirm or deny the putative relationships [9].

The most indispensable objectives of security requirements considerations of any data transferring communication in the IT network security are known as CIA-triad, which stands for Confidentiality, Integrity, and Availability, respectively. According to The National Institute of Standards and Technology (NIST)’s guide on cybersecurity strategy, architecture, and high-level requirements, Confidentiality refers to “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44, U.S.C., Sec. 3542], and a loss of confidentiality results in unauthorized disclosure of information. Whereas Integrity is “Guarding against improper

information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44, U.S.C., Sec. 3542] in other words, integrity is the unauthorized modification or destruction of transferred information. Availability, on the other hand, means "Ensuring timely and reliable access to and use of information…" [44, U.S.C., Sec. 3542] as if altering availability will lead to the disruption of the access to or use of information or an information system.

Smart grid security is also built upon the previous trestles, but with a difference in priority order, where availability comes on top of the requirements, followed by integrity, accountability, and finally confidentiality. Other referencing emphasizes accountability as additional security criteria [10]. This sequence of importance goes back to the severity of impacts resulting from tampering with these criteria.

Attackers can penetrate the smart grid communication systems using vulnerable entry points in the logical border surrounding a network, known as the Electronic Security Perimeter (ESP). Interventions may occur with the help of numerous mediums, such as the Universal Serial Bus (USB) thumb drive, viruses, and even software patches and updates [11].

Despite the fact that cyber intrusions on cyber-physical systems (CPSs) can be found under different terms, such as bias injection attack, zero dynamics attack, denial of service (DoS) attacks, eavesdropping attack, replay attack, stealthy attack, covert attack, and dynamic false data injection attacks [12]. These attacks can still be classified according to the one or multiple security criteria they are jeopardizing, as set forth in Figure 2.

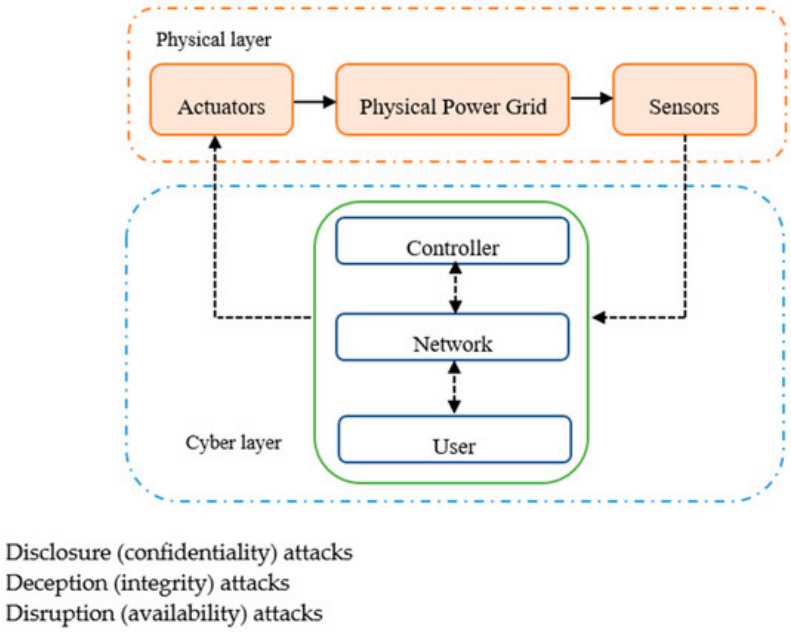


**Figure 2.** Three types of cyber-attacks.

Intentionally introduced faults or malicious attacks triggered by the cyber layer leaving serious impacts on not only the technical aspects, but also on economic and social correlations in power network operations, are the focus of this research.

Effects range from tampering smart meters data or manipulating the forecasted load profiles up to reaching equipment damage or even complete blackouts [13].

However, achieving such results is never an easy business. Indeed, physical prerequisites and the current state of the power system architecture with contemporary defense mechanisms, such as controllers prepared to re-examine each input parameter against a selection of acceptable values preventing possible physical damages [14], burden the attacker with the mandatory acquisition of a customized knowledge about the physical nature of the system added to the already required computer-related competencies. But then again, this does not mean that the conventional ways of protection, such as the ones adopted to restrain the spread of fault effects by isolating a malfunctioning entity, are enough to prevent an attacker from achieving an unacceptable condition in the grid [14].

In that vein, reasonable strategies to fend off such incidence fall into two complementary categories. The first one is about developing measures that tend to detect malicious attacks and tackle down the cause of infection in the system in order to deal with either the compromised unit or entity through isolation or the direct cause from wherein the adversary

could have accessed the network. The second important aspect is cyber resiliency, in which we anticipate the behavior of our system under attack and elaborate on what could be done to expeditiously recover from these attacks in a passive protection fashion.

At any rate, we must keep in mind that keeping the system utterly safe, over and above maintaining a level of simplicity allowing the intuitive understanding of the entangled operation, is a paradox that preoccupies the power system researchers and engineers.

### 1.2. Modern Distribution Network Vulnerabilities

Distribution systems play a major role in the electricity sector value chain linking transmission to consumption and providing direct contact with consumers [15]. Knowing that their systems were originally designed for passive energy delivery (in one direction), Distribution System Operators (DSOs) find themselves nowadays forced to cope up with the tremendous changes pertaining to the electrical networks, especially on the medium to low voltage scale.

Unlike in transmission systems that have adopted the Energy Management Strategy (EMS) early in the 1970s, the application of proper EMS at the distribution level was not put into action until recently, since it did not have much of added avail [16].

Following the foregoing tendency, measures continue to offer incentives that consolidate the integration of all the flexible distributed resources into the market, side by side, with new demand–response technologies on the demand side [17].

Dispatchable generation units owned by the DSO, which could be turned on and off by the energy operator to match a scheduled output that meets the network requirements, are a very useful avenue that has been widely exploited over the years in peak shaving and declining stress over the network components at times of high demand. Nevertheless, the surplus of the distributed generation (DG), especially the non-dispatchable (renewable) type, can adversely affect the performance of the distribution systems causing power quality issues, augmented fault levels, voltage violations, protection issues, in addition to line overloading or congestion [16].

Certain DSOs have set rules of thumb that determine the adequate segment of DG that should enter the distribution networks depending on the hosting capacity of each of them. In general, an estimated 15% of the network's peak demand could be connected to the distribution network without causing significant problems [18].

The needed elements for DG metering and monitoring change from country to country or even between regions. Hence, more or less data might participate in the decision that determines whether a DG participates in the energy markets or not, in respect to its impact on the local network, keeping in mind that larger DG installations could also have an extended disconcerting impact on the regional or national transmission system [16].

#### 2.3. Microgrids as a Cyber-Physical System (CPS)

Despite the tendency to associate the term microgrid with the power sector, we find that the concept represents itself in a larger context related to the energy community with different means of energy production, transition, and storage, all along with achieving the mutual goals of boosting technical and economic resilience [19].

Through the years, different definitions have been placed in the technical literature to describe the concept of a microgrid. The first one was proposed in [20][21] imagining the microgrid as the ultimate solution for the reliable integration and control of the ensemble of Distributed Energy Resources (DERs), including Energy Storage Systems (ESSs) and controllable loads [22].

Similarly, in [23][24], the microgrid paradigm is foreseen as a very appealing strategy to overcome challenges in integrating the massive renewable resources resulting from summing up all community-scale capacities, which is still being kept on hold due to the inflexibility of the current networks. Furthermore, these individual DERs are often too small to enter the electricity market, which is another problem that has been solved thanks to this new topology.

This goes in line perfectly with what is stated by the US Department of Energy, with only one difference stressing the clear barriers with respect to the distribution network, in the way that it permits the microgrid to have the ability to operate not only within grid-connected mode but also in autonomous island mode [25], which in turn was found, in numerous studies, to be considered as a sine qua non to denote a microgrid [3].

With microgrid pushing the power system over the edges of decentralization, a geographically localized distributed power model makes more sense regarding risk-management in terms of regional resilience and preventing cascading failure in the event of weather events, cyber-attacks, etc. [23]. Knowing that the electricity supply for small urban or industrial communities (isolated microgrid) where the main grid connection is inaccessible was never a novel trend in the world of electrical alimentation [22].

There were numerous attempts to create a standardized configuration of the smart grid's building block, namely microgrid. However, its structure is yet considered to be arbitrary and any technically well functioning connection is valid [7] [22]. It is important to notice that the microgrid's ability to fit in different configurations and to be customized as a function of the present requirements and constraints is the exact same reason why it is so hard to classify it in a fixed frame. Figure 3 illustrates a generalized structure for modern microgrids.

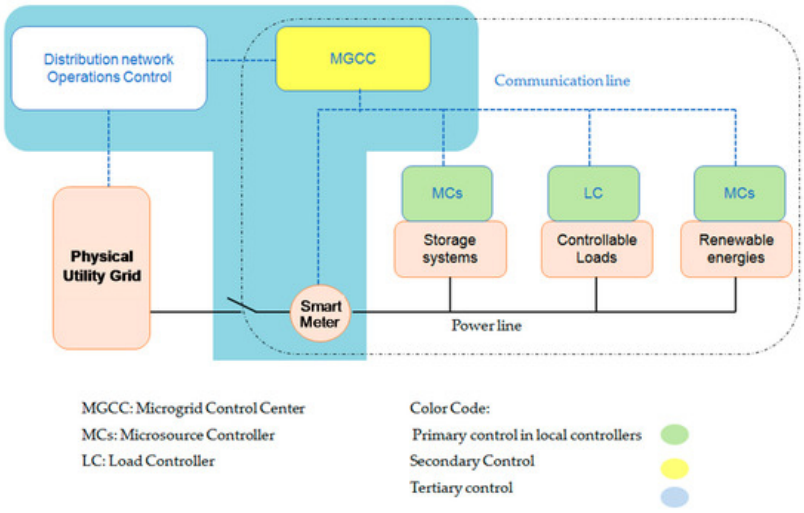


**Figure 3.** Modern basic structure of a microgrid.

From an operational perspective, there are only two types of microgrids (MGs):

A grid-connected MG, which is built to operate in either islanded or connected mode, might have one or several connection points with the grid. A single point of connection is very common though [1].

An isolated or stand-alone microgrid does not even have a point of common coupling (PCC) with the main grid [13]. Microgrids' implementation into utility does not always have to follow the classical case where a single MG is connected directly. Other alternatives can still exist, such as multiple tie line-based interconnected microgrids and small MGs within larger ones, so as the biggest takes the role of the governor large areas electrical power system [23].

The operational efficiency of microgrids necessitates sophisticated but most importantly secure measurement, communication, and control realized by various controlling methods, sensors, actuators, and field devices [12]. Moreover, microgrids are a highly sensitive cyber-physical system [7], in which the physical part is strongly influenced by the integrity of the cyber part, due to more entry point, very low required latency and the absence of multi-stage security detection. Consequently, attackers have more of a chance to cause serious problems in microgrids, leading to overall catastrophic consequences [26].

Recent papers have gone through securing the cyber-physical structure of the microgrid from different standpoints. Preliminary efforts probing cyber-attacks against the power systems would usually treat these attacks as a sort of noise or disturbance. So they tried their best to eliminate these disturbances using filtration techniques [27][28]. However, these techniques are based on pre-defined statistics which lose their effectiveness when facing slightly more fine-tuned attacks [5].

In the following sections, we reviewed the recently proposed approaches from different domains.

## References

1. Sridhar,S.; Govindarasu, M. Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid 2014, doi:10.1109/TSG.2014.2298195.
2. Leszczyna, R. Standards on cyber security assessment of smart grid. Int. J. Crit. Infrastruct. Prot. 2018, 22, 70–89.

3. Chlela, M., Cyber Security Enhancement Against Cyber-Attacks on Microgrid Controllers; McGill University Montréal: Montréal, Canada, 2017; pp. 1–177.
4. Knapp, E.D.; Samani, R. Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure,1st ed; Syngress: Massachusetts, United States, 2013.
5. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. Int. J. Electr. Power Energy Syst. 2017, 99, 45–56.
6. Lee, R.M.; Assante, M.J.; Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case.; E-ISAC, .Washington DC, USA. 2016, 1–23.
7. Rekik, M.; Chtourou, Z.; Gransart, C.; Atieh, A. A cyber-physical threat analysis for microgrids. In Proceedings of 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD). Hammamet, Tunisia, 19–22 March 2018. Avalable Online: https://ieeexplore.ieee.org/document/8570411 (accessed on 6 May 2020).
8. Cai, Y.; Huang, T.C. Cascading failure analysis considering interaction between power grids and communication networks. IEEE Trans. Smart Grid 2016, 7, 530–538.
9. Zhang, H.; Peng, M.; Guerrero, J.M.; Gao, X.; Liu, Y. Modelling and Vulnerability Analysis of Cyber-Physical Power Systems Based on Interdependent Networks. Energies 2019, 12, 3439.
10. Liu, J.; Xiao, Y.; Gao, J. Achieving accountability in smart grid. IEEE Syst. J. 2014, 8, 493–508.
11. Srivastava, A.; Morris, T.; Ernster, T.; Vellaithurai, C.; Pan, S.; Adhikari, U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Trans. Smart Grid 2013, 4, 235–244.
12. Fooladivanda, D.; Hu, Q.; Chang, Y.H.; Sauer, P. Secure State Estimation and Control for Cyber Security of AC Microgrids. 2019Secure 2019. Doi: arxiv.org/pdf/1908.05843.pdf.
13. Esmalifalak, M.; Shi, G.; Han, Z.; Song, L. Bad data injection attack and defense in electricity market using game theory study. IEEE Trans. Smart Grid 2013, 4, 160–169.
14. Friedberg, I.; Laverty, D.; McLaughlin, F.; Smith, P. A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation. In Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015. Belfast, Swindon, UK. 52–62 September 2015. Avalable Online: https://dl.acm.org/doi/10.14236/ewic/ICS2015.6 (accessed on 27 May 2020).
15. Prettico, G.; Gangale, F.; Mengolini, A.; Lucas, A., Fulli, G. Distribution system operators from european electricity distribution systems to representative distribution networks. JRC Tech. Rep, Luxembourg. 2018, 99, 273–280. DOI: 10.2790/701791
16. Hayes, B.P. Distribution Generation Optimization and Energy Management; In Distributed Generation Systems, Gharehpetian, G.B., Agah S.M.M.; Elsevier Inc: Oxford, UK, 2017; 415–451. doi:10.1016/B978-0-12-804208-3.00009-1
17. Prettico, M.; Flammini, G.; Andreadou, M.G.; Vitiello, N.; Fulli, S.; Masera, G. Distribution System Operators Observatory 2018: Overview of the Electricity Distribution System in Europe. Publications Office of the European Union: Ispra, Italy. 2019; pp. 1–77.
18. Stavros A.P.; Nikos D.H.; Pierre A.; Luiz M.A.; Bernhard B.; Clinton G.C.-B.; Drossos N.; Bayez E.; Mingtian F.; Vincent G.; et al. Capacity of Distribution Feeders for Hosting Distributed Energy Resources; In Proceedings of the Papathanassiou 2014 Capacity ODCIGRE 2014. June 2014. Avalable Online: http://cigreaustralia.org.au/assets/ITL-SEPT-2014/3.1-Capacity-of-Distribution-Feeders-for-hosting-Distributed-Energy-Resources-DER-abstract.pdf (accessed on 5 June 2020).
19. Feng, X.; Shekhar, A.; Yang, F.; Hebner, R.E.; Bauer, P. Comparison of hierarchical control and distributed control for microgrid. Electr. Power Components Syst. 2017, doi:10.1080/15325008.2017.1318982.
20. Lasseter, B. Microgrids distributed power generation. Power Eng. Soc. Winter Meet. 2001, 1, 146–149.
21. Lasseter, R. Microgrids. IEEE Power Engineer. Soc. Winter Meet. 2002, 1, 305–308.
22. Katiraei, F.; Iravani, M.R. Power management strategies for a microgrid with multiple distributed generation units. IEEE Trans. Power Syst. 2006, 21, 1821–1831.
23. Olivares, D.E. Trends in microgrid control. IEEE Trans. Smart Grid 2014, 5, 1905–1919.
24. Buason, P.; Choi, H.; Valdes, A.; Liu, H.J. Cyber-physical systems of microgrids for electrical grid resiliency. ICPS 2019, 492–497, doi:10.1109/ICPHYS.2019.8780336.
25. Ton, D., Bryan, E., Marnay, C.; Microgrids Program Overview, Power Systems Engineering Research and Development. Aalborg 2015 Symposium on Microgrids. 2015, 1–22. doi:eeexplore.ieee.org/stamp/stamp.jsp?arnumber=7420793

26. Rana, M.M.; Li, L.; Su, S.W. Cyber attack protection and control of microgrids. IEEE/CAA J. Autom. Sin. 2018, 5, 602–609.
27. Peach, N.; Basseville, M.; Nikiforov, I.V. Detection of Abrupt Changes: Theory and Applications. J. R. Statal Soc. Ser. A (Stats in Soc.). 1993, 1, 185. doi:10.2307/2983416
28. Jiao, Q.; Modares, H.; Lewis, F.L.; Xu, S.; Xie, L. Distributed Ⱶ2-gain output-feedback control of homogeneous and heterogeneous systems. Automatica 2016, 71, 361–368.