A Cyber-Physical Threat Analysis for Microgrids

Mouna Rekik, Zied Chtourou, Christophe Gransart

A Cyber-Physical Threat Analysis for Microgrids

Mouna Rekik
IFSTTAR, COSYS, LEOST, France
Email: mouna.rekik@ifsttar.fr

Zied Chtourou
CRNS, SERCOM, Tunisia
Email: ziedchtourou@gmail.com

Christophe Gransart
IFSTTAR, COSYS, LEOST, France
Email: christophe.gransart@ifsttar.fr

***Abstract*—MicroGrids (MGs) are foreseen as a building block of the smart grid. They allow for the integration of distributed energy resources and storage within the conventional grid. This is partly possible through deployment of Information and Communication Technologies (ICTs) within these structures. Therefore cyber security is a major concern for MGs. This paper investigates cyber-physical security aspects of the MG, including vulnerabilities and threat landscape. A cyber-physical security risk assessment is presented for evaluating impacts of exploiting existing vulnerabilities by potential threats on MG operations.**

***Keywords*—Microgrid, cyber-physical security, vulnerability, threat landscape, risk**

I. Introduction

The MGs group Distributed Energy Resources (DERs), energy storage devices and loads within restricted geographic area and present them as a single controllable entity to the utility grid. They can operate connected or islanded to/from the main grid whenever required by physical or economic conditions. This concept allows effective integration of DERs at distribution level. In fact, individual DERs are too small to be granted access to the energy market. Likewise power utilities are unable to effectively control and manage small DERs. Moreover, MGs have the potential to integrate large quantities of renewable generation through highly localized optimization of distributed generation output, demand flexibility and storage assets. These control and automation systems are supported by massive integration of ICT within the MG and to the utility grid. This comes with new challenges especially for cyber-security. In fact, all these features act to increase the entry points to the system and thus its exposure to cyber-threats.

The work presented in this paper investigates cyber-physical security aspects of the MG. The remainder of this paper is structured as follows. Section II describes the conecpt of MG as a cyber-physical system. Then, in section III, we discuss MG threat landscape through a vulnerabilities, threats and threat agents analysis. In section IV, we present a detailed analysis of potential attacks and thier impacts on MG operations and we review some good practices to be used in order to minimize risks. Finally, section V concludes the paper.

II. System Identification

A cyber-physical system is co-engineered interacting networks of physical and computational components [1]. The main task of the system is accomplished by its physical part, whereas the cyber part is the enabler for smarter services to maximize the system efficiency. The MG can be identified as a cyber-physical system. The physical system is the power infrastructure, while the cyber system is composed of the control, automation and communication infrastructure. In the following, we describe MG subsystems.

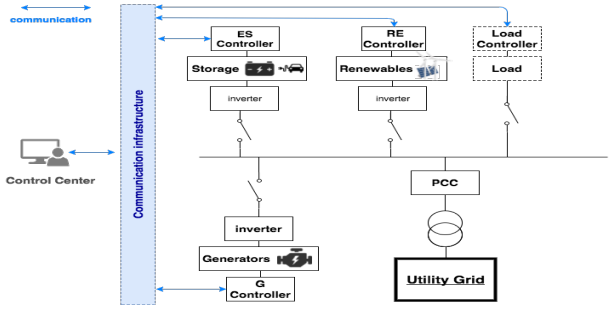

Fig. 1: Basic structure of a microgrid

A. *MicroGrid (*MG*) as a Power System*

From physical perspectives, a MG is a distributed electric power system. It is formed by the aggregation of geographically localized distributed energy resources that are controlled to provide end-users with predefined load profiles and power quality and reliability. These resources could be renewable or non-renewable power sources, storage, electric vehicles, loads, etc. There are no conceptual restrictions on interconnections between components within the MG and any technically feasible connections between sources loads and storage are allowed. MGs could be built to operate in either islanded, grid-connected or both modes. For the connected MG, the number of connection points to the utility grid varies although a common connection point is commonly used. Remains that the whole system is presented to the main grid as a single controlled entity. Figure 1 shows the basic structure of a MG.

B. *Microgrid Cyber system*

MGs should provide reliable electric service when connected to the main power grid, when operating in islanded mode, and during the transition between these two modes [2]. This is accomplished using efficient control, automation and communication that are realized by the its cyber-system.

Figure 2 presents a layered architecture of the MG highlighting its cyber-physical aspect. Components of MG physical system, presented at the component layer, are locally controlled by control and automation devices, sensors and actuators presented at the local control layer (e.g. Smart Meter (SM), Building Management System (BMS), Load Controller (LC), Electric Vehicle Supply Equipment (EVSE), etc...) [3]. The control Layer comprises a HMI (Human Machine Interface), a server and a historian. The HMI provides an interface to monitor MG operations. The historian is a database used to store information and collected data for the functioning of MG. The server comprises Supervisory Control And Data Acquisition (SCADA) and Energy Management System (EMS).

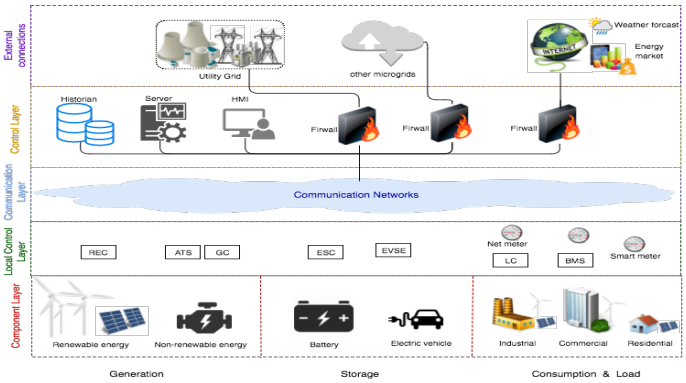

Fig. 2: Microgrid Layered architecture

The control center is interconnected to MG components by a communication layer through the intermediary of local controllers. The communication network may be heterogeneous using several technologies ranging from wired such as fiber-optics, cables to wireless technologies [4], [5]. In addition to the insider communication, MG control center should be connected to utility grid, others adjacent MGs and internet to accomplish optimal operations. For that, firewalls should be used to protect the control center external communications.

III. Microgrid Threat Landscape

A threat landscape defines the list of potential threats and threat agents against a considered system. A threat can result in attacks whenever it exploits system vulnerabilities. As such, in this section, we study the MG vulnerabilities, then we identify potential threats and threat agents against MGs.

A. Microgrid Vulnerabilities

Although the integration of cyber systems into critical physical infrastructures brings benefits, it introduces also a new set of vulnerabilities that may expose the system to a variety of threats. The exploitation of such cyber-vulnerabilities can lead to physical consequences. MG, being a cyber-physical system, inherits of their common cyber-vulnerabilities added to vulnerabilities brought from the specificity of distributed power systems. These vulnerabilities are created by:

- **The use of Wireless communications**. Although such communication technologies bring several advantages to the system, they introduce typical vulnerabilities because communications take place "through the air" using radio frequencies and thus it is difficult to prevent physical access to them, especially in open and accessible areas like public power infrastructure. Risk of attacks such as interception and intrusion is greater than with wired networks.
- **The use of heterogeneous communication technologies**. Modern power systems are supposed to be handled by communication networks using a variety of technologies. The co-existence of different technologies either wired or wireless will complicate the implementation of a robust and uniform cyber-secure policy to protect the communication infrastructure.
- **Increasing exposure to external networks**. A MG should continuously exchange data with the main grid operators and other MGs at the aim to improve the overall performance of the main grid and ensure the safety of its operations. Such communications with other external networks exposes the system to additional external threats.
- **Exposure to Internet**. Exchanging data with Internet is essential for MG ancillary services such as weather forecast data, fuel prices, etc, which exposes the MG to numerous attacks conducted through Internet.
- **Increasing system automation**. Usually, automation control is intended to improve flexibility and effectiveness of a system operations by removing possibility of human error. However, it introduces new vulnerabilities since more access points for the system are available and therefore risk of attacks increases.
- **Increasing use of distributed control and automation devices**. The sophisticated distributed control of flexible assets and demand within a MG provide the promise of resilience; however, the increased penetration of monitoring and control capabilities open up the possibilities for breaches of security. The digital era will extend and stretch MGs boundaries.
- **Cohabitation between legacy and new systems**. Since power distribution grid is a shared common infrastructure used by different distribution operators, MG controller is expected to be continuously in contact with these operators in order to improve the overall grid operations, the use of legacy equipment and infrastructures introduces new vulnerabilities.
- **Multiple independent systems**. Power systems and in particular MGs are composed of diverse systems such as sensors, actuators, computers, payment systems, emergency systems, etc. It is crucial, but difficult, to ensure smooth interfacing, communication and securing between such independent and heterogeneous systems. This increases vulnerabilities.

As presented above, the nature of MG makes it severly vulnerable. A vulnerability is considered as a weakness that can be exploited by one or more threats [6]. Thus MGs are increasingly exposed to cyber-physical threats. In the next section, we identify potential threats for MGs.

B. Potential threats against Microgrid

In order to identify potential threats against MGs, we choose to use the threat model of European Union Agency for Network and Information Security (ENISA) [7]. This model covers mainly cyber-security threats; which are threats directly applied to ICT assets and thus affecting the system operations. It also includes non-IT threats to cover threats to a system physical assets that are necessary for main operations. Based on this model, we identified a set of potential threats that can endanger MGs. These threats can be classified into the following categories:

- **Physical attacks** caused by intentional offensive actions aiming to achieve maximum distraction, disruption, destruction, theft or unauthorized access to MGs assets. This category is not considered in the current analysis.
- **Eavesdropping/Interception/Hijacking**. This contains cyber-attacks and intentional malicious activities or abuse targeting digital assets of a system. Threats from this category consist of altering communication between two parties without installing additional tools/software on victim's site .
- **Nefarious Activities**. This category also contains cyber-attacks and intentional malicious activities or abuse targeting digital assets of a system. However, these attacks usually require the use of tools by the attacker. As such, the threat is accomplished through the installation of additional tools/software or performing additional steps on the victim's IT infrastructure/software.

C. Potential threat agents against Microgrid

Determination of the agent behind the attack may help to identify the criticality of the attack. We distinguish 8 types of threat agents:

• **Corporations, organizations or enterprises** that are engaged in offensive tactics. In this context, they are considered as hostile threat agents and their motivation is to build competitive advantage over competitors. Depending on their size and sector, corporations usually possess significant capabilities, ranging from technology up to human engineering intelligence, especially in their area of expertise.

• **Cyber-criminals**. Threat agents from this category are hostile by nature. Moreover, their motivation is usually financial gain and their skill level is, nowadays, quite high. Cyber-criminals can be organized on a local, national or even international level.

• **Insider threat agents** including employees and third party. Employees refers to the staff, contractors, operational staff or security guards working for the MG operator. Utilities rely on vendors, system integrators, and other third party service and product providers in order to operate their power facilities. These threat agents can have insider access to private facilities and resources of the MG, they also possess a significant amount of knowledge that allows them to place effective attacks against sensitive assets of the system.

• **Hacktivists**. This kind of threat agents are politically and socially motivated individuals that use computer systems in order to protest and promote their cause. Moreover, they are usually targeting high profile websites, corporations, intelligence agencies and military institutions.

• **Nation states (NS)** that have offensive cyber capabilities and use them against an adversary. Nation states have recently become a prominent threat agent due to the deployment of sophisticated attacks that are considered as cyber weapons. From the sophistication of these malware it can be confirmed that nation states have a plethora of resources and they have a high level of skills and expertise.

• **Terrorists** have expanded their activities and engage also in cyber-attacks. Their motivation can be political or religious and their capability varies from low to high. Preferred targets of cyber terrorists are mostly critical infrastructures (e.g. public health, energy production, telecommunication etc.), as their failures causes severe impact in society and government.

• **Cyber-fighters**. This type of threat agents presents an emerging phenomenon, the profile consists of patriotic motivated groups of citizens with the potential to launch cyber-attacks. Such groups might have strong feelings when their political, national or religious values seem to be threatened by another group and are capable of launching cyber-attacks. Having said that, one can argue that such groups are special cases (maybe an evolution or yet another instance) of hacktivism. To an extent, such groups may be supporters of totalitarian regimes and, rightly or wrongly, act on behalf of their supporting parties (i.e. governments) by contributing to national activities in the cyber-space. Their activities may include conflicts with other groups (i.e. hacktivists).

IV. Cyber-physical threat assessment

In this section, we perform a detailed threat analysis at the aim to identify their impact on MG operations. We also provide a first level of recovery, mitigation and good practices to protect the system.

A. Physical threats

In this category of threats, the attacker aims to disturb the cyber-system (including communication and control system) through damaging or destroying physical assets of the system, which lead to a partial or global dis-functioning of the system. We describe in table I, the physical attacks that may be performed against a MG control system and communication assets.

TABLE I: Physical Threats

Threat	Attack senarios	Threat agents	Assets
Sabotage Vandalism	These threats may result of several attack scenarios aiming to disturb the MG operations by destroying, damaging or obstructing physical equipment from components, communication and control layers.	Corporations Cybercriminals Hacktivists NS Employees Terrorists	Central control system Local control Comm
Theft	Theft of devices/hardware	Corporations Employees NS Terrorists	Central control system Local control Comm
Information leakage	Confidential information about the MG operations or state can be shared with unauthorized entities due to intentional human actions (mainly by employees that have access to restricted facilities)	Corporations Cybercriminals Hacktivists NS Employees Terrorists	Central control system Local control
Unauthorized physical access Unauthorized entry to premises	An attacker could access to facilities that he is not allowed to. E.g. he can access the setpoints in a power or voltage controller and attempt to violate the limitation of safety thresholds and thus damage equipment. He can also access the energy manager and send malicious commands to MG components which may lead to several dysfunctions such as consuming resources, or damaging components.	Employees Hacktivists Terrorists	Central control system

Physical attacks may result in damaging physical assets of the control system of a MG including central control and monitoring system, local control and monitoring equipment and the communication infrastructure. Impacts severity of such attacks varies depending on the degree of the damage and the criticality of the assets damaged. In order to mitigate physical attacks facing MGs, a physical security program should be set up. A physical security program is a combination of physical and procedural measures designed with the aim to deter attackers, detect an occurring (or occurred) unauthorized physical activity, delay an occurring attack by impeding the adversary during and slowing his progress. This allows to respond before attacked assets are compromised and take the right measures once an attack or event has occurred in order to prevent, resist or mitigate the attack and recover from the incident and restore normal operations (as soon as possible).

The first protection technique comes from employees maintaining a high level of security awareness. As such, employees must be well formed about physical security policies and procedures such as: types of threats to which the system is exposed, degree of security of each asset, security responsibilities in each work area and location, measures to take to protect the system for each threat and attacker type, requirements to report security issues or incidents in work areas, etc.

Another mandatory aspect to protect from physical threats is access and physical entry control. In fact, access should be controlled and/or restricted to system facilities for both information and physical assets, especially for control center

facilities (server room, data-center, backup repositories and storage area). This can be achieved through a mixture of physical security measures such as monitored alarm systems, closed circuit television (CCTV), access control systems, locks and keying, guards and patrols, etc.

B. Unintentional data damage

This category covers mainly threats created by unintentional staff members errors. According to [8], although data damage incidents caused by errors has decreased (from 32% in 2015 to 17.5% in 2016) it is still the highest cause of data damage incidents. We detail in Table II potential unintentional employees errors that may threaten the functioning of a MG.

TABLE II: Unintentional data damage

Threat	Attack scenarios	Threat agents	Assets
Erroneous information leakage	Confidential private or sensitive data can be distributed or shared with unauthorized entities due to human errors, using applications for mobile devices, web application or by insecure network traffic	Employees	All assets
Erroneous use or administration of devices, systems	Such threat may lead to errors in maintenance process, errors in configuration and/or installation, technological obsolescence, unpatched software and increasing recovery time.	Employees	All assets
Usage of information from unreliable source	This may lead to bad decision in control process, especially in critical situations, based on unreliable sources of information or unchecked information.	Employees	Central control system Local control
Unintentional alteration of data	Loss of information integrity due to human error	Employees	All assets
Inadequate design, planning, adaptation	Threats caused by improperly IT Assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors)	Employees	All assets

Unintentional threats may lead to sharing sensitive information which results in loss of information confidentiality. They may also endanger system integrity since they introduce software-based vulnerabilities to the system. The best practice to decrease the occurrence of unintentional data damage incidents resulted by unintentional employees errors is engaging in staff training to increase the awareness about security issues facing the system. Additional set of techniques should be implemented in order to reduce the exposure of the system to such threats, such as employing identity management systems and advanced authentication techniques (to request additional Identification, authentication and authorization techniques when modifying or discarding data), employing alarms to protect digital assets (to setup additional alerting notifications and alarms when modifying or discarding data), establishing recovery processes and maintain backups of the recorded data, employing encryption for recorded data in order to limit the impact of sharing it with unauthorized entities.

C. Eavesdropping, Interception, Hijacking

Eavesdropping attacks are insidious, because it's difficult to know they are occurring. Indeed, wireless communication are insecure by nature due to the use of radio transmissions which can be intercepted by anyone with an antenna, especially for the case of MG since the network is deployed in public. As such, a combination of techniques are needed to protect against and limit the impact of eavesdropping attacks. These techniques comprise :- engage in staff training to rise awareness and to learn about good practices concerning such attacks, - employ encryption in order to protect data. In case of eavesdropping attack, using strong encryption makes an attacker's mission far more difficult since he can not decode data intercepted, - network segmentation by limiting access to critical parts of the network, - the use of probes when designing the network in order to detect such events, - physical security is usually based on "keep the bad guys away" philosophy. For that, even if parts of MG communication network entities are placed in public, limiting access to them may reduce some types of eavesdropping attacks.

D. Nefarious Activities

The main target of attacks from this category is usually the control and monitoring components. This can be done using insecure exposure to the internet or the external network. Attackers may uses vulnerabilities in all assets in order to penetrate to the control center devices and as such he takes control of the whole system. Such attacks may result in catastrophic impacts on MG operations, but can also impact other connected MGs or even the main grid. Using a highly secure system by design is critical to defending against threats listed in table IV. This is achieved by applying a set of security techniques and policies including (but not limited to): - the use of advanced authentication capabilities, e.g. multifactor authentication, professional password-generating program, - the establishment of a well-defined privilege rights management system, restricting employees' access to certain information and allowing them to only perform specific functions, - the implementation of a robust patch management program that identifies vulnerable software applications and regularly updates the software security to ensure ongoing protection from known threats,- the implementation of a holistic approach to data security and use preventative measures to ensure the network security, - the use of firewalls and anti-virus software to help identify and block potentially risky web pages, - the use of anti-malware solutions, - the use of strategies for botnet detection involve analyzing patterns of data sent over the network, and monitoring computer resources usage and external connections, - setting a configuration management policy for connecting any hardware to the network. The policy should specify security mechanisms and procedures for various types of hardware, including computers, printers, and networking devices, - implementing a Network Access Control solution to enforce configuration policy requirements (e.g., by automatically preventing network access to the devices that do not comply with the network security policies), - implementing a strict mobile device usage policy (data encryption, user authentication, anti-malware solutions, etc).
All these techniques and policies should be coupled with up-to-date periodic staff training in order to maximize the effectiveness of the security solutions. As such, employees should be aware about threats risking the system, especially those resulting from their on-line bad habits. They should be forbidden from accessing to social media websites while using the system resources and equipment, they should learn about the security threats generated by visiting these sites. In addition to that, employees should be aware about social engineering threats and educated on how to avoid being manipulated. And

TABLE III: Evesdropping/Interception/Hijacking

Threat	Attack Scenarios	Threat agents	Assets
Wardriving	Threat of searching, locating and possible exploitation of connection to wireless networks. The motivation of such attack varies from performing it as a hobby, or to steal data and/or perform malicious activities, as such the criticality of this threat depends of the type of threat agent performing the attack		comm
Intercepting compromising emissions	Threat of disclosure transmitted information using interception and analysis of compromising emission	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	Comm
Interception of information	Threat of interception of information improperly secured in transmission or improperly actions of staff. Corporate espionage and unsecure Wi-Fi and rogue access point are examples of interception of information attacks	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	Comm
Interfering radiation	Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted from an another source	Corporations, NS, Terrorists	Comm
Replay of messages	Threat in which valid data transmission is maliciously or fraudulently repeated or delayed. For example, an attacker may manipulate the incoming DR signals, they can be delayed or repeated, DR adherents may receive these signal not in the right moment and response to the false event, which may cause instability of the grid in addition to the financial impacts on both customers and (utility).	Cybercriminals, Employees, Terrorists	Comm
Network reconnaissance and information gathering	Threat of collecting information about network to identify security weaknesses	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	Comm
Man in the middle/ session hijacking	This type of attacks is a form of active eavesdropping in which an attacker makes independent connections with the victims and relay or alters of communication between them. The attacker makes the victims thinking that they are talking directly to each other over a private connection while he is controlling and manipulating the whole communication process.	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	Comm
Repudiation of actions	People, including public authorities, may modify data (such as AMI data) and thus refuse to acknowledge an action that took place	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	Comm

most important, they should learn about how to maintain the security of their passwords. Other feature putting data at risk and undermining the effectiveness of its IT operations is the insufficiency or lack of a robust data backup and recovery solution. As such, it is mandatory to establish a specified policy defining procedures for data backup, storage, and retrieval. In fact, data and system recovery capabilities allow to reduce the risk of damage associated with a data breach. Thus, it is essential to conduct routine backups of critical data and store backup media in a safe and secure manner.

V. Conclusion and Next Steps

This paper presented an analysis of cyber-physical aspects of MGs. In this analysis, we conducted a vulnerabilities assessment, and we studied MG threat landscape by identifying potential threats and threat agents that could endanger MGs. Then, we performed a detailed cyber-physical threat assessment at the aim of identifying their impacts on MGs. In the future, we will continue exploring cyber-physical security aspects of MGs, we intend to detail cyber-physical attack scenarios and carry out simulations to quantify the impacts of specific attacks on MG operations.

References

[1] National Institute of Standards and Technology (NIST). Cyber-physical systems. https://www.nist.gov/el/cyber-physical-systems.

[2] N. Hatziargyriou et al. *Microgrids: architectures and control*. Wiley Online Library, 2014.

[3] A. Bidram and A. Davoudi. Hierarchical structure of microgrids control system. *IEEE Transactions on Smart Grid*, 3(4):1963–1976, 2012.

[4] A. Bani-Ahmed, L. Weber, A. Nasiri, and H. Hosseini. Microgrid communications: State of the art and future trends. In *Renewable Energy Research and Application (ICRERA), 2014 International Conference on*, pages 780–785. IEEE, 2014.

[5] K. Monteiro, M. Marot, and H. Ibn-khedher. Review on microgrid communications solutions: a named data networking–fog approach. In *Ad Hoc Networking Workshop (Med-Hoc-Net), 2017 16th Annual Mediterranean*, pages 1–8. IEEE, 2017.

[6] ISO/IEC 18028-1: Information technology - Security techniques - IT network security : Part :1 Network security management. International standard, ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2006.

[7] L. Marinos. Enisa threat taxonomy: A tool for structuring threat information. Technical report, European Union Agency for Network and Information Security (ENISA), 2016.

[8] Verizon 2016 data breach investigations report. Technical report, Version Entreprise solutions, 2016.

TABLE IV: Nefarious Activities

Threat	Attack Scenarios	Threat agents	Assets affected
Identity theft (Identity Fraud/ Account)	Identity theft attacks by exploiting existing vulnerabilities, or using Trojans over private PCs. Once an attacker steals identity of an employee or administrator, he gains high privileges in the system and access to privileged data. As a result, he may take control of the system as such disturb the global functioning of the MG. He may also change configuration or sensitive data to perform more sophisticated attack, for example, he can leverage implementation weaknesses or lenient access control lists to elevate his privilege level and abuse the new access rights gained as a result.	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	All assets
Receive of unsolicited E-mail	This can affect information security and efficiency of work (SPAM, unsolicited infected e-mails)	Cybercriminals	Central control system
Denial of service (DoS)	Threat of deny of service type attacks at information systems/services. In a DoS attack, a perpetrator uses a single source connected to the network (or from the internet) to either exploit a software vulnerability or flood a target with fake requestsusually in an attempt to exhaust system resources (mainly the communication network and the server). This type of attack can also be launched from multiple connected devices that are distributed across the network (or from the internet), it is then called a distributed DoS (DDoS). This disturb the communication network and probably makes it unavailable, as such it leads to prevention of authorized access to multiple system resources or the delaying of system operations and functions. A of DoS attack on network layer may, for example, result in blocking the incoming broadcast DR signals. A example of DoS attack on application layer may consist of flooding the server at the control center with fake requests leading to blocking the control system.	Cybercriminals Hacktivists	Central control system communication
Malicious code/ software/ activity	Threat of malicious code or software execution including search Engine Poisoning, exploitation of fake trust of social media, worms/ Trojans, mobile malware, alternation of software, infected trusted mobile apps, elevation of privileges, phishing attacks, web injection attacks (Code injection: SQL, XSS), exploit Kits. Using such type of attacks, an attacker can gain complete control of the system.	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	Central control system, Local control system,
Social engineering	attacks involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises. Such attacks are performed using malicious software such as : Rogue security software like Rogueware (a malicious software pretending to detect and fix problems on victim's computer, and uses this pretense to convince the victim to provide money or install more malware), Scareware (a malicious software meant to raise uncertainty or to scare a victim, its purpose is to make the victims feel threatened of imminent (unreal) danger and to make them pay to eliminate it), Ransomware (a malicious software used by a hackers to take control of a computer system and block access to it until a ransom is paid)	Cybercriminals Hacktivists	Central control system
Abuse of information leakage	Leakage affecting mobile privacy and mobile applications, leakage affecting web privacy and web applications, leakage affecting network traffic	Corporations, Cybercriminals, Hacktivists, NS, Employees	Central control system
Generation and use of rogue certificates	Loss of (integrity of) sensitive information, man in the middle/ Session hijacking, Social Engineering / signed malware (e.g. install fake trust OS updates)	Corporations, Cybercriminals, Hacktivists, NS, Employees	Central control system
Manipulation of hardware and software	Threat of unauthorized manipulation of hardware and software such as anonymous proxies, abuse of 0-day vulnerabilities (0-day vulnerabilities are vulnerabilities that are not publicly reported or announced before becoming active. Such attacks consists of exploiting a software vulnerability before the software owner becomes aware of it and before the vulnerability becomes widely known to the internet security community, this makes these attacks are among the hardest to mitigate and leave computer systems and networks extremely vulnerable), access of web sites through chains of HTTP Proxies (Obfuscation), access to device software, alternation of software, rogue hardware	Corporations Cybercriminals Hacktivists NS Employees	All assets
Manipulation of information	Threat of intentional data manipulation to mislead information systems or somebody or to cover other nefarious activities (loss of integrity of information), falsification of records	Corporations, Cybercriminals, Hacktivists, NS, Employees	All assets
Misuse of audit tools	Threat of nefarious actions with use of audit tools (discovery security weaknesses in information systems)	Corporations, Cybercriminals, Hacktivists, NS, Employees	All assets
Unauthorized activities	including unauthorized use or administration of devices and systems, unauthorized access to the information system or network, unauthorized installation or use of software	Corporations, Cybercriminals, Hacktivists, NS, Employees	All assets
Compromising confidential information	Threat of data breach	Corporations, Cybercriminals, Hacktivists, NS, Employees	All assets
Hoax	Threat of disruption of work due to false rumor and/or a fake warning	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	Central control system
Badware	Spyware (a malicious software installed on a victim's computer to collect information or monitor his activities) or deceptive adware (advertising-supported software)	Corporations, Cybercriminals, NS	Central control system
Remote activity (execution)	Threat of remote activities over controlled IT assets such as remote command execution, Botnets (Botnets are networks of compromised computers used by hackers for malicious purposes)	Corporations, Cybercriminals, Hacktivists, NS, Employees, Terrorists	Central control system
Targeted attack	Threat of sophisticated targeted attack with combination of many attack techniques	Corporations, Cybercriminals, NS	All assets