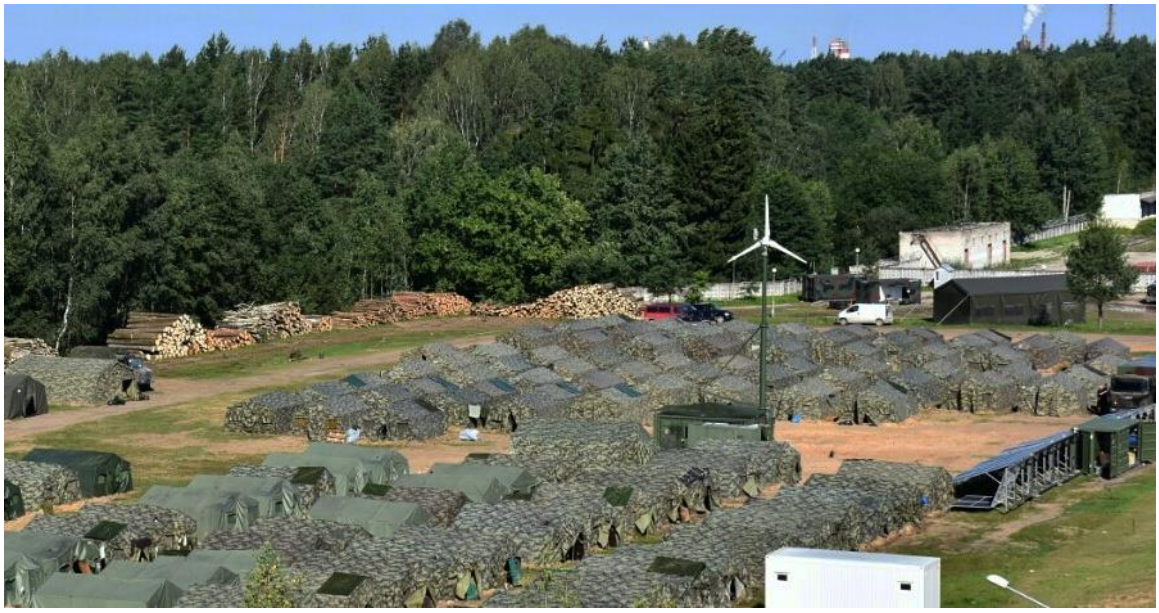
NATO
ENERGY SECURITY
CENTRE OF EXCELLENCE



Assessment study of cybersecurity of smart-grid technologies employed in operational camps

VYTAUTAS BUTRIMAS (Version 1.2.2, August 11 , 2021)

Table of Contents

[1] https://www.smartgrid.gov/the_smart_grid/distribution_intelligence.html
[2] https://pesco.europa.eu/project/energy-operational-function/
[3] https://energy.sandia.gov/programs/electric-grid/defense_energy/
[4] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf
[5] https://www.nato.int/cps/en/natolive/news_101896.htm

1. Preface

The French Ministry of the Armed Forces (FMAF) has developed a new strategy for energy defense. One of the goals of this strategy is the development and implementation of advanced technology solutions to reduce dependence on fossil fuels in order to increase operational performance and energy resilience. However, the new technologies and the enabling features employed also come with vulnerabilities that an adversary can exploit for harming personnel, equipment and the environment. As one of the means of safely achieving the strategy's goal on October 16, 2020 the Ministry requested support from the NATO Energy Security Center of Excellence (NATO ENSECCOE) in Vilnius to perform an assessment study on cybersecurity of smart-grid technologies employed in operational camps (see Appendix 1).

To execute the assessment and prepare an evaluation report, NATO ENSECCOE appointed its subject matter expert (SME) - Mr. Vytautas Butrimas, as its project lead and FMAF accordingly appointed Mme. Noémie Rebiére and Lt-Col Nicolas Mazzucchi as Points of Contact (PoC) from the FMAF Operational Energy Division. This assessment commenced with an on line project orientation meeting which took place on January 20, 2021. The project proposal's expectations, scope and method of work were discussed and agreed upon (see Appendix 2).

The major focus of the work was to evaluate the cybersecurity aspects of industrial control systems and intelligent electronic devices (IED) used in smart grid operations and recommend appropriate cybersecurity measures to address identified gaps. To clarify, the interest was in looking at the operational technology side (OT)[6][7] or the way physical processes are monitored and managed as opposed to the information technology (IT) found in the business parts of IT operations found in office environments. The relevant legal and regulatory environment in France[8] were also consulted during the preparation of this assessment[9].

The report's intended audience are decision makers at the Joint Staff. However, it should also be useful to lower level specialists and those tasked with the design and development of cybersecurity and system specifications leading to procurement and implementation of a smart grid solution for an operational military camp.

2. Introduction: what is a smart grid?

The concept of a smart grid is derived from a traditional power grid, which is a network that delivers electrical power from power plants where it is generated and distributed to users. An electrical grid includes wires, substations, transformers, relays switches and other mechanical and intelligent electrical devices. The term "smart grid" reflects a broad concept of load management. However, there is no precise definition[10] that covers exactly what that concept includes, and in

[6] http://icsmodel.infracritical.com/

[7] operational technology (OT): Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events and the applicable procedures performed by personnel (e.g. engineering, operations, maintenance) to operate and maintain with the purpose of safe and secure operation.
Note 1 to entry: In the context of facilities, this represents the IACS control system devices, including IACS network and networking devices (e.g. firewalls, switches, routers, etc.), all controls and smart instrumentation, analyzers, etc. down to level 0 in the reference architecture and those responsible for its management, operation, engineering support and maintenance.[Source: International Society of Automation ISA-TR84.00.09, 3rd edition]

[8] https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

[9] https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

[10] Alternative definition used by US DoE "A microgrid is a group of interconnected loads and distributed energy

particular who decides what load should be dispatched when. If you ask most people it amounts to fancy meters on the sides of homes and buildings that prices energy according to demand.

In the context of this study a smart grid is two-way communications between a complex set of intelligent electronic devices used to monitor and control physical processes that result in generation, distribution and storage of electricity in a safe, reliable and efficient way. The technologies used which include an energy management system, allow for combining existing power generation sources (diesel, gas turbine, coal, hydro, nuclear) with solar and wind power generation, energy storage, and waste heat recovery technologies, all connected to an intelligently (automated) managed microgrid, ensuring uninterrupted supply of electricity.

In short, the smart grid is the integration of existing electrical power systems with the communication and automation systems that monitor and control it, with the aim of improving the safety, efficiency, reliability resilience and economy of operation of the electricity supply. Smart grid encompasses such control devices and the data stream that flows through them. Sensors for example play a key role in smart grids. Sensor data sent to the controller needs to be trusted since the system will use the telemetry to adjust the flow of power accordingly. The concern here is the compromise of the sensor or a malfunctioning sensor that sends bad data to the controller. Data of course is important but also the equipment that produces data. For example, sun sensors are used in the operation of movable solar panels and wind direction sensors help in pointing the windmill toward the wind. If the sensor data is compromised, it will affect the function of the equipment. The compromise can happen both unintentionally (maintenance/manufacturer issue) or intentionally (cybersecurity issue)

3. Smart Grids and their components

A smart grid is "smart" because it has enhanced capabilities for monitoring and utilizing two-way communication among devices that belong to a system of power generation, distribution and storage. This smart capability allows for more efficient transmission of power between where the power is produced and where it is used. This is done in a variety of ways by automatically reacting to changes in demand by controlling and redirecting the generation and usage of power in the system. The smart grids control systems ability to autonomously react and correct a problem in the grid improves the system's safety, availability and resilience. For example if a critical piece of bulk power equipment was overloaded or overheating, a message would go out to the smart grid control system. The management system would automatically isolate the device and re-balance the grid until the equipment is checked, repaired or replaced. The power needed to fill gap may come from a smart grid connected centralized power plant, wind farm, photovoltaic (PV) array, energy storage system or power utility.

Life cycle costs including design, configuration, purchase costs, efficiencies, power outputs, maintainability, mobility, installation, set up, dismantling and other parameters are dependent upon the configuration of the smart grid and choice of components.

Smart grids come in different or hybrid forms:
Distributed Energy Resources (DER) are power generation technologies installed close to the loads (users) being served. DER systems can include PV arrays, wind turbines, diesel generators, and

resources within clearly defined electrical boundaries that act as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island-mode. (DOE Microgrid Exchange Group, 2010)

other power systems. A DER system may be the only source of power for residential, industrial or remotely accessible areas. A DER system may be a stand-alone system or combined with a centralized power distribution system.

Interactive distributed energy resources (IDER) are local smart grid (DER) systems that allow for two-way communications and two-way power exchanges with the central utility's power grid. For local users, these systems can both provide power to meet on-site loads and access the utilities power in the event of a local power outage. For utilities, when the local DER has surplus power it can provide it to the utility in times of high loads.

a. Power generation sources
    1. Traditional
        a. Diesel internal combustion engine generator (100-150kW) that generate power for the load and charge battery storage draw fuel from an internal or external tank. In the case of linked generators, a controller is added to allow for parallel operation and load sharing among the generators. The controllers use a communication protocol to enable communication between the controller and the camp energy management system. In a smart grid a key feature of this arrangement is optimal generator load sharing and sensing with the benefit of longer equipment lifetimes and fuel savings[11].
    2. Renewable
        a. Photovoltaic (PV) arrays (about 6.5kW generation capacity per array) that convert solar energy into electrical (DC) energy. Inverters are used to convert DC power produced from the array to AC for camp use. PV arrays can be expanded subject to available space and set up/dismantling times for a mobile camp.

Figure 1. NATO ENSEC COE HPGS Array of PV panels "climate trials" in Canada March 2019.[12]

        b. Wind power generator (6.6-7.5 kW[13]) connected to inverter to convert from DC to AC power and connected to EMS. Is transportable and able to be set up in 3-4 hours with a crane and 4 personnel.

[11] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf
[12] https://www.enseccoe.org/en/newsroom/climate-trial-of-the-hybrid-power-generation-and-management-system-in-canada/401
[13] Power outputs vary according to the size of the mast, propeller diameter, and other variables.

Figure 2. [14] NATO ENSEC COE HPGS windmill set up.

b. Storage of surplus energy[15]

One of the required features for the use of renewable energy sources such as wind or solar to power a smart grid is the ability to store the excess energy produced for later use. Energy storage technologies and their applications vary. There are 5 categories[16]: Mechanical, Electrochemical, Electrical, Chemical and Thermal energy storage technologies[17].

This assessment will limit its considerations to electrochemical (with brief mention of thermal technologies and other experimental) technologies that can be located at mobile military camps. An electrochemical storage system consists of a set of connected electrochemical cells, which produce electricity from an electrochemical reaction. The individual cell contains two electrodes (one anode and one cathode) with an electrolyte that can be at solid, liquid or viscous (flow resistant) states. During discharging, the electrochemical reactions occur at the anodes and the cathodes simultaneously. To the external circuit, electrons are provided from the anodes and are

[14] PHASE 1 REPORT Performance Analysis of HPGS, NATO ENSEC COE October 2018 https://www.enseccoe.org/data/public/uploads/2019/03/phase-1-report-hpgs-performance-analysis.pdf

[15] Good discussion of the various available energy storage systems is found here: Achkari, O., Fadar, A., Renewable Energy Storage Technologies - A Review, ATS-2018 Proceedings of Engineering and Technology – PET Vol.35 pp.69-79. http://ipco-co.com/PET_Journal/vol35/32.pdf

[16] Achkari, O., El Fadar, A., Renewable Energy Storage Technologies - A Review http://ipco-co.com/PET_Journal/vol35/32.pdf 2018

[17] EU Publication, Study on energy storage contribution to the security of the electricity supply in Europe, 2020-05-08, https://op.europa.eu/en/publication-detail/-/publication/a6eba083-932e-11ea-aac4-01aa75ed71a1/language-en?WT.mc_id=Searchresult&WT.ria_c=37085&WT.ria_f=3608&WT.ria_ev=search

collected at the cathodes. During charging, the reverse reactions happen and the battery is recharged by applying an external voltage to the two electrodes[18]. Electrochemical storage types covered in this study are:

1. Lead-Acid battery array housed in a ISO standard (20 feet)[19] transportable container with bidirectional inverter (convert DC to AC power) is perhaps the most economical in term of battery storage cost but does require a heating, ventilation and air conditioning (HVAC) unit. One downside should be noted - power requirements for HVAC in keeping the batteries at operating temperatures will subtract from the available power for the base camp.

Figure 3. Transportable external HVAC module regulating temperature of battery container[20]

2. Li-ion
   Characterized by movement of lithium ions between the electrodes during the charge and discharge reactions. Li-ion cells do not contain metallic lithium; rather, the ions are inserted into the structure of other materials, such as lithiated metal oxides or phosphates in the positive electrode (cathode) and carbon (typically graphite) or lithium titanate in the negative (anode)[21]. The battery modules are connected together to form a battery array at the required voltage, with each array being controlled by a battery management system.[22] Li-ion is suited to deliver high power but over shorter periods than Sodium-Sulfur storage.
3. Sodium-Sulfur (NaS) thermal storage
   NaS battery storage is made from liquid sodium (Na) and sulfur (S). This battery has the advantages of high energy density, high efficiency of charge/discharge and long cycle life, made-up from inexpensive materials and is transportable in a storage container. The operating temperatures of 300 to 350 °C and the highly corrosive nature of the sodium polysulfides, make them suitable for stationary energy storage applications. The cell also becomes more

[18] Achkari, O., El Fadar, A., Renewable Energy Storage Technologies - A Review http://ipco-co.com/PET_Journal/vol35/32.pdf 2018
[19] https://blog.intekfreight-logistics.com/iso-container-defined-and-facts
[20] PHASE 1 REPORT Performance Analysis of HPGS, NATO ENSEC COE October 2018 https://www.enseccoe.org/data/public/uploads/2019/03/phase-1-report-hpgs-performance-analysis.pdf
[21] https://energystorage.org/why-energy-storage/technologies/lithium-ion-li-ion-batteries/
[22] Ibid.

economical with increasing size. New advances in NaS technology have produced NaS storage that can operate at lower temperatures and reduced fire hazard[23].

"NaS has the capacity to store large amounts of electricity for hours. The NAS battery system boasts an array of superior features, including larger capacity, higher energy density and longer life compared to other battery technologies. These features are beneficial for stationary applications[24]."

4. Redox-Flow Battery (RFB)
   RFB are electrochemical storage devices based on a liquid storage medium. It is basically reversible fuel cell, is typically made up of a positive and negative electrolyte stored in two separate tanks. When the liquids are pumped into the battery cell stack situated between the tanks, a redox reaction occurs, and generates electricity at the battery's electrodes[25]. Flow batteries have lower energy densities but are scalable and have longer life cycles which is advantageous for supplying continuous power.[26]

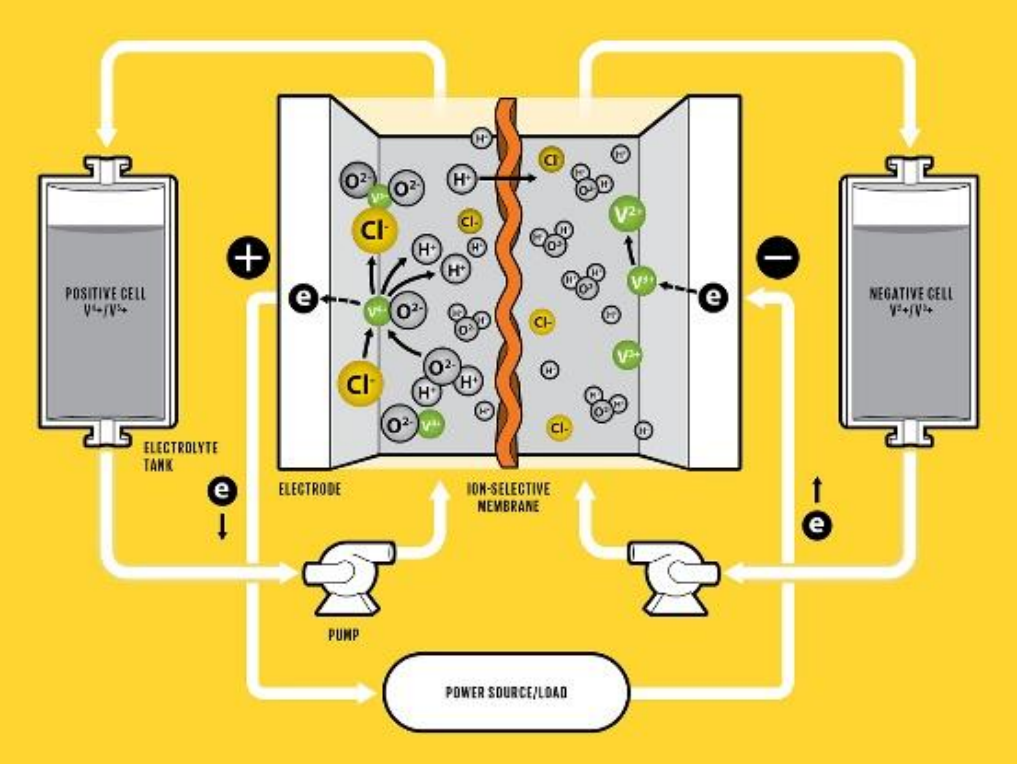


Figure 4. The positive and negative sides are separated by a membrane. During charging, an applied voltage causes vanadium ions to each lose an electron on the positive side. The freed electrons flow through the outside circuit to the negative side, where they are stored. During discharge, the stored electrons are released, flowing back through the outside circuit to the positive side[27].

[23] Sun, H., Zhy, G. et al. A safe and non-flammable sodium metal battery based on an ionic liquid electrolyte, Nature Communications, 24 July 2019. Accessed 2021-04-02 https://www.nature.com/articles/s41467-019-11102-2.pdf

[24] https://www.basf.com/global/en/who-we-are/organization/group-companies/BASF_New-Business-GmbH/news/press-releases/2019/p-19-241.html

[25] https://spectrum-ieee-org.cdn.ampproject.org/c/s/spectrum.ieee.org/energywise/energy/renewables/storing-renewable-energy-hydrogen-redoxflow-cell.amp.html

[26] https://www.eesi.org/papers/view/energy-storage-2019

[27] https://spectrum.ieee.org/green-tech/fuel-cells/its-big-and-longlived-and-it-wont-catch-fire-the-vanadium-redoxflow-battery

5. Power to gas is a promising technology option for long-term energy storage. Excess power from surplus renewable resources can be used to break water into hydrogen and oxygen in a process called electrolysis. The hydrogen can also be converted into methane by a methanation reaction that combines CO2 and H2 to form CH4. Either hydrogen or methane can be stored until their energy is needed, at which point the energy can be extracted in a fuel cell (for hydrogen) or through combustion (for methane)[28].
6. Renewable power-to-gas-to-power (green hydrogen production through water electrolysis using RES and hydrogen storage for fuel cell to be used on the grid later on). Slovenian energy companies in a partnership with the Government have an innovative project for the conversion of renewable electricity to green hydrogen and synthetic methane[29]. The Slovenian military are actively exploring the possibility of building a "Hydrogen highway" for the defense system, The PV's installed at barracks to supply electricity have enough surplus electricity to make and store hydrogen. This hydrogen is used to also produce electrical power and heat for the base and power electric vehicles[30].
7. Grid (vehicle to grid) integrated electric vehicles. Charged electric vehicles when not on the road can be used as back-up storage . Most electric vehicles today are not designed to supply energy back into a grid. However, in-development vehicle-to-grid (V2G) car technologies[31] could be used to store electricity in car batteries and then transfer that energy back into the grid later[32] . The United States Marine Corps. and automobile manufacturer GM have tested prototype hydrogen vehicles with vehicle to grid capabilities.

Figure 5. RFB stacks housed in a container like enclosure[33].

[28] Thurber, M., Power-to-gas for long-term energy storage, Energy for Growth Hub, January 16, 2020 https://www.energyforgrowth.org/memo/power-to-gas-for-long-term-energy-storage/
[29] Spasic, V., Four Slovenian energy firms to convert renewable power to hydrogen, methane, Balkan Green Energy News, November 5, 2020 https://balkangreenenergynews.com/four-slovenian-energy-firms-to-convert-renewable-power-to-hydrogen-methane/
[30] Šipec, R.,Col.,Virtualisation of Multi Energy Systems – VirMES", MoD of the Republic of Slovenia, Directorate for Logistics, Presentation made during NATO SP G5525 Project Meeting held (on-line) on May 10-11, 2021
[31] https://www.ovoenergy.com/guides/electric-cars/vehicle-to-grid-technology.html
[32] https://www.eesi.org/papers/view/energy-storage-2019
[33] Ibid.

c. Power distribution system (PDS)

Power distribution refers to all the hardware and cabling linking power sources to users. An intelligent power distribution system monitors for faults and outages, locates where the trouble is and automatically responds to them. Sensors are placed in the system indicate when parts of the distribution System have lost power, and by combining automated switching with an intelligent System that determines how best to respond, power can be promptly rerouted to customers. Devices that store and release energy, such as capacitors, or that use coils of wire to induce magnetic fields, such as electrical motors, have the ability to cause increased electrical currents. If not managed properly excess reactive power can cause damage to power distribution hardware[34]. An intelligent PDS can help optimize the balance between real and reactive power and protect equipment[35].

d. Energy management system (EMS)

The many devices in a smart grid ranging from those involved with renewable power generation to distribution and storage require an energy management system to ensure safety, reliability, resilience and timely response to load changes. This includes functionality that prioritizes power output and switches among different power generators that provide for operation at optimum efficiencies. An example of one of the efficiencies possible with new distribution technologies is the ganging of separate generators to work as one unit[36]. The EMS's serves not only to optimize smart grid operations but is able to automatically respond to anomalies.

4. Rationale for use of smart micro grids in the military

The current energy inefficiencies when using spot generation in relocatable temporary camps of the troops create logistic challenges associated with fuel supply. The energy needs of these camps are primarily satisfied by diesel engine generators, which imply that a significant amount of fuel needs to be continuously provided to these camps, which may be located in remote areas and in hostile environments.

Power reliability and quality are important since electrical equipment, especially computer-based, can be sensitive to unstable power conditions. Power reliability refers to the resilience of the power system and its capability to provide continuous power. Power quality refers to the stability of certain electrical parameters in a power system. When large loads engage and disengage, they can briefly affect the grids frequency and voltage. In stressful operations, poor power conditions can damage or destroy sensitive electronics. A smart grid is able to rapidly accommodate such deviations and protect electrical equipment. Achieving power quality can be challenging at military camps. Large commercial grids have large generation capacities and a range of equipment to help maintain grid health.[37] However, smaller camp grids, **are susceptible to power quality issues** given the camp's limited generation capacity and grid stabilization systems.

Management of networked power systems in a smart microgrid promise advantages in both power quality and reliability over spot generation. Should any generator in the microgrid fail, other generators and power sources (from wind, solar, and storage) can automatically accommodate lost generation capacity. On the other hand, a failed spot generator will immediately result in lost power, and power will not be restored until the generator is repaired or replaced. A malfunctioning or mismanaged spot

[34] https://www.smartgrid.gov/the_smart_grid/distribution_intelligence.html
[35] https://www.smartgrid.gov/the_smart_grid/distribution_intelligence.html
[36] Linking a number of generators together—allows them to be controlled as a single unit.
[37] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf

generator may produce poor-quality power and eventually damage or destroy important mission-related equipment, perhaps more harmful than a short-term power outage.[38] Moving from spot generation to smart microgrids can help reduce problems and issues stemming from poor power quality.

The advances in electronics together with their miniaturization and portability combined with the development of economical renewable/green energy technologies offer significant opportunities to reduce the "carbon military bootprint" and improve the reliability and efficiency of electric power for mobile military camps. The employment of a portable smart grid solution for a mobile military camp offers additional benefits:

i. Reliability of supply as the reduced need for fuel[39] reduces the numbers of convoys that have to travel through hostile territory;
ii. Reduced noise and heat signatures, less maintenance, and a lighter force;
iii. Portability for mobile military camps as components are increasingly able to fit inside standard shipping containers that can be placed on ships or rail cars and later transported over land on trucks.
iv. Efficient local diesel power generation by automated management of connected loads to a common set of generators;
v. More energy-efficient buildings and the ability to automatically shift power to higher-priority uses;
vi. Improved protection of mobile and even larger stationary camps from national grid power blackouts by automatically disconnecting from the utility provided power to self-sufficient camp provided power or island mode;
vii. Other opportunities to make use of surplus energy by supporting the hot water system and even supplying power to the public utility during times when the utility is unable to meet demand.

One of the main challenges towards the development of isolated microgrids is the management of various devices and energy flows to optimize their operations, particularly regarding the hourly loads, the availability of power produced by renewable energy systems and dealing with reverse power effects from blackouts, especially when there is connectivity to a utility[40]. Without a microgrid, a typical renewable energy resource such as a PV array would automatically disconnect from the grid during a power outage or distribution instability. This is a required safety feature because the renewable energy resource could back-feed the grid and thus energize circuits. Workers (and equipment) who may have been isolated from forward-feeding power could be exposed to back-fed energy. Formation of the isolated microgrid allows the safe reintroduction of renewable energy during a grid failure. This is done by disconnecting the microgrid from the primary grid before reconnecting the renewable resource. Careful management of the microgrid generators and loads prevents the renewable resource from creating reverse power conditions[41].

Next a review of some efforts to test, evaluate and overcome those challenges.

[38] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf 4.1.2
[39] Mostly just for power generation at the camp
[40] https://www.energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf
[41] https://www.energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf

5. Smart grid at military camps case studies

In order to investigate the challenges and the applicability of the smart grid for mobile military camps several pilot and research programs are underway.

a. North America

1. Smart Power Infrastructure Demonstration for Energy Reliability and Security project (SPIDERS)[42]

The U.S. SPIDERS project was a 4-year (2011-2015) technology demonstration to validate a solution for microgrid with integration of smart grid technologies, distributed and renewable generation and energy storage on military installations. The testing was done however on a stationary (non-mobile) and large military base. Starting from a small scale the project eventually covered the power needs of a large military base of over 14,000 personnel using onsite utility/industrial quality generating equipment integrated with renewable solar energy and stationary energy storage, with the possibility of providing surplus power to the local utility.[43]

SPIDERS had to meet the following demonstration criteria:

1. Protect task-critical assets from loss of power due to of cyber-attack.
2. Integrate renewable and other distributed generation to power task-critical assets in times of emergency.
3. Sustain critical operations during prolonged power outages.
4. Manage installation electrical power and consumption efficiency to reduce petroleum demand, carbon "boot print," and cost[44].

The initial phase 1 of the project did not include an energy storage solution but tested the parallel coupling of two diesel generators supplemented with a solar panel array and EMS in a separate microgrid that could connect/disconnect with the main base grid and assist in meeting base power requirements.

Phase 2 of the project added vehicle-to-grid technologies to store excess power from the generators and from the solar panels. 3 diesel generators were used to support the power needs of 7 stationary buildings on the base and EMS managed interactions among the base's extensive solar arrays and with the main base grid and with the outside utility.[45]

Figure 6. Existing base 2 MW solar array (1 MW connected to the test microgrid) that participated in the SPIDER tests[46]. This massive arrangement however is not an optimal size for a mobile camp where there is limited time and resources for extensive transportation/installation and dismantling..

[42] https://energy.sandia.gov/programs/electric-grid/defense_energy/
[43] https://www.energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf
[44] Ibid.
[45] https://www.energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf
[46] Ibid.

The SPIDERS project made use of a customized EMS where control is provided by a set of distributed intelligent power controllers with embedded software that can be installed on a wide range of power sources, distribution gear, and/or end loads. Networked elements are connected with a shared communication system[47], creating a responsive, resilient system that continuously adjusts performance. The system is managed by pre-set general rules used to maintain the desired behavior of the system during normal operation and during stresses on the loads. The system can automatically adapt to changing conditions of the equipment allowing for expansion.[48]

The SPIDERS test however was focused on supporting the power needs of large stationary camps when power from the local utility was reduced or lost. It did not extensively test battery storage technologies nor assume a need for the system to be mobile.

2. US Army evaluation of smart energy technologies for base camps (SAGE)

The U.S. Army Logistics Innovation Agency (LIA) the Department of Energy's Pacific Northwest National Laboratory (PNNL), conducted an evaluation and demonstration of Smart and Green Energy (SAGE) commercial off-the-shelf (COTS)[49] technologies to improve energy efficiency and reduce the quantity of fuel needed to operate base camps. Field tests at the Base Camp Integration Laboratory (BCIL) at Fort Devens, Massachusetts, demonstrated that significant fuel reductions of 49% to 84% are achievable depending on camp size and location[50].

Figure 7. SAGE test camp viewed from the air.

The testing platform designed for a camp of 150 personnel[51] consisted of:
- a smart microgrid with a common control system
- 3 parallel controlled and coupled 100 kW diesel generators
- power distribution system consisting of portable transmission box

[47] The SPIDERS source material did not have any detailed information about communications other than a vague reference to "underground electrical" that was installed in setting up the test system.
[48] https://www.energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf 3-14
[49] In the reference material on military testing of smart grid projects cybersecurity aspects of the technologies used was not specifically included. Testing focused on aspects of energy measurements.
[50] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf
[51] Scalable to a camp of 6000 personnel Ibid.,

- lead-acid battery energy storage and a bidirectional inverter contained in a 20-foot ISO freight container (with heating, ventilating, and air conditioning (HVAC) unit). Storage power capacity allowed for a camp load of 100 kW for two hours or a larger camp load of 250 kW for 20 minutes;
- Separate PV arrays provided 1500 liters (50 hot showers a day) of solar hot water to supplement fuel-fired water heaters with preheated water. A system controller regulated the collection of solar heated water and transferred to the main fossil-fueled hot water system reducing fuel needs;
- 2 solar electric photovoltaic (PV) arrays with a combined power output of 12.9 kW (6.5 kW per array)[52].
-3 modular, insulated hard-walled shelters sized to match the 20 ft × 32 ft footprint of a standard air-beam tent. Electric breakers for devices (for example heat pumps) and thermostats were remotely controllable by the camp Energy Management System (EMS), allowing manual and automated load management. The greatest savings and efficiencies were achieved by using energy efficient shelters[53].
- a prototype camp (EMS) with dashboard human machine interface (HMI) that actively monitored and managed the power supply to camp equipment and buildings[54].

The system also featured direct manual and automatic control[55] of the following parameters: shelter thermostat setting, various shelter electric loads, configurable-tiered load shedding in shelters, microgrid modes (silent mode, individual generator control)[56].

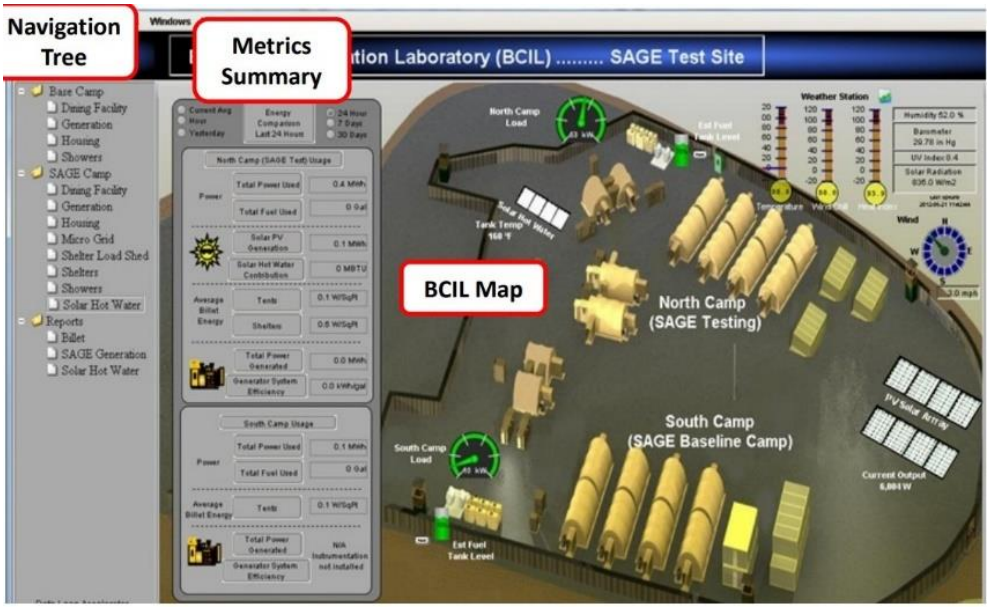


Figure 8. SAGE EMS control screen and HMI

[52] The 6.5 kW size was selected to represent study's conceptual electrical load estimate for a 20 ft × 30 ft insulated building with 22 occupants.
[53] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf
[54] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf
[55] SAGE source material did not have any detailed information about communications. In the case of SAGE the PNNL report mentions the use of these communication and control protocols
-CAN
– RS-485 annunciator data link
– Modbus TCP (10BT Ethernet)
– Modbus RTU (RS-485 Half duplex)
– BACnet
https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf
[56] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23133.pdf

3. Canada[57] and Smart Hybrid Energy System (SHES)

SHES combines the existing diesel generators with solar power generation, energy storage, and waste heat recovery technologies, all connected to a microgrid, ensuring uninterrupted electricity and hot water supplies. All components are controlled by an EMS that prioritizes output and switches between different power generators, ensuring operation at optimum efficiencies. The SHES components were selected to be easily transportable in standard shipping 20 ft containers. The modularity of the solution tested is scalable from a base camp of 150 personnel and includes on-site renewable power sources, allowing for energy optimization of different camp sizes in different climates[58].

The SHES is designed to work in stand-alone mode or connected to the local grid. The basic SHES configuration which provides a single, integrated system makes use of the following technologies:

(a) Photovoltaic (PV) array, combined power output of 100 kW with a surface of 446 m^2
    - AC inverters to transform direct current (DC) produced from PV
(b) Energy storage system composed of containerized Sodium Sulfur (NAS) lithium-ion batteries
    - Battery management system (BMS) to monitor and protect
(c) Integration of existing diesel generators to ensure continuous power supply
(d) Waste-to-heat energy recovery system (WHRU) for space heating,
(e) Solar hot water (SHW) system for domestic hot water
(f) EMS that actively monitors and controls base camp equipment and zones.

In summary, the limited test indicated that up to 37% of fuel savings and up to 37% annual CO_2 emissions savings over current base camp configurations are achieved when all the SHES technologies are implemented in a temperate climate. However, the test was conducted at a smaller scale that did not cover the power needs of the entire camp of 150 personnel. In order to achieve full power provision 4 times as many PVs would be required or the addition of another source like wind power would need to be considered[59].

b. NATO

NATO has tested smart energy camp solutions since 2013.[60]

1. The NATO Energy Security Center of Excellence in Vilnius has developed and tested a prototype Hybrid Power Generation and Management System (HPGS)[61]

From 2016 to 2019 the NATO ENSEC COE obtained and tested a prototype HPGS. The HPGS is a deployable modular hybrid power generation system that is capable of producing up to 2500 kWh per day with 150 kW peak loads for the power needs of a camp of 100-150 personnel. The HPGS was designed to reduce power generators fuel consumption and to increase energy security in a military infrastructure via battery storage and MEMS. It also utilized renewable energy sources - sun and wind – reducing fuel consumption. HPGS operates as stand-alone generator system but can also integrate with existing power grid architecture.

[57] https://www.mdpi.com/1996-1073/13/9/2279?type=check_update&version=1
[58] https://www.mdpi.com/1996-1073/13/9/2279/htm
[59] This study did not use wind power as a renewable energy generation source.
[60] https://www.nato.int/cps/en/natolive/news_101896.htm
[61] https://www.enseccoe.org/data/public/uploads/2019/03/phase-1-report-hpgs-performance-analysis.pdf

The HPGS is a mobile energy generation and management system that combines the power from two diesel generators, solar panels and a wind mill. The system has lithium-ion battery storage and an energy management system which is configured to use renewable energy when available and only use the diesel generators when renewable energy cannot satisfy the power requirements. It's modular and can be deployed as a completely independent system or integrated with an existing energy generation infrastructure.

The basic configuration of the HPGS[62] consists of:

- 2 * 75kW diesel generators
- PV system 25 kWp
- Wind Turbine 6.5 kWp
- Lead-Acid Battery storage 100 kWh
- Mobile Energy Management System (MEMS)
- External Cooling/Heating Unit
- Transportable containers (ISO standard 2*20')[63]

Figure 9. NATO ENSEC COE test of HPGS during Canadian AF "Climate Trial" in 2019.[64] And during NATO Exercise Trident Juncture in 2019[65]

2. The NATO Science for Peace and Security (SPS) has a program NATO SPS G5525 that is investigating the application of smart energy technologies for military camps. The objective of the project is to find ways to "reduce the fossil fuel consumption – in fact – any wasteful energy consumption – in deployable camps."[66] It's current focus is on developing energy metering kits to aid in the collection of data for analysis of energy use at camps.

c. European Defence Agency has a program called Military Green, which is looking at the possibilities of applying smart grid and renewable energy technologies to the military. 6 EU

[62] https://cmea-agmc.ca/sites/default/files/doc20190528072400.pdf
[63] https://www.enseccoe.org/data/public/uploads/2019/03/phase-1-report-hpgs-performance-analysis.pdf
[64] https://cmea-agmc.ca/fr/node/8010
[65] https://www.enseccoe.org/en/newsroom/nato-ensec-coe-representatives-in-trident-juncture-2018-exercise-presenting-energy-efficiency-solutions/373
[66] From Martin Kegel's NATO SPS G5525 Milestone 2 & 3 Project Update during on-line project meeting on May 10, 2021

nations that include Hungary[67] are participating in the Military Green program.[68] MoD of Slovenia is leading an EDA project with EU funding called RESHUB or "Defense RESilience Hub Network in Europe"[69] which seeks to develop a renewable energy harvesting and hydrogen (H2) energy storage capability to improve cross-Europe transportation, which will lower CO2 emissions and contribute to energy sustainability in the EU defence and security sector. In addition the French have a program called ENSSURE which seeks to explore possibilities to improve the energy self-sufficency and resilience of military bases[70].

d. Others in Europe
    i. The Dutch army has a Fieldlab Smartbase, a military base where various renewable energy solutions are being tested[71]. One of them is a container-based systems that takes base waste water and converts it to drinking water and natural gas that can be used as a source of energy.[72] There is also a Green Energy Mill (GEM) Tower project which generates power from the wind[73].

Figure 10. Netherlands military transporting and delivering container with GEM system[74].

[67] https://www.smart-energy.com/regional-news/europe-uk/european-defence-agency-pushes-for-low-energy-military-ops/
[68] https://eda.europa.eu/docs/default-source/news/military-green-leaflet.pdf
[69] https://eda.europa.eu/news-and-events/news/2020/03/10/first-energy-consultation-forum-project-to-receive-eu-funding
[70] https://eda.europa.eu/docs/default-source/events/eden/phase-ii/information-sheets/cfii-wg-3-infosheet-military-camp-study.pdf
[71] http://www.gem-tower.com/digitaltour/
[72] https://xflow.pentair.com/en/news/dutch-army-tests-membrane-technology-in-afghanistan
[73] http://www.gem-tower.com/digitaltour/
[74] http://www.gem-tower.com/digitaltour/

Figure 11. Netherlands military setting up GEM wind tower at Smart BaseLab[75]

ii. The Fraunhofer Institute of Chemical Technology (ICT) has a pilot project called "RedoxWind" which is testing a smart grid solution that uses a 2MW windmill to power its campus in Pfinztal and employs a 20MWh redox flow energy storage solution to store excess power[76]. The Fraunhofer Institute is the biggest applied research (partner with industry, small to medium enterprises) organizations linked to 72 research institutes in Germany, works in applied electrochemistry, and advises e.g. German military on energy use questions. One of the most impressive achievements of the Fraunhofer ICT was to employ a working renewable energy and managed storage system based on redox flow energy storage technologies to supply the power needs of the entire ICT campus. A redox flow storage solution based on Iron Chloride electrolyte offers significant advantages for military basecamp applications due to its low toxicity, easy transport (electrolyte transportable in powdered from) and is in a modified version already being tested by the US Army Corps of Engineers

[75] http://www.gem-tower.com/digitaltour/
[76] https://www.ict.fraunhofer.de/en/comp/ae/rw.html

Figures 12 and 13. Fraunhofer ICS 2MW campus Windmill and part of integrated redox flow battery storage site[77]

6. Issues of cybersecurity for a smart grid powered military camp

A missing feature in the provided examples above of experimental projects integrating renewable power sources and prototype smart grid systems is the employment of cybersecurity in the design process. This is most unfortunate since the technologies used have exploitable vulnerabilities, which can be leveraged by an adversary to effect mission effectiveness. Cybersecurity measures should be part of the design process and not left for adding on later which can be a difficult and expensive process. One classic example of what can happen when security is added after a product is released is the Microsoft Windows Operating System where the manufacturer must issue new patches for discovered vulnerabilities every first Tuesday of the month[78]. Microsoft Windows was already widely used before Bill Gate's famous email about getting serious about security was sent in 2002[79].

The components of a smart grid were listed and discussed above. Their safe, reliable and efficient operations can be degraded or denied through traditional kinetic attacks. However, as the smart grid is made up of an integrated system of hi-tech components that communicate over a common network, the technologies and intelligent electronic devices (IED's) used can also be compromised and even destroyed using cyber means. A cyber-based attack can also be done stealthily and even after the attack, it may not be possible to determine the identity of the perpetrator.

S**ensors** for example **can be a single source of failure** that can severely affect the safe, reliable and efficient application of renewable energy and smart grid technologies. Sensors play a key role in smart grids. Sensor data sent to the controller needs to be trusted since the automated system or EMS will use this information to take actions to maintain system stability. The concern here is the compromise of the sensor or a malfunctioning sensor that sends bad data to the controller. For example, sun sensors are used in the operation of movable solar panels and wind direction sensors

[77] https://www.flowcamp-project.eu/?page_id=45
[78] https://en.wikipedia.org/wiki/Patch_Tuesday
[79] Delio, M., Gates Finally Discovers Security, Wired January 17, 2002 https://www.wired.com/2002/01/gates-finally-discovers-security/

help in pointing the windmill toward the wind. If the sensor itself or the data sent to the controller is compromised, it will affect the safe and efficient functioning of the system. The compromise can happen both unintentionally (maintenance issue) or intentionally (cyber issue). The various control systems and devices reporting to the EMS can be fooled into taking wrong actions in response anomalous events in the system, which can lead to degraded or denied system performance. A system failure can come by accident or through malicious intent. A well-known case of a non-malicious failure of a sensor leading to an error in the control systems which resulted in loss of life is the Boeing 737 Max air crashes of 2018 and 2019[80]. A bad sensor sent bad data to an automated flight control system[81].

Malicious actors can also intercept and change data from a sensor that can result in system malfunctions and damage to equipment. The STUXNET malware (further discussed below) that was planted on the control networks of a nuclear enrichment facility succeeded in disabling safety systems and sending false data to operators in the control room[82].

There are 3 fundamental questions that concern the cybersecurity of a smart grid for a mobile military camp: What to protect? From what threats? and How to protect identified assets from identified threats in the most cost effective way? It is important to answer them in sequence for any error in the analysis of the first and second will have an impact on determining the "how" or the policy implemented.

a. What is being targeted and how?

Since 2010, there are several examples in the public domain of cyber-attacks targeting industrial control systems[83] used to monitor and control physical operations found in the energy and other sectors of critical infrastructure. The most dangerous of these attacks have not been about just planting a computer "virus" or malware but instead focused on compromising the control logic of devices that monitor and control a physical process. Five examples will illustrate this: cyber-attack on a nuclear enrichment facility in 2010, the loss of operator view and control of a power grid in in 2015, attempt to compromise electrical relays of a power grid in 2016 and the attempt to compromise safety systems resulting in 2 shutdowns of a petrochemical plant in 2017.

Stuxnet 2010: STUXNET, the first state developed cyber weapon, that is a computer code capable of producing a physical/kinetic effects on the target device or system, used to attack the critical infrastructure (nuclear enrichment process) of another state, was in many ways a turning point in the security of cyberspace. Cybersecurity professionals began to understand that the most sophisticated cyber-attacks now extended to the engineering behind the technologies used to support the operations of critical infrastructure. The methods employed in this attack such as compromising the control logic of a program logic controller used to control a centrifuge, disabling

[80] Langewiesche, What Really Brought Down the Boeing 737 Max W. Sept. 18, 2019, Updated Jan. 9, 2021https://www.nytimes.com/2019/09/18/magazine/boeing-737-max-crashes.html

[81] https://www.bbc.com/news/business-50177788

[82] Langner, R., "To kill a centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve" , Langner Group 2013 https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[83] Industrial control systems (ICS) are mostly computer based, used by infrastructures and industries to monitor and control sensitive processes and physical functions. They collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. They are the hardware and software closest to the actual physical process: Remote Terminal Units (RTU's), Program Logic Controllers (PLC's), Actuators, Drives, Sensors, Safety Instrumented Systems (SIS) and Field Devices. Also known as Industrial Automation and Control Systems as defined by the International Society for Automation, https://gca.isa.org/hubfs/2129%20%20ISAGCA/ISAGCAIACS%20Taxonomy%20Definitions%20of%20Terms.pdf

safety systems, providing false data to operators about the physical process, manipulating and causing physical destruction of equipment to the great surprise of the control room personnel. In short using cyber means in order to take away operator view and control of a physical process[84].

Ukraine December 2015: Cyber-attack on a power grid succeeded in penetrating the Office IT of a utility providing electricity to customers in one of Ukraine's regions. From there after a period of reconnaissance, mapping and acquiring access privileges, they succeeded in acquiring operator view and control at the OT[85] level and proceeded to open breakers at over 30 substations. Over a ¼ of a million customers lost power in the winter just before the Christmas Holiday. The attackers planted malicious firmware on the serial port servers used to communicate between SCADA control and the remotely located affected substations causing them to become permanently disabled. In one instance the attackers were able to access and disable a backup UPS which eliminated a power reserve that could have been used in the recovery work[86]. The perpetrator just before ending the attack ran previously planted disk wiper malware attack on the workstations in the control room. With loss the hardware and software (SCADA) used for the view and control of the power grid the operator was left with no choice but to re-establish power and operations manually (sent engineers out to the substations to manually close the breakers and restore power)[87].

Ukraine December 2016: Partial blackout of the Ukrainian capital of Kyiv[88]. More sophisticated attack on the relays - devices which trip (disconnect the circuit) to protect bulk power and other critical equipment used to distribute electricity on the grid. While this cyber-attack was more limited in duration and scope then the previous year's attack, subsequent analysis showed this to be a more sophisticated and potentially far more damaging attack. The attempt made by the attacker to compromise the relays or the equivalent of a safety system to insure the safe and reliable operation of a power grid implied that one of the attackers goals was to make the operators option of restoring power through manual control a dangerous one. It is dangerous for in restarting power after a blackout any fluctuations in power would have caused damage to very expensive and hard to replace bulk power equipment such as a transformer if the relays were not there to perform their function[89].

Triton/Trisis/Hatman 2017: An attempt to compromise the safety functions of a petrochemical plant.

In June and again in August 2017, cyber-attacks targeted the Safety Instrumented Systems (SIS) of a large petrochemical plant in the Middle East.

---

[84] Langner, R., "To kill a centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve" , Langner Group 2013 https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[85] Special computer hardware and software (for example SCADA) used with the help of a human machine interface (HMI) to access and present data coming from IED's to the physical process.

[86] https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf

[87] Lee, R., Assante, M., Conway, T., "Analysis of the Cyber Attack on the Ukrainian Power Grid", SANS 2016 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[88] I have no evidence of weather being a contributing cause, however even if it was the malware that was discovered and discussed in the Dragos report (see footnote) was a significant malicious activity on the safety systems of the local power grid. Slovik, J., "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack", Dragos Inc. 2019. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[89] Slovik, J., "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack", Dragos Inc. 2019. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

The intentional attempt to compromise a safety system represents a serious escalation of the cyber threat to critical infrastructure. Control and safety systems are used in an industrial process to protect property, the environment and most importantly, people from serious harm resulting from an industrial process that has gone outside of set parameters. These parameters are used to program an automatic response in the SIS to bring a system back to a safe state when changes in frequency or other system state indicators exceed safe levels. These are the systems that automatically respond to open or close valves on a gas pipeline when pressures or flow rates go beyond pre-set parameters. The same systems such as relays which automatically disconnect expensive power equipment during a blackout. If something is done to intentionally neutralize the functions of these systems, serious harm can result if a system state exceeds set parameters. It is like disabling the breaks and seat belts of an automobile traveling down a highway without the knowledge of the driver. Nothing immediately bad will happen to the driver of the car but if there was a sudden need to stop or turn the steering wheel, the consequences could be most serious. In other words, safety systems are the last line of defence provided by automated technologies to save us from having to deal with something 'going boom in the night.'

What is of most concern[90] is that this attack almost succeeded in fully compromising safety-instrumented systems made by Schneider Electric. These and similar SIS devices by other manufacturers are used in many industrial plants around the world. If the perpetrators have developed a technique against the equipment of Schneider Electric, they can apply the same technique in any of the plants that use this or similar equipment. While the cyber-attack only worked on a specific version of the device and software, the potential escalation for disruption of Trisis is unsettling.[91]

One important point to mention is that the victim was unaware of the compromised state of their control systems. Even the manufacturer after the first shutdown in June found no fault with the equipment and returned it to the victim where it resumed its place in the plant's operations. The victim had no cyber forensics capability on site to investigate the incident but had to pay top dollar to bring in specialists from the outside. In short, **the industrial site had little or no cybersecurity capability** available to monitor and react to the first cyber intrusions, which took place months earlier.

SolarWinds-Orion 2020/2021: advanced persistent threat actor's entering the victim's supply chain to compromise a software company's network monitoring and control software.

SolarWinds software is used by many government, business and industrial enterprises around the world for network monitoring and management. Reminiscent of the Havex cyber-attack 6 years earlier, this was a more widespread, successful and highly sophisticated supply chain compromise affecting 18,000 organizations[92]. Many of these organizations work in industrial operations including the energy sector. What is of concern in this incident is that major original equipment manufacturers (OEM's) that supply on-line services to infected customers were also infected

[90] One other concern is the possibility of sophisticated (made by a state as in the Shadowbrokers case or by a security company such as FireEye) malware falling into the hands of cyber criminals and less skilled adversaries.
[91] Perlroth, N. and Krauss, C. "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try." *New York Times*. March 15, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html. Accessed July 15, 2018.
[92] SolarWinds Compromise and ICS/OT Networks Webinar Recording, Dragos Inc. December 22, 2020 https://f.hubspotusercontent10.net/hubfs/5943619/Webinar-Assets/Dragos%20webinar%20-%20SolarWinds%20Compromise%20-%20v10_KT%20%20-%20%20Read-Only.pdf

raising the potential number of compromised businesses and industrial operations[93]. What made this incident particularly insidious was that the vendor's supplied legitimate software update to the targeted Orion product was tainted with a malware that provided the attacker with a backdoor[94]. The customers' efforts to apply industry cybersecurity best practice (keep software patched and up to date) ironically only made matters worse. Analysis indicates that the initial infection of the vendor's Orion software occurred in the spring of 2020. Months before its discovery at the end of the year.

One other interesting outcome of this incident in terms of the available cyber capability found in industrial operations was the lack of such capability. Meaning that if an industrial operator became suspicious of a cybersecurity breach there was little means available onsite to determine the extent of the compromise. The operator had either to embark on a massive replacement of suspected IT equipment or hire a security firm from the outside to come in and do the diagnostic and clean-up work.

The above are examples of what the civilian energy sectors have experienced. However, **the military sector is of course also being targeted from cybersp**ace and has experienced disruptions to operations.

As far back as 2009 it has been reported that French and British military aircraft were grounded due to a computer virus infection in the flight planning systems.[95] This occurred during outbreak of the Conficker virus, which computers using the Microsoft OS and spread throughout the world causing great concern for the functioning of government and military networks[96].


HOME » NEWS » WORLD NEWS » EUROPE » FRANCE

French fighter planes grounded by computer virus

French fighter planes were unable to take off after military computers infected by a computer virus, an intelligence magazine claims.

French fighter jets were unable to take off after military computers were attacked by a virus Photo: AFP

by Kim Willsher in Paris
11:43AM GMT 07 Feb 2009

The aircraft were unable to download their flight plans after databases were infected by a Microsoft virus they had already been warned about several months beforehand.

At one point French naval staff were also instructed not to even open their computers.

France
News » Wor
Europe »

Related Part

The best way
money overse

In France

Calais Jung
evictions, ir

Eagles of D
in concert

Figure 14. Military aircraft are vulnerable to threats from cyberspace.

[93] Zetter, K., "SolarWinds Hack Infected Critical Infrastructure, Including Power Industry", The Intercept December 24 2020 https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/

[94] Schneier, B., "The US has suffered a massive cyberbreach. It's hard to overstate how bad it is", The Guardian, Dec 23, 2020 https://amptheguardiancom.cdn.ampproject.org/c/s/amp.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols

[95] https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html

[96] Bowden, M., Worm: The First Digital World War, Grove Press 2012.

In 2018 a US Government report noted that its newly developed Stryker-Dragoons and Stryker CROWS combat vehicles "experienced select degraded capabilities by adversaries when operating in cyber contested environment."[97]

What is behind the increasing cybersecurity risks to implementing an energy solution based upon renewable power and the smart grid?

First it should be remembered that power grids provided power to people long before the arrival of the Internet. However, the improved functionality of today's power grids and the devices and control systems used also come with significant risks arising from:

- Increased automation and complexity of the grid through the employment of the latest advances in information, communications and process control technologies also introduces new vulnerabilities that can cause accidental failures as well as being exploited by an adversary;
- Interconnected networks of systems and devices can introduce common vulnerabilities;
- Increasing vulnerabilities to communication disruptions and the introduction of malicious software/firmware or compromised hardware (via compromised supply chain) could result in denial of service (DoS) or other malicious attacks;
- Increased number of entry points and paths are available for potential adversaries to exploit;

The use of the hardware and software used to operate and manage smart grid and renewable technologies also comes with additional risks from compromised supply chains. Risks include the compromise of electrical power equipment when it is manufactured[98] and later during the various stages in shipment to the customer[99]. Software/firmware updates provided by the manufacturer have also been targeted by adversaries as recently demonstrated by the recent SolarWinds-Orion software compromise[100]. Similar compromises have occurred with other manufactures and in other countries[101]. Another threat of interest to the military is Electronic Warfare (EW) which can be used to degrade or disable electronic equipment.[102]

b. Who are the threat actors?

The most likely attacks are perpetrated by knowledgeable insiders and, less frequently, by sophisticated nation states. Insiders will always be a threat and the military has not been immune to espionage and personnel problems in its ranks. It can happen with disgruntled personnel; it can happen with contractors who felt they were cheated. There are enough reasons that it is the most commonly seen attack against infrastructure.[103]

Another worrisome trend is the increasing pervasiveness of "ransomware" attacks, where the software and data in a control system is silently encrypted and then the key to the encrypted system

---

[97] http://scid.infracritical.com/pages/scid-00093/

[98] https://www.forbes.com/sites/llewellynking/2021/01/28/how-the-supply-chain-in-heavy-bulk-power-equipment-is-vulnerable-to-undetected-cyberattack/?sh=d7dfa907213a

[99] https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

[100] https://www.securityweek.com/solarwinds-says-18000-customers-may-have-used-compromised-product

[101] Happened in France, see: https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-005/

[102] ELECTRONIC WARFARE TECHNIQUES, U.S. Army , ATP 3-12.3 July 2019, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18105_ATP%203-12x3%20FINAL%20WEB.pdf

[103] For more on problem of insider threats see: Marcel, G., Insider Threats as the Main Security Threat in 2017 , Tripwire Apr 11, 2017, https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/

is held for ransom. Until the ransom is paid, the system data is not accessible. To date, although there have been cyber intrusions and incidents on windfarms and other renewable energy technologies[104], there have been random ransomware cases with ICS[105], no publicly known ransomware has been specifically designed to target an industrial control system. However, the ransomware attack that took place at Norsk Hydro, an aluminum manufacturing company with connected operations (spanning 40 countries operating at 170 sites with 22,000 computers affected (22,000 computers were hit across 170 different sites in 40 different countries) caused significant disruptions in its industrial operations to the point of returning to paper documentation to run manufacturing operations[106]. The initial cost so far of "going to manual control" has reached over 45 million EUR.

However, simply causing "cyber fear" can be an effective tactic of the attacker. Witness the responses of some industrial sites that for safety reasons chose to close or reduce operations to check for malware in the aftermath of the WannaCry,[107] NotPetya[108]malware and most recently in shutdown of an 8000 km long oil pipeline in the US after ransomware appeared on their office IT networks[109]. While in most cases no malware was found but in others the sites (such as Maersk loss of 300 M. EUR) incurred real financial damage (some of it collateral and not the result of a targeted attack on the company) from NotPetya to industrial operations. This only reinforces the need to be aware of what is going on beyond our "operational perimeter" and share information with a trusted community of interest to reduce fear-based actions. We need to monitor what is going on in the control network, to know for sure that the "crown jewels" are safe.

If good backups are available that have not been infested with the ransomware then the system can be restored, without the recent history since that backup was made. However, many of these attacks are devious in that they lurk on the computers for many weeks or even months. Many patches and configuration changes may have been made in the interim. If there is no one monitoring for signs of intrusion or unusual activity then the execution of an attack when it comes will be a complete surprise as it was for example to Norsk Hydro or that petrochemical plant in Saudi Arabia where investigators looking into the causes of plant shutdowns discovered alien software in the safety and control systems[110].

It is the state or state-sponsored adversary also known as the Advanced Persistent Threat (APT) which has the potential to be the most effective in terms of resources that can be applied and the amount of harm to property, environment and human life that can result. Up till this time while there have been some publicly known cases of successful APT attacks resulting in significant disruption and damage to critical operations most of the activity is focused on stealthy reconnaissance, probing, and intelligence gathering that can be used for the purposes of espionage or in planning a successful attack. One unsettling trend is the experimentation being done on using cyber means to cause physical damage. This first appeared in the STUXNET attack on a nuclear enrichment facility reported in 2010, the attempt to disable relays in attacks against Ukraine's

[104] Greenberg, A., Researchers Found They Could Hack Entire Wind Farms, Wired, 06.28.2017 https://www.wired.com/story/wind-turbine-hack/

[105] Wattles, J, Who got hurt by the ransomware attack WannaCry? May 14, 2017 http://money.cnn.com/2017/05/13/technology/ransomware-attack-who-got-hurt/

[106] Tidy, J., "How a ransomware attack cost one firm £45m", https://www.bbc.com/news/business-48661152 25 June 2019.

[107] Sherr, I., WannaCry ransomware: Everything you need to know, May 19, 2017 CNET. https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

[108] Greenberg. A., The untold story of NotPetya, the most devastating cyber-attack in history", Wired, 08.22.18 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/amp?__twitter_impression=true

[109] Nakashima, E., Yeganeh, T., Englund, W., "Ransomware attack leads to shutdown of major U.S. pipeline system" , May 8, 2021, https://www-washingtonpost-com.cdn.ampproject.org/c/s/www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/?outputType=amp

[110] See references to Triton\Trisis malware in Appendix 2

power grid in 2016 (using CrashOverride attack tool)[111] and attempts to manipulate safety instrumented systems at a petrochemical plant in 2017 (Triton attack).

The ransomware threat is evolving with cybercrime groups of increasing sophistication and skills focusing on disruption of critical infrastructure. The "Dark Side" cybercrime group that executed a ransomware attack on the Colonial oil pipeline in the United States which resulted in the operator shutting down pipeline operations in May of 2021 is a troubling trend[112]. While the cyber-attack focused on the IT systems, the fear generated caused the operator to take precautionary measures to ensure the attack did not jump across the office IT side to the physical process side of pipeline operations. Groups like the "Dark Side" in seeking financial gain from their chosen victim are likely to be more reckless in the actions then perhaps the careful considerations a state actor may take before executing such an attack. If this trend continues to develop the cybercrime threat may eclipse the more sophisticated and resourced threat posed by a state actor as the most dangerous of threats emanating from cyberspace.

Finally, there is the possibility of terrorist use of cyber weapons to cause a physical disruption of the controlled process leading to some physical effect. However, while terrorists have targeted critical energy infrastructure in the past these attacks have mostly been performed using kinetic attacks (bombs) with cyber means being limited to information gathering and propaganda. However, the possibility of ideologically or religiously motivated cyber terrorism developing in the future cannot be discounted [113]

Nevertheless, the point is to design a secure system that can deal with the more likely threats and still allow enough flexibility to adjust to changes in the cyber threat environment[114].

c. Motives for attacking smart grid technologies used at mobile military camps

One should never discount the possibility of one becoming a target. Especially from a threat actor hostile to NATO and/or Alliance member coming from a state or receiving its support. The APT threat actor does not stop when encountering a defensive measure. If the "wall is too high" it will find a "taller ladder" or find a way around the back. Application of smart grid technologies can significantly contribute to the successful energy independent functioning of military camps. These technologies therefore offer the adversary an attractive and important target for the following reasons:

- To contribute to service disruptions of dependent command, control, communication and intel systems that require a source of power to operate;
- To disrupt the energy supply just when the adversary does something they know will draw a military response from the camp;
- To show that they can do bad things in order to intimidate;
- To sow fear, uncertainty and doubt (FUD) that disrupts well-being and trust in the unit's safety and effectiveness;

[111] Slowik, J., CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf , Dragos, Inc. August 2019

[112] Hoffman, M., Winston, T., Recommendations Following the Colonial Pipeline Cyber Attack, Dragos Accessed June 2, 2021. Cyber Attack: Recommendations Following the Colonial Pipeline Ransomware Attack (dragos.com)

[113] Gucuyener, A., Cyber terrorism and energy security, perConcordiam V8N4 2018, pp.58-61. http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pc_v8n4_en.pdf

[114] For more on the relationship of system, threats, and developing appropriate security strategies read: http://scadamag.infracritical.com/index.php/2018/02/21/towards-cyber-safe-critical-infrastructure-answering-3-questions/

- Economize on offensive assets, cyber weapons are reusable while physical (bombs and humans) are not. One example of this is when in September of 2007 the Israeli Air Force penetrated Syrian airspace to bomb a suspected secret nuclear facility. One of the most sophisticated air defense systems in the Middle East apparently failed to record or deter the violation of its airspace and bombing on its territory. This aroused some suspicion on the part of aviation and security experts. Later that year[115] reports surfaced alleging that Israel used a cyber-attack to confuse or disable Syrian air defenses[116].
- Use of cyber means as a first step[117] in a combined attack with kinetic means or nearly simultaneously[118];
- Using disruptive cyber tools is a very attractive option as it is effective, cheap (for a state or state sponsored adversary), and most importantly, deniable malicious activity to achieve a desired military objective.

7. Specific cyber threats to military camps using smart grid technologies

An important task in designing a smart grid is making sure that user requirements for electric power quality and reliability (PQR) are met[119]. For a military camp, the PQR is quite high and there are significant challenges that include control of power flow, voltage and frequency balance[120]. The smart grid while more decentralized than a traditional power network is a complex and dynamic system. The integration of renewable energy sources, traditional power generation and storage in an interactive self-healing network comprised of a wide variety of respective intelligent electronic devices (IED) provides attractive functionalities but also significantly broadens the potential sources of failure and exploitable attack surfaces. The following is a list of possible attack vectors and sources of failure found in a smart grid environment:

a. Cyber intrusion to control network

IED's, power generating equipment and associated devices interact and exchange information on a common computer network. If a malicious actor were to succeed in obtaining access and gaining administrator privileges on that network, the connected devices will be put at risk. Sensors which send information to the control system do not have any security protections on them and if visible on a network can be compromised.

b. Compromise and hostile manipulation of EMS to cause damage

---

[115] David A. Fulghum, Robert Wall and Amy Butler, „Israel Shows Electronic Prowess", Aviation Week, Nov 25, 2007 http://www.aviationweek.com/aw/generic/story.jsp?channel=defense&id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess&next=30

[116] David Eshel, „Cyber-Attack Deploys In Israeli Forces", Aviation Week, September 15, 2010. http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/dti/2010/09/01/DT_09_01_2010_p42-248207.xml

[117] Fulghum, D., Barrie, D., Israel used electronic attack in air strike against Syrian mystery target, ABC News, 8 October 2004 https://abcnews.go.com/Technology/story?id=3702807&page=1

[118] Shakarian, P., The Russian Cyber-Campaign Against Georgia, Military Review, January 2011, https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia

[119] Hlalele, T., Sun, Y., Wang, AZ., Faults classification and identification on Smart Grid: Part-A Status Review, 2nd International Conference on Sustainable Materials Processing and Manufacturing, 2019. https://www.sciencedirect.com/science/article/pii/S235197891930722X

[120] Marnay, C., Zhou, N., Qu, M., Romankiewicz, J., Lessons learned from microgrid demonstrations worldwide, Berkeley lab, January 2012. https://www.osti.gov/servlets/purl/1210908

Since the EMS monitors and control all the devices and equipment of the smart grid any compromise of the EMS could have the most severe of consequences for the safety, reliability and performance of the system. In addition to the EMS there are sub systems that manage the battery storage, local generators, and solar panel array which can also be compromised and damaged through unauthorized access.

c. Through the supply chain

The electronic components of a smart grid system operate with software for applications and firmware on devices that require frequent security and performance updates and patches supplied by the manufacturer. The attacker has been able to defeat the users cybersecurity defenses by poisoning the software and firmware provided directly from the manufacture's web site.

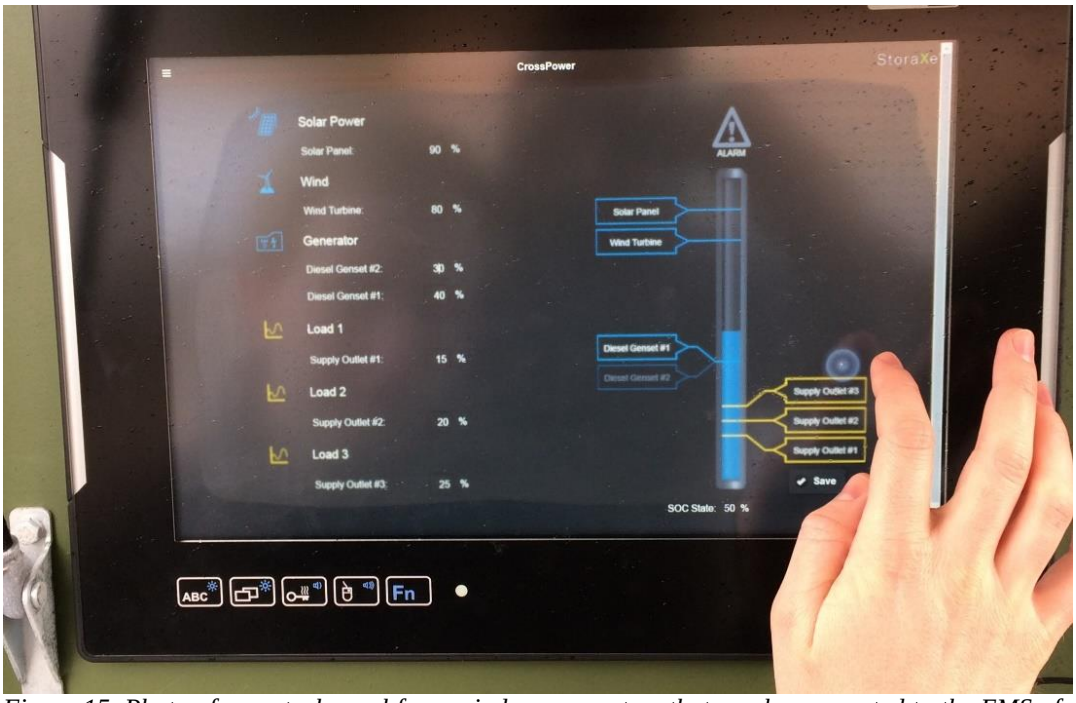


Figure 15. Photo of a control panel for a wind power system that can be connected to the EMS of a smart grid in a camp. The HMI is software that presents information about operations and easy access to the devices monitoring and controlling the equipment. Unauthorized access to this panel for malicious purposes or human operator error can lead to service disruptions of damaged equipment.

d. Insider threats

One of the most dangerous threats to smart grid operations comes from trusted personnel in the camp itself that has physical access to the system. This includes operators of the system, those that maintain it and those that can come in close proximity to the equipment.

Figure 16. Access of maintenance and other local personnel to EMS and associated equipment requires strict control

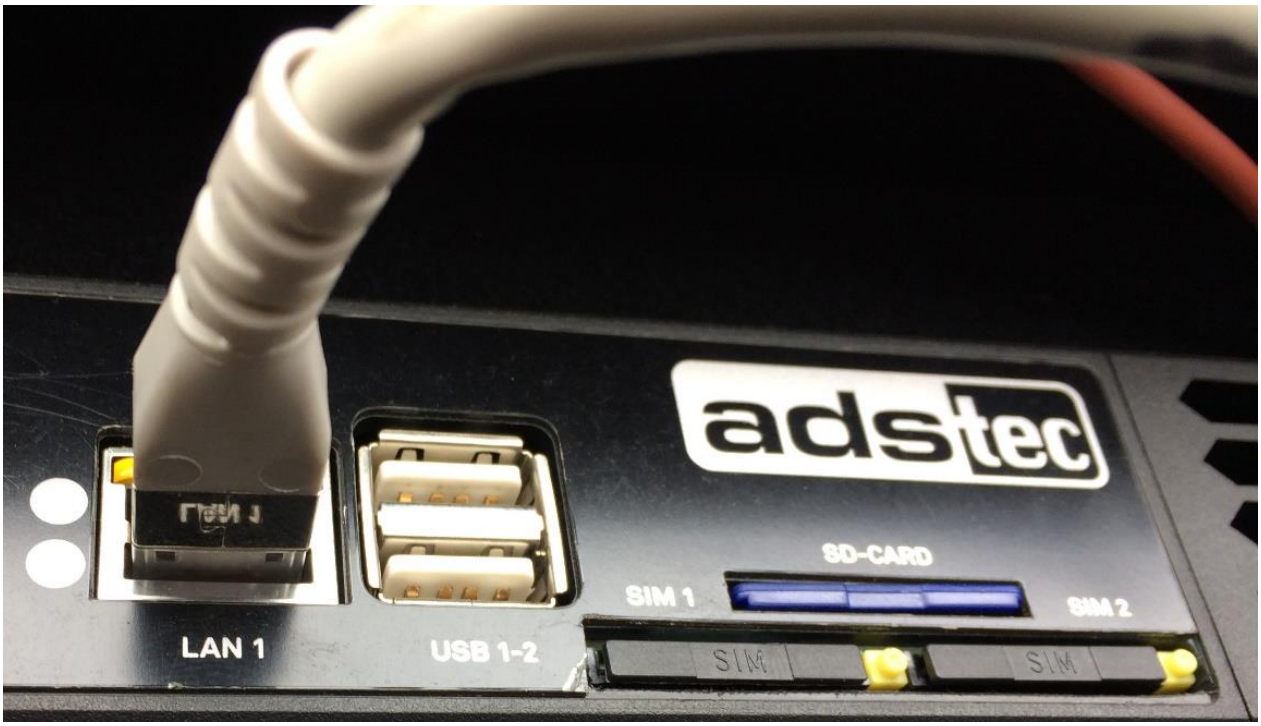


Figure 17. This photo from an energy storage (lead-acid battery container) control panel represented are several threat vectors that could arrive externally or internally that can be used to compromise safe, reliable, efficient operations of a smart grid: network access through unauthorized use of the LAN, USB sticks, GSM Sim Cards, SD memory cards.

8. Initial recommendations to introduce a smart grid solution for a military camp that will improve safety, reliability and resilience.
   a. In terms of resilience and interoperability for multinational operations, employ common system design life cycle methodology that take into account cyber risks. PERA[121] and ISA/IEC 62443 offer good approaches that include cybersecurity.

   The most important security decisions made that will be influence whether the project will be successful is at the very beginning of the project. Cybersecurity considerations that keep in mind what has to be protected and from what threats must play an integral part of the system design and its architecture. If they are added later after the system has been designed, tested and delivered, it will be a most difficult process to bolt on security to a complex system of diverse components.

   b. Start with a risk assessment (what to protect, from what threats, what measures to mitigate risk).

Coordinate with other parts of the defense system to select a standard framework for security risk assessment. The assessment should not be guided by just office enterprise IT standards like ISO 27001 which focuses on information management[122] but rather address the peculiar security requirements of process control or industrial control systems. There are several to choose from and they all have different levels of detail. Two examples that would apply to smart grid camp operations are: Process Hazard Analysis (PHA) and Consequence-driven Cyber-informed Engineering (CCE)[123]. It is important however to include cyber risks in the PHA which have not been done in traditional PHA's. The goal would be to achieve and maintain a common "baseline" level of cybersecurity among all camps to avoid any "weak links in the chain" that can affect the safety and reliability of smart grid operations. Two important standards are the Industrial Society for Automation's (ISA) 62443 standard on Automation and Control System Cybersecurity[124] (see Appendix 3) and ISA-TR84.00.09-2017 Cybersecurity Related to the Functional Safety Lifecycle[125].

Conduct a formal Risk assessment considering networks, processes, staffing, costs, and cybersecurity policies with a focus on the assets behind the firewall. Since many security efforts appear to be focused on the "protecting the perimeter" the assessment should be focused on protecting the smart grid control network and IED's in operation behind the firewalls. Firewalls are very good at keeping out bad things from the outside but will not be much help if something bad has already made its way to the smart grid or operations zone.

   c. Employ relevant smart grid standards

Standards to guide the design and development of a smart grid solution for a military camp are available. The system designer and integrator should be required to consult and apply them. A sample of the relevant standards are listed below:

---

[121] http://www.pera.net/Pera/PERA_Guide/PERA_Guide.pdf
[122] https://www.iso.org/isoiec-27001-information-security.html
[123] The two approaches are discussed in this video. https://www.linkedin.com/posts/dale-peterson-a5b21011a_consequence-based-ics-risk-management-activity-6575057871917191168-X0II Also see Annex for a brief visual description.
[124] See Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems, https://gca.isa.org/isagca-quick-start-guide-62443-standards
[125] https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f

1. IEC 61850: core standards for the smart grid
    i. IEC 61850-7-420:2009 Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes[126]
2. IEC 61400-2:2013 Small wind turbines[127]
3. IEC, IEEE, UL[128], NREL[129] and ASTM standards for Photovoltaic Systems[130]

d. System architecture

Work toward developing a robust and resilient system architecture that recognizes the differences in the roles data and information play in smart grid system between the information technology and operational technology (where the physical process is) parts. Best efforts should result in a design where a failure on the enterprise of Office IT side do not spill over and hurt the the operational side. Operational technology is defined as:

Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events and the applicable procedures performed by personnel (e.g. engineering, operations, maintenance) to operate and maintain with the purpose of safe and secure operation[131].

An example of where robustness and resilience of a system can be enhanced are in the way sensors are applied. Sensors play an important role in PV panels and in windmills. Extra redundant sensors (sometimes only one is used) should be included in the design for sun and wind sensing so a single failure in one sensor can be detected and compared with the other sensor to ensure accurate data is being sent to the control system.

e. Develop a prototype system for testing

It would be useful to start with a pilot system for learning and testing purposes before designing an operational system used for other camps. There are opportunities for partnerships with other militaries exploring the same questions and benefitting from lessons learned that have been already produced. Some of these were discussed above in section 5.

f. Establishing on-site support and maintenance capacity

Ensuring that the system is maintained and managed effectively will require the formation of a new unit with personnel trained in working with the new technologies employed. Traditional communication background will need to be supplemented with training in operating an energy management system and in troubleshooting. Adding this capability will require an additional investment of resources for equipment and specialist training. For suggestions on the role and responsibilities of a cybersecurity operations center or for a smaller operation where this work is assigned to one or two personnel are found in the Annex section (Appendix 4) of this report.

[126] https://webstore.iec.ch/publication/6019
[127] https://cdn.standards.iteh.ai/samples/17450/e5cae286e9db41acbba3fa476e735833/IEC-61400-2-2013.pdf
[128] https://www.ul.com/news/international-safety-standards-photovoltaic-modules
[129] Cybersecurity standards specific to PV are found at this site https://www.nrel.gov/docs/fy21osti/78768.pdf
[130] List of relevant standards in available on this site. https://www.usaid.gov/energy/powering-health/technical-standards/photovoltaic-systems
[131] ISA-TR84.00.09 Cybersecurity Related To The Functional Safety Lifecycle,

g. Explore option for interaction of military smart grid with civilian power systems

While increasing the level of system complexity in further adding equipment and maintenance costs, the option of supplementing power needs by accessing power from a local utility and even being able to sell power back to the local utility would be advantageous.

9. Conclusion

The military has a good set of conditions for developing a variety of advanced, "smart" technologies centered on “green’ electricity generation, storage and delivery. It’s capacity to innovate with fewer layers of stakeholders than what is found with public utilities is a distinct advantage. The technologies offer several advantages and provide attractive functions which can reduce the requirements and dependency on fossil fuels to power military camps. However, as has been noted in the prototype systems being reviewed in this assessment, cybersecurity does not seem to be a priority. It would be most unfortunate if this missing element of cybersecurity would become apparent only after some mission failure caused by an outage at a critical moment. It must be kept in mind in developing these new systems that the technologies can both enable the user to do wonderful things or could be used against them by an adversary to disable them.

These risks however can be managed effectively through the application of available best practices that insure that the smart grid camp systems are developed and implemented in a safe, reliable and sustainable way.

10. Acknowledgements

The author would like to thank the following industry professionals for sharing their deep knowledge and experience in the cybersecurity of industrial control systems, smart grids and renewable energy technologies:

Agustin Valencia Gil-Ortega
Jake Brodsky
Joe Weiss
Gary Rathwell
Ray Parks

Special thanks to NATO ENSEC COE Deputy Director, LTC Christophe Nave of the Armed Forces of France for his valuable support.

Vytautas Butrimas
NATO ENSEC COE
2021-08-11
Vilnius

MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

The 16th of October 2020

General Staff Headquater
Energy Policy and Foresight Analysis Branch
Operational Energy Department

POC : Mme. Noemie Rebière
Noemie.rebiere@intradef.gouv.fr

REQUEST FOR SUPPORT TO THE NATO ENERGY SECURITY CENTER OF EXCELLENCE.

The French Ministry of the Armed Forces recently developed a new defense energy strategy. One of the pillars of this strategy is the development of advanced technological solutions to reduce dependence on fossil fuels in order to increase operational performance and energy resilience. To this end, the ENSEC NATO COE is requested to conduct an assessment on the cybersecurity of the *smart -grid* of an operational camp.

Assessment of the Cybersecurity of an operational camp's smart grid.

The future of energy support for operational camps will combine:

- Different sources of energy for electricity production (diesel generators, renewable energy sources, etc.) and energy/electricity storage systems (fuell cells, batteries),
- Different types of energy consumers (human support, IT, heating ventilation, air, conditioning (HVAC), hybrid vehicles ...),
- An efficient and secure electricity T&D network,
- A real-time information network of all energy-related data,
- A Security Operation Center/Security Information Management System to monitor and control physical processes taking place in the smart grid (in order to monitor and check on anomalous Process Flows, Equipment Performance, and Data Flows with a goal of detecting a cybersecurity breach within 24 hours),

1/2

- An appropriate and secure system for storing and processing this data in order to effectively, efficiently and appropriately manage the energy system of the camp.

A solution to ensure improved safety, reliability, security and performance of the smart grid's SCADA supporting the operational camp.

- A solution for operators training and maintenance to reduce costs of ownership and improve resilience.

This *smart grid* of the future, however, creates a new risk attached to the information system.

Data related risks : This will bring together a mass of sensitive and confidential data, as it will provide information on the camp operational activity, energy supply and organization. Thus, the adversaries could use these data in order to neutralize the camp operations, for example in identifying specific critical areas within the camp to attack them.

It is therefore necessary to make an inventory of the data that will be available and identify the potential vulnerabilities in their storage (on-site data center and/or cloud) system, in order to anticipate solutions that will guarantee their protection (e.g. encryption).

Risks on physical integrity of energy systems : On the other hand, besides data-related issues, the technologies used to operate the smart grid (Industrial control system) can also be targeted resulting in service degradation, equipment damage and broadly loss of life (even indirect) or harm to the environment. Thus, the adversaries could disrupt the physical processes involved with the generation, storage and distribution of power along the grid and also degrade or neutralize camp operations. It is therefore necessary to apply best industry practices and industrial standards (e.g. ISA 99 for SCADA) to ensure the cyber security, safety and reliability of the smart grid technologies and control systems.

Request :

To this end, an evaluation report will be provided describing what needs to be protected, from what threats and recommendations on how to protect identified smart grid assets from foreseeable threats.

A quarterly situation update will be carried out with the French Armed Forces General-staff / Operational Energy Department that include information technology and industrial control system engineering specialists.

Appendix 2

Assessment study of cybersecurity of smart-grid technologies employed in operational camps

Meeting minutes

Prepared by Vytautas Butrimas (NATO ENSEC COE)

Location:	On-line via MS-Teams
Date:	20 January 2021
Time:	13:00 CET/14:00 EET
Attendees:	NATO Energy Security Center of Excellence (DDIR Col. Christophe Nave , Research and Lessons Learned Division Dr. Col. Reiner Zimmermann, Vytautas Butrimas)
	Ministère des Armées General Staff HQ, Energy Policy and Foresight Analysis Branch, Operational Energy Department (Nicolas Mazzucchi, Noémie Rebière)

Agenda items

Who is the target audience?

The main audience will be decision makers at the General Staff HQ. However, the audience may also be useful to lower level specialists and those tasked with developing system specifications.

What are the expectations for this project?

This work will result in an evaluation report and recommendations for implementing a smart grid solution for the safe, reliable and efficient use at a military camp.

What kind of military camp will be the object of the study?

A stationary camp from 200 up to 1000 personnel, which with some preparation can change to a mobile or forward operational basecamp. The camp may also use other energy technologies in an integrated way such as renewable energy generation, energy storage (redox, fuel cells), vehicle to grid, energy island operation with the option to interact with the national grid, solar, wind, ganging generators (link to control as a single unit) and for monitoring and control.

Will travel be required to perform this study?

It is not a required although one possible trip to France (according to an invitation from the Ministère des Armées) is feasible to formally present study findings to the General Staff HQ.

Research scope of the study?

The project will survey non-classified information about current best practices in applying smart grid technologies to modern military camps currently in use in NATO and partner countries.

Points of contact

For NATO ENSEC COE: Vytautas Butrimas, Reiner Zimmermann, Christophe Nave

For French General Staff HQ: Nicolas Mazzucchi, Noémie Rebière

Other support required?

NATO ENSEC COE will provide additional support as is appropriate for performing the study

French General Staff HQ will provide additional support as is appropriate for performing the study. Some of this support may include providing unclassified information about local energy policies, standards, and regulations.

Working language?

The study will be conducted, the final report and all written materials will be presented to the French General Staff in the English language

Method of work?

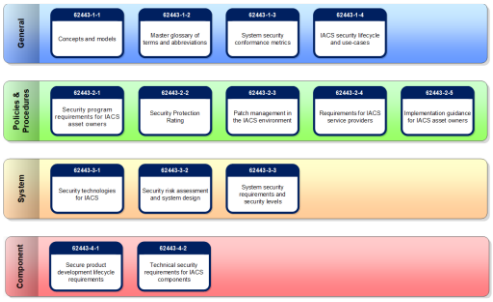
NATO ENSEC COE will provide drafts of the work in progress to the French General Staff PoC's for review and comment before officially presenting the Study to the General Staff. Technical/engineering information should be presented at a level appropriate to a non-technical audience.

Term for submission of the study?

Summer of 2021 (NLT August 2021)

Action items	Owner(s)	Deadline	Status
Minutes of the Meeting	Vytautas Butrimas	January 22	Complete
Draft outline for review	Vytautas Butrimas	January 29	in progress
Relevant study material (in English) about French energy policy (regulations, standards, strategies, law)	Nicolas Mazzucchi, Noémie Rebière	February 22	In progress

ISA/IEC 62443 Industrial Automation and Control System Cybersecurity Standard[132]



Graphic reproduces with permission of the International Society for Automation

1. General – This group includes documents that address topics that are common to the entire series.
• 62443-1-1 introduces the concepts and models used throughout the series. The intended audience includes anyone wishing to become familiar with the fundamental concepts that form the basis for the series.
• 62443-1-2 is a master glossary of terms and abbreviations used throughout the series.
• 62443-1-3 describes a series of quantitative metrics derived from the foundational requirements, system requirements and associated.
• 62443-1-4 provides a more detailed description of the underlying life cycle for IACS security, as well as several use cases that illustrate various applications.
2. Policies and Procedures – Documents in this group focus on the policies and procedures associated with IACS security.
• 62443-2-1 describes what is required to define and implement an effective IACS cyber security management system. The intended audience includes end users and asset owners who have responsibility for the design and implementation of such a program.
• 62443-2-2 provides a methodology for evaluating the level of protection provided by an operational IACS against cyber-security threats and how to apply what is required by 62443-2-1.
• 62443-2-3 provides guidance on patch management for IACS. The intended audience includes anyone who has responsibility for the design and implementation of a patch management discipline.
• 62443-2-4 specifies requirements for suppliers of IACS systems and related components. The principal audience include suppliers of control systems solutions. This standard was developed by IEC TC65 WG10.
• 62443-2-5 provides guidance on what is required to operate an effective IACS cyber security management system. The intended audience includes end users and asset owners who have responsibility for the operation of such a program.
3. System Requirements – The documents in the third group address requirements at the system level.
• 62443-3-1 describes the application of various security technologies to an IACS environment. The intended audience includes anyone who wishes to learn more about the applicability of specific technologies in a control systems environment.
• 62443-3-2 addresses security risk assessment and system design for IACS. This standard is primarily directed at asset owners or end users.
• 62443-3-3 provides the foundations for assessing the security levels provided by an automaton system. The principal audience include suppliers of control systems, system integrators and asset owners.
4. Component Requirements – The fourth and final group includes documents that provide information about the more specific and detailed requirements associated with the development of IACS products.
• 62443-4-1 describes the derived requirements that are applicable to the development of products. The principal audience include suppliers of control systems products and of components included in control systems solutions.
• 62443-4-2 contains sets of derived requirements that provide a detailed mapping of the system requirements to subsystems and components of the system under consideration. The principal audience include suppliers of components embedded in control systems solutions.

[132] "The ISA-99/IEC 62443 standard is the worldwide standard for security of the Industrial Control Systems in the Operational Technology (OT) domain of organizations. The standard was created by the International Society of Automation (www.isa.org), a leading worldwide nonprofit organization. The standard offers organizations handles to improve the digital security and safety of their process and SCADA environments. Implementation of the standard brings your organization to a higher level for security of the OT domain, the process or production environments." The ISA-99/IEC 62443 standard is derived from the ISO/IEC 27000 series standard and fully adapted with the focus on Industrial Control Systems environments. https://isaeurope.com/iec62443/

Appendix 4

Tasks of an Industrial Security Operations Center. (ISOC)

- Monitor and check on anomalous Process Flows, Equipment Performance, and Data Flows with a goal of detecting a cybersecurity breach within 24 hours*. Identification and recording of all the component pieces and versions in a control system
- Review available patches and updates of OT devices found closer to the industrial process such as PLC's and other intelligent electronic devices (IED)
- According to configuration, change management and safety procedures test and apply selected patches and updates
- Responsibility for monitoring control and safety system cybersecurity vulnerabilities
- Monitoring the current patch levels, malware notifications, and newly discovered vulnerabilities as announced by cybersecurity institutions and by vendors
- Take part in regular training and education on ICS cybersecurity including attendance at organized ICS security conferences and trainings such as S4, DEFCON, and Black Hat
- Participation (sending at least one staff person or more per year) in NATO, EU and other tabletop and "Live Fire" exercises such as "Locked Shields" where cyber-attacks on control systems are included in the scenarios.
- Implementing the recommendations in this report that are beyond the means of current staff capabilities and resources
- Operation of network management system, Intrusion Detection, or Security Information and Event Management (SIEM) system
- Use of internal operating system health tools that can be used in both an investigative and in a forensic capacity to identify source of a problem
- Organize and control use of A/V scanning based solution according to established policies and procedures.
- Conducts and/or organizes (in keeping with established industrial safety requirements) with help of vendors with Certified Ethical Hackers full offline black box and white box penetration testing against the switches, routers, firewalls, controllers and instruments that the operator uses.
- Use of available tools, such as Metasploit, where one can use benign attack scripts to prove the existence of a device vulnerability in an automated fashion. This way one can demonstrate a conceptual attack on a test bench without damaging anything
- Operation of a security test lab. This should be used to validate patches before deployment, to test security exploits on existing equipment and firmware, and to find and diagnose other bugs and test code before downloading it to the field
- Ensure that user log-ons to the system and IED configuration changes are documented, updated and made available on-site for operations personnel.

*After 24 hours the chances of discovering an intruder who is actively seeking to establish a stealth presence and cover tracks will drop considerably.