The AURORA vulnerability: The sword of Damocles over the heads of rotating machines

MARC POTVIN, P. Eng.
BBA Inc.
Canada

SUMMARY

AURORA is the acronym for "Avoiding Unwanted Reclosing On Rotating Apparatus" and is used in the electrical field. The AURORA vulnerability refers to the likelihood of damage to rotating electrical equipment resulting from a brief disconnection from the electric power grid, followed by a rapid out of phase reconnection to the power grid. Upon reconnection, large torques are applied to the rotating shafts and gearboxes.

After the US Department of Homeland Security (DHS), the North American Electric Reliability Corporation (NERC), and the Electricity Information Sharing and Analysis Center (E-ISAC) were made aware of the AURORA vulnerability in February 2007, it was tested and demonstrated on a diesel generator in March 2007 at Idaho National Laboratory. The objective of the AURORA generator test was to demonstrate the possibility that a cyberattack could cause physical damage to rotating equipment.

At that time, the damage to physical assets resulting from a cyberattack was still very hypothetical, and people remained skeptical. The unequivocal results of the demonstration sparked media attention when CNN publicly released them in September 2007.

However, in 2019, it seems that this vulnerability is still a concern since very few responsible entities in the utility and industrial sectors have taken the necessary steps to protect their assets adequately. Answers about this specific topic are few and far between. Mitigation methods to prevent unwanted closing and reclosing of breakers on rotating machinery require three different types of protection on the breakers: electrical protection, physical security, and cybersecurity.

Remember that when the AURORA vulnerability is exploited, it damages the targeted rotating machinery permanently. Therefore, if exploited by malicious actors, this physical asset vulnerability could have significant consequences and remain unsuspected. During the cyberattack in Ukraine on December 23, 2015, the AURORA vulnerability could have easily been exploited by the people behind the attack, whose goal was to open the circuit breakers to serve as a warning to the Ukrainian authorities during the tensions between Russia and Ukraine following the events in Crimea.

The objective of this publication is to raise awareness of this threat of electrical origin that could strike at any time and that hangs like a sword of Damocles over our critical infrastructures and industries. In the current situation, the question is no longer whether this can happen and how, but rather where and

marc.potvin@bba.ca

when it will happen, and with what catastrophic consequences on the rotating machines that are used extensively in critical infrastructures as well as in the industrial environment.

Cyberattacks are anonymous and can be stealthy. Because they can happen at any time regardless of distance, weather or borders, they are also sneaky. Cyberwar is no longer science fiction; it is now very topical and within the reach of even those nation states with more modest financial means. If this vulnerability is well understood and acknowledged by the relevant stakeholders and decision makers, this will be a first step to prioritize the protection these critical equipment to mitigate this opportunity for hacker of all type or nation state opponent to damage rotating machines until they become out of use very quickly.

KEYWORDS

AURORA vulnerability, cyberattack, cybersecurity, physical security, electrical protection, critical infrastructures, mitigation methods, rotating machines, damage to rotating electrical equipment, avoiding unwanted reclosing on rotating apparatus.

What is AURORA vulnerability?

The AURORA vulnerability refers to the likelihood that a rotating electrical equipment identified in this article as a "rotating machine" is damaged due to a brief disconnection of the power grid, followed by a rapid reconnection. When reconnecting on the power grid, important couples are applied to rotating shafts and gears.

AURORA is the acronym for “Avoiding Unwanted Reclosing On Rotating Apparatus” and is used in the electrical field.

Take note that AURORA is not a cyber security vulnerability. This vulnerability origins from electrical and more specifically to electrical protection and control.

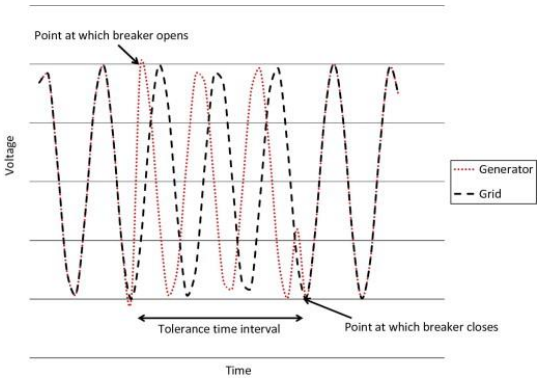
However, it could be exploited by malicious actors when combined with other vulnerabilities in physical security or cybersecurity.

Can you explain this phenomenon more in details?

AURORA must be considered as a vulnerability whose fundamental cause is an electrical protection gap.

The circuit breaker opening/closing sequence is slow enough to allow widening of the voltage angle between the disconnected rotating machine and the power grid, but too fast to be detected and triggered by electrical protection systems. Current circuit breakers can run a close-open-close sequence in less than 10 cycles.

Therefore, although very short, this "deadband" of electrical protection provides a window of opportunity to cause significant damage to a rotating machine.



The AURORA vulnerability is an accidental or intentional event of rapid reconnection of the out-of-phase, out-of-sync circuit breaker on a rotating machine whether it is generating power or consuming it.

Out-of-phase reconnection generate torque and electrical stresses that could damage rotating machine. The resulting torque may exceed the mechanical design limits and damage or destroy the electric rotating machine as well as its coupled mechanical load (drive shaft, gearboxes, pump, combustion engine, belt, etc.).

The severity of the damage varies depending on the mechanical and electrical characteristics of the equipment as well as the way it is connected to the grid.

Why is it considered as a sword of Damocles?

First, since this electrical protection vulnerability appears to be implicit in many cases with respect to the protection of rotating machinery, it must first be considered to have a high potential for hazardous operation.

If an HAZOP (HAZardous OPeration) risk assessment of the AURORA vulnerability is performed, the team of expert of the HAZOP will quickly discover this open gap of electrical protection that could result with significant impact and consequences.

Thus, in an ideal world where there would be no physical security or cybersecurity threat, the AURORA vulnerability could remain a potential cause of operational incident.

In other words, let's first look at this vulnerability based on operating incident rather than a malicious attack.

Knowing that its consequences are significant even if probabilities are low, it remains necessary to reduce this potential risk in order to bring the residual risk into an acceptable level (tolerable risk) for the company and its management.

The most effective mitigation plan is always to solve the problem at its source: the electrical protection and engineering. Any alternative means would only be palliative.

Whether accidental or intentional, the AURORA vulnerability represents a threat that hangs over rotating machines and that could strike at any time just like a Damocles sword on critical infrastructures and industrial environment.

Why is it so important?

Although the AURORA vulnerability cause risk such as operating hazards, by considering with its impact on the availability of rotating machines in addition to health and safety of workers as well as the environmental impact, there are also additional risks that are not resolved by electrical protection such as physical security and cybersecurity.

On circuit breakers upstream of rotating machines, unintentional or accidental reclosing are commonly referred to as "events" while those that are intentional or malicious are called "attacks".

Cyber-attacks are anonymous and can be stealth. Because they can happen at any time, no matter the distance, the weather or the borders, they are also sneaky. Due to its potential impact on rotating machines, an attack resulting from an AURORA vulnerability could be exploited by malicious actors of any type to damage critical rotating machines until they quickly become out of order for several months.

A reminder, the AURORA vulnerability is not a software or hardware information technology vulnerability that can be resorbed by adding security patches.

How could this vulnerability be exploited?

When we talk about exploited vulnerability, we no longer talk about an incident but an intentional and malicious attack. Summarily, an AURORA vulnerability attack could occur locally or remotely.

Examples of local attacks:

1. A malicious individual could locally, operate the manual switch of a power circuit breaker upstream of a rotating machine running. In this case, individuals with physical access to a critical component (the circuit breaker) of the rotating machine do not need any means of network communication, of any computer knowledge and even of any engineering knowledge.
2. Malware present locally could compromise operational technologies of protection and controls to automatically initiate an opening/closing sequence of a power circuit breaker upstream of a rotating machine (e.g. the attacks of the computer worm Stuxnet targeting uranium enrichment centrifuges at the Natanz site in Iran in 2010).

Examples of remote attacks:

1. A group of malicious individuals could remotely compromise the controls and/or electrical protections in order to manually operate the circuit breaker upstream of a rotating machine. In this particular case, the group of hackers doesn’t need physical access to a critical component (the

circuit breaker) of the rotating machine but in counterpart, they need electronic access to the communication networks and systems, a level of knowledge in computer science as well as in engineering in addition to considerable means and high motivation. (e.g. cyberattack in Ukraine on 23 December 2015 which targeted the circuit breakers of several electricity distributors).

2. Malware launched remotely or via email phishing technique could be installed locally in order to compromise the operational technologies of protection and controls in order to engage automatically an opening/closing sequence of a circuit breaker upstream of a rotating machine running (e.g. infection by the BlackEnergy malware in preparation for cyberattack 0f 2015 in Ukraine).

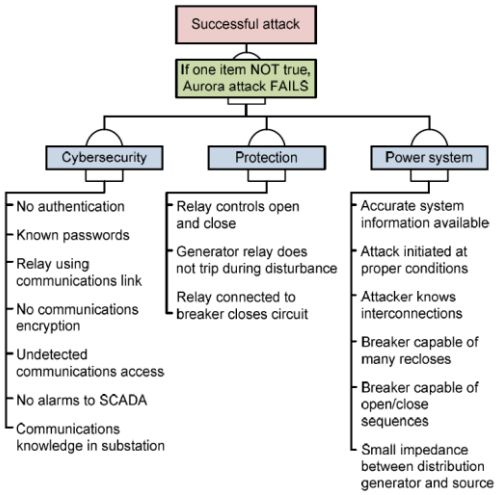
This is not result of luck if there are so many requirements to the NERC CIP standards that apply when there is external connectivity by means of a two-way communication link with routable protocol (e.g. Ethernet connections) commonly known as external routable connectivity (ERC).

External Routable Connectivity: ability to access a BES cyber system, from an electronic asset located outside the associated electronic security perimeter, by means of a two-way, routable protocol link.

Finally, cyberwarfare is no longer science fiction. It is now actual and within the reach of nation-states with modest financial means.

Is this type of sabotage damaging rotating machines possible?

The AURORA vulnerability is not easy to exploit for a malicious actor wishing to damage a rotating machine, but this remains technically possible if however, several conditions are met. This was also one of the reasons behind the demonstration test on a diesel generator on March 2007 at the Idaho National Laboratory (INL).



According to the previous graph, for an AURORA attack to be successful, all conditions listed above must be true. If at least one of them isn't true, the AURORA attack will not be able to damage a rotating machine. These conditions are divided into three distinct groups: cybersecurity, electrical protection and the power supply system.

Since this remains possible, detection measures, but especially adequate defense in depth protections are necessary in order to eliminate factors of the AURORA vulnerability to damage critical assets or infrastructures at a convenient time for a malicious opponent.

What are rotating machines exactly?

In this paper, the term "rotating machine" refers to a rotating electrical equipment synchronized to the alternating current (AC) power grid. The rotating machine comprises an electrical part as well as a mechanical part since these two forms of energy are used either to generate electricity from a rotating mechanical movement or to consume electricity in order to generate a rotating mechanical movement.

During a HAZOP risk assessment or during an onsite security audit, special attention must be paid to critical rotating machines with significant torque and moments of inertia:

- Turbine generator units,
- Wind turbine generators,
- Generators,
- Dynamic rotating uninterruptible power supplies with diesel engine (DRUPS),
- Dynamic energy storage systems with flywheel,
- Synchronous motors coupled to a mechanical load,
- Synchronous compensators,
- Induction motors coupled to a mechanical load.

In addition, the mechanical design tolerances are narrower on large-size rotating machines than on small ones. For rotating machines having a direct coupling between their electrical and mechanical part via a common transmission shaft, the electrical and thermal damage to the winding of the electric part (motor or alternator) may to occur first but mechanical damage remains possible and eventuality, these will be important especially if there is no coupling device between the two parts.

Otherwise, when a gearbox is used as a coupling between the electrical and mechanical parts, this component is undoubtedly the weakest, as by analogy, the use of a fuse to protect an electrical circuit from a current overload.

Finally, the AURORA vulnerability does not concern DC-based engines since the phenomenon of grid synchronization is not involved.

What could be the potential targets for such attacks?

Critical infrastructures are and will always remain targets of choice for malicious actors. Rotating machines are found in quantity especially in the electricity power sector with all equipment generating electricity. The electrical utilities are also subject to NERC's regulatory compliance in North America to ensure the reliability and stability of the interconnected power grid in the United States and Canada.

However, if attacks would affect this nerve sector, important consequences could result to all other critical infrastructure sectors since being interconnected, the possibility of a major outage could occur similarly to a domino effect.

Other critical infrastructure sectors include government, finance, energy and utilities, manufacturing, information technologies and communications, health, safety, water, food, and transportation. In fact, there are a total of 10 critical infrastructure sectors in Canada and 17 in the United States.

Who could be the author of such attacks?

During the cyber-attack in Ukraine on 23 December 2015, the AURORA vulnerability could have been exploited by the nation-state hackers, whose objective was only to open the circuit breakers in order to serve as a warning to the Ukrainian authorities during the conflict between Russia and Ukraine in response to the Crimean events.

Remember, when the AURORA vulnerability is exploited, targeted rotating machines are permanently damaged. Therefore, if exploited by malicious actors, this vulnerability could have significant consequences and impacts remain unsuspected especially for critical infrastructures.

Since an AURORA attack is not easy to exploit for a malicious actor wishing to damage a rotating machine, this is not within the reach of all types of hackers. In fact, according to standard IEC 62443-3-3, there are only 2 potential categories of attackers:

Terrorists and hacktivists requiring the protection level SL 3 against intentional violations using sophisticated means with moderate resources, industrial automation control systems (IACS) specific skills and a moderate motivation. They try to be furtive and prepare for a burst of the type of terrorist act and service interruption.

Nation States requiring the protection level SL 4 against intentional violations using sophisticated means with extensive resources, IACS-specific skills and great motivation. They are very stealth and are preparing for a cyber war.

Why the demonstration test was done?

After the U.S. Department of Homeland Security (DHS), the North American Electric Reliability Corporation (NERC) and the Electricity Information Sharing and Analysis Center (E-ISAC) were informed of the AURORA vulnerability in February 2007, tests and demonstrations took place on a diesel generator in March 2007 at the Idaho National Laboratory (INL).

The objective of the AURORA generator test was to demonstrate the possibility that a cyber-attack could physically damage a rotating machine.

At that time, material damage caused by a cyber-attack remained hypothetical and people remained skeptical that such an eventuality might be possible. The unequivocal results of the demonstration test attracted media attention especially when the CNN news channel made them public in September 2007.

However, due to the confidentiality of the results of this test, several erroneous myths still present in the minds of several people have generated a lot of distortion and incredulity on the facts.

How can we protect ourselves?

As noted in the voluminous literature on this matter, there is not only one way to eliminate or mitigate the risks related to AURORA vulnerability. This is case by case and there is no silver bullet to mitigate these risks.

Mitigation methods to prevent the unwanted reclosure of power breakers upstream of rotating machines includes the following categories:

1. Engineering measures in electrical protection and control: design of a protection and control scheme capable of detecting and preventing the reclosure of a phase-out circuit breaker. (e.g. installation of hardware mitigation devices (HMD), interlocks, addition of hard wired or logical timers to prevent rapid reclosure of circuit breaker, etc.)
2. Physical security mitigation measures: physical security for the local switch of power circuit breaker (e.g. physical security perimeters, physical access control, intrusion detection, etc.)
3. Cybersecurity mitigation measures: cybersecurity of the remote controls such as power circuit breakers, industrial automation and control systems (IACS), electrical protection devices, intelligent electronic devices (IED), human-machine interfaces (HMI), supervisory, control and data acquisition (SCADA) systems, etc. (e.g. establishment of electronic security perimeter, control of electronic access, change of passwords, encryption of remote communication links, intrusion detection, anti-virus with updated of signatures, application of security patches, protection of sensitive information, etc.).
4. Mitigation measures for personnel security: e.g. awareness and training of personnel with physical and electronic access to critical equipment, background check for staff, external resources and suppliers.

Finally, it is important to not rely on a single measure of protection in order to ensure the security and the safety of rotating machines. The proper protection for these critical equipment remains the well-deployed combination of all previous protection methods.

Conclusion

If the AURORA vulnerability is well understood and acknowledged by stakeholders and decision-makers concerned, it will be a first step in prioritizing the protection of these critical equipment in order to mitigate this possibility for the actors of any kind to damage rotating machines until they become quickly out of order.

Still today, the AURORA vulnerability seems to be a misunderstood matter of neophytes who don't have the relevant technical background in physics, and which unfortunately, by its silence and confidentiality, leaves room for all sorts of myths or misunderstandings that only divert attention from this gap of electrical protection which, in fact, is nothing revolutionary.

It seems that very few utilities, private producers and industries have taken the necessary actions to protect their critical assets in an adequate way against AURORA vulnerability which isn't a transient vulnerability that will disappear from by itself. It obeys the immutable laws of physics and it is there to remain there the same way as Newtonian physics.

A nation-state wishing to develop an offensive cyber weapon to destroy critical infrastructures will benefit from this vulnerability in order to attack an opponent. Today, the question is no longer whether this can happen and how, but rather where and when it will occur and what will be the catastrophic consequences.

Finally, let's imagine a malware that would combine the reproductive and selective efficiency of Stuxnet, stealth and exploration features of BlackEnergy toolkit, new adaptive features of artificial intelligence (AI) to successfully accomplish its mission autonomously with a payload of AURORA vulnerability attacks, for me it would represent a real nightmare of cyber warfare.

For those who say that this will never happen or who think it's hard to believe this could even be possible, remember if people would have imagined that terrorist attacks could use civilian airplanes full of kerosene as a destructive weapon by crashing them on symbolic buildings within a period of a few hours the same day.

BIBLIOGRAPHY

[1] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, M. Donolo. "Mitigating the Aurora Vulnerability With Existing Technology" (64th Annual Georgia Tech Protective Relaying Conference, Atlanta, Georgia, May 5–7, 2010).

[2] NERC. "AURORA Mitigation - Protection and Control Engineering Practices and Electronic and Physical Security Mitigation Measures" (Recommendation to Industry, October 13, 2010).

[3] U.S. Department of Defense. "AURORA Overview" (November 2009).

[4] M. Swearingen, S. Brunasso, J. Weiss, D. Huber. "What You Need to Know (and Don't) About the AURORA Vulnerability" (POWER e-newsletter, January 09, 2013).