ID	Method	Component	Risk list
1.	Risk factors	Photovoltaic panel	The presence of cracks and fissures in solar panels can generate hot spots, resulting in a reduction in energy generation efficiency in the affected area and increasing the risk of fires.
2.	Risk factors	Photovoltaic panel	Accumulated dirt on the surface of solar panels can cause shaded areas on the panel and reduce the amount of captured sunlight, resulting in decreased efficiency of electricity generation.
3.	Risk factors	Photovoltaic panel	Panels manufactured with inadequate or low-quality materials can lead to internal corrosion of solar panels, resulting in the rapid deterioration of solar cells and, in turn, a decrease in the capacity to convert sunlight into electricity.
4.	Risk factors	Photovoltaic panel	Theft of solar panels or their components results in financial losses, system malfunctions, and hampers efficiency in energy generation.
5.	Risk factors	Photovoltaic panel	Obstruction of solar panels by hail can cause physical damage to system components, creating new circuit paths, resulting in short circuits, fires, and reduced efficiency in energy generation.
7.	Risk factors	Photovoltaic panel	Adverse or extreme weather conditions such as snowstorms, hailstorms, windstorms, and hurricanes can cause physical damage to solar panels, resulting in partial or total loss of device functionality.
8.	Risk factors	Photovoltaic panel	Manufacturing defects can cause electrical contact between photovoltaic cells, altering the current-voltage characteristic curve of the module, resulting in negative impacts on panel performance.
9.	Risk factors	Photovoltaic panel	Oxidation of solar panels due to poor material quality or weathering can affect the panel's surface and generate an oxide layer, resulting in reduced energy storage.
11.	Risk factors	Photovoltaic panel	Exposure of the photovoltaic panel in locations with high humidity (>0.85%) can cause loss of encapsulant adhesion and allow greater moisture penetration inside the module, resulting in cell damage and reduced energy efficiency of the panel.
12.	Risk factors	Photovoltaic panel	The use of inadequate tools during maintenance of panel connectors can lead to cable connection breakage, resulting in current leakage and increased fire risk.
13.	Risk factors	Photovoltaic panel	Placing the panel in shaded areas can reduce current production, decreasing electricity generation.
14.	Risk factors	Photovoltaic panel	Failure in the welding of photovoltaic module components can increase contact resistance, resulting in a reduction in energy generation efficiency.
15.	Risk factors	Photovoltaic panel	Overdimensioning of direct current or alternating current can cause overload on the solar panel, resulting in the burning of components connected to the panel and a reduced system lifespan.
16.	Risk factors	Photovoltaic panel	Photovoltaic modules with low-quality materials can create shaded areas on the panel surface, resulting in reduced energy generation and a decrease in the panel's lifespan.
17.	Risk factors	Photovoltaic panel	current (AC), impairing the operation of solar panels and reducing efficiency in energy generation.
18.	Risk factors	Photovoltaic panel	Failure in the connectors and junction box of solar panels can allow moisture ingress, accelerating corrosion and increasing the risk of short-circuit in system components.
19.	Risk factors	Photovoltaic panel	accumulation, resulting in hot spots that reduce local energy generation and degrade the panel.
20.	Risk factors	Photovoltaic panel	The use of inadequate materials during maintenance, such as abrasives, can cause physical damage to the surface of the panel, resulting in cracks or fissures that compromise energy generation.
23.	Risk factors	Photovoltaic panel	Sabotage to the electrical grid can disrupt the production and distribution of energy from photovoltaic panels, resulting in financial losses, energy theft, and panel damage.
27.	Risk factors	Photovoltaic panel	Inverter failure can prevent the conversion of stored energy by the panel into direct current (DC), resulting in a lack of energy generation and storage.
29.	Risk factors	Photovoltaic panel	Preventive maintenance carried out by inexperienced professionals can damage the electrical and mechanical components of the panel, resulting in reduced efficiency and system safety of the energy generation system.

30.	Risk factors	Photovoltaic panel	Inefficient diagnosis of failures in photovoltaic panels can lead to interrupted energy generation, reducing system efficiency and increasing corrective maintenance costs.
32.	Risk factors	Photovoltaic panel	Exposure of solar modules to high temperatures and high voltage levels can result in Potential Induced Degradation (PID), leading to defects in semiconductor materials and decreasing panel efficiency.
34.	Risk factors	Inverter	Inverter failure can interrupt the energy transfer to the grid and equipment, resulting in reduced system efficiency.
35.	Risk factors	Inverter	Inverter overheating due to malfunction can lead to rapid deterioration of its components, resulting in fires and frequent equipment replacement.
36.	Risk factors	Inverter	Installing the inverter in an inappropriate location with direct exposure to sunlight can increase the inverter's temperature, resulting
37.	Risk factors	Inverter	Inadequate connection between string cables and the inverter can cause electrical connection failures, resulting in equipment shutdown and difficulties in identifying electrical arcs.
38.	Risk factors	Inverter	Defective RS485 indicator LEDs can cause operational failures, resulting in misinterpretation of the equipment status, which, in turn, can lead to other failures.
39.	Risk factors	Inverter	Theft of the inverter can interrupt the energy transfer to other devices due to the lack of equipment, resulting in reduced system efficiency and financial losses.
40.	Risk factors	Inverter	Excessive distance between the communication network and the inverter can cause a significant potential difference between locations, resulting in degradation of the communication signal.
41.	Risk factors	Inverter	The undersizing of the inverter's communication speed and the network can lead to more retransmissions, resulting in increased latency in the communication system.
42.	Risk factors	Inverter	Failure to change the default passwords established by the manufacturer can simplify access to inverter data, increasing the likelihood of unauthorized breach and possible theft of information.
44.	Risk factors	Inverter	The absence of an intrusion detection system, such as alarms and sensors, can prevent the identification and monitoring of breaches in the inverter, allowing silent access to data.
45.	Risk factors	Inverter	Overvoltage exceeding the limit established in the technical specification can cause damage to the inverter components, resulting in malfunction or even equipment failure.
46.	Risk factors	Inverter	Lack of integrity verification and failures in non-standardized software loading processes can enable manipulation or deletion of data, resulting in loss of accuracy, consistency, and reliability of the performed update.
47.	Risk factors	Inverter	The absence of cryptographic keys or the use of default manufacturer keys can seriously compromise data security, resulting in unauthorized access and theft of sensitive information.
48.	Risk factors	Inverter	Problems in cable connections and crimps can cause electrical resistance, resulting in power losses and decreased system efficiency.
49.	Risk factors	Inverter	Lack of maintenance on electrical protections, such as circuit breakers and fuses, can decrease the efficiency of these devices in protecting the electrical system in case of electrical leakage or insulation failures, increasing the vulnerability of the electrical system to electrical safety issues.
50.	Risk factors	Inverter	Lack of maintenance and cleaning of the inverter's fan, grille, and heat exchanger can interfere with proper heat dissipation and increase the internal temperature of the equipment, resulting in automatic shutdown of the inverter.
51.	Risk factors	Inverter	Lack of general maintenance of the photovoltaic inverter, including detecting damages or breaks in components, can interfere with energy conversion and the overall operation of the equipment, resulting in shutdown, reduced performance, power loss, or, in extreme cases, fires.
52.	Risk factors	Inverter	Tapping into the communication network can allow control of multiple inverters connected to the bus, resulting in possible manipulation of control signals sent to the inverters.

53.	Risk factors	Inverter	Failure to verify the authenticity of the software load by the inverter can allow the installation of tampered versions of the firmware, resulting in unauthorized and malicious access to private information and enabling the transmission and reception of unauthorized data.
54.	Risk factors	Inverter	Improper installation or repositioning of the photovoltaic inverter can result in electrical shock hazards for the installer and loss of functionality of electrical components.
55.	Risk factors	Inverter	Inadequate cable diameter can lead to voltage drop and reduce current conversion efficiency, resulting in power loss in the system.
57.	Risk factors	Inverter	The presence of a malicious file in the software load can compromise the operation of management software responsible for inverter commands, such as Aurora Manager, resulting in improper control and management of inverter information.
58.	Risk factors	Inverter	Improper installation of network communication, such as installing two RS485/Modbus-RTU masters on the same network, can lead to network intermittency, resulting in inverter shutdown and interruption of power supply.
59.	Risk factors	Inverter	Incorrect installation of communication cables alongside power cables can result in cable interference, causing network malfunctions as a whole.
60.	Risk factors	Inverter	Not following manufacturer guidelines and technical standards can lead to inadequate sizing of inverter electrical current, resulting in the risk of electrical shocks and fires.
61.	Risk factors	Inverter	Improper current sizing can cause unintentional tripping of the circuit breaker, resulting in power supply interruption, equipment damage, and electrical hazards for professionals responsible for maintaining the photovoltaic system.
62.	Risk factors	Inverter	Inadequate sizing of the inverter (tilt angle greater than 5° from vertical) can reduce the energy generation capacity of the photovoltaic system, resulting in lower energy conversion efficiency and, consequently, reduced electricity generation.
63.	Risk factors	Inverter	Installing inverters vertically with a tilt angle greater than 5° can hinder proper heat dissipation of the components, leading to equipment overheating and increasing the risk of fire.
65.	Risk factors	Inverter	Installing the inverter in locations with high humidity and inadequate cable sealing can allow electrical current leakage, resulting in low equipment insulation resistance, electrical shock hazards, and accelerated corrosion of electrical components, reducing the equipment's lifespan.
66.	Risk factors	Inverter	Electric arcs raise the temperature of components, exceeding technical limits, causing premature wear, failures, and reducing equipment efficiency and lifespan.
67.	Risk factors	Inverter	Aging of inverters and their components over time can result in wear and tear due to equipment usage, leading to operational failures and costs associated with corrective maintenance.
68.	Risk factors	Inverter	Lack of regular maintenance on inverter components such as the fan, grille, heat exchanger, and filter can lead to dust accumulation in the equipment, reducing cooling efficiency, shortening the inverter's lifespan, and increasing costs associated with corrective maintenance.
69.	Risk factors	Gateway (ModBus TCP)	Overheating of the gateway beyond technical specification limits can lead to accelerated degradation of electronic components, resulting in reduced equipment efficiency and increased fire risks.
70.	Risk factors	Gateway (ModBus TCP)	Improper installation of the inverter can compromise the functionalities and integrity of the gateway, resulting in overall poor performance of the photovoltaic system due to impaired control and monitoring.
71.	Risk factors	Gateway (ModBus TCP)	Defects in the gateway's indicator LEDs can lead to incorrect indications about its operation, resulting in failures that compromise both efficiency and hardware integrity.
72.	Risk factors	Gateway (ModBus TCP)	TCP to RTU protocol, which is essential for integrating equipment that uses different protocols, impairing communication and plant security.

73.	Risk factors	Gateway (ModBus TCP)	The absence of a firewall with a proxy can allow unauthorized external connections, enabling access to information from the supervisory system to which the network lacks security measures, posing risks to information availability and integrity.
74.	Risk factors	Gateway (ModBus TCP)	A damaged connection cable can result in loss of connection (between the supervisory system and inverters) via cable, rendering software updates, control, and monitoring of the inverters impossible, thereby impairing their operation.
75.	Risk factors	Gateway (ModBus TCP)	Lack of password protection to authorize firmware changes can facilitate the actions of hackers, compromising the security and privacy of information and allowing data theft.
76.	Risk factors	Gateway (ModBus TCP)	Intrusion into a wired network can allow unauthorized and immediate access to all gateway information, facilitating the installation of malware and malicious software.
77.	Risk factors	Gateway (ModBus TCP)	Lack of source authentication mechanisms, such as IP spoofing, can allow the forging of source IP addresses from other hosts, resulting in unauthorized access to sensitive data associated with those IP addresses.
78.	Risk factors	Gateway (ModBus TCP)	Weak authentication and encryption can lead to TCP desynchronization attacks, allowing the capture and control of third-party connections, compromising sensitive information, and jeopardizing network security.
79.	Risk factors	Gateway (ModBus TCP)	Use of predictable initial sequence numbers can lead to TCP sequence number prediction, enabling the generation of malicious packets targeted at a specific host, resulting in network traffic manipulation, information theft, injection of false packets, or even denial of service (DoS).
81.	Risk factors	Gateway (ModBus TCP)	Lack of encryption in communication can enable source routing attacks, allowing an attacker to monitor and intercept communications on the network, gaining access to confidential information and compromising network security as a whole.
83.	Risk factors	Gateway (ModBus TCP)	A DoS attack or large-scale transmission of SYN packets with spoofed IP addresses can cause excessive resource consumption, resulting in the gateway's unavailability.
85.	Risk factors	Gateway (ModBus TCP)	Inadequate maintenance of the gateway can alter its settings, resulting in operational failures and potential security breaches.
86.	Risk factors	Gateway (ModBus TCP)	Disconnection or damage to cables or connections during maintenance can disrupt the gateway's communication with other network devices, resulting in data loss or loss of important information stored in the gateway.
87.	Risk factors	Gateway (ModBus TCP)	Lack of technical skills and the use of inadequate tools during gateway maintenance can exacerbate existing device failures, accelerating the deterioration of system integrity.
88.	Risk factors	Gateway (ModBus TCP)	Data loss stored in the gateway during maintenance can compromise information integrity, affect system productivity and security, and result in financial losses and process downtime.
91.	Risk factors	Gateway (ModBus TCP)	Physical access to the gateway by malicious actors can allow the replacement of the device with tampered hardware, resulting in financial losses, anomalous behavior, and unauthorized access to the original owner's data.
93.	Risk factors	Gateway (ModBus TCP)	Failure to verify the authenticity and integrity of software loads can enable the installation of malicious software on the gateway, leading to vulnerability and compromise of security.
94.	Risk factors	Gateway (ModBus TCP)	Failures during software loading can cause service disruptions or security vulnerabilities in the gateway.
95.	Risk factors	Gateway (ModBus TCP)	Lack of standardization in software loading processes can lead to increased maintenance costs and time, resulting in decreased system efficiency, security, and reliability.
96.	Risk factors	Gateway (ModBus TCP)	Failure to update software and firmware can leave the gateway vulnerable to known attacks that could be prevented by applying security patches.

97.	Risk factors	Gateway (ModBus TCP)	Inadequate gateway installation and incorrect network configuration, drivers, and specific settings can generate communication problems between devices, resulting in data loss, delays in information transmission, and communication failures or interruptions.
98.	Risk factors	Gateway (ModBus TCP)	RS485 networks with incorrectly configured different Modbus addresses can lead to communication issues such as interruptions and failures in communication between devices.
99.	Risk factors	Gateway (ModBus TCP)	Natural aging of hardware, including cables, can result in communication failures from Modbus TCP to RTU protocol, leading to communication disruption or loss of data packets.
100.	Hazop	Inverter	Increased ambient temperature above specified limits can cause thermal stress on the photovoltaic panel, resulting in physical damage and higher maintenance and replacement costs.
101.	Hazop	Inverter	Extreme weather conditions such as snowstorms can lower the ambient temperature below specified limits, resulting in decreased efficiency of the photovoltaic panel and financial impacts on the solar power plant.
103.	Hazop	Inverter	Decreased ambient temperature below specified limits can cause excessive cooling of the photovoltaic cells, leading to breaking or cracking of the panels and consequently reducing the energy generation efficiency.
104.	Hazop	Inverter	Zones with high relative humidity (>0.85%) can cause water condensation inside the photovoltaic cells, reducing thermal insulation and increasing the risk of electrical shocks.
105.	Hazop	Inverter	Zones with high relative humidity can lead to oxidation and corrosion of cables in the photovoltaic power plant.
106.	Hazop	Inverter	Voltages above the specified limit can cause overvoltage in the photovoltaic power system, resulting in irreparable damage to the solar cells and leading to short circuits and fires.
107.	Hazop	Inverter	Impact speed of hailstones above 50 mph can cause micro cracks or fissures in the photovoltaic cells, reducing their mechanical strength and increasing the risk of short circuits in the system.
108.	Hazop	Inverter	Excessive accumulation of snow on photovoltaic panels can damage the photovoltaic cells, reducing the system's energy generation capacity.
109.	Hazop	Inverter	Extreme weather conditions, such as strong winds above the specified limit, can lead to panel detachment and internal damage to the
110.	Hazop	Inverter	Increasing direct current beyond the specified technical limits can cause overvoltage, resulting in the shutdown of the inverter and potential short circuits.
111.	Hazop	Inverter	Defects in the inverter's electrical circuits can cause a drop in direct current, resulting in insufficient input voltage to power the energy storage system.
112.	Hazop	Inverter	Lack of electrical grounding can compromise protection against leakage currents and lightning strikes, resulting in equipment damage and electrical accidents.
113.	Hazop	Inverter	Oversizing the power capacity can result in lower output power compared to the input power, leading to prolonged operation time of the inverter with reduced efficiency and electrical energy loss.
114.	Hazop	Inverter	Increasing alternating current above the specified technical limits and inadequate infrastructure can cause overvoltage of the alternating current, resulting in the shutdown of the photovoltaic inverter or burning of electronic equipment connected to the grid.
115.	Hazop	Inverter	Decreasing equipment voltage supply can cause undervoltage of the alternating current, which can result in equipment malfunction or burning of connected devices.
116.	Hazop	Inverter	Increasing the frequency above the technical specification limit, usually caused by an excess supply of energy compared to demand, can cause network disconnections, resulting in mass shutdowns of the photovoltaic inverter and connected equipment.
117.	Hazop	Inverter	Climate changes, inadequate installation, and improper sizing can cause overheating of the inverter, resulting in a reduction in the power generated by the system and, in extreme cases, complete shutdown of the inverter.

118.	Hazop	Inverter	Excessive cooling of the inverter, usually due to climate changes such as snowstorms, can lead to temperature sensor failures and corrosion of metal components, compromising the proper functioning of the equipment and causing economic losses for the photovoltaic system.
119.	NCSF	Inverter	Absence of asset inventory and responsible definitions can compromise asset management, access authorization, and identification of responsible parties.
120.	NCSF	Inverter	Absence of software inventory can compromise software management and identification of owners.
121.	NCSF	Inverter	Lack of mapping of organizational communication and data flow can hinder device management processes, resulting in lower protection against network service attacks.
122.	NCSF	Inverter	Absence of threat monitoring processes and tools and lack of information classification can hinder the detection of network security threats and effective information management.
123.	NCSF	Inverter	Absence of security requirements and controls for management can hinder the management and control of information security.
124.	NCSF	Inverter	Lack of standards for reporting incidents and procedures for responding to them can compromise incident response and management.
125.	NCSF	Inverter	Absence of defined roles and responsibilities can make it difficult to map, document, and handle cybersecurity incidents.
126.	NCSF	Inverter	Absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersecurity risks.
127.	NCSF	Inverter	Lack of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management and compliance analysis.
128.	NCSF	Inverter	Absence of specialized forums for mapping cyber threats can make it difficult to manage these threats.
129.	NCSF	Inverter	Lack of identification and documentation of internal threats can compromise asset integrity.
130.	NCSF	Inverter	Absence of technical vulnerability management and software installation restrictions can make it difficult to gather information about these vulnerabilities and define criteria for software installation.
131.	NCSF	Inverter	Lack of a risk treatment plan can make it difficult to define the form, process, and controls for addressing information security risks.
132.	NCSF	Gateway (ModBus TCP)	Absence of asset inventory and responsible definitions can compromise asset management, access authorization, and
133.	NCSF	Gateway (ModBus TCP)	Lack of software inventory can compromise software management and identification of owners.
134.	NCSF	Gateway (ModBus TCP)	Absence of organizational communication mapping and data flow can make it difficult to comprehensively manage devices and attacks against network services.
135.	NCSF	Gateway (ModBus TCP)	Absence of processes and threat monitoring tools and lack of information classification can hinder the detection of network security threats and effective information management.
136.	NCSF	Gateway (ModBus TCP)	Absence of security requirements and controls for management can hinder the management and control of information security.
137.	NCSF	Gateway (ModBus TCP)	Lack of standards for reporting incidents and procedures for responding to them can compromise incident response and management.
138.	NCSF	Gateway (ModBus TCP)	Absence of defined roles and responsibilities can make mapping, documentation, and treatment of cybersecurity incidents difficult.
139.	NCSF	Gateway (ModBus TCP)	Lack of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersecurity risks.
140.	NCSF	Gateway (ModBus TCP)	Absence of vulnerability information and tools for system and network compliance analysis can make vulnerability management and compliance analysis difficult.
141.	NCSF	Gateway (ModBus TCP)	Lack of specialized forums for mapping cyber threats can make managing these threats difficult.
142.	NCSF	Gateway (ModBus TCP)	Absence of identification and documentation of internal threats can compromise asset integrity.

143.	NCSF	Gateway (ModBus TCP)	Absence of technical vulnerability management and software installation restrictions can make gathering information about these vulnerabilities difficult and hinder the definition of criteria for software installation.
144.	NCSF	Gateway (ModBus TCP)	Lack of a risk treatment plan can make it difficult to define the form, process, and controls for addressing information security risks.