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 reduced energy generation efficiency in the affected area and increasing the risk of fires.
2.	Risk factors	Photovoltaic panel	Shadows caused by accumulated dirt on solar panels can prevent the capture of sunlight, resulting in a decrease in electricity production.
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 ability to convert sunlight into electricity.
4.	Risk factors	Photovoltaic panel	Theft of solar panels or their components results in financial losses, system malfunctions, and impairs energy generation efficiency.
5.	Risk factors	Photovoltaic panel	Exposure of solar panels to adverse weather conditions such as hailstorms, snowstorms, windstorms, and hurricanes can result in physical damage to system components, including the creation of new circuit paths, short circuits, fires, partial or total loss of device functionality, and reduced energy generation efficiency.
8.	Risk factors	Photovoltaic panel	Manufacturing defects can cause electrical contact between photovoltaic cells, modifying the module's current-voltage characteristic curve and negatively impacting panel performance.
9.	Risk factors	Photovoltaic panel	The use of low-quality materials in the manufacturing of photovoltaic modules can easily affect the panel's surface, creating oxide layers that wear down the surface, resulting in a decrease in panel lifespan.
11.	Risk factors	Photovoltaic panel	Exposure of the photovoltaic panel to high humidity locations (>0.85%) can cause damage to cells, such as loss of encapsulation adhesion, allowing increased moisture penetration inside the module, resulting in accelerated corrosion in connectors and junction boxes, increasing the risk of system short circuits.
12.	Risk factors	Photovoltaic panel	Inadequate maintenance, performed with improper tools and materials or by inexperienced professionals, can result in cable connection breakages, physical damage to the panel surface (cracks or fissures), and damage to electrical components, leading to reduced energy generation efficiency.
14.	Risk factors	Photovoltaic panel	Failure in the welding of photovoltaic module components can lead to increased contact resistance, resulting in reduced energy generation efficiency.
15.	Risk factors	Photovoltaic panel	Inadequate sizing of the photovoltaic system, including over-sizing of direct current or alternating current, can cause overload on the solar panel, resulting in the burning of components connected to the panel, reduced system lifespan, and decreased energy generation efficiency.
19.	Risk factors	Photovoltaic panel	Lack of regular panel maintenance can lead to dirt accumulation, resulting in hot spots that reduce local energy generation and degrade the panel.
23.	Risk factors	Photovoltaic panel	Sabotage of the power grid can disrupt the production and distribution of energy from photovoltaic panels, resulting in financial losses, energy theft, and panel damage.
27	Risk factors	Inverter	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.
30.	Risk factors	Photovoltaic panel	Inefficient diagnosis of faults in photovoltaic panels can lead to interrupted energy generation, reduced system efficiency, and increased 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	Overheating of the inverter, due to failure, can lead to rapid deterioration of its components, resulting in fires and frequent equipment replacement.
36.	Risk factors	Inverter	Installing the inverter in an unsuitable location with direct exposure to sunlight can increase its temperature, resulting in accelerated degradation and, in extreme cases, overheating and burning.
37.	Risk factors	Inverter	Inadequate connection between string cables and the inverter, along with improper current sizing, can cause electrical connection failures, resulting in equipment shutdown, unintentional breaker tripping, and power supply interruption.
38.	Risk factors	Inverter	Defective RS485 indicator LEDs can cause operational failures, resulting in misinterpretation of the equipment status, which 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 large potential difference between the locations, resulting in communication signal degradation.

41.	Risk factors	Inverter	Undersizing the communication speed of the inverter and the network can lead to more retransmissions, increasing latency in the communication system.
42.	Risk factors	Inverter	Lack of proper security measures, such as failure to change default passwords and using manufacturer's standard cryptographic keys, can increase the likelihood of unauthorized breaches, enabling access to confidential information and possible theft of sensitive data.
44.	Risk factors	Inverter	Lack of an intrusion detection system, such as alarms and sensors, can prevent the identification and monitoring of inverter breaches, allowing silent access to data.
45.	Risk factors	Inverter	Overvoltage exceeding the specified limit in the technical specification can cause damage to inverter components, resulting in malfunction or even equipment burnout.
46.	Risk factors	Inverter	Failure to verify integrity and flaws in non-standardized software loading processes can enable data manipulation or deletion, resulting in loss of accuracy, consistency, and reliability of the performed update.
48.	Risk factors	Inverter	Problems in cable connections and crimping can cause electrical resistance, resulting in energy losses and decreased system efficiency.
49.	Risk factors	Inverter	Lack of maintenance in electrical protections, such as circuit breakers and fuses, can decrease the effectiveness 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 proper maintenance on inverter components such as the fan, grille, heat exchanger, and filter can interfere with proper heat dissipation and result in dust accumulation, increasing the internal temperature of the equipment. This can lead to frequent automatic shutdowns and increased costs for corrective maintenance.
51.	Risk factors	Inverter	General lack of maintenance on the photovoltaic inverter, including detection of damages or breakages in components, can interfere with energy conversion and overall operation of the equipment, resulting in shutdowns, reduced performance, power loss, or, in extreme cases, fires.
52.	Risk factors	Inverter	Network eavesdropping can allow control over multiple inverters connected to the bus, potentially manipulating the 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 firmware versions, leading to unauthorized and malicious access to private information and enabling transmission and reception of unauthorized data.
54.	Risk factors	Inverter	Improper installation or repositioning of the photovoltaic inverter can pose an electrical shock risk to installers and cause loss of functionality in electrical components.
55.	Risk factors	Inverter	Inadequate cable diameter can result in voltage drop and reduce current conversion efficiency, leading to power loss in the system.
57.	Risk factors	Inverter	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 cause network intermittence, resulting in inverter malfunction and power supply interruption.
59.	Risk factors	Inverter	Incorrect installation of communication cables alongside power cables can cause interference, leading to malfunctioning of the entire network.
60.	Risk factors	Inverter	Failure to follow manufacturer's guidelines and technical standards can result in inadequate sizing of inverter electrical current, posing the risk of electrical discharge and fires.
62.	Risk factors	Inverter	Inadequate inverter sizing (tilt angle greater than 5° vertically) can reduce the energy generation capacity of the photovoltaic system, resulting in lower energy conversion efficiency and, consequently, electricity generation.
63.	Risk factors	Inverter	Installing inverters vertically with an inclination greater than 5° can hinder proper heat dissipation from components, leading to equipment overheating and increased fire risk.
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, risk of electrical shock, and accelerated corrosion of electrical components, reducing the equipment's lifespan.
66.	Risk factors	Inverter	Electrical arcs raise component temperature beyond technical limits, causing premature wear, failures, and reducing efficiency and equipment lifespan.
67.	Risk factors	Inverter	Aging of inverters and their components over time can result in wear and tear due to prolonged equipment usage, leading to operational failures and increased costs for corrective maintenance.

69.	Risk factors	Gateway (ModBus TCP	Overheating of the gateway beyond the limits specified in the technical specification can lead to accelerated degradation of electronic components, resulting in reduced equipment efficiency and increased fire risk.
70.	Risk factors	Gateway (ModBus TCP	Improper installation of the inverter and gateway, along with incorrect network configurations, drivers, and specific settings, can compromise the functionalities and integrity of the photovoltaic system, impairing control, monitoring, and communication between devices, resulting in overall low performance and data loss.
71.	Risk factors	Gateway (ModBus TCP	A defect in the signaling LEDs of the gateway can lead to incorrect indications of its operation, resulting in failures that compromise both the efficiency and integrity of the hardware.
72.	Risk factors	Gateway (ModBus TCP	Theft of the gateway hardware can disable the Modbus TCP to RTU protocol conversion, essential for integrating equipment that uses different protocols, impairing communication and plant security.
73.	Risk factors	Gateway (ModBus TCP	Lack of adequate security measures, such as the absence of a firewall with a proxy and lack of wired network protection, can allow unauthorized access to supervisory system and network information, resulting in risks to information integrity and availability, facilitating the installation of malware and malicious software.
74.	Risk factors	Gateway (ModBus TCP	Cable connection problems, such as damage or disconnections, can compromise communication between the supervisory system, inverters, and the gateway, resulting in the loss of important data, inability to update the software, and inadequate control and monitoring of the inverters.
75.	Risk factors	Gateway (ModBus TCP	Lack of password to authorize firmware changes can facilitate the actions of hackers, compromising the security and privacy of information, as well as enabling data theft.
77.	Risk factors	Gateway (ModBus TCP	Lack of source authentication mechanisms, such as IP Spoofing, can allow the forgery 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	The use of predictable initial sequence numbers can lead to TCP Sequence Number Prediction, allowing the generation of targeted malicious packets to a specific host, resulting in manipulation of network traffic, data 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.
85.	Risk factors	Gateway (ModBus TCP	Inadequate maintenance on the gateway can alter its configurations, 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 or important information loss 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, resulting in accelerated deterioration of system integrity.
88.	Risk factors	Gateway (ModBus TCP	Loss of data stored in the gateway during maintenance can compromise the integrity of information, 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 agents can allow for 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 the software load can enable the installation of malicious software on the gateway, resulting in vulnerability and compromised security.
94.	Risk factors	Gateway (ModBus TCP	Failures during software loading can cause service interruptions 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.
98.	Risk factors	Gateway (ModBus TCP	RS485 networks with incorrectly configured different Modbus addresses can lead to communication issues such as disruptions and communication failures 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 interruption or data packet loss.
100.	Hazop	Photovoltaic panel	Increased ambient temperature above specified limits can cause thermal stress on the photovoltaic panel, resulting in physical damage and increased maintenance and replacement costs.

101.	Hazop	Photovoltaic panel	Extreme weather conditions such as snowstorms can cause the ambient temperature to drop below specified limits, resulting in excessive cooling of the photovoltaic cells and cracking or fracturing of the panels, negatively impacting the efficiency of power generation.
104.	Hazop	Photovoltaic panel	Areas 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	Photovoltaic panel	Areas with high relative humidity can lead to oxidation and corrosion of cables in the photovoltaic power plant.
106.	Hazop	Photovoltaic panel	Voltages above the specified limit can cause overvoltages in the photovoltaic power system, resulting in irreparable damage to the solar cells and leading to short circuits and fires.
107.	Hazop	Photovoltaic panel	Hailstone impact speeds above 50 mph can cause micro cracks or fissures in the photovoltaic cells, reducing their mechanical strength and increasing the risk of system short circuits.
108.	Hazop	Photovoltaic panel	Excessive snow accumulation on photovoltaic panels can damage the photovoltaic cells, reducing the system's capacity to generate power.
109.	Hazop	Photovoltaic panel	Extreme weather conditions such as strong winds above the specified limit can lead to panel dislodgment and internal damage to the photovoltaic cells, resulting in decreased efficiency in power generation.
110.	Hazop	Inverter	Exceeding the specified technical limits of direct current (DC) can cause overvoltage, resulting in the shutdown of the inverter and potential short circuits.
111.	Hazop	Inverter	Presence of defects in the electrical circuits of the inverter can lead to a DC undervoltage, 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 atmospheric discharges, resulting in equipment damage and electrical accident risks.
113.	Hazop	Inverter	Oversizing the power capacity can lead to lower output power compared to input power, resulting in prolonged operation time of the inverter with lower efficiency and electrical energy loss.
114.	Hazop	Inverter	Raising the alternating current (AC) above the specified technical limits and inadequate infrastructure can generate AC overvoltage, resulting in the shutdown of the photovoltaic inverter or burning of electronic equipment connected to the grid.
115.	Hazop	Inverter	Lowering the supply voltage of equipment can cause AC undervoltage, which may result in operational interruption or burning of connected equipment.
116.	Hazop	Inverter	Increasing the frequency above the limit specified in the technical specification, 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, improper installation, and inadequate 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, often due to climate changes like snowstorms, can lead to sensor failures and corrosion in metallic components, compromising the proper functioning of the equipment and causing economic losses for the photovoltaic system.
119.	NCSF	Inverter	The lack of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorization, identification of responsible parties, mapping, documentation, and handling of cybersecurity incidents.
120.	NCSF	Inverter	Absence of software inventory can compromise software management and identification of owners.
121.	NCSF	Inverter	Lack of organizational communication mapping and data flow can hinder the device management process, 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	Lack of security requirements and controls for management can hinder the management and control of information security.
124.	NCSF	Inverter	Absence of standards for reporting incidents and response procedures can compromise incident response and management.
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 make vulnerability management and compliance analysis difficult.
128.	NCSF	Inverter	Absence of specialized forums for cyber threat mapping can hinder the management of 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 hinder the collection of information about these vulnerabilities and make it difficult to define criteria for software installation.
131.	NCSF	Inverter	Absence 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)	The lack of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorization, identification of responsible parties, mapping, documentation, and handling of cybersecurity incidents.
133.	NCSF	Gateway (ModBus TCP)	Absence 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 protect against network service attacks.
135.	NCSF	Gateway (ModBus TCP)	Absence of threat monitoring processes and tools and lack of information classification can make it difficult to detect network security threats and effectively manage information.
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)	Absence of standards for reporting incidents and response procedures can compromise incident response and management.
139.	NCSF	Gateway (ModBus TCP)	Absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersecurity risks.
140.	NCSF	Gateway (ModBus TCP)	Lack of vulnerability information and tools for system and network compliance analysis can make vulnerability management and compliance analysis difficult.
141.	NCSF	Gateway (ModBus TCP)	Absence of specialized forums for cyber threat mapping can hinder the management of these threats.
142.	NCSF	Gateway (ModBus TCP)	Absence of identification and documentation of internal threats can compromise asset integrity.
143.	NCSF	Gateway (ModBus TCP)	Lack of technical vulnerability management and restrictions on software installation can hinder the collection of information about these vulnerabilities and make it difficult to define criteria for software installation.
144.	NCSF	Gateway (ModBus TCP)	Absence of a risk treatment plan can make it difficult to define the form, process, and controls for addressing information security risks.