CPRIM Artefacts - Risks' unified list after agregating risks in Phase-3 (i.e., final list)

ID	Process	Asset	Risks
1.	Risk factors	Photovoltaic panel	Cracks and fissures in solar panels can generate hot spots, reducing 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, decreasing electricity production.
3.	Risk factors	Photovoltaic panel	Internal corrosion of the panels due to exposure to extreme weather conditions, or the use of inadequate materials, can result in the deterioration of solar cells and decrease 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 hampers 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, altering the characteristic current-voltage curve of the module, resulting in negative impacts on the panel's performance.
9.	Risk factors	Photovoltaic panel	The use of low-quality materials in manufacturing 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 and physical damage to the panel surface (cracks or fissures) and electrical components, leading to reduced energy generation efficiency.
14.	Risk factors	Photovoltaic panel	Failure in the soldering of photovoltaic module components can increase contact resistance, reducing 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 periodic maintenance of the panels can lead to dirt accumulation, resulting in hot spots that reduce local energy generation and degrade the panel.
23.	Risk factors	Photovoltaic panel	Sabotaging the electrical grid can disrupt the production and distribution of energy from photovoltaic panels, leading to financial losses, energy theft, and panel damage.
27	Risk factors	Photovoltaic panel	Improper installation of inverters and inadequate configuration of their communication protocols can decrease energy generation efficiency.
30.	Risk factors	Photovoltaic panel	Inefficient diagnosis of faults in photovoltaic panels can lead to interruptions in 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 disrupt the energy transfer to the grid and equipment, rendering the entire system useless.
35.	Risk factors	Inverter	Inverter overheating due to malfunction can rapidly deteriorate 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 burnout.
37.	Risk factors	Inverter	Inadequate connection between string cables and the inverter and 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 erroneously indicate the equipment's operating status, resulting in failures such as overvoltage, overheating, and inverter errors, leading to inverter burnout.
39.	Risk factors	Inverter	The theft of the inverter can interrupt the energy transfer to other devices due to the absence of the equipment, resulting in a complete system shutdown and financial losses.
40.	Risk factors	Inverter	Excessive distance between the communication network and the inverter can cause a significant potential difference between the locations, interfering with the communication signal.
41.	Risk factors	Inverter	Undersizing the communication speed of the inverter and the network can lead to more retransmissions, resulting in lower inverter efficiency.
42.	Risk factors	Inverter	Lack of proper security measures, such as failure to change default passwords and using the 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	The absence of an intrusion detection system, such as alarms and sensors, can prevent the identification and monitoring of inverter breaches, allowing silent access to the data.
45.	Risk factors	Inverter	Overvoltage that exceeds the specified technical limit can cause damage to the inverter components, resulting in malfunction or even equipment burnout.
46.	Risk factors	Inverter	The absence of integrity verification and failures 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 crimps can cause electrical resistance, resulting in energy losses and decreased system efficiency.
49.	Risk factors	Inverter	Lack of maintenance of electrical protections, including circuit breakers and fuses, can result in insulation failures and electric current leakage.
50.	Risk factors	Inverter	Lack of proper maintenance on inverter components such as the fan, grille, heat exchanger, and filter can interfere with adequate 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	Lack of overall maintenance of the photovoltaic inverter, including detection of component damage or breakage, can interfere with energy conversion and overall equipment operation, resulting in shutdown, performance reduction, power loss, or, in extreme cases, fires.
52.	Risk factors	Inverter	Tapping into the communication network can allow control over 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 receipt 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	A malicious file in the software load can compromise the operation of management software responsible for controlling the inverter, 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 intermittence, inverter malfunction, and power supply interruption.
59.	Risk factors	Inverter	Incorrect installation of communication cables alongside power cables can result in confusion and reversal of cable connections, resulting in malfunction of the entire network.
60.	Risk factors	Inverter	Not following manufacturer guidelines and technical standards can lead to inadequate sizing of the inverter's electrical current, resulting in the risk of electrical discharge and fires.
62.	Risk factors	Inverter	Inadequate inverter sizing can reduce the energy generation capacity of the photovoltaic system, resulting in lower efficiency in capturing sunlight and, consequently, generating electrical energy.
63.	Risk factors	Inverter	Installing inverters vertically with an inclination greater than 5° can impede proper heat dissipation from the 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 electric shock, and accelerated corrosion of electrical components, reducing the equipment's lifespan.
66.	Risk factors	Inverter	Overheating and electrical arcs raise the temperature of the components, exceeding technical limits and causing premature wear and failures, and reducing the efficiency and lifespan of the equipment.
67.	Risk factors	Inverter	Aging of inverters and their components over time can result in wear and tear due to equipment usage, resulting in malfunctions and costs associated with corrective maintenance.
69.	Risk factors	Gateway (ModBus TCP)	The gateway overheating 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)	Defective indicator LEDs on the gateway can provide incorrect indications of its operation, resulting in failures compromising efficiency and hardware integrity.
72.	Risk factors	Gateway (ModBus TCP)	Theft of the inverter hardware can disable the ModBus TCP to RTU protocol conversion, impairing communication, and 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 systems and network information, resulting in risks to information integrity and availability and 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 data, inability to update the software, and inadequate control and monitoring of the inverters.
75.	Risk factors	Gateway (ModBus TCP)	Using manufacturer default keys on the gateway can make it easier for hackers to gain unauthorized access to data, compromising the security and privacy of that information and enabling data theft.

77.	Risk factors	Gateway (ModBus TCP)	The 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 confidential data associated with those IP addresses.
78.	Risk factors	Gateway (ModBus TCP)	Weak authentication and encryption can enable desynchronization attacks on TCP communication and hijack third-party connections, resulting in access to sensitive information and compromising 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 malicious packets targeted at a specific host, resulting in network traffic manipulation, information theft, injection of fake packages, or even denial of service (DoS) attacks.
81.	Risk factors	Gateway (ModBus TCP)	The absence of encryption in communication can enable source routing, allowing an attacker to monitor and intercept communications on the network, gaining access to confidential information and compromising overall network security.
85.	Risk factors	Gateway (ModBus TCP)	Inadequate maintenance on 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 loss of information stored in the gateway.
87.	Risk factors	Gateway (ModBus TCP)	Lack of technical skills and inadequate tools during gateway maintenance can exacerbate device failures, accelerating system integrity deterioration.
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 disruptions.
91.	Risk factors	Gateway (ModBus TCP)	Physical access by malicious agents can enable substituting the device with tampered hardware, resulting in financial losses and unauthorized access to the original owner's data.
93.	Risk factors	Gateway (ModBus TCP)	The lack of software authenticity and integrity checking can allow 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 disruptions or security vulnerabilities in the gateway.
95.	Risk factors	Gateway (ModBus TCP)	The 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)	The absence of software and firmware regular updates can leave the gateway vulnerable to known attacks avoidable by security patches.
98.	Risk factors	Gateway (ModBus TCP)	RS485 networks with incorrectly configured different Modbus addresses can lead to communication problems, such as duplicated responses to commands, interruptions, and failures in device communication.
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 data packet loss.
100.	HAZOP	Photovoltaic panel	Ambient temperatures above specified limits can cause thermal stress on photovoltaic panels, 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 the 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 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	Lightning strikes can cause overvoltages in the photovoltaic power system, irreversibly damaging solar cells, leading to short circuits and fires.
107.	HAZOP	Photovoltaic panel	The impact speed of hailstones exceeding 50 mph can cause microcracks or fissures in photovoltaic cells, reducing their mechanical strength and increasing the risk of short circuits in the system.
108.	HAZOP	Photovoltaic panel	Excessive snow accumulation on photovoltaic panels can damage the solar 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 result in panel detachment and internal damage to photovoltaic cells, resulting in reduced efficiency in power generation.
110.	HAZOP	Inverter	Increasing DC above specified technical limits can generate overvoltage, resulting in inverter shutdown and possible short circuits.
111.	HAZOP	Inverter	Defects in the inverter's electrical circuits can cause a decrease in DC voltage, resulting in insufficient input voltage to power the source during nighttime.
112.	HAZOP	Inverter	Lack of electrical grounding can compromise protection against leakage currents and lightning strikes, resulting in equipment damage and electrical accident risks.
113.	HAZOP	Inverter	Oversized installation of photovoltaic panels can result in lower output power than the input power, leading to prolonged operation of the inverter with lower efficiency and electrical energy loss.
114.	HAZOP	Inverter	AC elevation above specified technical limits and inadequate infrastructure can generate overvoltage, resulting in the photovoltaic inverter shutdown or burning electronic equipment connected to the grid.
115.	HAZOP	Inverter	A decrease in equipment's supply voltage can cause AC undervoltage, interrupting equipment operation.
116.	HAZOP	Inverter	Increased frequency above the technical specification limit, usually caused by an excessive energy supply compared to demand, can cause network disconnections, resulting in the massive shutdown of photovoltaic inverters and connected equipment.
117.	HAZOP	Inverter	Climate change, improper installation, and inadequate sizing can cause inverter overheating, reducing system-generated power and, in extreme cases, complete inverter shutdown.
118.	HAZOP	Inverter	Excessive cooling of the inverter, often due to climate changes such as snowstorms, can cause temperature sensor failures and metal component corrosion, compromising the equipment's proper functioning and resulting in 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	The absence of software inventory can compromise software management and owners' identification.
121.	NCSF	Inverter	The absence of organizational communication mapping and data flow can hinder comprehensive device management and attacks against network services.
122.	NCSF	Inverter	The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of network security threats and effective information management.
123.	NCSF	Inverter	The absence of security requirements and controls for management can hinder the management and control of information security.
124.	NCSF	Inverter	The absence of standards for reporting incidents and response procedures can compromise incident response and management.
126.	NCSF	Inverter	The absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersecurity risks.
127.	NCSF	Inverter	The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management and compliance analysis.
128.	NCSF	Inverter	The absence of specialized forums for mapping cyber threats can hinder the management of such threats.
129.	NCSF	Inverter	The absence of identification and documentation of internal threats can compromise asset integrity.
130.	NCSF	Inverter	The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information about these vulnerabilities and impede the definition of criteria for software installation.
131.	NCSF	Inverter	The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information security risks.
132.	NCSF	Gateway (ModBus TCP)	The absence 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)	The absence of software inventory can compromise software management and owners' identification.
134.	NCSF	Gateway (ModBus TCP)	The absence of organizational communication mapping and data flow can hinder comprehensive device management and attacks against network services.
135.	NCSF	Gateway (ModBus TCP)	The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of network security threats and effective information management.
136.	NCSF	Gateway (ModBus TCP)	The absence of security requirements and controls for management can hinder the management and control of information security.
137.	NCSF	Gateway (ModBus TCP)	The absence of standards for reporting incidents and response procedures can compromise incident response and management.
139.	NCSF	Gateway (ModBus TCP)	The absence of requirements for identification, assessment, and risk treatment plans can hinder the management of cybersecurity risks.
140.	NCSF	Gateway (ModBus TCP)	The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management and compliance analysis.
141.	NCSF	Gateway (ModBus TCP)	The absence of specialized forums for mapping cyber threats can hinder the management of these threats.
142.	NCSF	Gateway (ModBus TCP)	The absence of identification and documentation of internal threats can compromise asset integrity.
143.	NCSF	Gateway (ModBus TCP)	The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information about these vulnerabilities and impede the definition of criteria for software installation.
144.	NCSF	Gateway (ModBus TCP)	The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information security risks.