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

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
2.	Risk factors	Photovoltaic panel	fires.  Shadows caused by accumulated dirt on solar panels can prevent the capture of sunlight, decreasing electricity production.
3.	Risk factors	·	Internal corrosion of the panels due to exposure to extreme weather conditions, or the use of inadequate materials, can result in the
		Photovoltaic panel	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.  Exposure of solar panels to adverse weather conditions such as hailstorms, snowstorms, windstorms, and hurricanes can result in physical
5.	Risk factors	Photovoltaic panel	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
<i>J</i> .	Misk ractors	Thotovoltale parier	down the surface, resulting in a decrease in panel lifespan.  Exposure of the photovoltaic panel to high humidity locations (>0.85%) can cause damage to cells, such as loss of encapsulation adhesion,
11.	Risk factors	Photovoltaic panel	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
27	Risk factors	Photovoltaic panel	theft, and panel damage.  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.  Exposure of solar modules to high temperatures and high voltage levels can result in Potential Induced Degradation (PID), leading to defects in
32.	Risk factors	Photovoltaic panel	semiconductor materials and decreasing panel efficiency.
34. 35.	Risk factors Risk factors	Inverter	Inverter failure can disrupt the energy transfer to the grid and equipment, rendering the entire system useless.
		Inverter	Inverter overheating due to malfunction can rapidly deteriorate its components, resulting in fires and frequent equipment replacement.  Installing the inverter in an unsuitable location with direct exposure to sunlight can increase its temperature, resulting in accelerated
36.	Risk factors	Inverter	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
44.	Risk factors	Inverter	increase the likelihood of unauthorized breaches, enabling access to confidential information and possible theft of sensitive data.  The absence of an intrusion detection system, such as alarms and sensors, can prevent the identification and monitoring of inverter breaches,
45.	Risk factors	Inverter	allowing silent access to the data.  Overvoltage that exceeds the specified technical limit can cause damage to the inverter components, resulting in malfunction or even
46.	Risk factors	Inverter	equipment burnout.  The absence of integrity verification and failures in non-standardized software loading processes can enable data manipulation or deletion,
48.	Risk factors	Inverter	resulting in loss of accuracy, consistency, and reliability of the performed update.  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
52.	Risk factors	Inverter	conversion and overall equipment operation, resulting in shutdown, performance reduction, power loss, or, in extreme cases, fires.  Tapping into the communication network can allow control over multiple inverters connected to the bus, resulting in possible manipulation of
		arta	control signals sent to the inverters.  Failure to verify the authenticity of the software load by the inverter can allow the installation of tampered versions of the firmware, resulting
53.	Risk factors	Inverter	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
60.	Risk factors	Inverter	malfunction of the entire network.  Not following manufacturer guidelines and technical standards can lead to inadequate sizing of the inverter's electrical current, resulting in the
62.	Risk factors	Inverter	risk of electrical discharge and fires.  Inadequate inverter sizing can reduce the energy generation capacity of the photovoltaic system, resulting in lower efficiency in capturing
63.	Risk factors	Inverter	sunlight and, consequently, generating electrical energy.  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.  Installing the inverter in locations with high humidity and inadequate cable sealing can allow electrical current leakage, resulting in low
65.	Risk factors	Inverter	equipment insulation resistance, risk of electric shock, and accelerated corrosion of electrical components, reducing the equipment's lifespan.  Overheating and electrical arcs raise the temperature of the components, exceeding technical limits and causing premature wear and failures,
66.	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
67.	Risk factors	Inverter	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.  Improper installation of the inverter and gateway, along with incorrect network configurations, drivers, and specific settings, can compromise
70.	Risk factors	Gateway (ModBus TCP)	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
72.		Gateway (ModBus TCP)	hardware integrity.  Theft of the inverter hardware can disable the ModBus TCP to RTU protocol conversion, impairing communication, and security.
73.		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
74.	Risk factors	Gateway (ModBus TCP)	the installation of malware and malicious software.  Cable connection problems, such as damage or disconnections, can compromise communication between the supervisory system, inverters,
74. 75.		Gateway (ModBus TCP)  Gateway (ModBus TCP)	and the gateway, resulting in the loss of data, inability to update the software, and inadequate control and monitoring of the inverters.  Using manufacturer default keys on the gateway can make it easier for hackers to gain unauthorized access to data, compromising the security
73.	MISK IACIUIS	cateway (wioubus ice)	and privacy of that information and enabling data theft.

solutioned caccast a confidency indexa assumed with throse Productions.  For Set Ections  Carlway (Motion 175)  For Set Ections  For Set Ections  For Set Ections  Carlway (Motion 175)  For Set Ections  For Set E				
second sourceaster information and outgrounding network security.  1. Sink factors. Genery Moditors. 107 (1985) and the company of the properties of the properties of the company of the company of the company. The company of the co	7. I	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.
The land function (an incompanies) are large functioned and seatons of many targets and particular seatons or many targets and particul	B. 1	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.
Commonwealth   Comm	a 1	Dick factors	Gatoway (ModRus TCP)	The use of predictable initial sequence numbers can lead to TCP sequence number prediction, allowing the generation of malicious packets
Key Modity 170 Key Key Key Modity 170 Key Key Modit	J. 1	NISK Idelois	dateway (Modbus TCF)	(DoS) attacks.
Role Richter   Role	1. I	Risk factors	Gateway (ModBus TCP)	
Testings from social following proteins to the province of the	5. I	Risk factors	Gateway (ModBus TCP)	Inadequate maintenance on the gateway can alter its settings, resulting in operational failures and potential security breaches.
selections of lease for the control of the selection of t	6. I	Risk factors	Gateway (ModBus TCP)	
and result in financial losses and process discoptions.  80 Biol Bartos Garowy (Mordins 17)  80 Photocolial panel Carlos Gar	7. I	Risk factors	Gateway (ModBus TCP)	Lack of technical skills and inadequate tools during gateway maintenance can exacerbate device failures, accelerating system integrity deterioration.
19.   Bisk fettors   Greeney Mindustry   Physical access by medicions agents comers \$4.5.   8.   Bisk fettors   Genrousy Mindustry   The lack of of otherwise and territory on disregally developing an allow the installation of malicious software on the gateway, mail the lack of otherwise and territory on disregally developing and south territory and south territo	B. 1	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,
9. Bisk frotton  6. Bis	1. I	Risk factors	Gateway (ModBus TCP)	Physical access by malicious agents can enable substituting the device with tampered hardware, resulting in financial losses and unauthorized
New Risk factors Seavery (Modilus TCP) Resk factors Resk				access to the original owner's data.  The lack of software authenticity and integrity checking can allow the installation of malicious software on the gateway, resulting in
Rok factors				
Risk factors Gateway (Modiblas TOP)  Risk factor				The lack of standardization in software loading processes can lead to increased maintenance costs and time, resulting in decreased system
Resk fictors   Stelland   Stell				
Selection of Selection (Selection) (Select				RS485 networks with incorrectly configured different Modbus addresses can lead to communication problems, such as duplicated responses to
description or data packet loss.  Ambient temperature above specified limits can cause thermal stress on photovortaic panels, resulting in physical damage are maintenance and replacement costs.  Littene weather conditions such as snowstorms can cause the ambient temperature to drop below the specified limits, resulting in physical damage are maintenance and replacement costs.  Littene weather conditions such as snowstorms can cause the ambient temperature to drop below the specified limits, resulting in physical damage are maintenance and replacement costs.  Littene weather conditions such as snowstorms can cause the ambient temperature to drop below the specified limits, resulting in physical damage, and maintenance and replacement costs.  Littene weather conditions such as showstorms can cause on evolutings in the photocounties, negatively impacting the cellificating of the panels, negatively impacting the cellification of the panels, negatively impacting the cellification of the panels, negatively impacting the cellification of the panels of the panels, negatively impacting the cellification of the panels, negatively in the panels of the panels, negatively in the panels can distance in the photocountaic panels and maintain of the panels of the panels, negatively in the panels of the panels can distance in floating the panels of				commands, interruptions, and failures in device communication.  Natural aging of hardware, including cables, can result in communication failures from Modbus TCP to RTU protocol, leading to communication
maintenance and replacement costs.  Arabop Photovoltaic panel  Arabop Inverter  Defects in the inverter's collection of panel	9. I	Risk factors	Gateway (ModBus TCP)	disruption or data packet loss.
to the photovoltaic panel photovoltaic panels photovoltaic photovoltaic photovoltaic panels photovoltaic p	00.	HAZOP	Photovoltaic panel	maintenance and replacement costs.
Accessed in support of the protocolar panel and protocolar panel protoco	01.	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.
MAZDP   Photovoltaic panel   Agraes with high-relative humidity can lead to oxidation and corrosion of cables in the photovoltaic power plant.	04.	HAZOP	Photovoltaic panel	Areas with high relative humidity (>0.85%) can cause water condensation inside photovoltaic cells, reducing thermal insulation and increasing
107. HAZOP Photovoltaic panel AZOP Photovoltaic panel Externe weather conditions, such as strong winds above the specified immitted and increasing the risk of short orticalis in the system. A capacity to generate power of the photovoltaic panel Externe weather conditions, such as strong winds above the specified immitting, can result in panel detachment and internal and photovoltaic panels. The photovoltaic panels can damage the solor cells, reducing the system's capacity to generate or photovoltaic panels. The photovoltaic panels can be provided efficiency in power generation. Increasing De above specified technical limits can generate overvoltage, resulting in inverter shuddown and possible short circ. Increasing De above specified technical limits can generate overvoltage, resulting in insufficient input voltage to power to applicate the inverter's electrical circuits can cause a decrease in DC voltage, resulting in insufficient input voltage to power to applicate the inverter's electrical circuits can cause a decrease in DC voltage, resulting in insufficient input voltage to power to applicate the inverter's electrical circuits can cause a decrease in DC voltage, resulting in inverter with voltage to power to applicate panels can result in lower output power than the input power, leading to prolonged oper inverter with lower efficiency applicate panels can result in lower output power than the input power, leading to prolonged oper inverter with lower efficiency applicate the chincial specification in link, usually caused by an excessive energy supply compared to demand the proposal	05.	HAZOP	Photovoltaic panel	
MAZOP   Photovoltaic panel	06.	HAZOP	Photovoltaic panel	Lightning strikes can cause overvoltages in the photovoltaic power system, irreversibly damaging solar cells, leading to short circuits and fires.
NAZOP   Photovoltaic panel   Excessive snow accumulation on photovoltaic panels can damage the solar cells, reducing the system's capacity to generate possible   Photovoltaic panel   Extreme weather conditions, such as strong winds above the specified limit, can result in janed detachment and internal dam photovoltaic cells, resulting in reduced efficiency in power generation.   Photovoltaic panel   Photovoltaic cells, resulting in reduced efficiency in power generation.   Photovoltaic panel   Photovoltaic cells, resulting in reduced efficiency in power generation.   Photovoltaic panel	07.	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.
Investor	08.	HAZOP	Photovoltaic panel	Excessive snow accumulation on photovoltaic panels can damage the solar cells, reducing the system's capacity to generate power.
14.20   Inverter   Defects in the inverter's electrical circuits can cause a decrease in DC votage, resulting in inverter shutdown and possible short circ.	09.	HAZOP	Photovoltaic panel	Extreme weather conditions, such as strong winds above the specified limit, can result in panel detachment and internal damage to
111   HAZOP   Inverter   Defects in the inverter's electrical circuits can cause a decrease in DC voltage, resulting in insufficient input voltage to power to inpititude.	10.	HAZOP	Inverter	Increasing DC above specified technical limits can generate overvoltage, resulting in inverter shutdown and possible short circuits.
lack of electrical grounding can compromise protection against leakage currents and lightning strikes, resulting in equipment electrical excident risks.  113. HAZOP Inverter Oversized installation of photovoltaic panels can result in lower output power than the input power, leading to prolonged operations are composed on the provided installation of photovoltaic panels can result in lower output power than the input power, leading to prolonged operations are considered installation.  114. HAZOP Inverter Acceleration above specified technical limits and inadequate infrastructure can generate overvoltage, resulting in the photovoltaic inverters and considered to the grid.  115. HAZOP Inverter Acceleration above specified technical limits and inadequate subject on the provided inverters and connected equipment. Climate change, improper installation, and inadequate sizing can cause inverter overheating, reducing system-generated pow cases, complete inverter shortdown.  118. HAZOP Inverter Excessive cooling of the inverter, often due to climate changes such as snowstorms, can cause temperature sensor failures an component corrosino, compromising the equipment's proper functioning and resulting encominic losses for the photovoltaic inverter.  118. NCSF Inverter The absence of software inventory can compromise savet management, access authorization responsibilities can compromise asset management, access authorization responsibilities. Inverter The absence of software inventory can compromise software management and owners' identification.  119. NCSF Inverter The absence of software inventory can compromise software management and owners' identification.  120. NCSF Inverter The absence of stordards for reporting incidents and response procedures can compromise incident response and management and the leak of information and relative spices.  121. NCSF Inverter The absence of stordards for reporting incidents and response procedures can compromise incident response and management and surface and process and control of	11.	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
lectrical accident risks.  Overside installation of photovoltaic panels can result in lower output power than the input power, leading to prolonged ope inverter with lower efficiency and electrical energy loss.  AC elevation above specified technical limits and inadequate infrastructure can generate overvoltage, resulting in the photovord shutdown or burning electronic equipment connected to the grid.  Accessed in equipment's supply voltage can cause AC undervoltage, interrupting equipment operation.  Increased frequency above the technical specification limit, usually caused by an excessive energy supply compared to deman network disconnections, resulting in the massive shutdown of photovoltaic inverse and connected equipment. Climate change, improper installation, and inadequate sizing can cause inverter overheating, reducing system-generated pow cases, complete inverter est-hutdown.  Excessive cooling of the inverter of endue to climate changes such as sonstorms, can cause temperature sensor failures and the photovoltane of the		HAZOP	Inverter	nighttime.  Lack of electrical grounding can compromise protection against leakage currents and lightning strikes, resulting in equipment damage and
Inverter   Inverter with lower efficiency and electrical energy loss.   ACE   Inverter   ACE   Evation above specified rechnical limits and inadequate infrastructure can generate overvoltage, resulting in the photox shutdown or burning electronic equipment connected to the grid.				
shutdown or burning electronic equipment connected to the grid.  115. HAZOP inverter A decrease in equipment supply voltage can cause AC undervoltage, interrupting equipment operation.  116. HAZOP inverter A decrease in equipment's supply voltage can cause AC undervoltage, interrupting equipment operation.  117. HAZOP inverter Climate change, improper installation, and inadequate sizing can cause involving system-generated pow cases, complete inverter shutdown.  118. HAZOP inverter Climate change, improper installation, and inadequate sizing can cause involving system-generated pow cases, complete inverter, often due to climate changes such as snowstorms, can cause temperature sensor failures and composition of the inverter, often due to climate changes such as snowstorms, can cause temperature sensor failures and composition of the inverter. Orden due to climate changes such as snowstorms, can cause temperature sensor failures and composition of the inverter. Orden due to climate changes such as snowstorms, can cause temperature sensor failures and composition of the inverter of the inverter of the inverter, often due to climate changes such as snowstorms, can cause temperature sensor failures and composition of the inverter of security of assets, roles, and defined responsibilities can downsers' identification.  120. NCSF Inverter The absence of organizational communication mapping and data flow can hinder comprehensive device management and attended to the composition of the proper security inverted or the absence of security requirements and controls for management can hinder the management and control of information as the proper of the absence of security requirements and controls for management can hinder the management and control of information and tools for system and network compliance analysis.  121. NCSF Inverter The absence of security requirements or includents and response procedures can compromise incident response and management a	13.	HAZOP	Inverter	inverter with lower efficiency and electrical energy loss.
116. HAZOP Inverter Increased frequency above the technical specification limit, usually caused by an excessive energy supply compared to deman 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 pow cases, complete inverter shutdown.  118. HAZOP Inverter Exercise Cooling of the inverter, often due to climate changes such as snowstorms, can cause temperature sensor failures and component corrosion, compromising the equipment's proper functioning and resulting in economic losses for the photovoltal responsible parties, mapping, documentation, and handling of cybersecurity incidents.  119. NCSF Inverter The absence of organizational communication mapping and data flow can hinder comprehensive device management and attended the network services.  119. NCSF Inverter The absence of organizational communication mapping and data flow can hinder comprehensive device management and extended the lack of information classification can inhibit the detection of networks and effective information management.  119. NCSF Inverter The absence of standards for reporting incidents and response procedures can compromise incident response and management.  119. NCSF Inverter The absence of standards for reporting incidents and response procedures can compromise incident response and management.  120. NCSF Inverter The absence of requirements for risk identification, assessment, and treatment plans can hinder the management or pybersective.  121. NCSF Inverter The absence of requirements for risk identification assessment, and treatment plans can hinder the management or pybersective inverted the absence of requirements for risk identification of information devices and treatment plans can hinder the management or such threats.  122. NCSF Gateway (ModBus TCP) The absence of requirements for risk identification of reference for software inst	14.		Inverter	
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 pow cases, complete inverter shutdown.  118. HAZOP Inverter Climate change improper installation, and inadequate sizing can cause inverter overheating, reducing system-generated pow cases, complete inverter shutdown.  119. NCSF Inverter The lack of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorization responsible parties, mapping, documentation, and handling of cybersecurity incidents.  120. NCSF Inverter The absence of songarizational communication mapping and data flow can hinder comprehensive device management and attentions and the lack of information classification can inhibit the detection of network services.  121. NCSF Inverter The absence of strandards for reporting incidents and response procedures can compromise incident response and management.  122. NCSF Inverter The absence of strandards for reporting incidents and response procedures can compromise incident response and management and control of informations.  123. NCSF Inverter The absence of strandards for reporting incidents and response procedures can compromise incident response and management.  124. NCSF Inverter The absence of strandards for reporting incidents and response procedures can compromise incident response and management and control of informations and response procedures can compromise incident response and management.  125. NCSF Inverter The absence of of undersality information and tools for system and network compliance analysis can hinder the management of sychesecurity incidents.  126. NCSF Inverter The absence of of undersality information and tools for system and network compliance analysis can hinder the management of such threats.  127. NCSF Inverter The absence of of undersality information and tools for system and				
118. HAZOP Inverter cases, complete inverter shutdown.  119. NCSF Inverter Exessive cooling of the inverter, often due to climate changes such as snowstorms, can cause temperature sensor failures an component corrosion, compromising the equipment's proper functioning and resulting in economic losses for the photovoltal 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 att network services.  122. NCSF Inverter The absence of organizational communication mapping and data flow can hinder comprehensive device management and attentive services.  123. NCSF Inverter The absence of security requirements and controls for management.  124. NCSF Inverter The absence of security requirements and controls for management can hinder the management and control of information 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 cybersect and proposed procedures are not promised incident response and management.  127. NCSF Inverter The absence of specialized forums for mapping cyber threats can hinder the management of cybersect procedures can compromise asset integrity.  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 specialized forums for mapping cyber threats can compromise asset integrity.  130. NCSF Inverter The absence of a six treatment plans can hinder the definition of methods, processes, and controls for addressing information threats under the definition of methods, processes, and controls for addressing information and processes and tools and the lack of information and asset m	16.	HAZOP	Inverter	network disconnections, resulting in the massive shutdown of photovoltaic inverters and connected equipment.
118. NCSF Inverter component corrosion, compromising the equipment's proper functioning and resulting in economic losses for the photovoltal The lack of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorization 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 att 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 services.  123. NCSF Inverter The absence of security requirements and controls for management and information and information of threats and effective information management.  124. NCSF Inverter The absence of security requirements and controls for management can hinder the management and control of informations and the lack of information classification can inhibit the detection of network compliance analysis can hinder vulnerability management.  125. NCSF Inverter The absence of requirements for risk identification, assessment, and treatment plans can hinder vulnerability management and extractions on software installation.  126. NCSF Inverter The absence of specialized forums for mapping cyber threats can binder the management of such threats.  127. NCSF Inverter The absence of identification and documentation of internal threats can compromise asset integrity.  128. NCSF Gateway (ModBus TCP)  139. NCSF Gateway (ModBus TCP)  130. NCSF Gateway (ModBus TCP)  131. NCSF Gateway (ModBus TCP)  132. NCSF Gateway (ModBus TCP)  133. NCSF Gateway (ModBus TCP)  134. NCSF Gateway (ModBus TCP)  135. NCSF Gateway (ModBus TCP)  136. NCSF Gateway (ModBus TCP)  137. NCSF Gateway (ModBus TCP)  138. NCSF Gateway (ModBus TCP)  139. NCSF Gateway (ModBus TCP)  139.	17.	HAZOP	Inverter	
The lack of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorization responsible parties, mapping, documentation, and handling of cybersecurity incidents.  The absence of organizational communication mapping and data flow can hinder comprehensive device management and attributes.  The absence of organizational communication mapping and data flow can hinder comprehensive device management and attributes.  The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of net threats and effective information management.  The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of net threats and effective information management.  The absence of security requirements and controls for management and inhibit the detection of net threats and effective information management.  The absence of security requirements and controls for management and inhibit the detection of net threats and effective information and tontrols for management and inhibit the detection of information and the properties of the absence of standards for reporting incidents and response procedures can compromise incident response and management.  NCSF Inverter The absence of standards for reporting incidents and response procedures can compromise asset integrity.  The absence of precialized forums for mapping cyber threats can hinder the management of such threats.  Inverter The absence of specialized forums for mapping cyber threats can hinder the management of such threats.  Inverter The absence of sechical vulnerability management and retwork compliance analysis.  NCSF Inverter The absence of sechical vulnerability management and metwork compromise asset integrity.  The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information responsible paties and impede the definition of criteria for software installat	18.	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.
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 attractive interests and effective information management.  122. NCSF Inverter The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of netherats and effective information management.  123. NCSF Inverter The absence of security requirements and controls for management can hinder the management and control of informations of the absence of standards for reporting incidents and response procedures can compromise incident response and management.  124. NCSF Inverter The absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersec.  125. NCSF Inverter The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management.  126. NCSF Inverter The absence of identification and documentation of internal threats can compromise asset integrity.  127. NCSF Inverter The absence of etechnical vulnerability management and restrictions on software installation can hinder the collection of information of information of criteria for software installation.  128. NCSF Gateway (ModBus TCP) The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information responsibility and impede the definition of criteria for software installation.  128. NCSF Gateway (ModBus TCP) The absence of organizational communication mapping and data flow can hinder comprehensive device management and extractions on software management and owners' identification.  129. NCSF Gateway (ModBus TCP) The absence of organizational communication mapping and data flow can hinder comprehensive device management and extractive information management.  129. NCSF Gateway (ModBus TCP)	19.	NCSF	Inverter	The lack of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorization, identification of
network services.  122. NCSF Inverter The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of nethods.  123. NCSF Inverter The absence of security requirements and controls for management can hinder the management and control of information in the special part of the processes.  124. NCSF Inverter The absence of security requirements and controls for management can hinder the management and control of information in the special part of the special part of the processes.  125. NCSF Inverter The absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersec.  126. NCSF Inverter The absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersec.  127. NCSF Inverter The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability mana compliance analysis.  128. NCSF Inverter The absence of identification and documentation of internal threats can compromise asset integrity.  138. NCSF Inverter The absence of identification and documentation of internal threats can compromise asset integrity.  139. NCSF Inverter The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information these vulnerabilities and impede the definition of criteria for software installation.  139. NCSF Gateway (ModBus TCP) The absence of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorize identification.  130. NCSF Gateway (ModBus TCP) The absence of software inventory can compromise software management and owners' identification.  130. NCSF Gateway (ModBus TCP) The absence of software inventory can compromise and part of cybersecurity incidents.  131. NCSF Gateway (ModBus TCP) The absence of standards for reporting incidents and response procedures can compromise incident response and management.  1	20.	NCSF	Inverter	
122. NCSF Inverter The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of net 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 in the process of the process of security requirements and controls for management can hinder the management and control of information in the process of the process of the process of standards for reporting incidents and response procedures can compromise incident response and management on the process of inverter The absence of videntification, assessment, and treatment plans can hinder the management of cybersect The absence of videntification and tools for system and network compliance analysis can hinder vulnerability management.  128. NCSF Inverter The absence of specialized forums for mapping cyber threats can compromise asset integrity.  139. NCSF Inverter The absence of identification and documentation of internal threats can compromise asset integrity.  130. NCSF Inverter The absence of identification and documentation 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 these vulnerabilities and impede the definition of methods, processes, and controls for addressing information of a defined responsibilities can compromise asset management, access authorized information of a defined responsibilities can compromise asset management, access authorized information of a defined responsibilities can compromise asset management and attractivent of the absence of organizational communication mapping and data flow can hinder comprehensive device management and effective information management.  132. NCSF Gateway (ModBus TCP) The absence of security requirements and controls for management can hinder the management and control of information and complian	21.	NCSF	Inverter	The absence of organizational communication mapping and data flow can hinder comprehensive device management and attacks against
123. NCSF Inverter The absence of security requirements for risk identification, assessment, and treatment plans can hinder the management and control of information in the absence of security requirements for risk identification, assessment, and treatment plans can hinder the management of cybersect inverter.  126. NCSF Inverter The absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersect inverter. The absence of vulnerability information and tools for system and network compliance analysis can hinder the management of cybersect inverter. The absence of vulnerability information and tools for system and network compliance analysis 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 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 of riteria for software installation.  132. NCSF Gateway (ModBus TCP) The absence of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authoriz identification of responsible parties, mapping, documentation, and handling of cybersecurity incidents.  133. NCSF Gateway (ModBus TCP) The absence of organizational communication management and owners' identification.  134. NCSF Gateway (ModBus TCP) The absence of organizational communication management and owners' identification can inhibit the detection of network services.  135. NCSF Gateway (ModBus TCP) The absence of secritive information management and controls for management and owners' identification can inhibit the detection of network services.  136. NCSF Gateway (ModBus TCP) The absence of secritive information management and co	22.	NCSF	Inverter	The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of network 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 cybersect morphisms and provided in the management of cybersect morphisms and provided in the management of such threats.  128. NCSF Inverter The absence of subnerability information and tools for system and network compliance analysis can hinder tunerability management and restrictions on software installation.  128. NCSF Inverter The absence of identification and documentation of internal threats can compromise asset integrity.  139. NCSF Inverter The absence of a risk treatment plan can hinder the definition on software installation.  130. NCSF Inverter The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information of the special dentification.  130. NCSF Gateway (ModBus TCP) The absence of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorize identification.  130. NCSF Gateway (ModBus TCP) The absence of organizational communication mapping, documentation, and handling of cybersecurity incidents.  130. NCSF Gateway (ModBus TCP) The absence of organizational communication mapping and data flow can hinder comprehensive device management and attentive services.  131. NCSF Gateway (ModBus TCP) The absence of stendards for reporting incidents and response procedures can compromise incident response and effective information management.  132. NCSF Gateway (ModBus TCP) The absence of security requirements and controls for management can hinder the management and control of information in the services.  133. NCSF Gateway (ModBus TCP) The absence of security requirements for identification, assessment, and risk treatment plans can hinder the management of cybersective information management and restrictions and incident response an				threats and effective information management.  The absence of security requirements and controls for management can hinder the management and control of information security.
127. NCSF Inverter The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability manacompliance 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 of 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 in the sevulnerabilities and impede the definition of methods, processes, and controls for addressing information of the definition of methods, processes, and controls for addressing information in the definition of methods, processes, and controls for addressing information of the definition of methods, processes, and controls for addressing information in the definition of methods, processes, and controls for addressing information in the definition of methods, processes, and controls for addressing information in the definition of methods, processes, and controls for addressing information in the definition of methods, processes, and controls for addressing information in the definition of methods, processes, and controls for addressing information.  132. NCSF Gateway (ModBus TCP) The absence of software inventory can compromise software management and owners' identification.  133. NCSF Gateway (ModBus TCP) The absence of of threat monitoring processes and tools and the lack of information classification can inhibit the detection of information in the definition of the definition of management can hinder the management and control of information in the definition of the definition of management can hinder the management and cont				The absence of standards for reporting incidents and response procedures can compromise incident response and management.
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 of internal threats can compromise asset integrity.  131. NCSF Inverter The absence of a risk treatment plan can hinder the definition of criteria for software installation.  132. NCSF Gateway (ModBus TCP) The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information 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 enteror and effective information management.  135. NCSF Gateway (ModBus TCP) The absence of security requirements and controls for management can hinder the management and control of information and processes and tools and the lack of information classification can inhibit the detection of networks services.  136. NCSF Gateway (ModBus TCP) The absence of security requirements and controls for management can hinder the management and control of information and risk treatment plans can hinder the management of cybersec of a processes and tools and the lack of information can be proceed to the processes of the processes and tools and the lack of information can be proceed to the processes of the absence of requirements and controls for management can hinder the management and control of information and risk treatment plans can hinder the management of cybersec of a processes and tools for system and network compliance anal	26.	NCSF	Inverter	The absence of requirements for risk identification, assessment, and treatment plans can hinder the management of cybersecurity risks.
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 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 of the sex vulnerability and impede the definition of methods, processes, and controls for addressing information of responsible parties, mapping, documentation, and handling of cybersecurity incidents.  132. NCSF Gateway (ModBus TCP) The absence of software inventory can compromise software management and owners' identification.  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 threat monitoring processes and tools and the lack of information classification can inhibit the detection of information and exponse procedures can compromise incident response and management and effective information management.  135. NCSF Gateway (ModBus TCP) The absence of standards for reporting incidents and response procedures can compromise incident response and management and eff	27.	NCSF	Inverter	The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management and compliance analysis.
130. NCSF Inverter The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information (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 (address). The absence of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorize 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 attractive information management.  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 services.  136. NCSF Gateway (ModBus TCP) The absence of security requirements and controls for management can hinder the management and control of information services.  137. NCSF Gateway (ModBus TCP) The absence of security requirements and controls for management can hinder the management and control of information services.  138. NCSF Gateway (ModBus TCP) The absence of requirements for identification, assessment, and risk treatment plans can hinder the management of cybersed compliance analysis.  139. NCSF Gateway (ModBus TCP) The absence of specialized forums for mapping cyber threats can hinder the management of these threats.  140. NCSF Gateway (ModBus TCP) The absence of feechnical vulnerability management and restrictions on software installation can hinder the collection of information of criteria for software installation.	28.	NCSF	Inverter	·
these vulnerabilities and impede the definition of criteria for software installation.  NCSF Inverter The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information dedication.  NCSF Gateway (ModBus TCP) The absence of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorize identification of responsible parties, mapping, documentation, and handling of cybersecurity incidents.  NCSF Gateway (ModBus TCP) The absence of organizational communication mapping and data flow can hinder comprehensive device management and attractions and the lack of information classification can inhibit the detection of new threats and effective information management.  NCSF Gateway (ModBus TCP) The absence of standards for reporting incidents and response procedures can compromise incident response and management.  NCSF Gateway (ModBus TCP) The absence of requirements for identification, assessment, and risk treatment plans can hinder the management of cybersective information and tools for system and network compliance analysis can hinder vulnerability management.  NCSF Gateway (ModBus TCP) The absence of specialized forums for mapping cyber threats can hinder the management of these threats.  NCSF Gateway (ModBus TCP) The absence of specialized forums for mapping cyber threats can hinder the management of these threats.  NCSF Gateway (ModBus TCP) The absence of identification and documentation of internal threats can compromise asset integrity.  The absence of technical vulnerability management and restrictions on software installation can hinder the collection of informations of these vulnerabilities and impede the definition of criteria for software installation.	29.	NCSF	Inverter	
131. NCSF Inverter The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information identification.  132. NCSF Gateway (ModBus TCP) The absence of an inventory of assets, roles, and defined responsibilities can compromise asset management, access authorize 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 attractions and the lack of information classification can inhibit the detection of new 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 software inventory.  137. NCSF Gateway (ModBus TCP) The absence of standards for reporting incidents and response procedures can compromise incident response and management.  138. NCSF Gateway (ModBus TCP) The absence of requirements for identification, assessment, and risk treatment plans can hinder the management of cybersection of the absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management.  140. NCSF Gateway (ModBus TCP) The absence of specialized forums for mapping cyber threats can hinder the management of these threats.  141. NCSF Gateway (ModBus TCP) The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information of criteria for software installation.	30.	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.
identification of responsible parties, mapping, documentation, and handling of cybersecurity incidents.  NCSF Gateway (ModBus TCP) The absence of software inventory can compromise software management and owners' identification.  NCSF Gateway (ModBus TCP) The absence of organizational communication mapping and data flow can hinder comprehensive device management and att network services.  NCSF Gateway (ModBus TCP) The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of network services.  NCSF Gateway (ModBus TCP) The absence of security requirements and controls for management can hinder the management and control of informations of Sateway (ModBus TCP) The absence of standards for reporting incidents and response procedures can compromise incident response and management and control of NCSF Gateway (ModBus TCP) The absence of requirements for identification, assessment, and risk treatment plans can hinder the management of cybersect of Sateway (ModBus TCP) The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management and source of specialized forums for mapping cyber threats can hinder the management of these threats.  NCSF Gateway (ModBus TCP) The absence of identification and documentation of internal threats can compromise asset integrity.  NCSF Gateway (ModBus TCP) The absence of identification and documentation of criteria for software installation can hinder the collection of information of criteria for software installation.	31.	NCSF	Inverter	The absence of a risk treatment plan can hinder the definition of methods, processes, and controls for addressing information security risks.
133. NCSF Gateway (ModBus TCP) The absence of software inventory can compromise software management and owners' identification.  134. NCSF Gateway (ModBus TCP)  135. NCSF Gateway (ModBus TCP)  136. NCSF Gateway (ModBus TCP)  137. NCSF Gateway (ModBus TCP)  138. NCSF Gateway (ModBus TCP)  139. NCSF Gateway (ModBus TCP)  140. NCSF Gateway (ModBus TCP)  150. NCSF Gateway (ModBus TCP)  161. NCSF Gateway (ModBus TCP)  170. NCSF Gateway (ModBus TCP)  170. NCSF Gateway (ModBus TCP)  170. NCSF Gateway (ModBus TCP)  171. NCSF Gateway (ModBus TCP)  172. NCSF Gateway (ModBus TCP)  173. NCSF Gateway (ModBus TCP)  174. NCSF Gateway (ModBus TCP)  175. The absence of security requirements and controls for management and response procedures can compromise incident response and management and response procedures can compromise incident response and management and response procedures can compromise incident response and management and response procedures can compromise incident response and management and response procedures can compromise incident response and management and response procedures can compromise incident response and management of cybersed and response procedures can compromise and management of cybersed and response procedures can compromise analysis can hinder the management of cybersed and response procedures can compromise analysis can hinder vulnerability management and response procedures can compromise asset integrity.  143. NCSF Gateway (ModBus TCP)  144. NCSF Gateway (ModBus TCP)  145. NCSF Gateway (ModBus TCP)  146. Draw (ModBus TCP)  147. NCSF Gateway (ModBus TCP)  148. NCSF Gateway (ModBus TCP)  149. NCSF Gateway (ModBus TCP)  140. NCSF Gateway (ModBus TCP)  141. NCSF Gateway (ModBus TCP)  142. NCSF Gateway (ModBus TCP)  143. NCSF Gateway (ModBus TCP)  144. NCSF Gateway (ModBus TCP)	32.	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.
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 net 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 in threats and effective information in threats and response procedures can compromise incident response and management management.  137. NCSF Gateway (ModBus TCP)  The absence of standards for reporting incidents and response procedures can compromise incident response and management management.  The absence of requirements for identification, assessment, and risk treatment plans can hinder the management of cybersed compliance analysis can hinder vulnerability management.  The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management.  NCSF Gateway (ModBus TCP)  The absence of specialized forums for mapping cyber threats can hinder the management of these threats.  NCSF Gateway (ModBus TCP)  The absence of identification and documentation of internal threats can compromise asset integrity.  The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information information in the detection of information in the detec	33.	NCSF	Gateway (ModBus TCP)	The absence of software inventory can compromise software management and owners' identification.
135. NCSF Gateway (ModBus TCP)  The absence of threat monitoring processes and tools and the lack of information classification can inhibit the detection of netherats 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 so	34.	NCSF	Gateway (ModBus TCP)	The absence of organizational communication mapping and data flow can hinder comprehensive device management and attacks against network services.
136.NCSFGateway (ModBus TCP)The absence of security requirements and controls for management can hinder the management and control of information of security requirements.137.NCSFGateway (ModBus TCP)The absence of standards for reporting incidents and response procedures can compromise incident response and management.139.NCSFGateway (ModBus TCP)The absence of requirements for identification, assessment, and risk treatment plans can hinder the management of cybersed compliance.140.NCSFGateway (ModBus TCP)The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management.141.NCSFGateway (ModBus TCP)The absence of specialized forums for mapping cyber threats can hinder the management of these threats.142.NCSFGateway (ModBus TCP)The absence of identification and documentation of internal threats can compromise asset integrity.143.NCSFGateway (ModBus TCP)The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information of criteria for software installation.	35.	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
139. NCSF Gateway (ModBus TCP) 140. NCSF Gateway (ModBus TCP) 141. NCSF Gateway (ModBus TCP) 142. NCSF Gateway (ModBus TCP) 143. NCSF Gateway (ModBus TCP) 144. NCSF Gateway (ModBus TCP) 145. NCSF Gateway (ModBus TCP) 146. NCSF Gateway (ModBus TCP) 147. NCSF Gateway (ModBus TCP) 148. NCSF Gateway (ModBus TCP) 149. NCSF Gateway (ModBus TCP) 140. NCSF Gateway (ModBus TCP) 141. NCSF Gateway (ModBus TCP) 142. NCSF Gateway (ModBus TCP) 143. NCSF Gateway (ModBus TCP) 144. NCSF Gateway (ModBus TCP) 145. NCSF Gateway (ModBus TCP) 146. NCSF Gateway (ModBus TCP) 147. NCSF Gateway (ModBus TCP) 148. NCSF Gateway (ModBus TCP) 149. NCSF Gateway (ModBus TCP) 149. NCSF Gateway (ModBus TCP) 140. NCSF Gateway (ModBus TCP) 140. NCSF Gateway (ModBus TCP) 140. NCSF Gateway (ModBus TCP) 141. NCSF Gateway (ModBus TCP) 142. NCSF Gateway (ModBus TCP) 143. NCSF Gateway (ModBus TCP) 144. NCSF Gateway (ModBus TCP) 145. NCSF Gateway (ModBus TCP) 146. NCSF Gateway (ModBus TCP) 147. NCSF Gateway (ModBus TCP) 148. NCSF Gateway (ModBus TCP) 149. NCSF Gateway (ModBus TCP) 149. NCSF Gateway (ModBus TCP) 140. NCSF Gateway (ModBus TCP) 140. NCSF Gateway (ModBus TCP) 141. NCSF Gateway (ModBus TCP) 142. NCSF Gateway (ModBus TCP) 143. NCSF Gateway (ModBus TCP) 144. NCSF Gateway (ModBus TCP) 145. NCSF Gateway (ModBus TCP) 146. NCSF Gateway (ModBus TCP) 146. NCSF Gateway (ModBus TCP) 147. NCSF Gateway (ModBus TCP) 148. NCSF Gateway (ModBus TCP) 149. NCSF Gateway (ModBus TCP)	36.	NCSF	Gateway (ModBus TCP)	The absence of security requirements and controls for management can hinder the management and control of information security.
140. NCSF Gateway (ModBus TCP)  The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management.  NCSF Gateway (ModBus TCP)  The absence of specialized forums for mapping cyber threats can hinder the management of these threats.  NCSF Gateway (ModBus TCP)  The absence of identification and documentation of internal threats can compromise asset integrity.  The absence of identification and documentation of internal threats can compromise asset integrity.  The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information in the collection of information and tools for system and network compliance analysis can hinder vulnerability management of these threats.				The absence of standards for reporting incidents and response procedures can compromise incident response and management.
141. NCSF Gateway (ModBus TCP) compliance analysis.  142. NCSF Gateway (ModBus TCP) The absence of specialized forums for mapping cyber threats can hinder the management of these threats.  143. NCSF Gateway (ModBus TCP) The absence of identification and documentation of internal threats can compromise asset integrity.  144. NCSF Gateway (ModBus TCP) The absence of identification and documentation of internal threats can compromise asset integrity.  145. NCSF Gateway (ModBus TCP) The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information of criteria for software installation.	39.	NCSF	Gateway (ModBus TCP)	The absence of requirements for identification, assessment, and risk treatment plans can hinder the management of cybersecurity risks.  The absence of vulnerability information and tools for system and network compliance analysis can hinder vulnerability management and
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 identification and documentation of internal threats can compromise asset integrity.  144. The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information in the collection in the collection of information in the collection in the co	40.	NCSF	Gateway (ModBus TCP)	
143. NCSF Gateway (ModBus TCP)  The absence of technical vulnerability management and restrictions on software installation can hinder the collection of information these vulnerabilities and impede the definition of criteria for software installation.			, , ,	
these vulnerabilities and impede the definition of criteria for software installation.				
				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	44.	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.