#	Threat Description
I1.1	**Basic Threat:** B1. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage access to the 5G slice and attempt to compromise the infrastructure responsible for distributing ICS process keys, generate a new key, and use the key to inject false data into the calculation of new DER setpoints.
I1.2	**Basic Threat:** B1. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may attempt to target a DC/CC node to extract application key material, (for instance exploiting Heartbleed-like vulnerabilities [18]) and use this to inject false data into the calculation of new DER setpoints.
I1.3	**Basic Threat:** None. **Attacker location:** Physical. **Relevant Architecture:** Centralized. **Threat Description:** An inside operator may attempt to tamper with legitimate data or inject false data into the calculation of new DER setpoints.
I1.4	**Basic Threat:** B4. **Attacker location:** Physical or in wireless range. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised CC/DC node and attempt to install malware which can tamper with legitimate data or inject false data into the calculation of new DER setpoints.
I1.5	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may attempt to leverage a compromised PS or SP to install malware on the DC/CC node, which can tamper with legitimate data or inject false data into the calculation of new DER setpoints.
I1.6	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Centralized. **Threat Description:** An attacker may attempt to leverage a compromised PD or SP to install malware in the control center through the supply chain, which can tamper with legitimate data or inject false data into the calculation of new DER setpoints.
I1.7	**Basic Threat:** B4. **Attacker location:** Physical. **Relevant Architecture:** Both. **Threat Description:** An attacker may attempt to steal a CC/DC node and physically manipulate the sensor readings directly (for instance by applying heat to it), potentially while also moving it to another location.
I1.8	**Basic Threat:** B1. **Attacker location:** Remote. **Relevant Architecture:** Centralized. **Threat Description:** An attacker may attempt to target the CC server to extract application key material, (for instance exploiting Heartbleed-like vulnerabilities [18]) and use this to inject false data into the calculation of new DER setpoints.
I1.9	**Basic Threat:** B4. **Attacker location:** Physical, wireless range. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised CC/DC node, attempt to extract 5G and application key material, and use this to inject false data into the calculation of new DER setpoints.

Table 1. Threats to integrity of processes, I2.

#	Threat Description
I2.1	**Basic Threat:** B1. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage access to the 5G slice and attempt to compromise application-level authentication to program or change control logic in the processes which are part of the ICS function.
I2.2	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised PS to embed a malware which can program or change control logic in the processes which are part of the ICS function.
I2.3	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised SP to reprogram or reconfigure the processes in the CC/DC nodes which are part of the ICS function.
I2.4	**Basic Threat:** None. **Attacker location:** Physical. **Relevant Architecture:** Centralized. **Threat Description:** An inside operator may attempt to change the logic/setpoints in the processes in the different CC nodes from the control center.
I2.5	**Basic Threat:** B4. **Attacker location:** Physical, wireless range. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised DC/ CC node and use this to attempt to change program logic.
I2.6	**Basic Threat:** B2. **Attacker location:** Remote. **Relevant Architecture:** Centralized. **Threat Description:** An attacker may attempt to compromise and gain privileges on the CC server in the control center which in turn can be used for changing ICS function logic.
I2.7	**Basic Threat:** B1 or B2. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage access to the 5G slice, or the DSO control center attempt to

	exploit the remote update/configuration functionality of the CC/DC nodes, administered through a server in the DSO control center.
I2.8	**Basic Threat:** B4. **Attacker location:** Physical, wireless range. **Relevant Architecture:** Distributed. **Threat Description:** An attacker may leverage a compromised DC node and attempt to spread malware in the form of a worm, which may be used to tamper with legitimate data or inject false data into the calculation of new setpoints.

Table 2. Threats to availability of transmitted data, A1.

#	Threat Description
A1.1	**Basic Threat:** None. **Attacker location:** Wireless range. **Relevant Architecture:** Both. **Threat Description:** An attacker may attempt to jam the 5G signal between the CC/DC and the RAN.
A1.2	**Basic Threat:** B1 or B2. **Attacker location:** Remote. **Relevant Architecture:** Distributed. **Threat Description:** An attacker may attempt to deny the functioning of the service keeping track of DC nodes in the network, for instance by obtaining privileges on the server implementing the service, or by flooding the server with traffic.
A1.3	**Basic Threat:** B5. **Attacker location:** Remote. **Relevant Architecture:** Centralized. **Threat Description:** An attacker may leverage access to the private network between the 5G CN and the DSO control center and launch a traffic-based DoS attack on the 5G CN and DSO control center interfaces.
A1.4	**Basic Threat:** B1 or B2. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage access to the 5G slice or the DSO control center to target the authentication infrastructure deployed there, to attempt to revoke the long-term cryptographic key/certificate used by ICS function processes running in the CC/DC nodes, to make the receiver discard communication encrypted with the key. This can for instance be done by exploiting an insecure implementation or compromising an admin account.
A1.5	**Basic Threat:** None. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may attempt to revoke the eSIMs used by CC/DC nodes, to deny the node access to the 5G network. This can for instance be attempted by pretending to be the DSO towards the MNO.
A1.6	**Basic Threat:** None. **Attacker location:** Physical. **Relevant Architecture:** Both. **Threat Description:** An attacker may attempt to cut cables connecting the 5G base stations, or otherwise destroy base stations.
A1.7	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised MNO supplier and attempt to deny the service of the 5G CN functions needed for the correct functioning of the 5G slice.
A1.8	**Basic Threat:** None. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An employee at the MNO may attempt to take down or alter 5G services needed for the correct functioning of the 5G slice.
A1.9	**Basic Threat:** None. **Attacker location:** Physical. **Relevant Architecture:** Centralized. **Threat Description:** An employee at the DSO may attempt to take down or alter services in the control center (e.g, crashing the algorithm solver, blocking all traffic to the firewall) needed for the correct functioning of the ICS function.

Table 3. Threats to availability of ICS function processes, A2.

#	Threat Description
A2.1	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised PS or SP delivering any of the software used by the processes in the ICS function, and embed malware which can compromise the availability.
A2.2	**Basic Threat:** B4. **Attacker location:** Remote. **Relevant Architecture:** Centralized. **Threat Description:** An attacker may leverage a compromised CC node and use it to attempt to launch a denial-of-service attack on the CC server.
A2.3	**Basic Threat:** B4. **Attacker location:** Remote. **Relevant Architecture:** Distributed. **Threat Description:** An attacker may leverage a compromised DC node and use it to attempt to launch a denial-of-service attack on neighboring DC nodes.

A2.4	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised PS to embed malware in the software running in the processes that are part of the ICS function. This malware can proceed to cause denial of service.
A2.5	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Distributed. **Threat Description:** An attacker may leverage a compromised SP to exploit the remote update functionality and install malware on the processes running in the CC/DC nodes or CC server. This malware can proceed to cause denial of service.
A2.6	**Basic Threat:** B4. **Attacker location:** Remote. **Relevant Architecture:** Distributed. **Threat Description:** An attacker may leverage a compromised DC node to attempt to spread malware to other DC nodes in the form of a worm. This malware can proceed to cause denial of service.

Table 4. Threats to availability of underlying infrastructure, A3.

#	**Threat Description**
A3.1	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker may leverage a compromised PS or SP developing software that the ICS function relies on, e.g., developers or maintainers of the relevant operating system, monitoring software or asset inventory software. By embedding denial of service malware in this software, an attacker can compromise the availability of the ICS function.

Table 5. Threats to confidentiality of ICS data, C1.

#	**Threat Description**
C1.1	**Basic Threat:** None. **Attacker location:** Physical. **Relevant Architecture:** Centralized. **Threat Description:** An employee at the DSO might attempt to sell market sensitive data.
C1.2	**Basic Threat:** None. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An insider at the SP might attempt to steal market sensitive data, for instance by transferring data to an online server or by transferring it to a hard drive.
C1.3	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker might leverage a compromised PS or SP to embed malware in their products, to later extract market sensitive data.
C1.4	**Basic Threat:** B3. **Attacker location:** Remote. **Relevant Architecture:** Both. **Threat Description:** An attacker might leverage a compromised SP to use their access to steal market sensitive data.
C1.5	**Basic Threat:** B4. **Attacker location:** Remote. **Relevant Architecture:** Distributed. **Threat Description:** An attacker may leverage a compromised DC node and use the access to attempt to spread malware in the form of a worm, which can be used to extract data.