
INCIDENT CLASSIFICATION SCALE

Incident Classification Scale Subgroup

4 December 2019

Table of Contents

1. General	3
2. General overview and criteria prioritization	4
3. Reporting rules	6
3.1. General rules	6
3.2. Reporting process and timeline	7
3.3. Procedure for multiple incidents and involving several TSOs	7
4. Definitions of ICS criteria	8
4.1 Blackout (OB)	8
4.2 Incidents on load (L)	9
4.3 Incidents leading to frequency degradation (F)	10
4.4 Incidents on network elements (T)	12
4.5 Incidents on power generating facilities (G)	14
4.6 N and N-1 violations (ON)	15
4.7 Separation from the grid (RS)	16
4.8 Loss of tools, means and facilities (LT)	17
4.9 Violation of standards on voltage (OV)	18
4.10 Reduction of reserve capacity (RRC)	21
5. Operational security indicators	22
5.1 Operational security indicators relevant to operational security	22
5.2 Operational security indicators relevant to operational planning	24
6. Procedure for the investigation of scale 2 and scale 3 incidents	25
6.1 Communication	25
6.2 Expert Panel	25
6.3 Timeline for the investigation of scale 2 and scale 3 incidents	26
6.4 Data Collection	26
6.5 Factual Report	26
6.6 Final Report	26
7. Annual Report	28
7.1 Contents of the annual reports	28
7.2 Process for the preparation of the annual report	28
Annexes	29
Annex 1 Common data for reporting	29
Annex 2 Specific data reported for depending on the ICS criterion	29
Annex 3 Additional data for the investigation of scale 2 and scale 3 incidents	30

1. General

Incident Classification Scale has been developed in accordance with Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 and updated to fulfil the objectives of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation [hereinafter SO GL] Article 15.

Article 15 of SO GL sets the obligation on transmission system operators [hereinafter TSOs] of each European Union Member State to provide ENTSO-E with the necessary data and information for the preparation of annual report based on Incident Classification Scale [hereinafter ICS], and on ENTSO-E to publish the annual report.

With the ENTSO-E System Operations Committee decision on 4 December 2019 approving the current methodology, all ENTSO-E member TSOs, including those from non-EU countries, agree to provide the necessary data and information for the preparation of annual report and the publication of the annual report, considering that each annual report will be approved separately by System Operations Committee for publication.

Incident Classification Scale aims at:

- providing overview of operational security indicators specified in article 15 of SO GL;
- identification of any necessary improvements, which are necessary in order to support sustainable and long-term operational security;
- identification of any appropriate improvements to network operation tools required to maintain operational security and related to real-time operation and operational planning to support TSOs in their task identified in the article 55(e) of SO GL;
- providing explanations of the reasons for incidents at the operational security ranking scales 2 and 3 as per the incidents classification scale adopted by ENTSO for Electricity; those explanations shall be based on an investigation of the incidents by TSOs which process shall be set out in the incidents classification scale.

The deliverable of Incident Classification Scale is the annual report based on the incidents classification scale prepared in accordance with article 15 of SO GL.

2. General overview and criteria prioritization

Incident Classification Scale consists of 4 scales (Scale 0, 1, 2 and 3) with levels of severity ranging from local incidents up to major incidents. System events which are not classified as incidents are recorded in a 'Below Scale' category. The severity levels are compliant with the system state classification in accordance with the article 18 of SO GL:

- Below Scale*: for anomalies, local event; the system remains in normal state;
- Scale 0: for noteworthy local incident, the system remains in normal state;
- Scale 1: for significant incident; violation of operational security limit; the system is in alert state;
- Scale 2: for extensive incident; probability of wide area incident; the system is in emergency state;
- Scale 3: for major incident in the control area of one transmission system operator; the system is in blackout state.

*Remark: 'Below Scale' level has been added to report events that are needed to be calculated for the operational security indicators that are relevant to operational security but these events are not included in the ICS Scale 0, 1, 2 and 3. These events are considered anomalies. 'Below Scale' only exists for reporting of violations of standards of voltage, incidents on power generating facilities and incidents leading to frequency degradation. For all other criteria the ICS scales of 0, 1, 2 and 3 are sufficient to calculate the operational security indicators.

Table 1 Incident Classification Scale

Scale 0 Noteworthy incident		Scale 1 Significant incident		Scale 2 Extensive incident		Scale 3 Major incident / 1TSO	
Priority/Short definition (Criterion short code)		Priority-Short definition (Criterion short code)		Priority-Short definition (Criterion short code)		Priority-Short definition (Criterion short code)	
#20	Incidents on load (L0)	#11	Incidents on load (L1)	#2	Incidents on load (L2)	#1	Blackout (OB3)
#21	Incidents leading to frequency degradation (F0)	#12	Incidents leading to frequency degradation (F1)	#3	Incidents leading to frequency degradation (F2)		
#22	Incidents on transmission network elements (T0)	#13	Incidents on transmission network elements (T1)	#4	Incidents on transmission network elements (T2)		
#23	Incidents on power generating facilities (G0)	#14	Incidents on power generating facilities (G1)	#5	Incidents on power generating facilities (G2)		
		#15	N-1 violation (ON1)	#6	N violation (ON2)		
#24	Separation from the grid (RS0)	#16	Separation from the grid (RS1)	#7	Separation from the grid (RS2)		
#25	Violation of standards on voltage (OV0)	#17	Violation of standards on voltage (OV1)	#8	Violation of standards on voltage (OV2)		
#26	Reduction of reserve capacity (RRC0)	#18	Reduction of reserve capacity (RRC1)	#9	Reduction of reserve capacity (RRC2)		
#27	Loss of tools and facilities (LT0)	#19	Loss of tools and facilities (LT1)	#10	Loss of tools and facilities (LT2)		

The priority of each criterion is shown in table 1 with a number from 1 to 27, where 1 marks the criterion with highest priority and 27 marks the criterion with lowest priority. **When an incident meets several criteria, the incident is classified according to the criterion that has the highest priority, however all sub criteria information also need to be reported.**

Scale 0 considerations

Incidents are classified as scale 0 incidents taking into account the following considerations:

The system is in normal state after the incident - the system is within operational security limits in the N situation and after the occurrence of any contingency from the contingency list, taking into account the effect of the available remedial actions (SO GL article 3(5)).

Scale 1 considerations

Incidents are classified as scale 1 incidents taking into account the following considerations:

The system is in alert state after the incident - the system is within operational security limits, but a contingency from the contingency list has been detected and in case of its occurrence the available remedial actions are not sufficient to keep the normal state (SO GL Article 3(17)).

Scale 2 considerations

Incidents are classified as scale 2 incidents taking into account the following considerations:

The system is in emergency state after the incident - one or more operational security limits are violated (SO GL Article 3(37)).

Scale 3 considerations

Incidents are classified as scale 3 incidents taking into account the following considerations:

The system is in blackout state after the incident - the operation of part or all of the transmission system is terminated (SO GL article 3(22)).

The real-time status of the system state (alert, emergency or blackout) is reported through the ENTSO-E Awareness System [hereinafter EAS]. The EAS is focused on real time consequences of incidents and the actual situation in the grid. Consequently, it should be possible to classify all the incidents which are declared in the EAS according to the scales defined in the ICS.

Since the EAS is operated in real time, the state of the system is determined using only the information that is readily available. Under certain circumstances, this can result in discrepancies between system state declared in EAS and classification of an incident at a later stage.

3. Reporting rules

3.1. General rules

The Incidents Classification Scale must be applied by each TSO as defined in SO GL and by each ENTSOE member TSO not bound by SO GL. The following principles shall be applied:

- each TSO shall nominate a single point of contact (ICS SPOC) that is responsible for:
 - reporting the incidents in accordance with Incident Classification Scale;
 - responding to inquiries regarding the reported incidents; and
 - validating the data of its TSO in the draft annual report.
- the incidents are reported in case the effect(s) or initiating event(s) occur in the network with an operating voltage at or above **220 kV** and in network with operating voltage levels below 220kV when relevant for maintaining operational security.
- each TSO shall define its own internal organization to apply the ICS;
- the list of common data to be reported for each incident is given in the Annex I of this methodology; depending on the type of incident, additional data is requested to allow the investigation of incidents, these additional data items are listed under each criterion;
- reporting shall be done by the TSO in whose control area the incident has occurred and by all other TSOs affected by the initiating incident in case the consequences in their own systems reach at least the thresholds for scale 0 incidents;
- frequency deviations are reported by one TSO per synchronous area, specified in chapter 4.3 on incidents leading to frequency degradation.

Each TSO must perform the following:

- identify the origin of the incident;
- identify the consequences of the incident in its control area;
- measure the effect of the incident to the transmission system parameters;
- assess the effect of the incident outside its control area.

3.2. Reporting process and timeline

The reporting period for ICS annual reports is one calendar year. Each TSO shall report the incidents occurring between 1 January and 31 December. When an incident begins in one calendar year and ends in another calendar year, the incident is included in the ICS annual report for the year in which the incident began.

Each TSO shall report an incident classified in accordance with the criteria of ICS in the reporting tool at the latest by the end of the month following the month in which the incident began. Subgroup Incident Classification Scale [hereinafter SG ICS] analyses the incidents reported by TSOs and freezes the database of incidents after the end of each quarter of the year:

- the data related to the incidents occurring from 1 January to 31 March is frozen on 1 May;
- the data related to the incidents occurring from 1 April to 30 June is frozen on 1 August;
- the data related to the incidents occurring from 1 July to 30 September is frozen on 1 November;
- the data related to the incidents occurring from 1 October to 31 December is frozen on 1 February of the following year.



TSOs may modify the data after the above deadlines subject to the approval of the SG ICS.

For clarity, the SO GL mandates by 1st March each TSO will provide the necessary data and information for the preparation of the annual reports based on the incident classification scale. The ICS report will be published each year by 30th September.

3.3. Procedure for multiple incidents and involving several TSOs

When an incident (knowingly or unknowingly) affects multiple TSOs, each TSO will report on the incident as it affects their transmission network to aid the incident investigation. When TSOs become aware that multiple incidents were caused by a single incident, such multiple incidents shall be combined into a single incident according to the prioritization of the ICS criteria. An incident report will be prepared containing all the system impacts for all affected TSOs.

4. Definitions of ICS criteria

4.1 Blackout (OB)

General description

After the incident occurs, the system is in blackout state. Blackout is only counted on scale 3 (OB3). An incident is classified according to this criterion in case one of the following conditions from SO GL article 18(4) is fulfilled:

- loss of more than 50% of demand in the concerned TSO's control area; or
- total absence of voltage for at least three minutes in the concerned TSO's control area, leading to the triggering of restoration plans.

Exceptions

The following exceptions apply for the description of the criterion above:

- A TSO of GB and IE/Ni synchronous areas may develop a proposal specifying the level of demand loss at which the transmission system shall be in the blackout state according to SO GL article 18.4
- For isolated systems, the system is in blackout in case of loss of more than 70% of load (loadshedding) at the time of the incident or total shut down.

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- An estimate of disconnected load (MW);
- Energy not supplied (MWh).

4.2 Incidents on load (L)

General description

Disconnection of load with duration of at least 3 minutes is classified according to this criterion in case one of the following conditions is fulfilled:

- Disconnection due to tripped network elements; or
- Activation of system defense plan measures (automatic low frequency and low voltage demand disconnection); or
- Manual disconnection of load or activation of controlled load reduction for adequacy.

Exceptions:

The following exceptions apply for the description of the criterion above:

- Disconnection of load less than 100 MW is not reported;
- Manual disconnections of load that participate in the interruptible load services are not reported.

Table 2 Thresholds by scale for incidents on load

	CE	Nordic	GB	IRE/NI	Baltic	Isolated systems
Scale 0	Loss of less than 1 % of load in a TSO's control area					Loss of 1% to 5% of load in a TSO's control area
Scale 1 L1	Loss of >1 to ≤10% of load in a TSO's control area					Loss of 5% to 15% of load in a TSO's control area
Scale 2 L2	Loss of >10 to ≤50% of load in a TSO's control area					Loss of 15% to 70% of load in a TSO's control area
Scale 3						

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- An estimate of disconnected load (MW);
- An estimate of disconnected generation (MW);
- An estimate of frequency deviation (mHz);
- Energy not supplied (MWh).

4.3 Incidents leading to frequency degradation (F)

General description

An incident is classified according to this criterion in case the frequency deviation reaches the thresholds defined in the table below. The thresholds for scale 0 are specified in accordance with SO GL article 18(1)(b), the thresholds for scale 1 in accordance with SO GL article 18(2)(c) and the thresholds for scale 2 in accordance with SO GL article 18(3)(b).

For Scale 2, the ‘time to recover frequency’ in SO GL is used for GB, IRE/NI and Baltics. For the Nordic, the values of the Nordic System Operational Agreement (Load Frequency Control & Reserves Annex) were used for Scale 2. For CE the FCR full activation time was used for Scale 2. The ‘time to recover frequency’ is not specified in SOGL for Nordic and CE.

The data for number of minutes outside the standard frequency range and number of minutes outside the 50 % of maximum steady state frequency deviation for each synchronous area will be used to calculate the operational security indicators relevant to operational security OS-G1 and OS-G2. ‘Below Scale’ data, highlighted in grey below, does not need to be reported as part of the ICS TSO monthly data collection process as this data will be collected as part of the existing Annual Load-Frequency Control Report data collection process.

Table 3 Thresholds by scale for incidents leading to frequency degradation

	CE	Nordic	GB	IRE/NI	Baltic	Isolated systems
F Below Scale	>50 and ≤100 mHz for >0 and ≤5 min. OR >100 and ≤200 mHz for >0 and ≤2 min.	>100 and ≤250 mHz for >0 and ≤5 min. OR >250 and ≤500 mHz for >0 and ≤2 min.	>200 and ≤250 mHz for >0 and ≤5 min. OR >250 and ≤500 mHz for >0 and ≤3 min.	>200 and ≤250 mHz for >0 and ≤5 min. OR >250 and ≤500 mHz for >0 and ≤3 min.	>50 and ≤200 mHz for >0 and ≤5 min. OR >200 and ≤400 mHz for >0 and ≤3 min.	
Scale 0 F0	>50 and ≤100 mHz for >5 and ≤15 min. OR >100 and ≤200 mHz for >2 and ≤5 min.	>100 and ≤250 mHz for >5 and ≤15 min. OR >250 and ≤500 mHz for >2 and ≤5 min.	>200 and ≤250 mHz for >5 and ≤15 min. OR >250 and ≤500 mHz for >3 and ≤10 min.	>200 and ≤250 mHz for >5 and ≤15 min. OR >250 and ≤500 mHz for >3 and ≤10 min.	>50 and ≤200 mHz for >5 and ≤15 min. OR >200 and ≤400 mHz for >3 and ≤10 min.	>100 and ≤250 mHz for >7 and ≤20 min. OR >250 and ≤500 mHz for >3 and ≤10 min.
Scale 1 F1	>50 and ≤100 mHz for > 15 min. OR >100 and ≤200 mHz for >5 min.	>100 and ≤250 mHz for > 15 min. OR >250 and ≤500 mHz for >5 min.	>200 and ≤250 mHz for >15 min. OR >250 and ≤500 mHz for >10 min.	>200 and ≤250 mHz for > 15 min. OR >250 and ≤500 mHz for >10 min.	>50 and ≤200 mHz for >15 min. OR >200 and ≤400 mHz for >10 min.	>100 and ≤250 mHz for >15min. OR >250 and ≤500 mHz for >10 min.
Scale 2 F2	>200 mHz for >30 sec.	>500mHz and ≤1 Hz for >1 min. OR >1 Hz	>500 mHz for >1 min.	>500 mHz for >1 min.	>400 mHz for >1 min.	>500 mHz for >1 min.
Scale 3						

Frequency deviations are reported by the synchronous area monitor of each synchronous area defined in the synchronous area operational agreement according to article 133 of SO GL. Until the synchronous area operational agreements are concluded, the frequency deviations are reported by the TSOs specified below:

- for Continental Europe (CE) synchronous area: Amprion for odd months and Swissgrid for even months;
- for Nordic synchronous area: Svenska Kraftnät;
- for Great Britain (GB) synchronous area: National Grid ESO;
- for Ireland and Northern Ireland (IE/NI) synchronous area: EirGrid;
- for Baltic synchronous area: AST.

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- Maximum frequency deviation (mHz);
- An estimate of disconnected load (MW);
- Energy not supplied (MWh);
- An estimate of disconnected generation (MW).

4.4 Incidents on network elements (T)

General description

Disconnection of an alternating current [hereinafter AC] network element with an operating voltage at or above **220 kV** (and in network with operating voltage levels below 220kV when relevant for maintaining operational security) that is included in the contingency list established according to SO GL article 33 is reported in case of:

- forced outage (for human and asset safety) in cases where there is no time for security analysis and/or activation of remedial actions; or
- tripping by a protection device.

For network element(s) not capable of automatic reconnection, tripping is deemed to be final if reconnection has not occurred after 3 minutes.

No reporting is required in the following cases:

- planned manual disconnection of the AC transmission system elements; or
- tripping of the transmission lines where successful automatic re-closure has occurred.

Disconnection of a high-voltage direct current [hereinafter HVDC] system is reported in case of:

- forced outage or reduction on the Maximum HVDC Active Power Transmission Capacity (for human and asset safety) in cases where there is no time for security analysis and/or activation of remedial actions; or
- tripping or reduction on the Maximum HVDC Active Power Transmission Capacity by the operation of protection devices; or
- forced outage or reduction on the Maximum HVDC Active Power Transmission Capacity results in degradation of operational security standards (voltage, frequency) and/or N-1 violation.

No reporting is required in the following cases:

- planned manual disconnection of HVDC interconnectors;
- Maximum HVDC Active Power Transmission Capacity to satisfy market/commercial conditions;
- loss of HVDC capacity to an island system.

In case of disconnection of a tie-line or a link between more than one TSO (including HVDC), only the TSO in whose control area the event which caused the incident was located should report in order to avoid double reporting.

Table 4 Thresholds by scale for incidents on network elements

	CE	Nordic	GB	IRE/NI	Baltic	Isolated systems
Scale 0 T0	Disconnection of: • network element(s), or • tie-line, or • HVDC system without any consequences reaching the threshold of any ICS criteria.					
Scale 1 T1	Disconnection of: • network element(s), or • tie-line, or • HVDC system in case, as a consequence of the incident, N-1 criterion ceases to be fulfilled, even after the curative remedial action(s)					
Scale 2 T2	Disconnection of: • network element(s), or • tie-line, or • HVDC system in case, • as a consequence of the incident, there is at least one violation of a TSO's operational security limits defined in accordance with Article 25 of SO GL; or • in case of wide area consequences on regional or synchronous area level resulting in the need to activate at least 1 measure of the system defense plan.					
Scale 3						

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- Type of disconnected network element(s);
- Estimated impact on cross zonal capacity in both directions between bidding zones (MW);
- Type of contingency (for disconnection of the network element): ordinary, exceptional, out-of-range.

4.5 Incidents on power generating facilities (G)

General description

An incident is classified according to this criterion when output in one TSO's control area is greater than the thresholds defined in the table below in case of:

- unexpected reduction of generation (no time for security analysis and/or activation of remedial actions) within 15 minutes or,
- disconnection of power generating facility connected to network or,
- sum of disconnected and reduced power generating facilities within 15 minutes.

The 'Below Scale' data is collected using the transparency platform¹ and this data is also used for calculating the operational security indicators relevant to operational security OS-B. The tripping of the generating facilities in the 'Below Scale' category are not considered incidents and are not required to be reported individually by the TSOs during the ICS monthly TSO data collection process.

Table 5 Thresholds by scale for incidents on power generating facilities

	CE	Nordic	GB	IRE/NI	Baltic	Isolated systems
G Below Scale	>100 to ≤600 MW	>100 to ≤600 MW	>100 to ≤600 MW	>100 to ≤200 MW	>100 to ≤200 MW	
Scale 0 G0	>600 to ≤1500 MW	>600 to ≤1500 MW	>600 to ≤1500 MW	>200 to ≤500 MW	>200 to ≤450 MW	Biggest unit in the system
Scale 1 G1	>1500 to ≤3000 MW	>1500 to ≤3000 MW	>1500 to ≤3000 MW	>500 to ≤800 MW	>450 to ≤900 MW	Larger than the biggest unit
Scale 2 G2	More than 3000 MW	More than 3000 MW	More than 3000 MW	More than 800 MW	More than 900 MW	Power plant with the biggest unit in the system
Scale 3						

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- Total loss of generation (MW)

¹ ICS subgroup is not responsible for the data quality within the Transparency Platform

4.6 N and N-1 violations (ON)

General description

The situations where a TSO is not required to comply with the (N-1) criterion are listed in the articles 35(4) and 35(5) of SO GL.

This criterion does not apply to isolated systems.

N state violations of standards on voltage only need to be reported under section 4.9 (OV).

Table 6 Thresholds by scale for N and N-1 violations

	CE	Nordic	GB	IRE/NI	Baltic	Isolated systems
Scale 0						
Scale 1 ON1	At least one contingency from the contingency list can lead to deviations from operational security limits with consequences² on neighbouring TSOs after the activation of remedial action(s), OR There is at least one deviation from operational security limits after the activation of curative remedial action(s) in N situation.					
Scale 2 ON2	There is at least one wide area deviation from operational security limits after the activation of curative remedial action(s) in N situation.					
Scale 3						

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- Description of the N or N-1 situation (transmission system elements affected, identification of out of-range contingencies, etc.).

² Consequences = with impact on Observability Area.

4.7 Separation from the grid (RS)

General description

An incident is classified according to this criterion in case of a system incident leading to a situation where a synchronous area is split into one or more synchronised regions³.

This criterion does not apply to isolated systems. DC interconnections are not considered for this criterion.

Table 7 Thresholds by scale for separation from the grid

	CE	Nordic	GB	IRE/NI	Baltic
Scale 0 RS0	Separation from the grid, involving only one TSO, in case at least one of the split synchronised regions has a load $>1\%$ to $\leq 5\%$ of total load before the incident				
Scale 1 RS1	Separation from the grid, involving only one TSO, in case at least one of the split synchronised regions has a load larger than 5% of total load before the incident				
Scale 2 RS2	Separation from the grid involving more than one TSO in case at least one of the split synchronised regions has a load larger than 5% of total load before the incident.				
Scale 3					

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- Frequency deviation (mHz);
- Load shedding (MW)
- Loss of generation (MW);
- Energy not supplied to end-user (MWh);
- Time to full restoration (hh:mm:ss);

³ synchronised regions as per Emergency and Restoration Network Code

4.8 Loss of tools, means and facilities (LT)

General description

An incident is classified according to this criterion in case a TSO experiences the loss of real time tools, means and facilities specified in SO GL article 24(1):

- facilities for monitoring the system state of the transmission system, including state estimation applications and facilities for load-frequency control;
- means to control the switching of circuit breakers, coupler circuit breakers, transformer tap changers and other equipment which serve to control transmission system elements;
- means to communicate with the control rooms of other TSOs and regional security coordinators [hereinafter RSCs];
- tools for operational security analysis; and
- tools and communication means necessary for TSOs to facilitate cross-border market operations.

Table 8 Thresholds by scale for loss of tools, means and facilities

	CE	Nordic	GB	IRE/NI	Baltic	Isolated systems
Scale 0 LT0	Loss of any tools, means and facilities for more than 30 minutes without consequences for neighbouring TSOs					
Scale 1 LT1	Loss of any tools, means and facilities with consequences for neighbouring TSOs for more than 30 minutes or the unplanned evacuation to the back up control room					
Scale 2 LT2	Loss of all tools, means and facilities , for more than 30 minutes					
Scale 3						

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- Type of the tools, means and facilities lost (based on the list provided in SO GL article 24(1) and NC ER article 42)

4.9 Violation of standards on voltage (OV)

General description

Violation of standards on voltage is reported when in steady-state a node of the transmission system is operated outside the voltage ranges defined in Article 27 of SO GL within time range (which are different for each synchronous area) specified in Article 16 of Regulation (EU) 2016/631 (RfG), taking into account the thresholds defined in the table below:

- For isolated systems, the violation of standards on voltage is reported when a node of the transmission system is operated at voltage exceeding the pre-incident voltage level by $\pm 10\%$ for more than 15 minutes.

The 'Below Scale' data is also used to report the remaining voltage violation events that are needed to calculate the operational security indicators OS-F1 and OS-F2. These events are not included in the Scale 0, 1 and 2 incidents and therefore need to be reported separately as part of the ICS monthly TSO data collection process.

Table 9a and 9b Thresholds by scale for violations of standards on voltage**Table 9a:** Voltage and time ranges at the connection point between >110 kV and ≤300 kV

	CE	Nordic	GB	IRE/NI	Baltic	Isolated system
OV Below Scale	>0,85 and ≤0,90 pu, for >5 and ≤15 min. OR >1,118 and ≤1,15 pu for >5 and ≤15 min.	>1,05 and ≤1,10 pu, for >5 and ≤15 min.			>0,85 and ≤0,90 pu, for >5 and ≤15 min. OR >1,118 and ≤1,15 pu, for >5 and ≤15 min.	
Scale 0 OV0	>0,85 and ≤0,90 pu, for >15 and ≤60 min. OR >1,118 and ≤1,15 pu for >15 and ≤60 min.	>1,05 ≤1,10 pu, for >15 and ≤60 min.			>0,85 and ≤0,90 pu, for >15 and ≤30 min. OR >1,118 and ≤1,15 pu, for >15 and ≤20 min.	
Scale 1 OV1	<0,85 pu, for >30 seconds OR >0,85 and ≤0,90 pu, for >60 min. OR >1,118 and ≤1,15 pu, for >60 min. OR >1,15 pu, for >30 seconds	<0,90 pu, for >30 seconds OR >1,05 and ≤1,10 pu, for >60 min. OR >1,10 pu for >30 seconds	<0,90 pu, for >30 seconds OR >1,10 pu, for >30 seconds	<0,90 pu, for >30 seconds OR >1,118 pu, for >30 seconds	<0,85 pu, for >30 seconds OR >0,85 and ≤0,90 pu, for >30 min. OR >1,118 and ≤1,15 pu, for >20 min. OR >1,15 pu, for >30 seconds	Voltage exceeding pre- incident voltage level ±10%
	with no consequences ⁴ on neighbouring TSO					
Scale 2 OV2	Range is same as Scale 1 but with consequences ⁴ at least on one neighbouring TSO					
Scale 3						

⁴ Consequences = with impact on Observability Area

Table 9b: Voltage and time ranges at the connection point above 300 kV

	CE	Nordic	GB	IRE/NI	Baltic	Isolated system
OV Below Scale	>0,85 and ≤0,90 pu, for >5 and ≤15 min. OR >1,05 and ≤1,10 pu, for >5 and ≤15 min.	>1,05 and ≤1,10 pu, for >5 and ≤15 min.	>1,05 and ≤1,10 pu, for >5 and ≤15 min.		>0,88 and 0,90 pu, for >5 and ≤15 min. OR >1,097 and ≤1,15 pu, for >5 and ≤15 min.	
Scale 0 OV0	>0,85 and ≤0,90 pu, for >15 min and ≤60 min. OR >1,05 ≤1,10 pu, for >15 and ≤60 min.	>1,05 and ≤1,10 pu, for >15 min and ≤60 min.			>0,88 and 0,90 pu, for >15 and ≤20 min. OR >1,097 ≤1,15 pu, for >15 and ≤20 min.	
Scale 1 OV1	<0,85 pu, for >30 seconds OR >0,85 and ≤0,90 pu, for >60 min. OR >1,05 and ≤1,10 pu, for >60 min. OR >1,10 pu, for >30 seconds	<0,90 pu, for >30 seconds OR >1,05 and ≤1,10 pu, for >60 min. OR >1,10 pu, for >30 seconds	<0,90 pu, for >30 seconds OR >1,05 and ≤1,10 pu, for >15 min. OR >1,10 pu, for >30 seconds	<0,90 pu, for >30 seconds OR >1,05 pu for >30 seconds	<0,88 pu, for >30 seconds OR >0,88 and ≤0,90 pu, for >20 min. OR >1,097 and ≤1,15 pu, for >20 min. OR >1,15 pu, for >30 seconds	Voltage exceeding pre-incident voltage level ±10%
	with no consequences ⁵ on neighbouring TSO					
Scale 2 OV2	Range is same as Scale 1 but with consequences ⁵ at least on one neighbouring TSO					
Scale 3						

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- Maximum voltage violation (kV)

⁵ Consequences = with impact on Observability Area

4.10 Reduction of reserve capacity (RRC)

General description

An incident is classified according to this criterion in case of reduction of reserve capacity in a TSO's control area reaching the thresholds defined in the table below.

The reduction of reserve capacity is calculated using the minimum reporting time which is according to each TSOs scheduling resolutions of power generating facilities. The scheduling resolutions can vary per TSO between 5 and 30 minutes and the reduction of reserve capacity is in relation to the pre-fault levels.

Table 10 Thresholds by scale for reduction of reserve capacity

	CE	Nordic	GB	IRE/NI	Baltic	Isolated systems
Scale 0 RRC0	More than 20 % reduction, with a duration is less than or equal to 30 minutes					
Scale 1 RRC1	More than 20 % reduction, with a duration of more than 30 minutes					
Scale 2 RRC2	Reserve capacity unavailable more than 30 minutes					
Scale 3						

Data to be reported in addition to common data for each incident report listed in Annex I of this methodology:

- FCR capacity reduction (MW);
- FRR capacity reduction (MW), separated by aFRR and mFRR;
- RR capacity reduction (MW).

5. Operational security indicators

The calculation of operational security indicators defined in articles 15(3) and 15(4) of SO GL is based on all the incidents reported on scales 0 to 3. In addition, the ICS annual report shall show each indicator per scale.

When TSOs become aware that multiple incidents were caused by a single incident, such multiple incident shall be combined into a single incident according to the prioritization of the ICS criteria (As explained in 3.3. Procedure for multiple incidents and involving several TSOs). After the deadline of data delivery (1 March), the TSOs will perform extra checks to avoid the risk of double counting. All TSOs will need to check their own data reporting and their neighboring TSOs to prevent double counting.

5.1 Operational security indicators relevant to operational security

Operational security indicators relevant to operational security are defined in article 15(3) of SO GL. The calculation rules for the operational security indicators relevant to operational security are provided in table 11.

Table 11 Operational security indicators relevant to operational security

Abbreviation	Name of the indicator and SO GL reference	Calculation rules	Reference in
OS-A	Number of tripped transmission system elements per year per TSO - SO GL article 15(3)(a)	Add up the number of transmission system elements tripped reported for all the incidents on scale 0, 1, 2 and 3	Table 4
OS-B	Number of tripped power generation facilities per year per TSO - SO GL article 15(3)(b)	Add up the number of power generation facilities tripped reported for all the events/incidents on 'Below Scale' and Scale 0, 1, 2 and 3. The number of tripped generation facilities collected for the 'Below Scale' category will be taken from the transparency platform.	Table 5
OS-C	Energy not supplied due to unscheduled disconnection of demand facilities per year per TSO - SO GL article 15(3)(c)	Add up the energy not supplied reported for all incidents on scale 0, 1, 2 and 3 due to unscheduled disconnection of demand facilities	Table 2
OS-D1	Time duration of being in alert and emergency states per year per TSO - SO GL article 15(3)(d)	Add up the time being in alert and emergency states reported for all incidents on scale 0, 1, 2 and 3	
OS-D2	Number of instances of being in alert and emergency states per year	Add up the number of incidents on scale 0,1, 2 and 3 in case alert or emergency state was reported	

	per TSO - SO GL article 15(3)(d)		
OS-E1	Time duration within which there was a lack of reserve identified per year per TSO - SO GL article 15(3)(e)	Add up the duration of incidents reported under the criteria RRC0, RRC1 and RRC2; and the duration of all other incidents on scale 0, 1, 2 and 3 in case the reduction of reserve capacity is reported	Table 10
OS-E2	Number of events within which there was a lack of reserve identified per year per TSO - SO GL article 15(3)(e)	Add up the number of incidents reported under the criteria RRC0, RRC1 and RRC2; and the number of all other incidents on scale 0, 1, 2 and 3 in case the reduction of reserve capacity is reported	Table 10
OS-F1	Time duration of voltage deviations exceeding the ranges from tables 1 and 2 of SO GL Annex II per year per TSO - SO GL article 15(3)(f)	Add up the duration of events/incidents reported under the criteria OV 'Below Scale' and Scale OV0, OV1 and OV2; and add up the duration of all other incidents on the 'Below Scale', Scale 0, 1, 2 and 3 in case voltage deviations are reported which exceed the ranges from SO GL Annex II.	Table 9
OS-F2	Number of voltage deviations exceeding the ranges from tables 1 and 2 of SO GL Annex II per year per TSO - SO GL article 15(3)(f)	Add up the number of events/incidents reported under the criteria OV 'Below Scale' and Scale OV0, OV1 and OV2; and add up the duration of all other incidents on the 'Below Scale', Scale 0, 1, 2 and 3 in case voltage deviations are reported which exceed the ranges from SO GL Annex II.	Table 9
OS-G1	Number of minutes outside the standard frequency range per year per synchronous area - SO GL article 15(3)(g)	Annual Load-Frequency Control Reporting will provide data for number of minutes outside the standard frequency range.	

OS-G2	Number of minutes outside the 50% of maximum steady state frequency deviation per year per synchronous area - SO GL article 15(3)(g)	Annual Load-Frequency Control reporting will provide data for number of minutes outside the 50% of maximum steady state frequency deviation.	
OS-H	Number of system-split separations or local blackout states per year – SO GL article 15(3)(h)	Add up the number of incidents reported under the criteria RS1 and RS2.	Table 7
OS-I	Number of blackouts involving two or more TSOs per year - SO GL article 15(3)(i)	Add up the number of incidents reported under the criteria OB3, in case two or more TSOs are involved.	

5.2 Operational security indicators relevant to operational planning

Operational security indicators relevant to operational planning are defined in article 15(4) of SO GL. The calculation rules for the operational security indicators relevant to operational planning are provided in table 12.

Table 12 Operational security indicators relevant to operational planning

Abbreviation	Name of the indicator and SO GL reference	Calculation rules
OPS-A	Number of events in which an incident contained in the contingency list led to a degradation of the system operation state - SO GL article 15(4)(a)	Add up the number of incidents on scale 0, 1, 2 and 3 in case degradation of system operation state is reported and in case the cause of the incident is a contingency from contingency list
OPS-B	Number of the events counted by indicator OPS-A (events in which an incident contained in the contingency list led to a degradation of the system operation state), in which a degradation of system operation conditions occurred as a result of unexpected discrepancies from load or generation forecasts - - SO GL article 15(4)(b)	Add up the number of incidents counted by indicator OPS-A in case unexpected discrepancies from load and generation forecasts were reported as the cause of the incident
OPS-C	Number of events in which there was a degradation in system operation conditions due to an exceptional contingency - SO GL article 15(4)(c)	Add up the number of incidents on scale 0, 1, 2 and 3 in case degradation of system operation state is reported and in case the cause of the incident is an exceptional contingency

OPS-D	Number of the events counted by indicator OPS-C (events in which there was a degradation in system operation conditions due to an exceptional contingency), in which a degradation of system operation conditions occurred as a result of unexpected discrepancies from load or generation forecasts - SO GL article 15(4)(d)	Add up the number of incidents counted by indicator OPS-C in case unexpected discrepancies from load and generation forecasts were reported as the cause of the incident
OPS-E	Number of events leading to a degradation in system operation conditions due to lack of active power reserves - SO GL article 15(4)(e)	Add up the number of incidents on scale 0, 1, 2 and 3 in case lack of active power reserves was reported as the cause of the incident

6. Procedure for the investigation of scale 2 and scale 3 incidents

For incidents on scale 2 and 3, a detailed report shall be prepared by an expert panel composed of representatives from TSOs affected by the incident, leader of the expert panel from a TSO not affected by the incident, relevant RSC(s), representative of SG ICS, regulatory authorities and ACER upon request. The ICS annual report shall contain the explanations of the reasons for incidents on scale 2 and scale 3 based on the investigation of the incidents according to article 15(5) of SO GL.

6.1 Communication

The TSO in whose control area the incident has occurred will report the event and should inform the ICS WG in due time and not later than 1 week after the start of the incident.

TSOs affected by the scale 2 and scale 3 incidents shall inform their national regulatory authorities before the investigation is launched according to article 15(5) of SO GL. ENTSO-E Secretariat will inform NRAs and ACER about the upcoming investigation in due time before it is launched and not later than 1 week in advance of the first meeting of the expert panel.

6.2 Expert Panel

An expert panel will be conduct the investigation on scale 2 and scale 3 incidents. The expert panel will consist of the following members:

- The leader of the expert panel: Steering Group Operations under ENTSO-E System Operations Committee shall nominate an expert from a TSO not affected by the incident as the leader of the expert panel to ensure neutrality of the investigation;
- Expert panel members: each TSO affected by the incident on scale 2 or scale 3 shall appoint an expert to represent the TSO in the expert panel, and when needed, a representative of the relevant RSC(s);
- SG ICS representative: Steering Group Operations under ENTSO-E System Operations Committee shall nominate a representative of SG ICS to ensure that the procedure for the investigation of scale 2 and scale 3 incidents is followed;
- Regulatory authorities and ACER, on request to be involved in the incident investigation.

Remark: In case of a scale 2 or scale 3 incident in the synchronous areas of Great Britain or Ireland and Northern Ireland, when the incident affects only one TSO, a TSO internal investigation is conducted. The

affected TSO shall also in this case inform its respective regulatory authority before the investigation launched.

6.3 Timeline for the investigation of scale 2 and scale 3 incidents

The investigation has the following timeline:

- **Each TSO shall report the incidents on scale 2 and 3 classified in accordance with the criteria of ICS in the reporting tool at the latest by the end of the month following the month in which the incident began;**
- Latest by 6 months after the end of the incident, the expert panel shall prepare a factual report that will provide the factual basis for the final report;
- Latest by the publication of the ICS annual report for the year of the incident, the expert panel will prepare a final report on the investigation of the incident;
- Latest by the publication of the ICS annual report for the year of the incident, the expert panel will prepare the explanations of the reasons for incidents on scale 2 and scale 3, that shall be included in the ICS annual report.,

In case the TSOs affected by the incident receive urgent inquiries from their regulatory authorities or external stakeholders regarding the incident, the expert panel may decide to expediate the incident investigation.

6.4 Data Collection

To perform relevant analysis of the incident, the expert panel shall use the data reported by the affected TSOs in the reporting tool covering the data listed in Annex 1, and depending on the type of the incident, additional data necessary for the investigation.

The expert panel shall gather the additional data and information, deemed necessary for the investigation, in the form of a questionnaire, that is to be filled and provided to the expert panel by the affected and other relevant TSOs.

6.5 Factual Report

After collecting the data, the expert panel shall prepare a **factual report** that provides at least:

- The description of the system conditions right before the incident;
- The description of the system conditions after the incident;
- Activated remedial actions and measures from system defence plan;
- The sequence of events, including the description of all violations of operational security limits and other consequences of the incident.

Each TSO that provided information shall approve the factual correctness of its information contained in the report, before the expert panel proceeds with performing further analysis and preparing the final report.

6.6 Final Report

The expert panel shall prepare the **final report** that shall include at least:

- The analysis on the causes of the incident;
- The evaluation of the activated remedial actions and measures from system defense plan;

-
- The evaluation of the actions of TSO employees in charge of real-time operation of the transmission system;
 - The description of the functioning of the network element(s);
 - The conclusions and the explanations of the reasons for the incident;
 - The recommendations based on the conclusions of the investigation.

The method used to analyze incidents should be based on a well-known method such as the “fault tree analysis”.

The final report of incident scale 2 and 3 shall be published on the ENTSO-E public website.

7. Annual Report

According to article 15(1) of SO GL, each year by 30 September, ENTSO-E shall publish on their website an annual report on operational security indicators based on the ICS.

7.1 Contents of the annual reports

The annual report includes at least the following information:

- Operational security indicators listed in articles 15(3) and 15(4) of SOGL and calculated according to Chapter 3;
- Statistical overview on all reported incidents on scale 0, 1, 2 and 3;
- Analysis on the incidents for scale 1 and above;
- Explanations of the reasons for incidents on scales 2 and 3 based on the investigation carried out according to Chapter 5.

7.2 Process for the preparation of the annual report

The main tasks and milestones are:

- 
- ICS SPOCs to provide incident reports – latest before the end of each month, incidents in the previous month
 - When needed, trigger the investigation procedure for incidents on scale 2 and 3
 - SG ICS to analyse data and freeze the database for previous quarter – after the end of each quarter
 - 1st March (SOGL): Freeze of the database. All TSOs should have delivered the necessary data and information for the preparation of the annual reports based on the incident classification scale.
 - Preparation of the annual report by SG ICS members, including calculation of the operational security indicators, analysis of the incidents, and retrieving the explanations of the reasons for scale 2 and scale 3 incidents, from the respective expert panel
 - Validation of its data by each ICS SPOC
 - Proofreading and layout of the annual report
 - Review of the final draft by Steering Group Operation
 - SOC review of the final draft
 - Finalisation of the report by SG ICS
 - SOC approval of the final report
 - Publication of the final annual report – by 30 September each year

Annexes

Annex 1 Common data for reporting

For each incident, at least the following data is reported:

- a) reporting person;
- b) phone number of the reporting person;
- c) e-mail of the reporting person;
- d) reporting TSO;
- e) synchronous area where the incident took place;
- f) other TSOs affected (checkmark);
- g) other TSOs affected – list all affected TSOs (predefined list);
- h) start time of the incident, date and time (CET, CEST);
- i) end time of the incident, date and time (CET, CEST);
- j) scale of the incident (predefined list: scale 0, scale 1, scale 2, scale 3);
- k) criterion (as classified by TSO according to the priority list of criteria, predefined list);
- l) comments (additional remarks regarding the incident that contribute to the investigation of the incident, initiating fault, geographical relevance, sequence of events etc.);
- m) voltage level(s) involved in the incident;
- n) system state: system in normal state (checkmark);
- o) system state: time in alert state;
- p) system state: time in emergency state;
- q) system state: time in blackout state;
- r) cause(s) of the incident and the specification of the cause(s) (predefined list), comment for additional information regarding the cause(s), duration of cause(s) if relevant;
- s) consequence(s) of the incident and the specification of the consequence(s) (predefined list), comment for additional information regarding the cause(s), duration of consequence(s) if relevant; t) remedial action applied – yes/no;
- u) no remedial action reason (predefined list);
- v) remedial action applied to mitigate the consequences of the incident (predefined list).

Annex 2 Specific data reported for depending on the ICS criterion

The data specific to each criterion is listed under the description of each criteria, and reported here for the purposes of having an overview. Additional data reported depending on the ICS criteria:

- a) An estimate of disconnected load (MW);
- b) Load shedding (MW);
- c) Energy not supplied (MWh);

- d) An estimate of disconnected generation (MW);
- e) An estimate of frequency deviation (mHz);
- f) Type of disconnected transmission system element(s);
- g) Estimated impact on cross zonal capacity in both directions between bidding zones (MW);
- h) Type of contingency (for disconnection of the transmission network element): ordinary, exceptional, out-of-range contingency;
- i) FCR capacity reduction (MW)
- j) FRR capacity reduction (MW), separated by aFRR and mFRR
- k) RR capacity reduction (MW)
- l) Description of the N or N-1 situation (transmission system elements affected, identification of out-of-range contingencies, etc.).
- m) Information about the management of the separated network.
- n) Type of the lost tool (from the list defined in SO GL article 24(1));
- o) Maximum voltage violation (kV).

Annex 3 Additional data for the investigation of scale 2 and scale 3 incidents

Additional data reported for scale 2 and scale 3 incidents:

- a) ex-ante data (day ahead and intraday);
- b) real time snapshots;
- c) measurements from SCADA or equipment in substation (behaviour of protection, actions of special protection schemes, automation, Wide Area Monitoring System, etc);
- d) Excerpts from operational logs for data on operators' activities;
- e) Information on the functioning of the equipment, transmission system elements, significant grid users;
- f) Information on stopping of the load frequency control;
- g) Automatic actions by the special protection system;
- h) All automatic and manual defence actions that were executed;
- i) If relevant, restoration and resynchronisation actions,
- j) Information about communication and timing with other TSOs, DSOs and significant grid users.