Index:

Introduction to Standard

This standard requires adherence to the subset of system operating limits[1] identified to prevent instability, uncontrolled separation or cascading outages that adversely impact the reliability of the bulk transmission system. These limits are called interconnection reliability operating limits and are under the authority of the entity performing the reliability authority function. (Note that there are many other system operating limits that are used by system operators working for entities performing the Reliability Authority function and for entities performing the Transmission Operator function. This standard only addresses Interconnection Reliability Operating Limits.)

This standard is aimed at preventing instances of exceeding IROLs – and for those rare occasions when an IROL may be exceeded, the standard is aimed at minimizing the impact of such an event.

The standard is subdivided into eight requirements. Each of the requirements addresses some aspect of monitoring or controlling the transmission system to operate within IROLs. Some of these requirements address underlying responsibilities that must be accomplished as a prerequisite to monitoring and controlling the transmission system relative to IROLs.

201 Interconnection Reliability Operating Limit Identification – requires identification of the facilities that are subject to IROLs, and requires RAs to be able to identify current IROLs. Each IROL must have a T_v and the T_v may not be greater than 30 minutes. The list of facilities subject to IROLs must be updated to reflect changes in topology and system conditions. Entities that share a facility must have an agreed upon process for determining whether that facility is subject to an IROL and for developing the IROL and its T_v. (The entity performing the Reliability Authority Function is responsible for this requirement.)

202 Monitoring – requires monitoring real time data and comparing the data to IROLs to determine if the RA Area is operating within its IROLs (The entity performing the Reliability Authority Function is responsible for this requirement.)

203 Analyses and Assessments – requires that an operational planning analyses be conducted at least once each day to look at the 'day ahead' and requires that real-time assessments be conducted at least once every 30 minutes. These analyses and assessments are done to see if the transmission system is expected to be operated within its IROLs and to see if the transmission system is operating within its IROLs. (The entity performing the Reliability Authority Function is responsible for this requirement.)

204 Actions – requires that actions be taken or directives issued to prevent or mitigate instances of exceeding IROLs. These actions and directives must be documented when an IROL is exceeded, and when an IROL is exceeded for a time greater than the IROL's T_v, this event must be reported to the Compliance Monitor. The entity that issues a directive relative to an IROL must include a statement in the directive to clarify that the directive is related to an IROL. (The entity performing the Reliability Authority Function is responsible for this requirement.)

205 Data Specification & Collection – requires that a data specification be developed that identifies the data needed for monitoring real-time parameters against IROLs, and for conducting operational planning analyses and real-time assessments relative to operating within its reliability area's IROLs. The Data Specification must be distributed to entities that are expected to provide data and needs to address what data to provide, a mutually agreeable format for the data, a timeframe and periodicity for providing data, and must address the data provision process to use when automated real-time system operating data is unavailable. The Reliability Authority must notify its Compliance

---

[1] System Operating Limits are established through the standard, "Determine Facility Ratings, Operating Limits and Transfer Capabilities"

Monitor if data is not provided as specified. (The entity performing the Reliability Authority Function is responsible for this requirement.)

206 Data Provision – requires that entities provide the Reliability Authority with data needed to monitor real-time parameters against IROLs, and to conduct operational planning analyses and real-time assessments relative to operating within its reliability area's IROLs. (The entities performing the following Functions are responsible for this requirement: Balancing Authorities, Generator Operators, Generator Owners, Load-serving Entities, Reliability Authorities, Transmission Operators, and Transmission Owners)

207 Processes, Procedures or Plans – requires that there be one or more processes, procedures or plans to address actions to take or directions to issue to prevent and mitigate instances of exceeding IROLs. The processes, procedures or plans must identify and be coordinated with all entities that have to take actions as part of the plan, and with entities that would be impacted by the actions taken in the plan. (The entity performing the Reliability Authority Function is responsible for this requirement.)

208 Reliability Authority Directives – requires that entities follow the Reliability Authority's directives issued to prevent or mitigate instances of exceeding IROLs. The directives issued and the actions taken in response to those directives must be documented. (The entities performing the following functions are responsible for this requirement: Balancing Authority, Interchange Authority, and Transmission Operator.)

Expansion on Definitions

Balancing Authority: Integrates resource plans ahead of time, and maintains load-interchange-generation balance within its metered boundary and supports system frequency in real time.
> (*Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.)*

Bulk Electric System: A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and high voltage transmission system (above 35 kV or as approved in a tariff filed with FERC).

> *(Note – the original definition of this term was 'circular' and did not reference any voltage class. The definition was changed to include the reference to a measurable voltage class.)*

Cascading Outages: The uncontrolled successive loss of system elements triggered by an incident at any location that results in the loss of 300 MW or more of networked system load for a minimum of 15 minutes.

> *(Note –this definition was developed to help provide some measurable basis for determining if a system operating limit is an Interconnection Reliability Operating Limit.)*

Generator Operator: Operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.

> *Note – This is the definition proposed by the Functional Model Review Task Group for inclusion in the second version of the Functional Model.*

Generator Owner: The entity that owns the generator.

> *Note – This is the definition proposed by the Functional Model Review Task Group for inclusion in the second version of the Functional Model.*

Instability: The inability of the transmission system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances.

Interconnection Reliability Operating Limit: A system operating limit which, if exceeded, could lead to instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the bulk electric system.

> *(Note – this term was adapted from the term, Interconnection Reliability Limit, drafted by the Operating Limit Definition Task Force.)*

Interconnection Reliability Operating Limit Event: An instance of exceeding an interconnection reliability operating limit for any length of time.

> *(Note – all IROL Events must be documented.)*

Interconnection Reliability Operating Limit Event Duration: The length of time an interconnection reliability operating limit is exceeded. The duration is measured from the point where the limit is first exceeded and ends when the value drops below the limit and remains below the limit for at least 30 seconds.

> *(Note –graphics in next section of this Technical Reference shows the application of this 30-second rule.)*

Load-serving Entity: Secures energy and transmission (and related generation services) to serve the end user.

> *(Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.)*

Occurrence period: The time period in which performance is measured and evaluated.

> *(Note – this is a term used by the Compliance Monitors. When you look at the Sanctions Tables, note that the first table's column headings reference the number of infractions within the Performance-reset period. As the number of infractions within a performance reset period increases, so does the severity of the sanctions.)*

Operating Procedure – A document that identifies specific steps or tasks that must be taken by one or more specific operating positions to achieve a single specific operating goal. The steps in an Operating Procedure must be followed in the order in which they are presented, and must be performed by the position(s) identified. A document that lists the specific steps to take in removing a specific transmission line from service is an example of an Operating Procedure.
> *(Note – this is a term defined within the Coordinate Operations standard.)*

Operating Process – A document that identifies general steps for achieving a generic operating goal. An Operating Process includes steps with options that may be selected depending upon real-time conditions. A guideline for controlling high voltage is an example of an Operating Process.
> *(Note – this is a term defined within the Coordinate Operations standard.)*

Operating Plan- A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.
> *(Note – this is a term defined within the Coordinate Operations standard.)*

Operational Planning Analysis:
An analysis of the expected system conditions for the next day's operation and up to 12 months ahead. Expected system conditions include things such as load forecast(s), generation output levels, and known system constraints (transmission facility outages, generator outages, equipment limitations, etc.)

> *(Note – this standard requires that an operational planning analysis be conducted at least once each day, looking at the day ahead. This does not mean that operational planning analyses are limited to being conducted on a day-ahead basis. For example an operational planning analysis should be conducted as part of approving a transmission line outage – and this operational planning analysis may be conducted several months ahead of the day being reviewed.)*

Performance-reset Period: The time period that the entity being assessed must operate without any violations to reset the level of non-compliance to zero.

> *(Note – this is a term used by the Compliance Monitors. When you look at the Sanctions Tables, note that the first table's column headings reference the number of infractions within the Performance-reset period. As the number of infractions within a performance reset period increases, so does the severity of the sanctions.)*

Real-time: Present time as opposed to future time.

Real-time Assessment: An examination of existing and expected system conditions, conducted by collecting and reviewing immediately available data.

Real-time Data: Real-time measured values, state estimator values derived from the measured values, or other calculated values derived from the measured values – may include directly monitored data, Inter-utility data exchange (e.g., Interconnection Control Area Communication Protocol or SCADA Data), and manually collected data.

Real-time Monitoring: The act of scanning data and drawing conclusions about what the data indicates.

> *(Note – this definition supports the concept that monitoring is an 'active' task. The system operator assigned to monitor system conditions should be prepared to answer questions about what he/she has been monitoring without any preparation time. Simple questions can be used to determine whether or not monitoring has taken place. For example, a system operator who has been monitoring real time data to see if the area under the operator's direction is approaching or exceeding any IROLs should be able to answer the question, " Are there any IROLs on your system that have been exceeded? If any have been exceeded, are you approaching or exceeding the IROL's T_v?*

Reliability Authority: Ensures the reliability of the bulk power transmission system within its Reliability Authority Area.
> (*Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.)*

Reliability Authority Area: The collection of generation, transmission, and loads within the boundaries of the Reliability Authority. Its boundary coincides with one or more Balancing Areas.

> *Note – This is the definition proposed by the Functional Model Review Task Group for inclusion in the second version of the Functional Model.*

Self-certification: A process by which an entity does a self-evaluation to determine if it is compliant with the specific requirements for a reliability standard.

> *Note: This is a term used by the Compliance Monitors.*

T_v: The maximum time that an Interconnection Reliability Operating Limit can be exceeded before the risk to the interconnection becomes greater than acceptable. T_v may not be greater than 30 minutes.
.

> *Note – Operating Policy 2 – Standard A.2 included the following requirement:*
>
> *Following a contingency or other event that results in an OPERATING SECURITY LIMIT violation, the CONTROL AREA shall return its transmission system to within OPERATING SECURITY LIMITS soon as possible, but no longer than 30 minutes.*
>
> *This new standard requires results within 'T_v' minutes. Some IROLs are so critical that exceeding them for 30 minutes may be too long. See the charts in the next section for examples of how T_v is used to determine whether an instance of exceeding an IROL must be reported to the Compliance Monitor.*

Transmission Operator: The entity that operates the transmission facilities and executes switching orders.

> (*Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.*)

Transmission Owner: Owns transmission facilities

> (*Note – this term was defined in the NERC Functional Model approved by the NERC Board of Trustees, June 12, 2001.*)

Uncontrolled Separation: The unplanned break-up of an interconnection, or portion of an interconnection, that is not the result of automatic action by a special protection system or remedial action scheme operating correctly.

Wide Area Impact: The impact of a single incident resulting in the uncontrolled loss of 300 MW or more of networked transmission load for a minimum of 15 minutes.

> (*Note – this term was modified to provide a more measurable basis for determining whether a System Operating Limit should also be an Interconnection Reliability Operating Limit. The Standard Drafting Team adopted the threshold criteria used for reporting major incidents to the Department of Energy as the threshold for determining whether an event had a 'wide area' impact.*)

.

Questions and Answers

Who needs to comply with this standard?

Each of the requirements in the standard assigns responsibility for that requirement to one or more 'functions.' The entities performing the listed functions are the entities that must comply with that requirement. Most of the requirements are applicable to entities that perform the Reliability Authority Function – but several functions are assigned responsibility for the Data Provision and RA Directives requirements.

Requirement	Entities that Perform these Functions Must Comply With the Requirements							
	Reliability Authority	Balancing Authority	Interchange Authority	Trans. Operator	Trans. Owner	Gen. Owner	Gen. Operator	Load Serving Entity
201 **IROL Identification**	X							
202 **Monitoring**	X							
203 **Analyses & Assessments**	X							
204 **Actions**	X							
205 **Data Specification & Collection**	X							
206 **Data Provision**	X	X		X	X	X	X	X
207 **Processes, Procedures or Plans**	X							
208 **RA Directives**		X	X	X				

When does compliance with this standard start?

Several things must be in place before entities are expected to come into full compliance with all of the requirements in this standard. Most importantly, the Operate within IROLs Standard can't be implemented until after the Determine Facility Ratings, System Operating Limits and Transfer Capabilities standard has been implemented. The methodology for developing system operating limits must be in place and the RA must identify system operating limits before the RA can be held accountable for identifying which of its system operating limits are IROLs. There are other parts of the standard that will take some time to put into place if they aren't already in place. Some entities performing the RA function may have a detailed data specification that could be used to meet the Data Specification requirement in this standard – but other entities may have handled this requirement on a more casual basis and may need some time to formalize their data specifications.

For a System Operator - how does this new standard differ from Operating Policy 2 - Transmission?

There are three significant differences between what is expected of system operators under Policy 2, and what is expected of system operators under Standard 200.

Major Difference #1 – Term, 'OSLs' replaced with term, 'IROLs'
The first difference is a terminology change. The NERC Director–Compliance reports on compliance violations at each NERC Board of Trustees Meeting. He noted an increase in the number of OSL violations, and was directed by the BOT to investigate the cause. The investigation results showed a widespread misunderstanding on what was/was not an OSL. The task force that worked on this problem, called the Operating Limits Definitions Task Force (OLDTF) recommended that the term, "Operating Security Limit" not be used in the future because of the widespread misunderstanding associated with this term. The new standard uses the term, 'Interconnection Reliability Operating Limit – IROL'.

From the Terms Used in the Operating Policies, here is the definition of an Operating Security Limit (OSL):

- The value of a system operating parameter (e.g. total power transfer across an interface) that satisfies the most limiting of prescribed pre- and post-contingency operating criteria as determined by equipment loading capability and acceptable stability and voltage conditions.

From the Operate within IROLs Standard, here is the definition of an Interconnection Reliability Operating Limit (IROL):

- A system operating limit which, if exceeded, could lead to instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the bulk electric system.

Major Difference #2 –Resolution time changed from a uniform '30-minutes' for all OSLs to a 'unique' T_v that can't exceed 30 minutes for each IROL

Policy 2 has a standard '30 minute' response time for resolving any instance of exceeding an operating security limit. The 30 minutes was established to give system operators enough time to recognize the problem and take corrective actions. The new Operate within IROLs standard is designed from a perspective of system risk, and doesn't have a standard '30 minute' response time.

T_v is the maximum amount of time the system operator has to return to a state that is at or below the limit before being subjected to compliance sanctions. T_v is based on system risk – and recognizes that some IROLs shouldn't be exceeded for longer than 10 minutes without causing an unacceptable risk to the interconnection. Each IROL may have its own T_v but no T_v may exceed 30 minutes.

Operating Security Limit Violation Occurs

t=0 Pre-contingency. Can securely withstand first contingency

Post-contingency. Cannot withstand next contingency. Must be 30 minutes or less.

Can again securely withstand first contingency

t=0   t=30

Time in Minutes
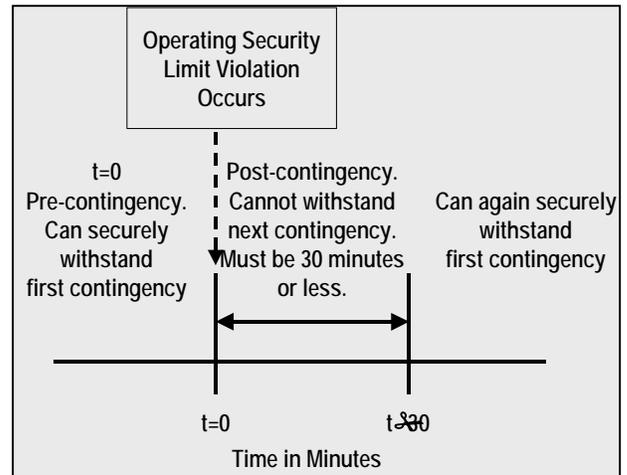
From Policy 2 – all OSLs addressed with the same 30-minute maximum resolution time

IROL

Time

t_0 T_v

Legend:
t_0 – Initiation of an IROL event
T_v – IROL violation time
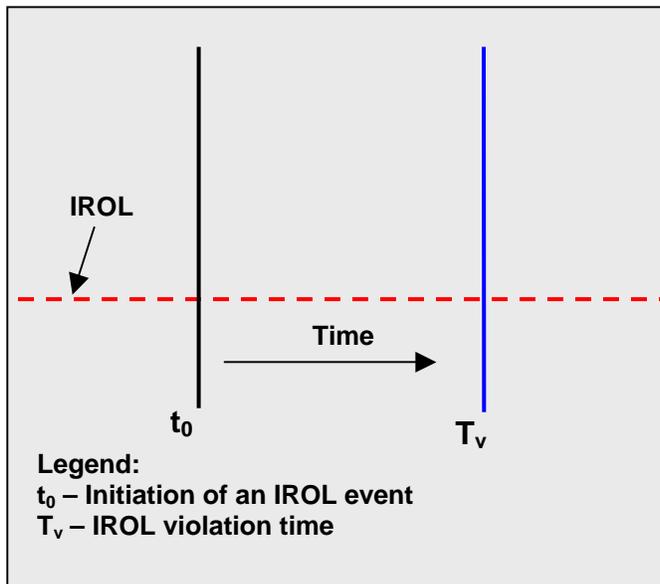
Operate within IROLs Standard - each IROL may have its own T_v.

For IROLs that should never be exceeded, T_v may be zero minutes.

Major Difference #3 – New Report for IROL Violations

Policy 2 requires that a NERC Preliminary Disturbance Report be completed for OSL Violations that exceed 30 minutes – The Preliminary Disturbance Report asks for a preliminary analysis to be conducted regarding the cause of the event – and is still needed. The new report is a compliance document and doesn't require the same data that is required of the Preliminary Disturbance Report.

The data that is collected in the IROL Violations Report is data that should be readily available to the system operator shortly after an instance of exceeding an IROL. The report doesn't ask for an analysis, just for a collection of the facts such as what limit was exceeded, how long was it exceeded, etc. The new report must be filed with the compliance monitor within 5 days of the event.

What is an IROL?

An IROL is a special type of system operating limit. While operating so that system operating limits aren't exceeded is always important, if an IROL is exceeded, there is an increased risk of voltage instability, cascading outages or uncontrolled separation that adversely impacts the interconnection.

System Operating Limits are monitored by system operators working for entities performing the Transmission Operator function and may also be monitored by system operators working for entities performing the Reliability Authority function.

IROLs are monitored by the Reliability Authority. The Reliability Authority may delegate this task to system operators working for entities performing the Transmission Operator function, but it is the Reliability Authority that is held accountable for ensuring that IROLs aren't exceeded.

What is the IROL's T_v?

T_v is the maximum amount of time the system operator has to return to a state that is at or below the limit before being subjected to compliance sanctions.

The T_v associated with each IROL is a time value used to assess how quickly the interconnection may deteriorate if an IROL isn't mitigated. IROLs should never be exceeded – but if one is exceeded, the T_v represents the maximum amount of time the limit can be exceeded before the risk to the interconnection becomes unacceptable. Under this standard, if a T_v is exceeded, there are financial penalties and additional reporting requirements.

Why don't all IROL's have the same T_v?

The IROL's T_v is based on system risk – and recognizes that exceeding some IROLs is unacceptable for any length of time, while exceeding other IROLs can probably be tolerated for a longer period of time before there is an unacceptable risk to the interconnection. By establishing a T_v for each IROL, the RA has information needed to anticipate the negative results of exceeding an IROL. If an IROL can't be exceeded for any length of time, then the RA may choose to install a special protection scheme to control the risk of exceeding the limit in real time. Note that T_v may not exceed 30 minutes.

If an RA installs a special protection scheme to reduce the probability of exceeding an IROL for time greater than the limit's T_v, does this eliminate the IROL?

No. The facility being protected by the special protection scheme would still need to be included in the list of facilities subject to IROLs, and the IROL would need to be listed with its T_v. Since special protection schemes don't always work as planned, it is important that system operators know where they have IROLs, know which facilities are subject to IROLs and know what the T_v is for each IROL. The system operator needs access to this data to make appropriate system operating decisions when special protection schemes don't work as planned.

How do you develop a list of IROL's?

The Determine Facility Ratings, System Operating Limits and Transfer Capabilities standard includes a requirement that entities responsible for developing system operating limits document their methodology for developing these limits. The RA is responsible for developing the subset of system operating limits that are called IROLs. The RA must follow its methodology for developing system operating limits and then must identify whether or not exceeding that limit could cause voltage instability, cascading outages, or uncontrolled separation from the interconnected transmission system. If the system operating limit could lead to one or more of these dire consequences, then the limit is an IROL.

How do you establish a T_v for an IROL?

Each RA may use whatever system it wants for establishing a T_v for its IROLs. This gives each RA the latitude to be as conservative as it desires. Some RAs may choose to use a default T_v of 30 minutes – currently some entities have a default of 20 minutes for all limits that would be categorized as IROLs. Here are some ways of setting T_v:
- Use study results showing the impact of a loss of a unit or line
- Set Tv at or lower than 'published' acceptable time overloads for critical facilities and
- Reference relay settings that have time delays before tripping overloaded facilities

Which instances of exceeding an IROL need to be documented?

All. Every instance of exceeding an IROL for any length of time must be documented. Most entities are expected to document the instance on a system operating log, but the standard does not require that the documentation be on an operating log, just that it be documented.

The value being monitored exceeded its IROL and the event must be documented.
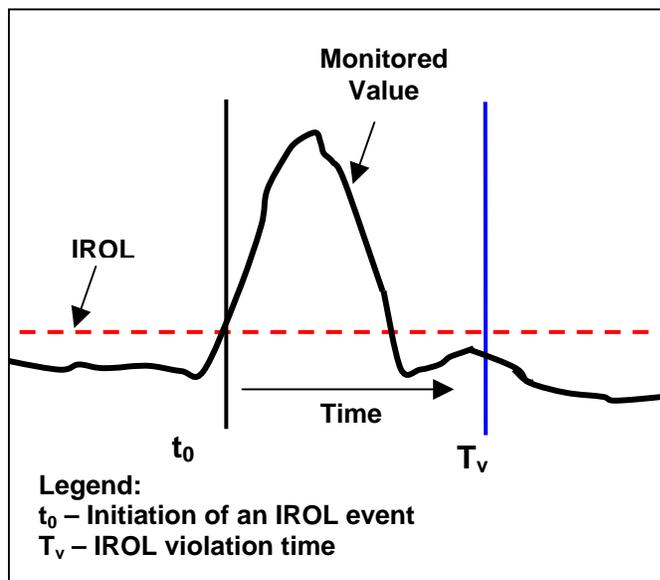
Does the standard require that exceeding an IROL be documented on the system operator's daily log?

No. Each entity can document IROL events using whatever documentation system works best for them. While each entity may use whatever system(s) it chooses to document instances of exceeding IROLs, the documentation must be retrievable so it can be shown to the Compliance Monitor. The data can be retrievable through computer screen displays, through paper or electronic logs, or other sources.

When you exceed an IROL, what do you have to document?

When you exceed an IROL for any length of time, you need to document the following three things:

- Actions taken or directives issued
- Magnitude of the event
- Duration of the event

How many IROLs do you expect the 'typical' RA to have in a year?

None! This standard focuses on preventing instances of exceeding an IROL. This standard requires the RA to use its tools to actively monitor and assess its Reliability Authority Area with respect to the current

and expected system conditions. For emerging system conditions, the RA is required to act to prevent exceeding an IROL. For unusual situations, such as a plane crash that knocks down 500kV lines, the RA is required to act to mitigate the instance within the IROL's T_v. Since most RA's can go many years without ever having a plane crash through their 500kV lines, most RAs won't experience any instances of exceeding an IROL for any length of time.

Which instances of exceeding an IROL need to be reported?

Every instance of exceeding an IROL for time greater than the IROL's T_v is reported to the Compliance Monitor within five business days.
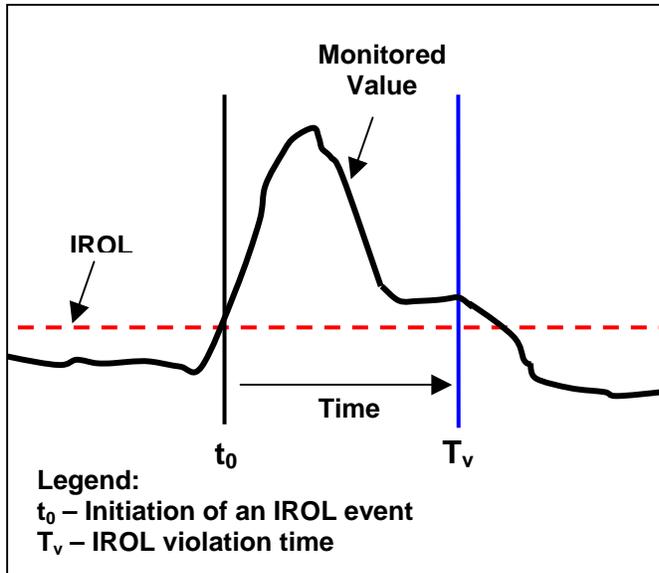
*The value being monitored exceeded its IROL for a time greater than the IROL's T_v and the event must be documented **and** reported.*

When you exceed an IROL for a time greater than the IROL's T_v, what do you have to report?

When you exceed an IROL for a time greater than the IROL's T_v, you have to report the following information to the Compliance Monitor:

- Date and time of the event
- Identification of which interconnection reliability operating limit was violated
- T_v for that limit
- Magnitude and duration of exceeding the interconnection reliability operating limit
- Actions taken or directives issued
- Time actions or directives were initiated or issued,
- Explanation of results of actions or directives

There is a report called the IROL Violation Report that captures this information. This report is available from the NERC Web Site and is provided at the end of this document.

How do you calculate the duration of an IROL event?

The duration of an IROL event is measured from the point in time when the IROL is first exceeded to the point in time where the parameter being monitored has returned to a value that is at or below the IROL, providing the actual value remains at or below the IROL for at least 30 seconds.
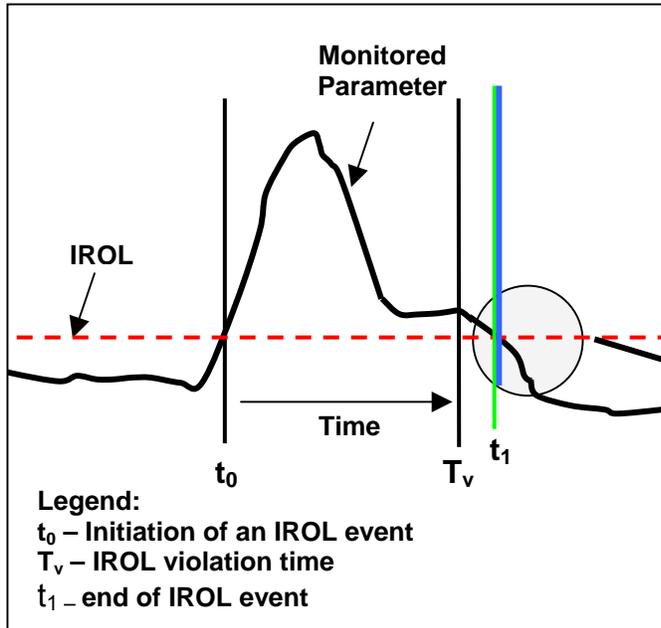

The monitored parameter must remain at or below the IROL for 30 seconds or more.

The line for t_1 shows the end of the IROL event, which is the point in time when the monitored value returns to a value that is at or below the IROL as long as the monitored value remains at or below the limit for at least 30 seconds. (From pt. A to pt. B is 30 seconds.)

Legend:
t_0 – Initiation of an IROL event
T_v – IROL violation time
t_1 – end of IROL event
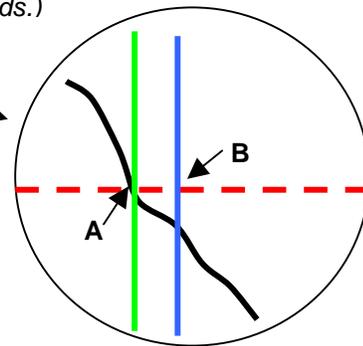
The following example is shown in the chart below. The IROL that has been exceeded has a T_v of 10 minutes. The monitored value exceeds the IROL for 15 minutes, then the monitored value returns to a value that is below that IROL for just 20 seconds, then the monitored value exceeds the IROL for another 10 minutes – then the monitored value returns to a value that is below the IROL for 2 hours. The duration of the event that must be reported is:

- 25 minutes, 20 seconds
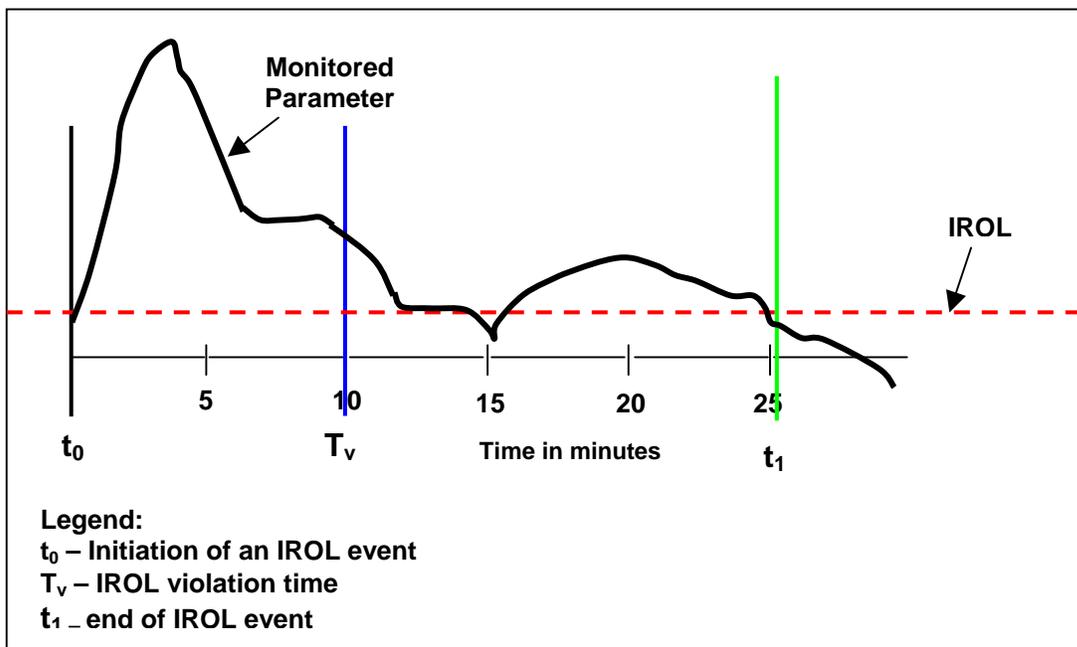
Legend:
t_0 – Initiation of an IROL event
T_v – IROL violation time
t_1 – end of IROL event

If you exceed an IROL for time greater than T_v, how big is the sanction?

This is the table used to determine the size of the sanction when an IROL is exceeded for time greater than T_v.

Example 1: There is an IROL set at 1000 MW with a T_v of 30 minutes. The IROL is exceeded for 35 minutes. During the time period after T_v was exceeded (the last 5 minutes of the event), the maximum value was 1100 MW. This is the first IROL violation for this RA.

Max Val % = (1100 MW/1000 MW – 1) * 100 = 10

The event duration exceeded its T_v by 5 minutes

The level 4 $ sanction for the first infraction is $2000

The sanction would be 10 * $2000 = $20,000

If the Maximum Value % over the Limit (measured after the event duration exceeds T_v) is: Max Value % = (Max Value/ IROL limit −1)*100	And the event duration exceeds its T_v by __ minutes:	Then Multiply the Level 4 $ sanction by:
0% < Max Value % ≤ 5%	T_v < Duration ≤ T_v + 5 minutes	5
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	10
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	15
	Duration > T_v + 15 minutes	20
5% < Max Value % ≤ 10%	T_v < Duration ≤ T_v + 5 minutes	10
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	15
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	20
	Duration > T_v + 15 minutes	25
10% < Max Value % ≤ 15%	T_v < Duration ≤ T_v + 5 minutes	15
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	20
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	25
	Duration > T_v + 15 minutes	30
15% < Max Value % ≤ 20%	T_v < Duration ≤ T_v + 5 minutes	20
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	25
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	30
	Duration > T_v + 15 minutes	35
20% < Max Value % ≤ 25%	T_v < Duration ≤ T_v + 5 minutes	25
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	30
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	35
	Duration > T_v + 15 minutes	40
25% < Max Value % ≤ 30%	T_v < Duration ≤ T_v + 5 minutes	30
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	35
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	40
	Duration > T_v + 15 minutes	45

March 1, 2004

> Example 2: There is an IROL set at 1000 MW with a T_v of 20 minutes. The IROL is exceeded for 35 minutes. During the time period after T_v was exceeded (the last 5 minutes of the event), the maximum value was 1200 MW. This is the second IROL violation for this RA.
>
> Max Val % = (1200 MW/1000 MW – 1) * 100 = 20
>
> The event duration exceeded its T_v by 15 minutes
>
> The level 4 $ sanction for the second infraction is $4000
>
> The sanction would be 30 * $4000 = $120,000

If the Maximum Value % over the Limit (measured after the event duration exceeds T_v) is: Max Value % = (Max Value/ IROL limit –1)*100	And the event duration exceeds its T_v by __ minutes:	Then Multiply the Level 4 $ sanction by:
0% < Max Value % ≤ 5%	T_v < Duration ≤ T_v + 5 minutes	5
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	10
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	15
	Duration > T_v + 15 minutes	20
5% < Max Value % ≤ 10%	T_v < Duration ≤ T_v + 5 minutes	10
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	15
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	20
	Duration > T_v + 15 minutes	25
10% < Max Value % ≤ 15%	T_v < Duration ≤ T_v + 5 minutes	15
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	20
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	25
	Duration > T_v + 15 minutes	30
15% < Max Value % ≤ 20%	T_v < Duration ≤ T_v + 5 minutes	20
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	25
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	30
	Duration > T_v + 15 minutes	35
20% < Max Value % ≤ 25%	T_v < Duration ≤ T_v + 5 minutes	25
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	30
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	35
	Duration > T_v + 15 minutes	40
25% < Max Value % ≤ 30%	T_v < Duration ≤ T_v + 5 minutes	30
	T_v + 5 minutes < Duration ≤ T_v + 10 minutes	35
	T_v + 10 minutes < Duration ≤ T_v + 15 minutes	40
	Duration > T_v + 15 minutes	45

March 1, 2004

What is the philosophy behind the sanction for exceeding an IROL for time greater than T_v?

Most RAs will not exceed an IROL. If there is an 'emerging' system condition that is causing operations in the Reliability Authority Area to approach operations outside of the IROLs, then the RA should take actions to prevent the system from exceeding the IROL. This standard requires that the RA monitor and assess its Reliability Authority Area so that emerging system conditions are noted and corrected before an IROL can be exceeded. There are unusual circumstances that do occur – such as a plane crashing through a set of 500 kV lines – that will cause an IROL to be exceeded. When this does occur, the RA needs to take action without delay to remedy the situation. If the RA achieves its goals within T_v, then there is no sanction.

Why isn't the sanction linked to the highest value over the course of the event?

Because unusual circumstances occur without warning, the sanction isn't linked to the highest value during the event, the sanction is linked to the highest value during the time period after T_v has been exceeded. This seemed to be the fairest way of applying the sanction – it gives the RA some time to resolve the situation and allows for 'credit' to be given if the RA was able to move the system in the right direction, but wasn't able to achieve the goal of getting within the limits before T_v.

What's the origin of the concept of these sanctions for exceeding IROLs?

These sanctions are very similar to the sanctions used for Policy 2 and for the WECC RMS program. The sanction for violating Requirement 204 is linked to the magnitude and duration of the infraction and to the history of the entity with respect to prior similar violations – Policy 2's sanction is linked to magnitude and duration of the infraction and to the size of the company that is responsible for preventing the infraction.

What are you expecting in the requirement for Processes, Procedures or Plans?

The RA needs to anticipate what actions to take to prevent exceeding IROLs as well as the actions to take when an IROL has been exceeded. The RA has to have some type of document that outlines the actions the RA will take to control the situation. The document can be as specific as needed. It is important that the documents be coordinated with entities that will be involved if the process, procedure or plan is invoked. The Coordinate Operations Standard defines these terms as follows:

> **Operating Procedure** – A document that identifies specific steps or tasks that must be taken by one or more specific operating positions to achieve a single specific operating goal. The steps in an Operating Procedure must be followed in the order in which they are presented, and must be performed by the position(s) identified. A document that lists the specific steps to take in removing a specific transmission line from service is an example of an Operating Procedure.

> **Operating Process** – A document that identifies general steps for achieving a generic operating goal. An Operating Process includes steps with options that may be selected depending upon real-time conditions. A guideline for controlling high voltage is an example of an Operating Process.

> **Operating Plan**- A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.

IROL Violation Report

Interconnection Reliability Operating Limit Violation Report
Compliance Template

| **Entity Performing Reliability Authority Function:** |

| **Report Date:** |

Event Date:	**Event Start Time:**	**Event End Time:**

Name of IROL that was exceeded:	**Value of the IROL that was exceeded:**	**The exceeded IROL's T_v:**
Magnitude of Limit Exceeded after T_v:	**Duration of Event:**	

List of Actions Taken or Directives Issued and Results Achieved:

Time Action Initiated or Directive Issued:	Action Taken or Directive Issued:	Time Action Completed:	Results Achieved:

Report completed by:

Name: **Phone:**

Title: __ __ __ __ __ __ __ __ __ __ __ __ __   **E-mail:**