

## **DIRECT CAUSE**

### **Procedural - Service Provider**

#### **Failure to follow standard procedures/documentation**

Work error by service provider personnel; correct procedures exist and were generally available, but correct procedures/documentation were not used, or were used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available.

#### **Followed procedures/documentation that were incorrect**

Flawed documentation or procedures used by service provider personnel; includes errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in service provider approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures/documentation did not exist, or were not generally available.

### **Procedural - System Vendor**

#### **Failure to follow standard procedures/documentation**

Work error by system vendor personnel; correct procedures exist and were generally available, but correct procedures/documentation were not used, or were used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available.

#### **Followed procedures/documentation that were incorrect**

Flawed documentation or procedures used by system vendor personnel; includes errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in service provider approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures or documentation did not exist, or were not generally available.

### **Procedural - Other Vendor**

#### **Failure to follow standard procedures/documentation**

Work error by other vendor personnel; correct procedures exist and were generally available, but correct procedures/documentation were not used, or were used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available.

#### **Followed procedures/documentation that were incorrect**

Flawed documentation or procedures used by other vendor personnel; includes errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in service provider approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures/documentation did not exist, or were not generally available.

**NRSC Outage Reporting**  
**Direct and Root Cause Definitions**  
**Page 2 of 10**

**DIRECT CAUSE** (continued)

**Design - Software**

Faulty or defective software design. Includes inadequate fault recovery strategies or failures; ineffective software fault isolation performance that triggers system re-initializations, or requires manual system recovery action for resolution. Includes insufficient software/memory capacity allocation problems.

**Design - Firmware**

Faulty or defective firmware design. Includes inadequate fault recovery strategies or failures, and ineffective fault isolation performance that require manual recovery action for resolution. Includes problems associated with incomplete firmware restoral (with or without accurate state indicators) following re-initialization.

**Design - Hardware**

Faulty or defective system hardware design. Includes problems with component independence and single-point-of-failure problems between otherwise-duplex components, as well as physical hardware design problems (i.e., bad connectors, inadequate grounding techniques). If failure was the result of a product change notice (PCN) inappropriately delayed by the vendor or service provider, or the PCN was waived by the service provider, consider root cause procedural.

**Hardware Failure**

Random hardware failure not related to design, but due to the inherent unreliability of the system components. Includes failures of dc/dc converters or fuses embedded in switches and transmission equipment, unless the problem was caused by the power plant. If (single) hardware failure causes loss of duplicated critical systems consider procedural or design fault. If system outage resulted from hardware failure occurring during simplex operation, consider root cause procedural if simplex mode resulted from inappropriate deferral of normal maintenance.

**External Environment**

**Natural (storms, lightning)**

External environmental conditions that exceed limitations documented in the vendor technical specifications. Includes direct effects of flooding, freezing, excessive temperature or rate of temperature changes. Includes outages resulting from lightning or external high voltage transients introduced into the system. If the entry of lightning into the system was caused by bonding and grounding violations, consider root cause procedural or design fault. If water damage was the result of cable pressurization failure, consider root cause procedural.

**Man-made (vandalism, accidents)**

External man-made conditions that exceed documented (or reasonable) service provider technical specifications. Includes direct effects of water system ruptures, fires, vehicular accidents, vandalism, and explosions. If incident was the result of inadequate security precautions, consider root cause procedural.

**Cable Damage**

Cable damage caused by dig-ups, (fiber) micro-bending, rodent damage, falling trees, etc. Includes underground and aerial cable failures associated with natural and man-made external environments. If incident was the result of faulty cable installation, or of cable locating activities, consider root cause procedural.

**NRSC Outage Reporting**  
**Direct and Root Cause Definitions**  
**Page 3 of 10**

**DIRECT CAUSE** (continued)

**Internal Environment**

**Water**

Entry of water into the system, including roof leaks, air conditioning leaks, excessive humidity, fire suppression activities, flooding, etc. If failure was the result of environmental systems failure (e.g., AC leaks, pressurization failures), or inadequate property management (e.g., unreasonable delay in repair or roof leak, predictable flooding), consider root cause procedural.

**Temperature**

Excessive ambient temperatures, excessive rates of temperature change. If failure was the result of environmental systems failure, and a more effective response to the failure would have prevented/minimized impact of incident, consider root cause procedural.

**Corrosion/contamination**

Corrosive contamination that enters the system from surrounding environment. Includes dust, airborne dirt, and smoke and/or fire suppression chemicals. If failure was the result of inadequate air filtration strategies or maintenance, consider root cause procedural or design fault.

**Fire**

Fires within the telecommunications facility environment. Includes fires in test sets, peripheral equipment, power equipment, and building systems. If incident was the result of service provider/others' activities, consider root cause procedural.

**Traffic/System Overload**

**Reduced capacity due to system trouble**

System overload or congestion associated with decreased system throughput or trouble-caused resource limitation; does not include system congestion associated with simple high volume traffic conditions. If failure was the result of excessive out-of-service conditions, consider root cause procedural. If failure was a result of overload triggered by moderate increase in traffic/attempts, or recovery-associated activities, consider root cause design fault.

**High call volume**

System overload or congestion associated with high traffic or load conditions that exceed the engineered capacity of the system. Includes unexpected traffic that was the result of media-stimulated calling, natural disasters, political or social activities, or other external conditions. If failure was the result of poor event notification and planning or network management response to media-stimulated call-in, or a result of inadequate capacity engineering, consider root cause procedural.

**Power Failure**

Instances of outage directly related to failure of the external power system, or failures of service provider back-up power systems. Includes failures associated with commercial power, standby generators, building electrical systems, dc power plants, dc distribution systems, and alarms/monitoring systems. Does not include failures of dc/dc converters or fuses embedded in switches and transmission equipment, unless the problem was caused by the power plant. If the failure was the result of inadequate/no response to (alarmed/un-alarmed) failures, consider root power alarm fault. If the failure was the result of overloaded or undersized power equipment, consider root cause procedural or design fault.

**NRSC Outage Reporting**  
**Direct and Root Cause Definitions**  
**Page 4 of 10**

**DIRECT CAUSE** (continued)

**Other/Unknown**

The cause of the outage cannot be determined, or the cause does not match any of the classifications above. Does not include cases where outage data was insufficient or missing, or where direct cause is still under investigation. When direct cause cannot be proven, it is usually still possible to determine probable cause, which is preferred to the use of "unknown." When classifications provided do not match direct cause, approximate match is preferred to the use of "other."

**Insufficient Data**

Failure report (and subsequent investigation, if any) did not provide enough information to determine direct cause of failure.

\*\*\*\*\*

**ROOT CAUSE**

**Procedural - Service Provider**

**Insufficient training**

Training not available from vendor; training not available from service provider; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

**Insufficient staffing**

Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or centralization arrangement; resource-intensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc.

**Insufficient supervision/control**

Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc. This category should be used when multiple procedural causes are reported

**Documentation/procedures unavailable/unclear/incomplete**

Documentation or procedures (vendor or service provider) not published; published, but not distributed; distributed, but not available on-site, etc. Documentation/procedures obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

**Documentation/procedures out-of-date unusable or impractical**

Documentation/procedures not updated; correction/update available but not incorporated locally. Documentation/procedures unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

**Inadequate routine maintenance/memory back-up**

Failure would have been prevented/minimized by simple maintenance routines; recovery action was delayed/complicated by old or missing program/office data tapes or disks, etc.

**Cable unlocated**

Prior notification was provided by the excavator but the facility owner or locating company failed to establish the presence of a cable which was then eventually damaged.

**Inaccurate cable locate**

The cables' presence was determined, but their locations were inaccurately identified.

**Other**

**ROOT CAUSE** (continued)

**NRSC Outage Reporting**  
**Direct and Root Cause Definitions**  
**Page 5 of 10**

**Procedural - System Vendor**

**Insufficient training**

Training not available from vendor; training not available from service provider; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

**Insufficient staffing**

Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or centralization arrangement; resource-intensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc.

**Insufficient supervision/control**

Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc. This category should be used when multiple procedural causes are reported

**Documentation/procedures unavailable, unclear, incomplete**

Documentation or procedures (vendor or service provider) not published; published, but not distributed; distributed, but not available on-site. Documentation obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

**Documentation/procedures out-of-date, unusable, impractical**

Documentation/procedures not updated; correction/update available but not incorporated locally. Documentation unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

**Ad hoc activities, outside scope of MOP**

Unapproved, unauthorized work or changes in agreed-to procedures.

**Other**

**Procedural - Other Vendor**

**Insufficient training**

Training not available from vendor; training not available from service provider; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

**Insufficient supervision/control**

Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc. This category should be used when multiple procedural causes are reported

**Documentation/procedures unavailable, incomplete**

Documentation or procedures (vendor or service provider) not published; published, but not distributed; distributed, but not available on-site. Documentation obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

**Documentation/procedures out-of-date, unusable, impractical**

Documentation/procedures not updated; correction/update available but not incorporated locally. Documentation unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

**Ad hoc activities, outside scope of MOP**

Unapproved, unauthorized work or changes in agreed-to procedures.

**Other**

**ROOT CAUSE** (continued)

**Design - Software**

**Inadequate defensive checks**

Changes to critical or protected memory were allowed without system challenge; contradictory or ambiguous system input commands were interpreted/responded to without system challenge. Failure of system to recognize or communicate query/warning in response to commands with obvious major system/network impact.

**Ineffective fault recovery or re-initialization action**

Simple, single-point failure resulting in total system outage; failure of system diagnostics that resulted in removal of good unit with restoral of faulty mate; failure to switch/protection switch to standby/spare/mate component(s).

**Faulty software load - program date**

Bad program code/instructions; logical errors/incompatibility between features/sets; software quality control failure; wrong/defective program load supplied.

**Faulty software load - office date**

Inaccurate/mismatched office configuration data used/applied; wrong/defective office load supplied.

**Other**

**Design - Firmware**

**Insufficient software state indications**

Failure to communicate or display out-of-service firmware states; failure to identify, communicate or display indolent or "sleepy" firmware states.

**Ineffective fault recovery or re-initialization action**

Failure to reset/restore following general/system restoral/initialization.

**Other**

**Design - Hardware**

**Inadequate grounding strategy**

Insufficient component grounding design; duplex components/systems sharing common power feeds/fusing.

**Poor backplane or pin arrangement**

Non-standard/confusing pin arrangements or pin numbering schemes; insufficient room or clearance between pins; backplane/pin crowding.

**Poor card/frame mechanisms (latches, slots, jacks, etc.)**

Mechanical/physical design problems.

**Insufficient component/redundancy/diversity**

System design with unnecessary aggregation of components or features; or system deployment with single-point-of-failure configurations.

**Insufficient network redundancy/diversity**

Network design with unnecessary aggregation of systems or network deployment (e.g., CCS network, self-healing rings) with single-point-of-failure configurations.

**Other**

**NRSC Outage Reporting**  
**Direct and Root Cause Definitions**  
**Page 7 of 10**

**ROOT CAUSE** (continued)

**Hardware Failure**

**Processor community failure**

**Memory unit failure**

**Peripheral unit failure**

**Other**

**External Environment** (for limited use when applicable root causes actionable by service provider or vendor cannot be identified)

**Lightning/transient voltage**

Component destruction or fault associated with surges and over-voltages caused by (electrical) atmospheric disturbances.

**Storm - wind/trees**

Component destruction or fault associated with wind-borne debris or falling trees/limbs.

**Storm - water/ice**

Component destruction or fault associated with fog, rain, hail, sleet, snow, or the accumulation of water/ice (flooding, collapse under weight of snow, etc.).

**Vehicular accident**

Component destruction or fault associated with motor vehicle (car, truck, train, etc.) collision.

**Vandalism/theft**

Component loss, destruction, or fault associated with larceny, mischief, or other malicious acts.

**Earthquake**

Component destruction or fault associated directly or indirectly with seismic shock (if damage was the result of inadequate earthquake bracing, consider hardware design fault).

**Fire**

Component destruction or fault associated with fire occurring/starting outside service provider plant, includes brush fires, pole fires, etc.

**Other**

**Cable Damage**

**Digging error**

Excavator error during digging (contractor provided accurate notification, route was accurately located and marked, and cable was buried at a proper depth with sufficient clearance from other sub-surface structures).

**Inadequate/no notification**

Excavator failed to provide any notification prior to digging, or did not accurately describe the location of the digging work to be performed. (Because of the success in avoiding dig-ups by acting upon prior notification, the lack of notification is considered to be the root cause of every dig-up in which prior notification was not provided.)

**Shallow cable**

The cable was at too shallow a depth, (notification was adequate, locate was accurate, excavator followed standard procedures).

**Other**

**ROOT CAUSE** (continued)

**Internal Environment**

**Roof/air conditioning leak**

Component destruction or fault associated with water damage (direct or electrolytic) caused by roof or environmental systems leaks into/in central office environment.

**Manhole/cable vault leak**

Component destruction or fault associated with water entering manholes cable vaults, CEVs, etc.

**Cable pressurization failure**

Component destruction or fault associated with cable damage resulting from cable pressurization failure.

**Environmental system failure (heat/humidity)**

Component loss or fault associated with extreme temperature, rapid temperature changes, or high humidity due to loss/malfunction of environmental control(s). If the failure was the result of inadequate/no response to (alarmed/un-alarmed) environmental failures, or due to incorrect manual control of environmental systems, consider procedural.

**Fire suppression (water, chemicals) damage**

Component loss or fault associated with corrosion (electrolytic or other) caused by fire suppression activities; root cause assumes no substantial failure was directly associated with the smoke/fire that triggered suppression.

**Fire, arcing, smoke damage**

Component loss or fault associated with damage directly related to central office or equipment fires (open flame or smoldering), corrosive smoke emissions, or electrical arcing (whether or not ignition of surrounding material occurs).

**Dirt, dust contamination**

Component loss or fault associated with dirt or dust, typically resulting in component overheating, or loss of connectivity.

**Other**

**Traffic/System Overload**

**Media-stimulated calling - insufficient notification**

System/network overload/congestion directly associated with media-stimulated calling event where event sponsor/generator failed to provide adequate advance notice, or provided inaccurate (underestimated) notification.

**Mass calling - focused/diffuse network overload**

System/network overload/congestion directly associated with unplanned, external trigger(s) causing a significant, unmanageable traffic load.

**Common channel signaling network overload**

CCS system/network overload associated with (true) high traffic loads congesting STP/SCP processors or CCS link network. If overload was associated with STP/SCP message handling congestion, false or reactivated link congestion, inappropriate or incorrect CCS network management message(s), protocol errors, etc., consider software design fault.

**Inappropriate/insufficient NM control(s)**

System/network overload/congestion associated with ineffective NM system/switch response, either because no effective NM control was available, system/switch response to control was inappropriate, or its implementation was flawed. If failure was related to inappropriate control strategy or execution by NM organization, consider procedural.

**NRSC Outage Reporting**  
**Direct and Root Cause Definitions**  
**Page 9 of 10**

**ROOT CAUSE** (continued)

**Traffic/System Overload** (continued)

**Ineffective engineering/engineering tools**

System/network overload/congestion directly associated with under-engineering of the system/network due to rapidly changing network demand, or introduction of new network components and/or technologies. If failure was associated with simple under-engineering (absent changing environment), consider procedural.

**Other**

**Power Failure** (does not include failures of dc/dc converters or fuses embedded in switches and transmission equipment, which should be reported as a hardware failure, unless the problem was caused by the power plant.)

**Inadequate/missing power alarm**

System failure associated un-alarmed (or under-alarmed) power failure; alarm not provided initially due to inadequate standards or failure to implement standards; alarm/alarm system failure (broken or modified). (Because of the success in avoiding severe, battery-depletion failure where power alarms are effective and effectively responded to, system failures directly associated with power alarms should be classified as such, instead of as procedural.)

**Insufficient response to power alarm**

System failure associated response to power failure: alarm system worked but support personnel did not respond properly. (Because of the success in avoiding severe, battery-depletion failure where power alarms are effective and effectively responded to, system failures directly associated with power alarms should be classified as such, instead of as procedural.)

**Lack of routine maintenance/testing**

System failure that could have been avoided had periodic power system testing, maintenance and/or detailed inspection been performed.

**Overloaded/undersized power equipment**

System failure attributable to insufficient sizing/design of power configuration.

**Lack of power diversification**

Failure to diversify equipment among redundant power system components, including ac rectifierschargers, battery power plant, dc distribution facilities, etc.

**Lack of power redundancy**

Failure directly associated with insufficient redundancy of power system components, including ac rectifierschargers, battery power plan, dc distribution facilities, etc.

**Inadequate site-specific power contingency plans**

System failure that could have been avoided/minimized had emergency operating procedures and contingency plans been available; outage was prolonged because of lack of site-specific information including equipment engineering data, portable engine hook-up hardware/procedures, load shedding plans, etc.

**Extended Commercial Power Failure**

System failure due to commercial power failure that extends beyond the design back-up capabilities at the location and beyond reasonable contingency planning assumptions.

**Other**

**NRSC Outage Reporting**  
**Direct and Root Cause Definitions**  
**Page 10 of 10**

**ROOT CAUSE** (continued)

**Operations Support/Strategy**

**Insufficient surveillance capability**

System failure that could have been avoided/minimized had remote operations been able to better "see" system performance; total/comprehensive view of system not available. Surveillance system/links unavailable/out-of-service.

**Inadequate control capability**

System failure that could have been avoided/minimized had remote operations been able to better control system performance; comprehensive controls only available on-site. Control system/links unavailable/out-of-service.

**Ineffective roll-down or hand-off activity**

System failure that could have been avoided/minimized had better communication and/or process control been in place between/among operations organizations.

**Ineffective alarm threshold/display**

System failure that could have been avoided/minimized had user-programmed threshold/display indicators/messages been more effective/explicit.

**Impactical trouble-correlation among operations systems**

System failure that could have been avoided/minimized had output of disparate operations systems been better integrated/intelligible - unreasonable output language/naming convention differences among operations systems.

**Other**

**Other/Unknown**

The cause of the outage cannot be determined, or the cause does not match any of the classifications above. Does not include cases where outage data was insufficient or missing, or where root cause is still under investigation. When root cause cannot be proven, it is usually still possible to determine probable cause, which is preferred to the use of "unknown." When classifications provided do not match root cause, approximate match is preferred to the use of "other."

**Insufficient Data**

Failure report (and subsequent investigation, if any) did not provide enough information to determine direct cause of failure.