NRSC Bulletin No. 2017-002

"Silent Alarm Failures" Investigation

March 2017

Background

The Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) has been investigating a concern raised by the FCC associated with what is perceived to be outages that are not detected by equipment alarming (e.g., non-intrinsic alarming for translation failures, input errors, etc.). The NRSC has reviewed the issue and determined that some existing industry recommendations can be provided to reduce the frequency of these failures from occurring and mitigating the impact of these types of failures if they do occur.

Methodology

NRSC members examined the examples of "Silent Alarm Failures" provided by the FCC and also looked at additional examples internal to their respective companies. The Committee held a series of meetings to discuss and compile the individual findings and to provide a consensus of the issues and concerns around these events. The examples were investigated and the applicable Best Practices were provided to form a comprehensive list of practices aimed at reducing the frequency of these types of outages and mitigating their impacts when they do occur. Given differences in NRSC member networks and technologies (i.e., vendors, frameworks, services provided, surveillance equipment, infrastructure, etc.), this general approach seems to be most applicable to operators and carriers.

Findings

The NRSC initiated a general review of Best Practices related to alarming and each member company initiated an internal review of their respective alarming practices. The NRSC found that the events around "Silent Alarm Failures" generally are attributed to situations that dealt with new technology, where existing processes and procedures did not anticipate the particular situation that occurred. Once these situations were identified, Root Cause Analysis (RCA) reviews were routinely conducted and the existing alarming, triggers, Key Performance Indicators (KPIs), and/or Methods of Procedures (MOPs) were modified to address identified issues. The NRSC recognizes that a vast number of alarm states from equipment software exist for carriers to utilize and must be filtered to enable an appropriate response from the service provider operating centers. These alarms range from minor in nature, but still alert carriers to non-critical events on the network, to service-affecting events to which carriers must focus their attention. Service providers must employ software options to trigger meaningful alarms through the interconnected nodes of their operating systems. There is no evidence pointing to a common primary contributor within the data collected from the NRSC or the FCC.

Recommendations

The NRSC recommends that Network Operators, Service Providers, Public Safety, and Equipment Suppliers review the findings of this Bulletin and revisit the Best Practices in this Bulletin and continue to implement those that are applicable, which will contribute to the reduction of "Silent Alarm Failures". The following Best Practices were selected from the existing Best Practices and were found to be applicable to the events that were reviewed, plus additional Best Practices suggested by NRSC members. These Best Practices address areas related to “Silent Alarm Failures”.

The NRSC recommends that in addition to reviewing Best Practices, carriers consider conducting a periodic review of their existing alarming, triggers, KPIs, and/or MOPs, as appropriate and recommends a new Best Practice: Network Operators, Service Providers, Public Safety, and Equipment Suppliers should conduct regular review of their alarming thresholds and selection.

The general NRSC recommendation for service providers is to provide a more proactive investigation of new MOPs and to provide regular reviews of existing alarming, particularly around evolving technologies.

Number	Best Practice
9-5-0514	When available, Network Operators and Service Providers should utilize a management system capability (e.g., Common Object Request Broker Architecture [CORBA], Simple Network Management Protocol [SNMP]) providing a single interface with access to alarms and monitoring information from all critical network elements.
9-9-0602	Network Operators and Service Providers should establish procedures to reactivate alarms after provisioning or maintenance activities (when alarms are typically deactivated).
9-9-0612	Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service.
9-6-0761	Network Operators and Service Providers should conduct periodic verification of the office synchronization plan and the diversity of timing links, power feeds, and alarms.
9-6-5235	Network Operators, Service Providers, and Equipment Suppliers should ensure that impacted alarms and monitors associated with critical utility vaults are operational after a disaster event.

NRSC recommends the following new Best Practice:

Recommended Addition	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should conduct regular review of their alarming thresholds and selection.