FailSafe Communications Inc.
"Because Lives Are On The Line"™

Eddie M. Pope, General Counsel
1510 North Hampton Road, Suite 230, DeSoto, TX 75115
Direct: (512) 689-7815 • empope@telesentient.com• www.telesentient.com

January 16, 2024

Shabbir Hamid
Attorney Advisor, Cybersecurity and Communications Reliability Division
Public Safety and Homeland Security Bureau,
Federal Communications Commission
45 L Street, NE, Washington, DC 20554

Via Electronic Filing

Re: Notice of Ex Parte Letter, PS Docket No. 15-80, PS Docket No. 13-75 and ET Docket No. 04-35

Dear Mr. Hamid,

FailSafe Communications, Inc. ("FailSafe") has filed several *ex parte* letters in these dockets with the aim of making a presentation to the FCC Staff regarding technologies that may help carriers detect and report outages affecting 911 call centers ("PSAPs").

Our presentation is in response to the Competitive Carrier Association ("CCA") Motion for Reconsideration. As you are undoubtably aware, the CCA (joined with other parties) and Intrado have recently filed additional comments regarding the Commission's Paperwork Reduction Act notice. We have reviewed those comments and do not believe they raise any issues not already raised in CCA's Motion for Reconsideration.

We have come to appreciate that an in-house presentation might present technical challenges and may not meet the Staff's current needs. Thus, I would like to propose a Zoom call sometime soon so that we can discuss our approaches and so that Staff can ask us questions about them. (After reviewing the materials, you may determine you do not need such a call. Please let me know if that is your conclusion.)

In order to facilitate such a call, I am attaching three Exhibits, along with corresponding attachments.

1. Exhibit "A" is draft language for an Order Denying the Motion for Reconsideration. As you will see, it only focuses on the issue raised by CCA regarding the detection and reporting of 911 calls within thirty minutes that do not go through to the PSAP. Our fundamental argument is that technology may resolve many of the CCA's concerns.
2. Exhibit "B" is a detailed explanation of those technologies. It is our hope that the Commission's technical Staff can review that Attachment in advance of our call.
3. Exhibit "C" is an open letter to the industry, containing a forward-looking explanation of the advances we see in the future that are possible utilizing our approaches, along with corresponding cost estimates. We invite the industry and stakeholders to brainstorm with us regarding both as to what innovations are possible and how those innovations might be implemented. FailSafe only sells licenses to our patents and consulting services. We anticipate that our licensees will be able to work with outside vendors to bring wonderful advances to the marketplace.

The FCC has been at the center of developments in the 911 universe – from "basic" 911, E911 and now NG911. At each step, new technologies allowed developments that would have amazed prior generations. FailSafe hopes to aid the FCC in adding to that legacy of innovation with an aim of making all Americans safer and more secure.

Please have someone call me at (512) 689-7815 to work on the logistics of the call.

Sincerely,

/ s /
Eddie M. Pope
General Counsel
FailSafe Communications, Inc.

EXHIBIT A

FAILSAFE PARTIAL[1] DRAFT ORDER ON RECONSIDERATION

In this Order on Reconsideration, we address the issues raised the Competitive Carriers Association (CCA) in its Petition for Reconsideration of the *Second Report and Order* regarding 911 outage reporting.[2] In that Order, we required carriers to notify Public Safety Answering Points ("PSAPs") within thirty minutes after an outage affecting 911 is detected. CCA specifically asks that the Commission have a different reporting requirement for VoIP carriers, CCA claimed "CCA carrier members frequently do not even receive a notification of potential outages within 30 minutes of it being discovered by its 911 solution vendors."[3]

We discussed this concern in the Order:

> *Reliance upon a third-party service provider to manage, route, or otherwise contribute to 911 call processing does not relieve a covered 911 service provider or an OSP, including an interconnected VoIP provider, of the obligation to provide notification to 911 special facilities under this rule. It is the duty of covered 911 service providers and OSPs, including interconnected VoIP service providers, to provide 911 service in accordance with the Commission's rules. Where a covered 911 service provider or an OSP supports 911 calling through a contractual arrangement with a third-party, we will hold those service providers accountable for compliance with their notification obligations. In this regard, "[t]he Commission has long held that licensees and other regulatees are responsible for the acts and omissions of their employees and independent contractors," and has recognized that "under long established principles of common law, statutory duties are nondelegable."*[4]

CCA's Motion should be rejected. It is a fundamental and well-recognized industry practice that network operators monitor their networks sufficiently to enable a quick response to network problems. To establish accepted industry standards for network design, operation, and maintenance, the Commission's Communications Security, Reliability and Interoperability Council (CSRIC) publishes a series of best practices. One of those practices requires network

[1] FailSafe takes no position with regard to other issues raised in CCA's Motion for Reconsideration. This draft is intended to focus solely on the question of detecting and reporting outages within 30 minutes.

[2] Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications, PS Docket No. 15-80; Improving 911 Reliability, PS Docket No. 13-75; New Part 4 of the Commission's Rules Concerning Disruptions to Communications, ET Docket No. 04-35; Resilient Networks, PS Docket No. 21-346; Location-Based Routing for Wireless 911 Calls, PS Docket No. 18-64, *Second Report and Order,* released November 18, 2022.

[3] CCA Motion for Reconsideration at 3.

[4] *Order,* ¶ 13. (internal footnotes omitted).

monitoring. CSRIC Best Practice 13-9-0401 ("Network Operators… should monitor their network to enable quick response to network issues.") (last revised 2013). These best practices also guide how calls to 911 should be monitored. CSRIC Best Practice 13-9-0574 ("Network Operators… should actively monitor and manage the 9-1-1 network components using network management controls, where available, to quickly restore 9-1-1 service and provide priority repair during network failure events. When multiple interconnecting providers and vendors are involved, they will need to cooperate to provide end-to-end analysis of complex call-handling problems") (last revised 2013).

Outages that can affect 911 providers can have serious repercussions. This Commission has been equally serious in enforcing its regulations regarding the detection and reporting of such outages. We have fined AT&T $460,000,[5] CenturyLink (now Lumen Technologies) $3,800,000[6], Intrado $1,750,000,[7] and Verizon Wireless $274,000[8], each for failure to detect and report outages affecting 911 facilities.

We are convinced that there are technological solutions that will aid CCA members in the swift detection of calls that do not reach PSAPs. For example, FailSafe Communications, Inc. ("FailSafe") has described several methodologies that will aid in giving carriers early warnings of potential outages. FailSafe describes one such methodology that should detect such calls in a matter of seconds. The FailSafe methodology relies upon the underlying intelligent signaling network. That network can detect the cause codes that relate to a call not going through.[9] The same network can identify the calling party's telephone number and supply information about the location of the calling party.[10] That information, when combined with other databases, allows a carrier to map such calls.[11] The FailSafe methodology would allow for the early detection and warning of an outage.

[5] https://docs.fcc.gov/public/attachments/DA-21-1542A1.pdf

[6] https://docs.fcc.gov/public/attachments/DA-21-1543A1.pdf.

[7] https://docs.fcc.gov/public/attachments/DA-21-1541A1.pdf.

[8] https://docs.fcc.gov/public/attachments/DA-21-1503A1.pdf

[9] FailSafe *ex parte* letter filed June 20, 2023; *see also* FailSafe Fourth Supplemental *ex parte* letter dated January 16, 2024. FailSafe has suggested that additional technological solutions would allow for the visual display of outages on maps, such as those provided by the Pacific Disaster Center. We encourage all developments that allow for useful information to be supplied to PSAPs and the public on a timely basis. FailSafe's Fourth Supplemental also provides estimates of costs of its methodologies. If FailSafe's estimates are accurate, we encourage the industry to implement such advances on a national basis.

[10] *Id.*

[11] *Id.*

The FailSafe methodology utilizes network components that we have required carriers to use for years. For example, we ordered the originating telephone number (also known as the Automatic Number Identification "ANI") be transmitted by carriers as early as 1994.[12] We required location data (Automatic Location Identification "ALI") be transmitted to PSAPs by cellular phones in 1999.[13] Of relevance to the CCA petition, we required the transmission of ANI and ALI by VoIP providers in 2005.[14]

We are also persuaded that there are vendors who can supply carriers with the equipment to detect incomplete calls to PSAPs. FailSafe states that it is working with Tekno Telecom ("Tekno").[15] In 2008, Tekno described its capabilities to this Commission:

> *Tekno Telecom is a manufacturer of SS7 probes that monitor and collect signaling information on public switched telephone PSTN and IP networks. Tekno Telecom started in 1968 in the telecom sector and has implemented over 10,000 systems worldwide, including systems deployed by over 200 U.S. rural ILEC's. Tekno Telecom customers use SS7 information to perform various network operations and engineering studies and to analyze inter-carrier billing issues.*[16]

We see no reason why the FailSafe methodology would not provide an early warning to carriers of potential outages. In short, we believe that there are technological solutions that will address CCA's concerns. We encourage CCA members to work with their underlying carriers and explore technological options such as that advocated by FailSafe. If the underlying carrier detects the start of an outage, it should notify the VoIP carrier and both should notify all affected PSAPs. All carriers should seek any advances in technology (such as that proposed by FailSafe) that will aid in their monitoring of 911 outages. The CCA Petition for Reconsideration is therefore DENIED.

[12] *See* In re Rules and Policies Regarding Calling Number Identification Service — Caller ID, Report and Order and Further Notice of Proposed Rulemaking, 9 FCC Rcd 1764, 1777 ¶ 77 (1994).

[13] In the Matter of Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems CC Docket No. 94-102 RM-8143 Third Report and Order RELEASED October 6, 1999.

[14] In the Matters of IP-Enabled Services E91 1 Requirements for IP-Enabled Service Providers WC Docket No. 04-36 WC Docket No. 05-196 -FIRST REPORT AND ORDER AND NOTICE OF PROPOSED RULEMAKING JUNE 3, 2005.

[15] FailSafe *ex parte.*

[16] Tekno Written Ex Parte Presentation CC Docket No. 01-92, Developing a Unified Intercarrier Compensation Regime (April 15, 2008).

FailSafe Communications Inc.
"Because Lives Are On The Line"™

Exhibit "B"

TELESENTIENT®

Conceptual Description of the Technology

by

Leo A. Wrobel, CEO and Inventor

United States Patents 10,812,663, 11,582,352 and 6,748,051

Forward

This document presents a conceptual view of an invention trade-named TeleSentient.® In it we describe at a high level how the use of *Intelligent Signaling Network* technology provides an early warning system for outages affecting 911 and 988, and allows for the reporting to both PSAPS and the FCC in less than a minute.

Many comments in this docket have cited significant financial and operational uncertainty associated with the FCC rules concerning 911 outage reporting. Those rules mandate that carriers notify 911 and eventually 988 centers, as well as the FCC, of service outages within 30 minutes. This report, styled as Exhibit B, assuages these concerns. It describes a patented methodology and emphasizes technology that is familiar to the Commission and the industry. It re-purposes existing equipment and processes that service providers have used for decades. The net result is ease of implementation and negligible net cost to network providers. Exhibit C which follows, describes possible future technologies that may emerge once these methods become commonplace in the industry.

We stand ready to answer your questions or to demonstrate TeleSentient.® Here is how it works.[1]

[1] In these documents, illustrations with arrows in the middle like the one above activate brief video explanations. Hyperlinks connect to supporting data and attachments.

How TeleSentient® Works – A Lay Person's Overview

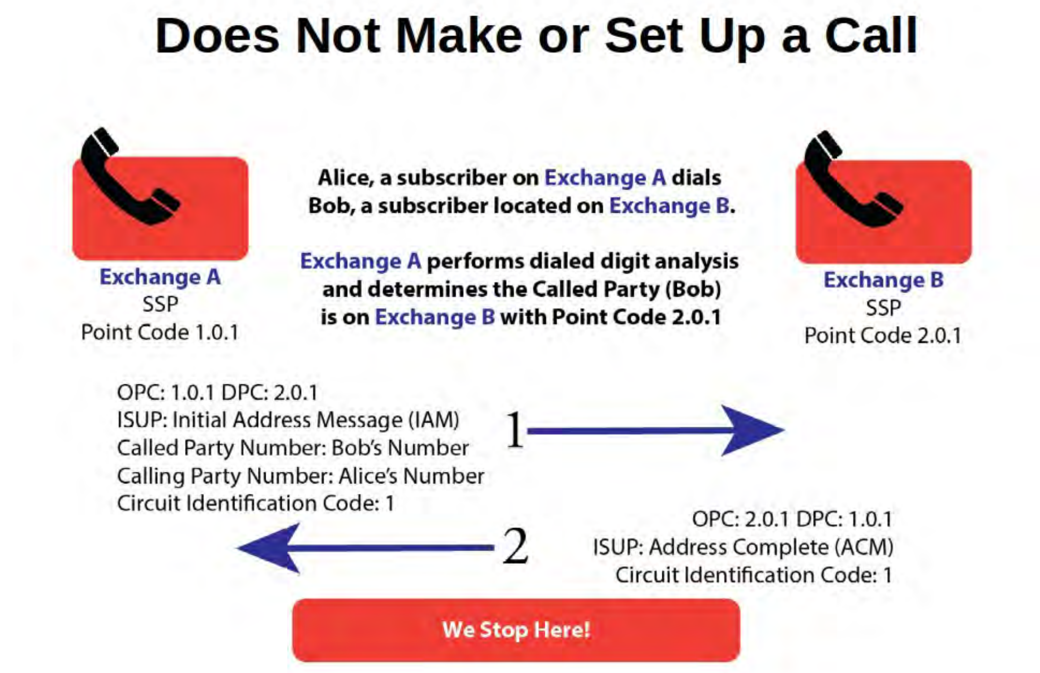
Telephone switching systems establish connections in response to actions by a caller. A caller initiates a call through a local wireless or landline switch. The switch processes dialed digits and extends the call to another subscriber, or to a tandem (intermediate) switch to reach a subscriber served by a different switch in another area.

As part of this process the local switch also transfers Intelligent Signaling Network information over a completely separate data network. The network may be Signaling System 7 (SS7) or Diameter, wireless or landline, I/p or TDM. The process described here remains the same.

Traditional Use of Signaling Networks
1 Can you take a call?
Boston
Dallas
Yes, I can. 2

Consider the illustration above, where a subscriber in Dallas makes a call from a landline or wireless phone to another party in Boston. Before a long distance carrier engages a trunk line from Dallas to Boston, it "looks ahead" by initiating a data query over an Intelligent Signaling Network. The query tells the carrier the status of the line in Boston. If it's busy, the Dallas caller still gets a busy signal, but it's from the switch in Dallas, not Boston. In this case the Intelligent Signaling Network returns Cause No. 17 – user busy. There are 128 possible Cause Codes, also known as ISUP Messages. A listing of all of these Cause Codes is in Attachment 1.

In most embodiments, TeleSentient® uses industry standard test equipment that has long been part of telephone company environments. For example, to learn the status of one or more phones in a specific geographic area, the equipment generates a **request** to make a call just like the example above. It queries the Intelligent Signaling Network the same way as an actual call would, but NEVER establishes a voice connection. Using the Intelligent Signaling Network only, can determine the status of users (in service, out of service, busy, etc) unobtrusively, in seconds. This includes 911 and 988 callers.



Does Not Make or Set Up a Call

Alice, a subscriber on Exchange A dials Bob, a subscriber located on Exchange B.

Exchange A performs dialed digit analysis and determines the Called Party (Bob) is on Exchange B with Point Code 2.0.1

Exchange A
SSP
Point Code 1.0.1

Exchange B
SSP
Point Code 2.0.1

1

OPC: 1.0.1 DPC: 2.0.1
ISUP: Initial Address Message (IAM)
Called Party Number: Bob's Number
Calling Party Number: Alice's Number
Circuit Identification Code: 1

2

OPC: 2.0.1 DPC: 1.0.1
ISUP: Address Complete (ACM)
Circuit Identification Code: 1

We Stop Here!

Since Intelligent Signaling Networks "know" so much about what is going on in the Public Switched Telephone Network (PSTN) they are a rich source of useful data. For example, if 100 telephones in Wichita Kansas all go off hook at the same time in response to a tornado, the Intelligent Signaling Network is network is instantly aware of this fact and can put that information to good use.

This Exhibit discusses three embodiments for this technology.

- Determining 911 and 988 callers who try to call but do not get through is accomplished by something called **"Triggers."**

- Determining the status of thousands of phone users over a broad area for (populating a heat map for example) is called **"Sweeps."**

- Showing callers in trouble in relation to the cause of their call is called **"Correlation."**

Uses Technology Familiar to Commission and Industry

> *"Signaling systems have evolved with the growth and evolution of the telecommunications networks they serve. What once was a simple mechanism managing call setup and billing is now a sophisticated system capable of optimizing the operation of the digital telecommunications network and supporting current and future services.."*[2]*... **Published July 1993***

The date above is not a misprint. *Intelligent Signaling Networks* like Signaling System 7 (SS7) have been used by phone companies to control calls since the 1980's. Although there are newer protocols today like Diameter, it is SS7 that maintains interoperability between wireless and landline operators.[3] Today, SS7 touches virtually every phone call in one way or another, since the "red" network must always be able to communicate with the "blue" network – regardless of the technology they use.[4] The requirement for interoperability between landline, wireless, I/p carriers, and legacy 911 centers will assure every network operator supports SS7 long into the future. For these reasons our emphasis is on SS7 since it can communicate with any Intelligent Signaling Network technology.

Taking another cue from the past, consider the evolution of 911 in a historical context. *Automatic Number Identification* (ANI) was in use by carriers long before it was paired up with an *Automatic Location Identifier* (ALI) database in the 1970s.[5] When ANI was introduced to ALI years ago, the **E911** system proliferated throughout North America. This paper proposes a similar technology migration into 911 for one big reason: During mass calling events, not everyone gets through to 911. Intelligent Signaling Network technology can identify unsuccessful callers. This paper includes a morsel of how this approach could have saved lives during the tragic Lahaina, Maui fires.

Concerns expressed by carriers regarding the rules established in this proceeding center largely around the feasibility of 911 outage notifications in a 30 minute time frame. The carriers have a point, but it only takes them so far. Indeed, experts agree that it is not unusual to see 40-50 alarms per second during major failures. This leads to serious difficulties in the network management process that have been noted for many years. It misses the use of automation, particularly automatic processes that employ alerts generated by Intelligent Signaling Networks.

[2] External, Network-Wide Monitoring of SS7 Networks: A Solution to Managing Digital Telecommunications Networks ©1993 Giovanni Marotta, Richard Brown Networks and Communications Laboratory HP Laboratories

[3] Diameter is the evolution of the SS7 that is used within and between the 4G Long Term Evolution (LTE) networks. SS7 is defined by ITU-T (International Telecommunication Union Telecommunication Standardization Sector)

[4] Leo A. Wrobel is author of 12 books, and some 1600 trade articles over a 45 year career. Also based in part on research paper entitled "We Know Where You Are" presented at the 2016 8th International Conference on Cyber Conflict. (Cyber Power N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.) 2016 © NATO CCD COE Publications) TeleSentient®

[5] Once carriers warmed up to the idea of sharing their ANI, a means was devised by regulators to price it with carriers. The result as a 911 environment that was revolutionized, with technology that still exists today.

> *"For gaining a thorough understanding of packet networks such as the CCSN, an integrated approach is needed consisting of (1) high quality traffic measurements, (2) sophisticated traffic data analysis methods, and (3) advanced traffic modeling tools that result in useful traffic and network engineering guidelines.*[6]*"**… Published in 1995***

Our supplier Tekno Telecom has produced probes capable of generating email or text alerts for decades. This is not a new idea. The following was taken from a 1995 research paper by experts at GTE Laboratories. It shows that capabilities existed for telecom service providers decades ago:

> *Event correlation is a conceptual interpretation procedure where a new meaning is assigned to a set of events that happen within a predefined time interval. The conceptual interpretation procedure could stretch from a trivial task of alarm compression to a complex pattern matching task. A typical event correlation is determined to be a dynamic pattern matching over a stream of network events. In addition, the correlation pattern may include network connectivity information, diagnostic test data, data from external databases, and any other information.*
>
> *Applying event correlation rules may yield several results. First, a new event (message) may be sent to the operator's terminal. Second, an action may clear or resolve existing events. Third, a diagnostic message may be sent about faults occurring in the network. Fourth, a procedure may be called to access a database, run a diagnostic test procedure, generate a trouble ticket, or perform any other executable external procedure. Fifth, an internal system action to store data, change the system mode of operation, or perform any other internal system procedure may be taken.*[7]

Like the earlier example of ANI begetting ALI (and ultimately E911) the recommended technology in this paper has simply has not made it yet to the emergency services environment. This is coupled with the fact that the industry has not yet completely come to terms with the notion that Intelligent Signaling Network data is a rich and powerful technology when correlated with other reliable sources to produce new, actionable, metadata. In its simplest form this means the ability to automatically trigger an alert to the FCC or a PSAP, or even visualize it as described in the next section.[8]

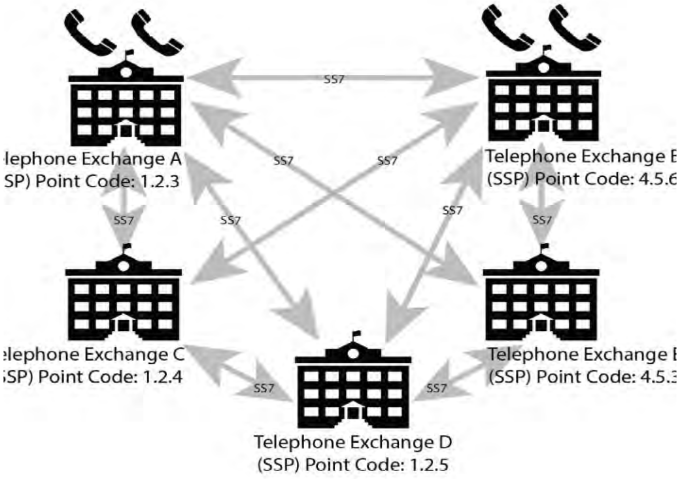
[6] Statistical Analysis of CCSN/SS7 Traffic Data from Working CCS Subnetworks, © 1995 by Diane E. Duffy, Allen A. McIntosh, Mark Rosenstein, Walter Willinger, Bellcore, Morristown, NJ

[7] Real-time Telecommunication Network Management: Extending Event Correlation With Temporal Constraints © 1993 G. Jakobson, M. Weissman GTE Laboratories Incorporated 40 Sylvan Rd, Waltham, MA 02254

[8] FailSafe's technical partner Tekno Telecom sells network probes that produce email and text alerts straight off the shelf. Thousands of these probes are in place in carrier networks but like the ANI/ALI example, have never been used for this purpose. Carriers may also be reluctant to implement changes that effectively make the PSAP and the FCC aware of outages in their network before they are. This is an important policy issue that probably can only be resolved by the FCC.

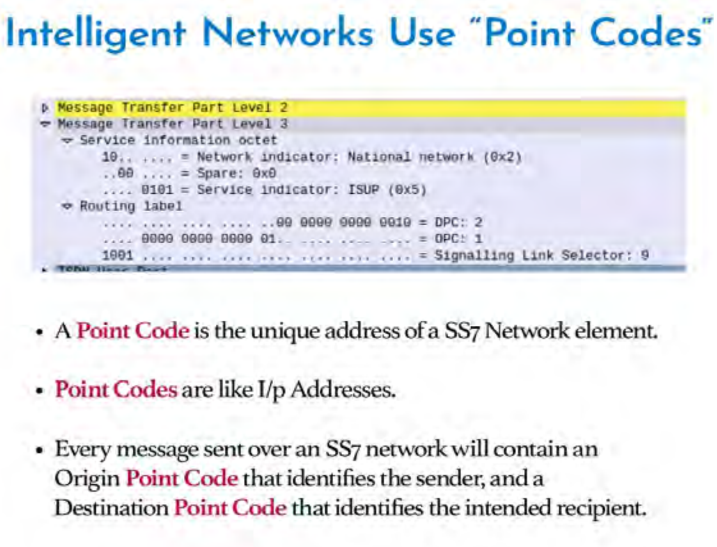
A. The Technology is Already In Place

SS7 was designed to use 24 channel TDM (Time Division Multiplexing) trunks set up between telephone exchanges. Each circuit is identified by a Circuit Identification Code (CIC) that is unique to each telecommunications carrier. This CIC code is included in SS7 data packets called ISUP messages. Switches use this information to determine which of their respective circuits should be connected together to provide an end to end speech path.[9]



A typical SS7 transaction is only around 40 bits counting overhead (not bytes) and can technically operate at "1980" modem speeds. It operates just fine at 56Kb speeds today since the typical transaction is so small. This comes in handy for some applications, like Sweeps, described later in this letter. When combined with today's much higher speed Internet, it has theoretically become possible to query every phone in North America just to learn its status and see whether it can take a call.[10] When this data is mapped over a heat map, one can imagine its value to an organization willing to pay for such information, e.g:

> *"Atlanta just turned red on the map! What happened there?"*[11]



Intelligent Networks Use "Point Codes"

```
▷ Message Transfer Part Level 2
▽ Message Transfer Part Level 3
  ▽ Service information octet
      10.. .... = Network indicator: National network (0x2)
      ..00 .... = Spare: 0x0
      .... 0101 = Service indicator: ISUP (0x5)
  ▽ Routing label
      .... .... .... .... ..00 0000 0000 0010 = DPC: 2
      .... 0000 0000 0000 01.. .... .... .... = OPC: 1
      1001 .... .... .... .... .... .... .... = Signalling Link Selector: 9
```

- A Point Code is the unique address of a SS7 Network element.
- Point Codes are like I/p Addresses.
- Every message sent over an SS7 network will contain an Origin Point Code that identifies the sender, and a Destination Point Code that identifies the intended recipient.

The CIC Codes described correspond to Point Codes. Point Codes correspond to specific locations and equipment for the network provider. Point Codes are like I/p addresses, and most major pieces of equipment in a carrier network have a Point Code. Without getting into too much detail, Point Codes can be easily adapted to V&H (Vertical and Horizontal) coordinates on a map. We have several examples of this using industry standard billing and rating software packages that are inexpensive and readily available.

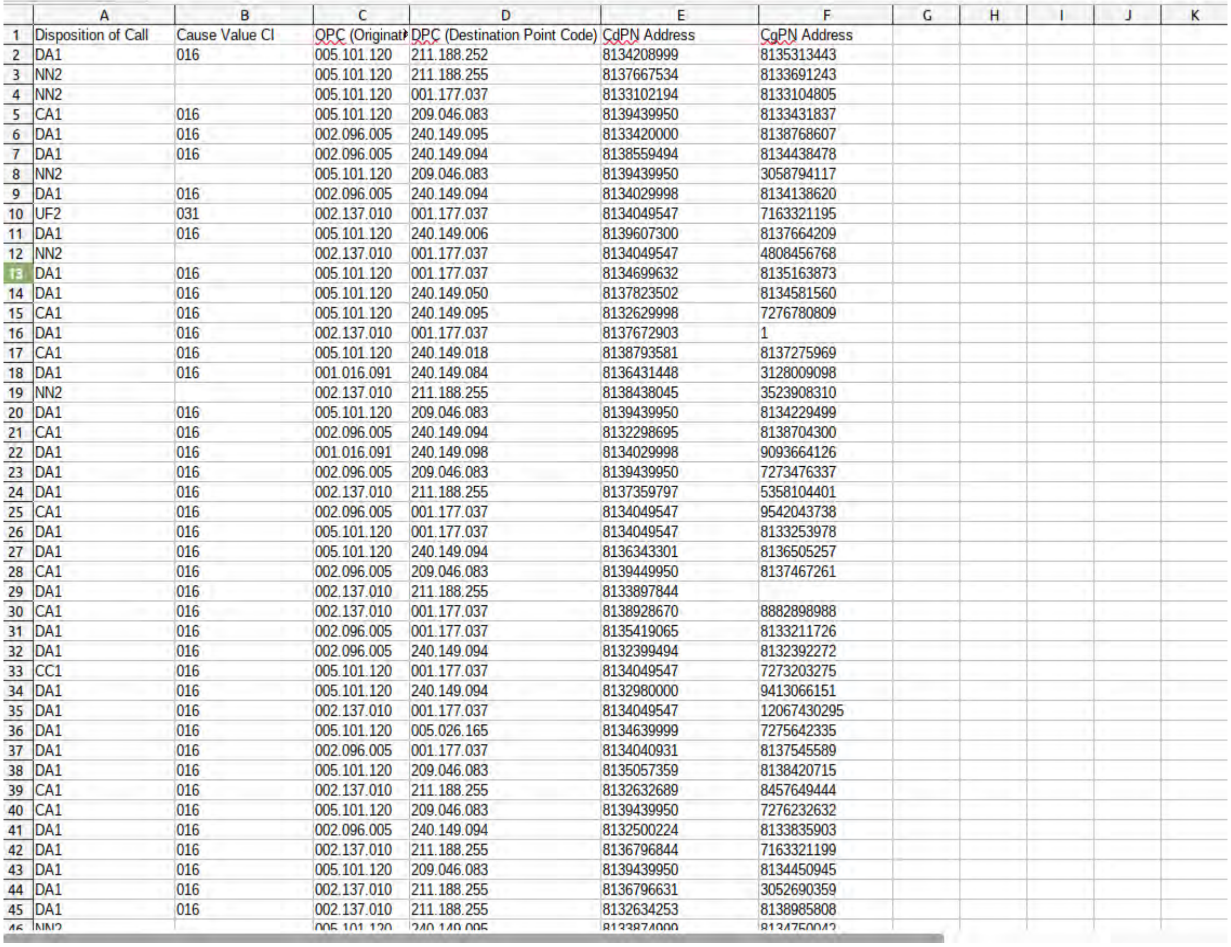
[9] Tekno Telecom often converts this data to industry standard 110120 or 110125 call detail records (CDR) for carrier access billing verification employed by carriers. These CDRs are in a format for TeleSentient® applications that is easy for the carrier to understand.

[10] Interfacing TeleSentient® data with Artificial Intelligence (AI) is a topic also under discussion.

[11] This is one kind of application that we have tested with the Pacific Disaster Center. You will recall in a previous *ex-parte* we described a map of telephone central offices in relation to a series of Oklahoma thunderstorms. We do not offer such a service, we license the technology to entities like the Pacific Disaster Center that otherwise would not have access to it.

As shown below, ISUP data associated with the point codes contains useful data about calling parties and called parties, including originating and terminating numbers, time of the call, etc. These can be output in the format of standard call detail records by carrier, a format which is familiar to all carriers. The output data can be in standard Excel or CSV format.

Point Codes Beget Useful and Actionable Information



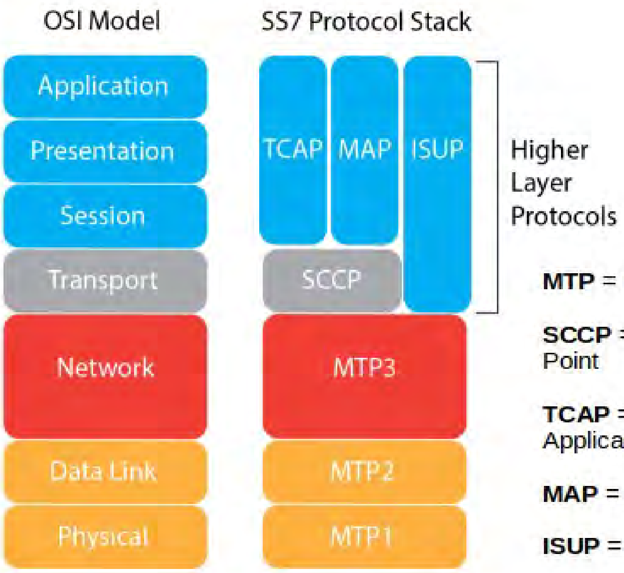
	A	B	C	D	E	F	G	H	I	J	K
1	Disposition of Call	Cause Value CI	OPC (Originati	DPC (Destination Point Code)	CdPN Address	CgPN Address					
2	DA1	016	005.101.120	211.188.252	8134208999	8135313443					
3	NN2		005.101.120	211.188.255	8137667534	8133691243					
4	NN2		005.101.120	001.177.037	8133102194	8133104805					
5	CA1	016	005.101.120	209.046.083	8139439950	8133431837					
6	DA1	016	002.096.005	240.149.095	8133420000	8138768607					
7	DA1	016	002.096.005	240.149.094	8138559494	8134438478					
8	NN2		005.101.120	209.046.083	8139439950	3058794117					
9	DA1	016	002.096.005	240.149.094	8134029998	8134138620					
10	UF2	031	002.137.010	001.177.037	8134049547	7163321195					
11	DA1	016	005.101.120	240.149.006	8139607300	8137664209					
12	NN2		002.137.010	001.177.037	8134049547	4808456768					
13	DA1	016	005.101.120	001.177.037	8134699632	8135163873					
14	DA1	016	005.101.120	240.149.050	8137823502	8134581560					
15	CA1	016	005.101.120	240.149.095	8132629998	7276780809					
16	DA1	016	002.137.010	001.177.037	8137672903	1					
17	CA1	016	005.101.120	240.149.018	8138793581	8137275969					
18	DA1	016	001.016.091	240.149.084	8136431448	3128009098					
19	NN2		002.137.010	211.188.255	8138438045	3523908310					
20	DA1	016	005.101.120	209.046.083	8139439950	8134229499					
21	CA1	016	002.096.005	240.149.094	8132298695	8138704300					
22	DA1	016	001.016.091	240.149.098	8134029998	9093664126					
23	DA1	016	002.096.005	209.046.083	8139439950	7273476337					
24	DA1	016	002.137.010	211.188.255	8137359797	5358104401					
25	CA1	016	002.096.005	001.177.037	8134049547	9542043738					
26	DA1	016	005.101.120	001.177.037	8134049547	8133253978					
27	DA1	016	005.101.120	240.149.094	8136343301	8136505257					
28	CA1	016	002.096.005	209.046.083	8139449950	8137467261					
29	DA1	016	002.137.010	211.188.255	8133897844						
30	CA1	016	002.137.010	001.177.037	8138928670	8882898988					
31	DA1	016	002.096.005	001.177.037	8135419065	8133211726					
32	DA1	016	002.096.005	240.149.094	8132399494	8132392272					
33	CC1	016	005.101.120	001.177.037	8134049547	7273203275					
34	DA1	016	005.101.120	240.149.094	8132980000	9413066151					
35	DA1	016	002.137.010	001.177.037	8134049547	12067430295					
36	DA1	016	005.101.120	005.026.165	8134639999	7275642335					
37	DA1	016	002.096.005	001.177.037	8134040931	8137545589					
38	DA1	016	005.101.120	209.046.083	8135057359	8138420715					
39	CA1	016	002.137.010	211.188.255	8132632689	8457649444					
40	CA1	016	005.101.120	209.046.083	8139439950	7276232632					
41	DA1	016	002.096.005	240.149.094	8132500224	8133835903					
42	DA1	016	002.137.010	211.188.255	8136796844	7163321199					
43	DA1	016	005.101.120	209.046.083	8139439950	8134450945					
44	DA1	016	002.137.010	211.188.255	8136796631	3052690359					
45	DA1	016	002.137.010	211.188.255	8132634253	8138985808					
46	NN2		005.101.120	240.149.095	8133874000	8134750042					

Compatible With TDM and I/p, SS7 and Diameter

ISUP stands for ISDN User Part. ISUP operates at the network layer of the OSI model, specifically in the Signaling Connection Control Part (SCCP) of the SS7 protocol. ISUP is the means used to exchange status information for available speech circuits. If no circuits are available at the intended destination, a code is sent to the originating switch to play a busy signal, all-circuits-busy recording, or other signal to the caller. [12]

All signaling networks including I/p must comport in one way or another with the OSI model shown below. Otherwise the "Red" network could not talk to the "Blue" network. SS7 is the most ubiquitous protocol and can interface to all other wireless and landline protocols.

Comparison of OSI and SS7 Protocol Stacks



MTP = Message Transport Part

SCCP = Signaling Connection Control Point

TCAP = Transaction Capabilities Application Part

MAP = Mobile Application Part

ISUP = ISDN User Part

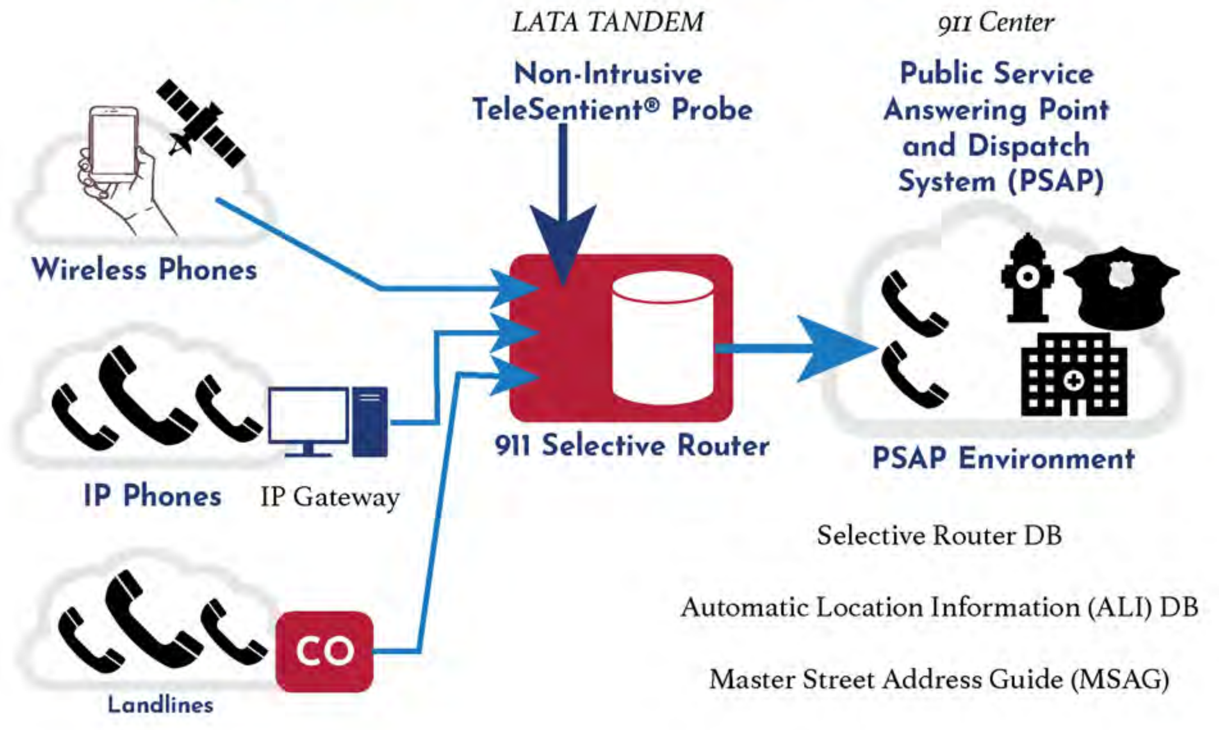
MTP 1 (Message Transfer Part 1) Physical layer. In this past this was often T1 lines.

MTP 2 (Message Transfer Part 2) Data link layer responsible for handling reliable transfer of data in sequence

MTP 3 (Message Transfer Part 3) The MTP3 header contains an **Originating and a Destination Point Code.**

[12] There are 128 ISUP Cause Codes. Approximately 40 of them are defined. About 20 or so are reserved. This might allow assignment of a special ISUP cause code at some time in the future, dedicated to 911 and 988 blockage or outages. Eventually it could be adopted by equipment manufacturers and carriers, simplifying the task even more.

Compatible With NG911 and FirstNet


LATA TANDEM
Non-Intrusive TeleSentient® Probe
911 Center
Public Service Answering Point and Dispatch System (PSAP)
Wireless Phones
IP Phones
IP Gateway
Landlines
CO
911 Selective Router
PSAP Environment
Selective Router DB
Automatic Location Information (ALI) DB
Master Street Address Guide (MSAG)

The optimal placement for a signaling network probe is adjacent to the Selective Call Router in the LATA tandem, although technically it could exist anywhere. From this point all networks are visible and independent of the signaling protocol used. Visibility exists to all landline, I/p and wireless networks through the use of gateways. Gateways will still be in use after the transition to NG911.

> ***"Since the legacy circuit-switched TDM network will very likely continue to be used for the foreseeable future (both wireline and wireless), the i3 architecture defines a Legacy Network Gateway (LNG) to interface between the legacy network and the ESInet/NGCS.***[13]

[13] NENA i3 Standard for Next Generation 9-1-1, NENA-STA-010.3b-2021, October 7, 2021 Executive Summary at 8.

Detailed Overview of Methodology

The SS7 data path utilizes a level 4 data protocol designed specifically for SS7 networks.[14] ISUP (Integrated Services Digital Network User Part) is the data standard used for controlling calls.[15] It is in the ISUP data where the feature richness of SS7 resides. TeleSentient® provides meaningful information about network anomalies and disasters in near real time. It is capable of generating queries on a wireline or wireless communications system without disturbing end users in any way. TeleSentient® is operationally coupled to the switching system by a signaling link to the SS7 network. In some embodiments, TeleSentient® includes SS7 test equipment that interfaces with a web browser operated by the user as illustrated below.

Considering that Intelligent Signaling Networks like SS7 have not changed much in over 30 years, sometimes the equipment can be of a "telecom stone age" vintage. The **INET SPECTRA SS7 Communications Analyzer** is one example. It has been in use since the 1980's but serves well for basic applications.

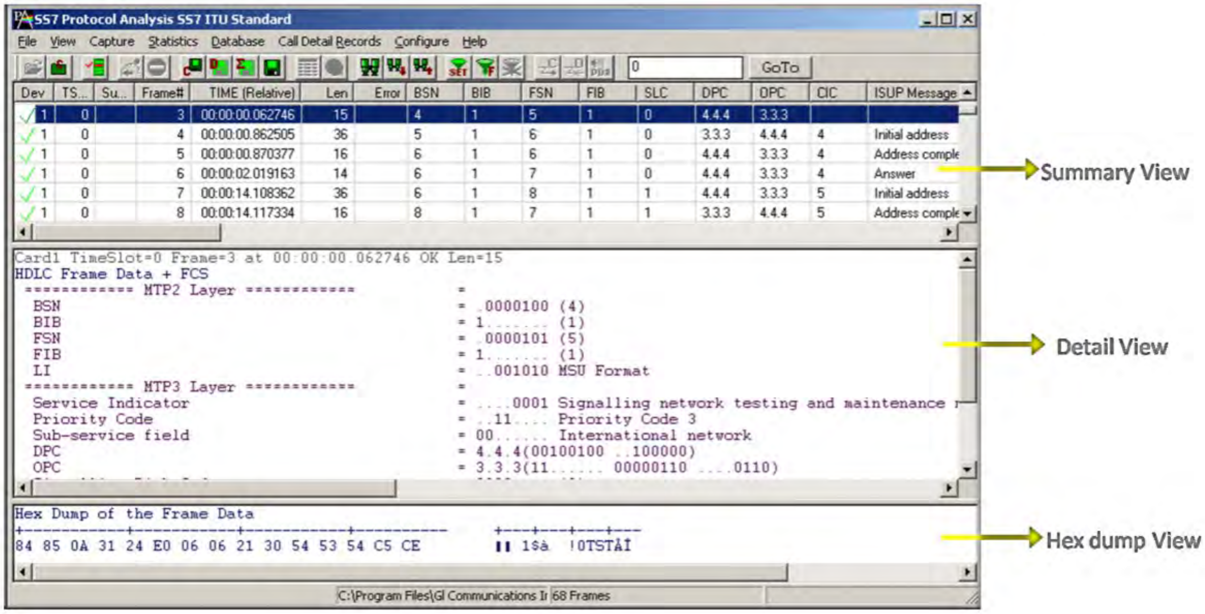
Other equipment purchased and tested by FailSafe provides far more sophisticated capabilities, such as the software-based network probes manufactured by GL Communications. A summary of its capabilities can also be found at www.GL.com.[16]

[14] SS7 uses out-of-band signaling, which means that signaling (control) information travels on a separate, dedicated 56 or 64 Kbps channel rather than within the same channel as the telephone call. Using SS7, telephone calls can be set up more efficiently and services such as call forwarding and wireless roaming service are easier to add and manage.

[15] ISUP is part of the Signaling System No. 7 (SS7), used to set up telephone calls in the public switched telephone network (PSTN). It is specified by the ITU-T as part of the Q.76x series. When a telephone call is set up from one subscriber to another, several telephone exchanges could be involved, possibly across international boundaries. To allow a call to be set up correctly, where ISUP is supported, a switch will signal call-related information like called party number to the next switch in the network using ISUP messages.

[16] The fact that GL Communications was able to secure the highly desirable URL "GL.com" underscores just how long this kind of equipment has been in use.

GL's SS7 Analyzer…


SS7 Protocol Analysis SS7 ITU Standard
File View Capture Statistics Database Call Detail Records Configure Help
0
GoTo
Summary View
Detail View
Hex dump View

Dev	TS...	Su...	Frame#	TIME (Relative)	Len	Error	BSN	BIB	FSN	FIB	SLC	DPC	OPC	CIC	ISUP Message
✓ 1	0		3	00:00:00.062746	15		4	1	5	1	0	4.4.4	3.3.3		
✓ 1	0		4	00:00:00.862505	36		5	1	6	1	0	3.3.3	4.4.4	4	Initial address
✓ 1	0		5	00:00:00.870377	16		6	1	6	1	0	4.4.4	3.3.3	4	Address comple
✓ 1	0		6	00:00:02.019163	14		6	1	7	1	0	4.4.4	3.3.3	4	Answer
✓ 1	0		7	00:00:14.108362	36		6	1	8	1	1	4.4.4	3.3.3	5	Initial address
✓ 1	0		8	00:00:14.117334	16		8	1	7	1	1	3.3.3	4.4.4	5	Address comple

```
Card1 TimeSlot=0 Frame=3 at 00:00:00.062746 OK Len=15
HDLC Frame Data + FCS
 ============ MTP2 Layer ============            =
  BSN                                           = .0000100 (4)
  BIB                                           = 1....... (1)
  FSN                                           = .0000101 (5)
  FIB                                           = 1....... (1)
  LI                                            = ..001010 MSU Format
 ============ MTP3 Layer ============            =
  Service Indicator                             = ....0001 Signalling network testing and maintenance r
  Priority Code                                 = ..11.... Priority Code 3
  Sub-service field                             = 00...... International network
  DPC                                           = 4.4.4(00100100 ..100000)
  OPC                                           = 3.3.3(11...... 00000110 ....0110)
```

```
Hex Dump of the Frame Data
+-----------+-----------+-----------+----------    +---+---+---+---
84 85 0A 31 24 E0 06 06 21 30 54 53 54 C5 CE       ▌▌ 1$à  !0TSTÅÎ
```

C:\Program Files\Gl Communications Ir 68 Frames

Finally, FailSafe has tested equipment that is 100% TDM, utilizing V.35 interfaces dating back to the 1980's and before. This kind of configuration is still used by many small independent phone companies. In those cases the Inventor purchased and tested equipment from Engage Communications, which converts TDM to a SIP connection. In other words, a do-it-yourself Sigtran link. Among other advantages, this allows SS7 queries to be made from any location in the world with a reliable Internet connection and I/p address.[17]

[17] Please note that during our studies we found many small 911 centers that still use Carrier Associated Signaling (CAS) trunks or analog phone lines. These do not provide Intelligent Signaling Network data directly, that is they send digits over the speech portion of the trunk rather than a separate signaling network channel. It turns out this does not matter for Alerts. The probes we use look "inward" toward the signaling network data in the switch and the PSTN, not "outward" to the 911 center over the CAS trunk. This is how the probes see the most important information – who is calling. No useful information can be derived from the CAS trunk since it has no out-of-band signaling. if the CAS trunk were cut however, or went out of service, the switch would still generate an alarm and an alert could be generated from Intelligent Signaling Network data associated with the switch and PSTN.

Equipment commonly used for testing of SS7 and ISDN signaling networks like Sigtran, HSL, ISUP, GSM, and TCAP as well as conformance, validation and regression testing exists with most network providers. Using the Network Element Emulation (SSP, STP, HLR, VLR, SG, ASP) modes for network element simulation (STPs, SCPs, HLRs) provides many new capabilities that are useful in the emergency services environment.

FailSafe has used equipment provided by Tekno Telecom and has successfully simulated many different network conditions.

The process for sending real-time alerts to PSAPS and Regulators can be defined in seven steps:

1. Define data needed
2. Set up trigger
3. Output Filter and Search signaling data based on triggers
4. Save results to a file
5. Export the file to cloud
6. Define business rules
7. Produce desired output from the saved cloud data

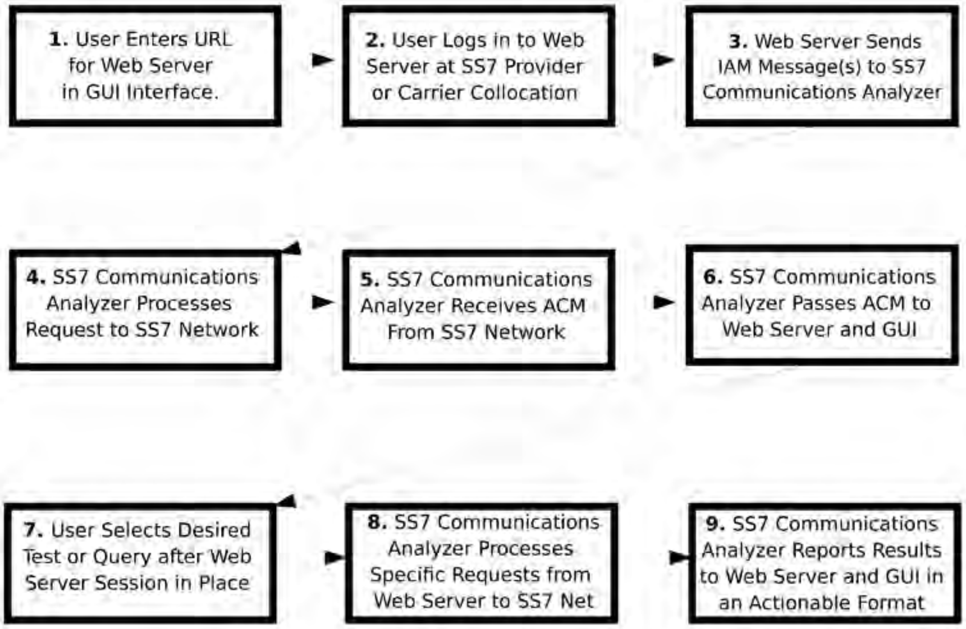
Technical Requirements for Alerts and Sweeps

Option 1 – Alerts

For purposes of 911 and 988 notifications, this equipment should be optimally located in a collocation in the Access Tandem Switch, and adjacent to the Selective Call Router for that LATA as outlined previously. Once the probe is established there are a number of options based on the type and format of notifications desired by the entity to be notified. A web server may be coupled to the SS7 Communications Analyzer, behind a suitable firewall, for several purposes. The first is to generate queries based on what the operator needs. The second is to log, archive and interpret the responses. The third is to transmit those responses to a remote customer location where they can be represented graphically in a manner that an operator using TeleSentient® can understand and interpret.

The SS7 Communications Analyzer and web server do not have to be in the same place as the GUI screen display. The GUI screen display can be any terminal that can display graphical screens to a user and allow the user to make selections and inputs. In some embodiments of TeleSentient® it is a personal computer running a web browser. The GUI screen initiates the generation and release of data calls and messages in the SS7 switching system by transferring SS7 signaling over the signaling link.

TeleSentient® may encompass several components shown below.


1. User Enters URL for Web Server in GUI Interface.
2. User Logs in to Web Server at SS7 Provider or Carrier Collocation
3. Web Server Sends IAM Message(s) to SS7 Communications Analyzer
4. SS7 Communications Analyzer Processes Request to SS7 Network
5. SS7 Communications Analyzer Receives ACM From SS7 Network
6. SS7 Communications Analyzer Passes ACM to Web Server and GUI
7. User Selects Desired Test or Query after Web Server Session in Place
8. SS7 Communications Analyzer Processes Specific Requests from Web Server to SS7 Net
9. SS7 Communications Analyzer Reports Results to Web Server and GUI in an Actionable Format

In some embodiments of TeleSentient,® the Intelligent Signaling Network data is derived in the context of Voice over Internet Protocol (VoIP), Asynchronous Transfer Mode (ATM), TR-303, ISDN PRI, T1 / ESF, Time Division Multiplexing (TDM), or Frame Relay networks. The switching system itself can be any SS7-based network that extends voice connections or SMS messages based on data messages in response to SS7 signaling.[18]

Of course, any network able to receive an ISDN bearer connections and SS7 switching is suitable, including TDM, ATM, SIP, Diameter or VoIP. In fact, TeleSentient® can originate, terminate, and simulate calls without the network at all if both the origination and termination are directly connected to the SS7 switching system. In various embodiments of TeleSentient,® the signaling link can be a SS7 A, B, C, D, E or F link to a Signal Transfer Point (STP) in the network.

As previously stated, various options are available to the licensee/operator. In some embodiments of the TeleSentient,® the Web Server is simply a conventional web server. The Web Server generates and releases data-only SS7 calls through the switching system by transferring signaling to the SS7 Communications Analyzer. The Web Server also directs the SS7 Communications Analyzer to run specific queries or tests selected by the user.

The SS7 Communications Analyzer formats the queries from the Web Server and forwards the request to the SS7 Communications Analyzer. The SS7 Communications Analyzer also receives SS7 signaling messages from the Signaling Point (SP) and forwards those back to the Web Server. If SS7 signaling is used, then the SS7 Communications Analyzer applies Message Transfer Part (MTP) functionality to the signaling message.

The following describes the operation of a specific configuration of TeleSentient® using a GUI end user interface, a Web Server and SS7 signaling. The patents are not restricted to this exact configuration or operation.

The session begins when the remote user/operator enters the Uniform Resource Locator (URL) of the Web Server into the GUI. The GUI connects to the Web Server via a secure Internet connection. The Web Server returns a start menu and requests a user password and a CIC. The user enters the password and the CIC into the GUI, and the GUI transfers the user information to the Web Server. The Web Server checks the password and the CIC. If the password is legitimate and the CIC is idle, then the server returns a main menu to the GUI. The main menu allows the user to select from a number of functions such as: 1) make a data-only query, 2) listen for specific data activity, 3) end the session, or (4) other functions. The GUI transfers the user selection to the Web Server for processing.

Various sub menus in the Web Server allow the user to input more specific information, such as telephone number range of queries, type of queries, SMS vs voice queries, and other selections. The GUI transfers these choices to the Web Server. The Web Server then generates an SS7 Initial Address Message (IAM) based on that information and sends the IAM to the SS7 Communications Analyzer. The SS7 Communications Analyzer forwards the IAM to the signaling point, which processes the IAM for the specific kind of data call to the SS7 network.

[18] The switching system could also be a distributed system comprised of a signaling processor and a network element where the network element could be an ATM multiplexer or switch. Such a system is disclosed in U.S. patent No.: 08/568,551, entitled "Method, System, and Apparatus for Telecommunications Control," 08/525,897, entitled "Broadband Communications System;" 08/525,050, entitled "System for Managing Telecommunications," and 09/027,008, entitled "System and Method for Connecting a Call with an Interworking System."

An SS7 Address Complete Message (ACM) is typically received from the network after the IAM. The ACM is passed to the Web Server through the signaling point. The Web Server sends an ACM indication to the GUI. An SS7 Answer Message (ANM) is typically received from the network after the ACM and is passed to the Web Server through the signaling points. The ANM indicates that the connection is established.

After the query is established, the Web Server sends a testing menu to the GUI. The testing menu allows the user to select tests to run, range of type of numbers for testing, to release the call and return to the main menu, and other functions. The GUI transfers a user request for "TEST A" to the Web Server. The Web Server transfers a new test instruction to the SS7 Communications Analyzer identifying the requested test. The SS7 Communications Analyzer initiates the test and returns the results to the Web Server. The Web Server forwards the test result to the GUI, along with another updated test menu. The GUI then transfers the next user selection to the Web Server.

If the user selects the “listening”[19] option from the main menu, the GUI transfers that selection to the Web Server. The Web Server awaits the response. The incoming data call is initiated by an incoming IAM from the SS7 Communications Analyzer. The IAM is passed to the SS7 network through the Signaling Points (SP). The Signaling Point (SP) initiates a ACM and an ANM for transfer to the SS7 network. The SS7 network establishes a data only call connection in response to the incoming IAM.

The Web Server sends an updated menu to the GUI. The menu allows the user to select a test, release the call and return to the main menu, or other functions. If the user selects "TEST B", then the GUI provides the user selection to the Web Server. The Web Server sends instructions to the SS7 Communications Analyzer to perform the selected actions. The SS7 Communications Analyzer initiates the selected action and returns the result to the Web Server. The Web Server sends the test result and the called menu to the GUI.

If the user selects the return to main menu option, the Web Server generates an REL and transfers the REL and CIC to the SS7 Communications Analyzer. The SS7 Communications Analyzer applies MTP based on the CIC and forwards the REL to the Signaling Point. (SP) The Signaling Point (SP) forwards the REL to the SS7 network. The SS7 network tears down the connection based on the REL. An RLC is typically received from the SS7 network in response to an REL. The RLC is passed to the Web Server through the Signaling Point (SP) The Web Server provides an RLC indication and the main menu to the GUI.

If the user / operator selects “End Session” the GUI sends that selection to the Web Server. The Web Server sends a session over indication to the GUI and sends instructions to the SS7 Communications Analyzer indicating that the session is over. The GUI disconnects from the Web Server and the SS7 Communications Analyzer de-allocates the CIC.

The raw data may be visually represented by the user/operator in a heat map that shows network conditions on a near-real-time basis based on data collected from the SS7 network.

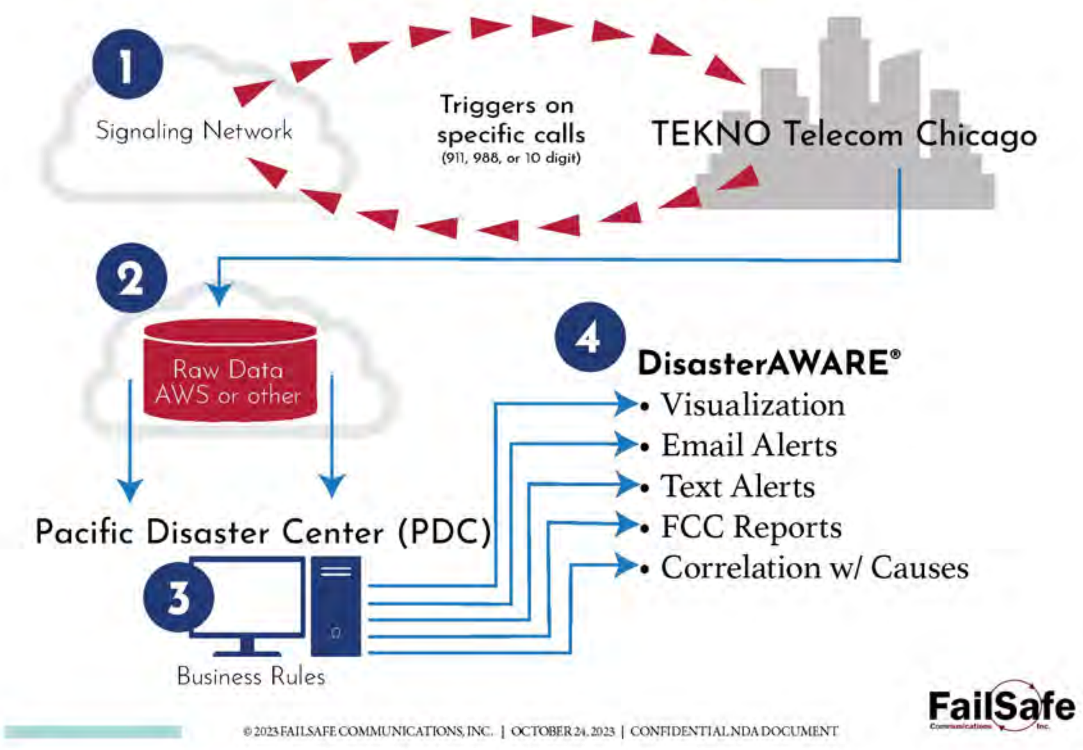
As a further example but not a limitation, the raw data can be further enhanced in the following manner by TeleSentient® before being passed to the user /operator.

[19] TeleSentient® does not allow that anyone can actually hear an underlying call, which is impossible anyway since a voice path is never set up. It is “listening” only to the underlying data messages in a non-intrusive configuration.

- The raw data can be processed through various call rating and geographic location services used by phone companies such as those identifying physical geographic location, local calling area, name of incumbent local phone company, and other data available to certified Incumbent Local Exchange Carriers (ILECs) and Competitive Local Exchange Carriers (CLECs).
- The raw data can be processed by the LIDB database.[20]
- The data may be filtered to include only the data or geographic areas of interest to a specific customer before being passed to that customer.
- The data may be filtered by traffic type. For example, it may be segmented only by callers attempting to call 911 or other emergency services. In that case TeleSentient® can show the numbers of callers to 911 in response to a specific event. TeleSentient® can also show the number of callers who tried to call 911 but did not get through, *and identify who and where they are* based on the SS7 ISUP messages. The diagram below illustrates the big picture.
- Output to an AI (Artificial Intelligence) system.

Embodiments of TeleSentient®

Visualization * Email Alerts * Text Messages * FCC and PSAP Reports



©2023 FAILSAFE COMMUNICATIONS, INC. | OCTOBER 24, 2023 | CONFIDENTIAL NDA DOCUMENT

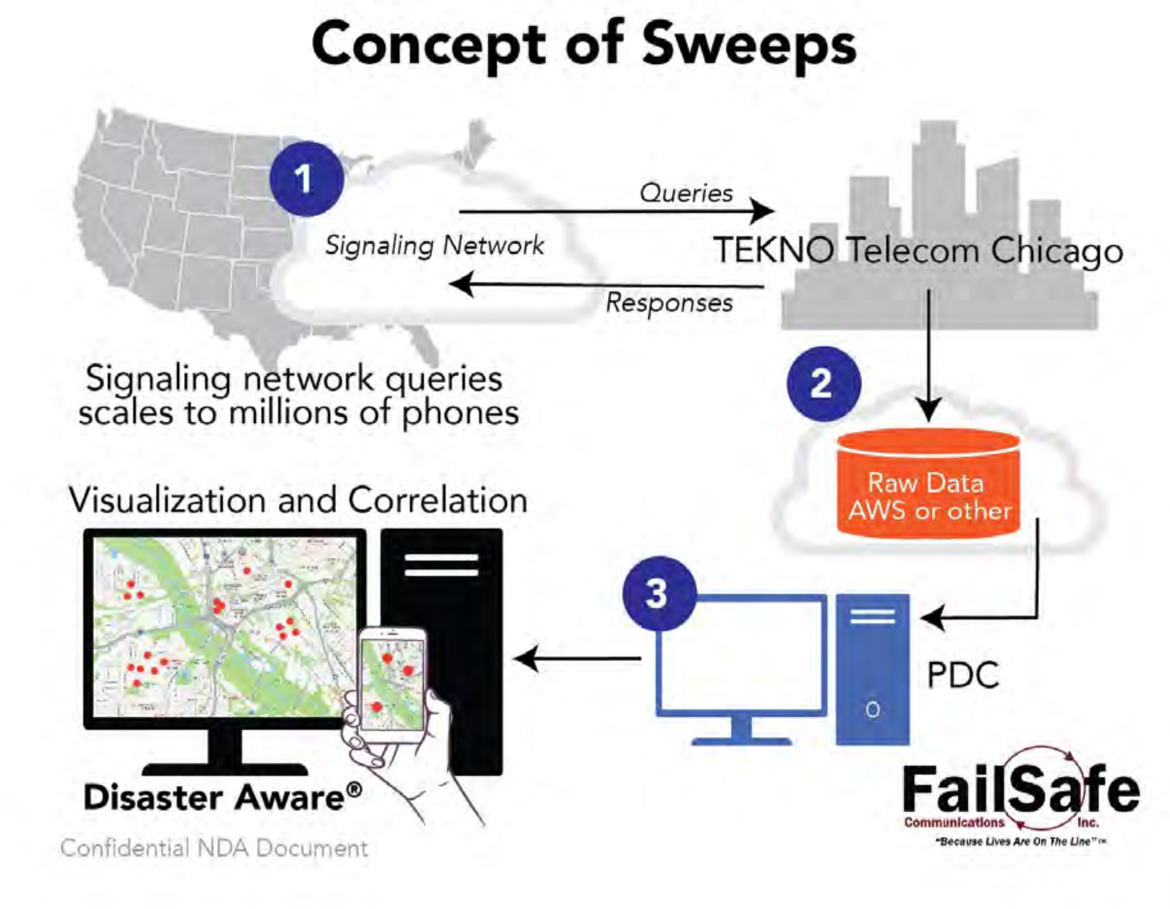
[20] **LIDB** is an acronym for Line Information Data Base, which is used in the U.S. and Canada by telephone companies to store and retrieve Caller ID records. Local phone switches, also known as Class 5 switches, use SS7 signaling to query LIDB databases and pass this information during call set up.

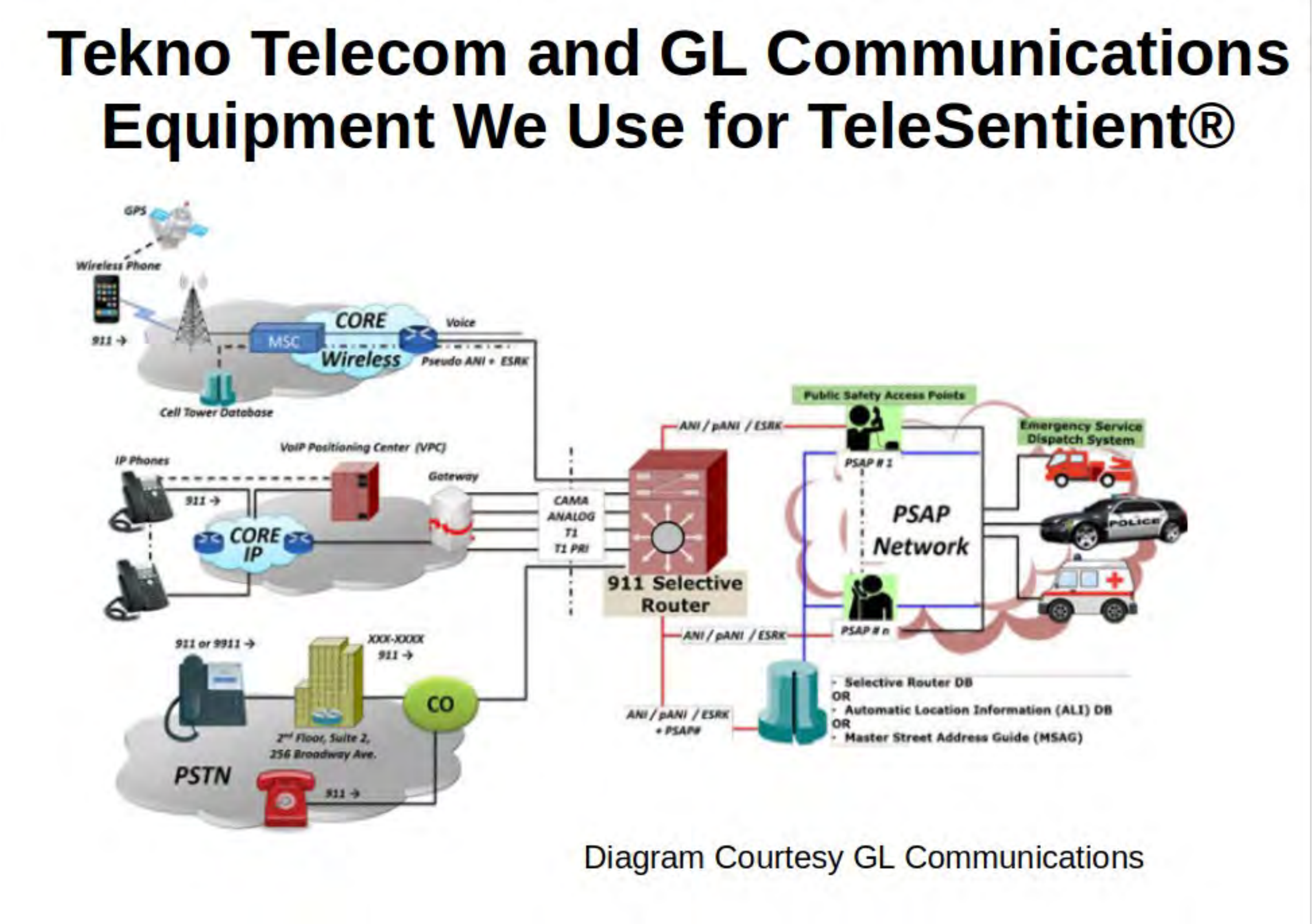
Application #2 – "Sweeps"

One technology by GL Communications is called Message Automation & Protocol Simulation, or (MAPS™). MAPS is a protocol simulation and conformance test tool that supports a variety of protocols such as SIP, MEGACO, MGCP, SS7, ISDN, GSM, MAP, CAS, LTE, UMTS, SS7 SIGTRAN, ISDN SIGTRAN, SIP I, GSM AoIP, Diameter and others. Along with automation capability, the application gives users the unlimited ability to edit messages and control scenarios. MAPS™ works on TDM, Ethernet and IP interfaces. TDM signaling protocols such as SS7, ISDN, MLPPP, CAS, MAP, CAP, GSM, INAP, and BICC operate over TDM networks, whereas VoIP protocols SIP, SIP-I, MEGACO, MGCP, SIGTRAN, Diameter, INAP, MAP, CAP, and BICC operate over IP networks.

MAPS™ also supports 3G & 4G mobile protocol standards for testing the rapidly evolving mobile technologies. MAPS™ can simulate radio signaling protocols such as LTE (S1, eGTP, X2) interfaces and UMTS (IuCS, IuPS, IuH), GPRG Gb and GSM A, GSM Abis over IP transport layer.

The diagrams that follow were taken from the website of GL Communications They illustrate a process for gleaning data from Intelligent Signaling Networks and converting it to useful metadata. We purchased some GL equipment as shown previously, but have no financial affiliation with them.


Concept of Sweeps
1
Signaling Network
Queries
Responses
TEKNO Telecom Chicago
Signaling network queries scales to millions of phones
2
Raw Data AWS or other
Visualization and Correlation
3
PDC
Disaster Aware®
Confidential NDA Document
FailSafe Communications Inc.
"Because Lives Are On The Line"™



Tekno Telecom and GL Communications Equipment We Use for TeleSentient®

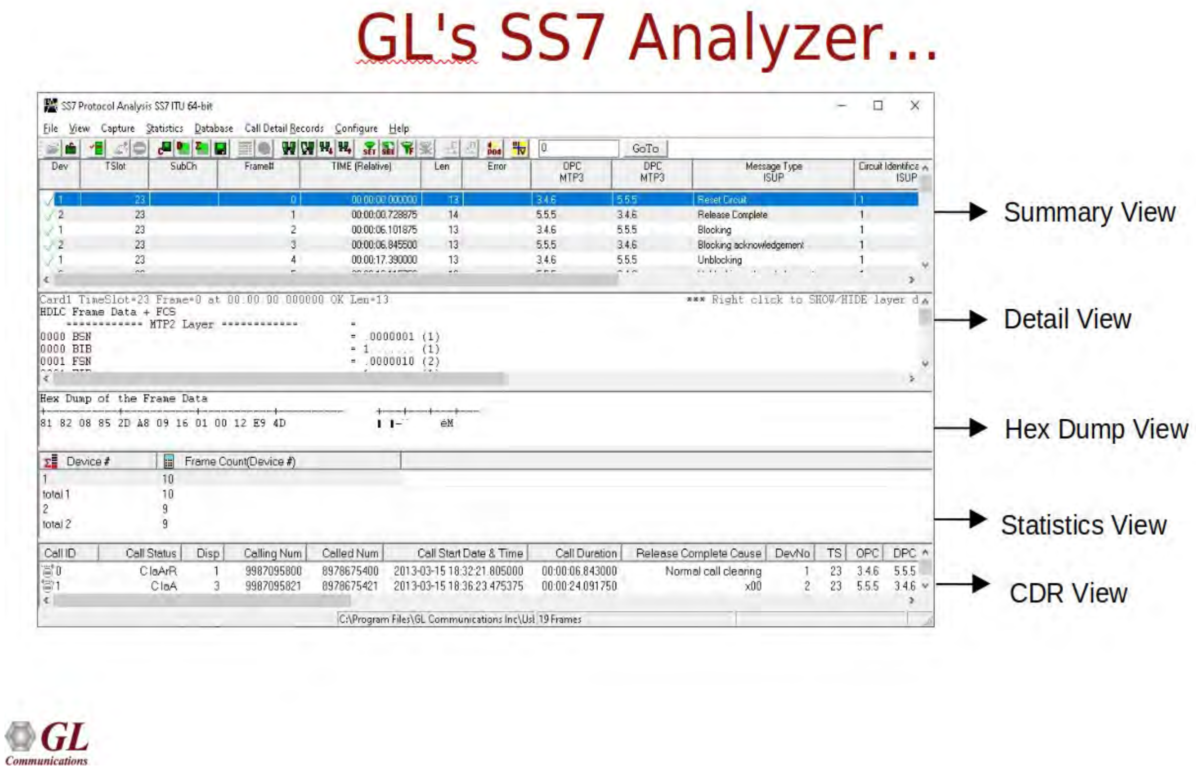
Diagram Courtesy GL Communications

GL has a good understanding of the 911 environment. Their diagram above shows a probe right where it ought to be in order to capture all 911 calls: The Selective Call Router adjacent to the LATA tandem.

FailSafe purchased GL equipment and is considering additional (MAPS^{TM}) equipment for its labs to conduct “Sweeps.” The cost of the GL equipment necessary to implement Sweeps on a nationwide basis starts at **$34,700**. That equipment can handle the first four of the 7 steps previously discussed. The remaining three are vendor and customer dependent.

- Define data needed
- Set up trigger
- Output filter and search based on triggers
- Save to a file
- Export file to cloud
- Define business rules
- Produce desired output

Initial Screen *(Step 1 and 2)*



GL's SS7 Analyzer...

SS7 Protocol Analysis SS7 ITU 64-bit

Dev	TSlot	SubCh	Frame#	TIME (Relative)	Len	Error	OPC MTP3	DPC MTP3	Message Type ISUP	Circuit Identifica ISUP
1	23		0	00:00:00.000000	13		3.4.6	5.5.5	Reset Circuit	1
2	23		1	00:00:00.728875	14		5.5.5	3.4.6	Release Complete	1
1	23		2	00:00:06.101875	13		3.4.6	5.5.5	Blocking	1
2	23		3	00:00:06.845500	13		5.5.5	3.4.6	Blocking acknowledgement	1
1	23		4	00:00:17.390000	13		3.4.6	5.5.5	Unblocking	1

```
Card1 TimeSlot=23 Frame=0 at 00:00:00.000000 OK Len=13                    *** Right click to SHOW/HIDE layer d
HDLC Frame Data + FCS
    ============ MTP2 Layer ============          =
0000 BSN                                          = .0000001 (1)
0000 BIB                                          = 1....... (1)
0001 FSN                                          = .0000010 (2)
```

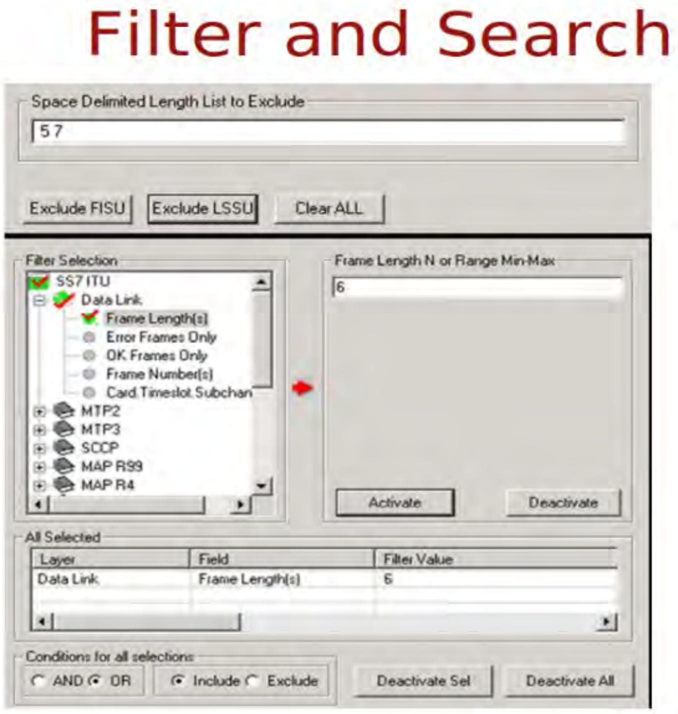
```
Hex Dump of the Frame Data
+-----------+-----------+-----------+-----------         +---+---+---+---
81 82 08 85 2D A8 09 16 01 00 12 E9 4D                   ▌ ▌-`    éM
```

Device #	Frame Count(Device #)
1	10
total 1	10
2	9
total 2	9

Call ID	Call Status	Disp	Calling Num	Called Num	Call Start Date & Time	Call Duration	Release Complete Cause	DevNo	TS	OPC	DPC
0	ClaArR	1	9987095800	8978675400	2013-03-15 18:32:21.805000	00:00:06.843000	Normal call clearing	1	23	3.4.6	5.5.5
1	ClaA	3	9987095821	8978675421	2013-03-15 18:36:23.475375	00:00:24.091750	x00	2	23	5.5.5	3.4.6

C:\Program Files\GL Communications Inc\Us| 19 Frames

Filter and Search *(Step 3)*



Filter and Search

Space Delimited Length List to Exclude: 5 7

Filter Selection

- ☑ SS7 ITU
  - ☑ Data Link
    - ☑ Frame Length(s)
    - Error Frames Only
    - OK Frames Only
    - Frame Number(s)
    - Card,Timeslot,Subchan
  - MTP2
  - MTP3
  - SCCP
  - MAP R99
  - MAP R4

Frame Length N or Range Min-Max: 6

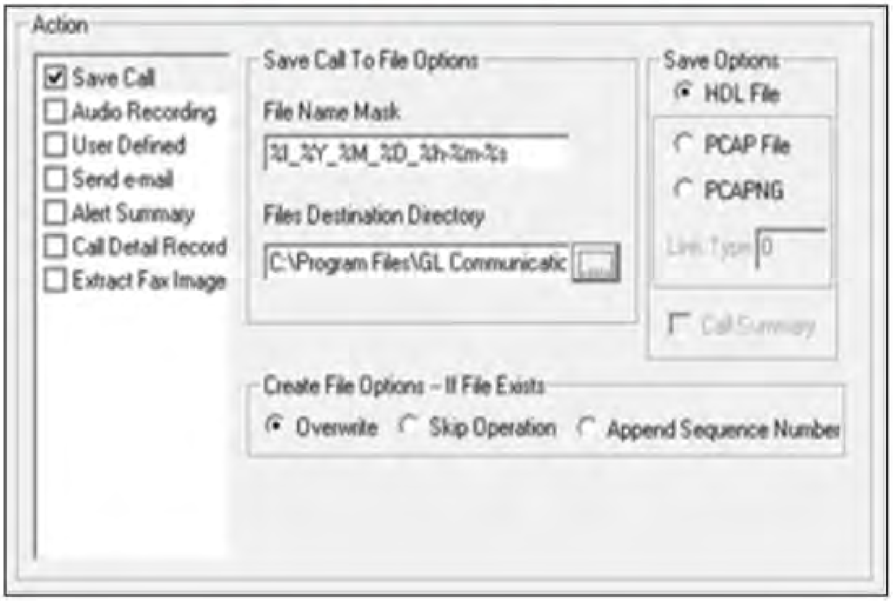
All Selected

Layer	Field	Filter Value
Data Link	Frame Length(s)	6

Conditions for all selections: ○ AND ● OR ● Include ○ Exclude

Step 4 – Save to a File

Save Call to File



Action

☑ Save Call
□ Audio Recording
□ User Defined
□ Send e-mail
□ Alert Summary
□ Call Detail Record
□ Extract Fax Image

Save Call To File Options

File Name Mask: %I_%Y_%M_%D_%h-%m-%s

Files Destination Directory: C:\Program Files\GL Communicatic

Save Options

● HDL File
○ PCAP File
○ PCAPNG

Link Type: 0

□ Call Summary

Create File Options – If File Exists

● Overwrite ○ Skip Operation ○ Append Sequence Number

Steps 5, 6 and 7 are Customer or Vendor Specified

- Export file to cloud
- Define business rules
- Produce desired output

The last three of the seven steps depend on the specific application, vendor selected, and desired product: (Alert, Visualization, Correlation, etc.)

Demonstration to the FCC

As discussed in our previous *ex-parte*, FailSafe subject matter experts had intended to demonstrate this technology in person to the FCC. We believe the detail in this Report negates the need for a demonstration. We stand ready however to meet in person or via a Zoom call to answer any specific questions about this technology. For your convenience in describing this Report internally, we have included a copy of the presentation slides as Attachment 2.

Summary, Conclusions and Next Steps

It is indisputable that the FCC has jurisdiction over the telephone numbering system in the United States. Past FCC rulings have allowed consumers to pick their toll free and long distance carriers, port phone numbers, and even keep their wireless phone number when they move to another state. If the undersigned were to use an axiom about the FCC over his 45 year career, it would have to be this one:

The number holder is the boss.

If something is *technically feasible* for carriers to do and clearly beneficial to the consumer, this Agency has not been bashful about implementing a new policy. When the issue has been important enough, like 911 or the 988 suicide hot line, the FCC has mandated that the carriers do it. This may be the case here, particularly since the cost is low to network providers and the benefits are many.

We envision starting with allowing any number holder to sign up. Whether it is an End User, a 911 center, a 988 center, or a telecom carrier, that entity should be allowed to add this option when it's technically feasible to do so, under the tried-and-true concept that the number holder is the boss.

Every great idea that the FCC has spawned over the last 40 years has had to start somewhere and with someone. Perhaps we are the latest catalyst for you. We are not bragging, but we are at the stage of our careers where we hope to leave a lasting legacy. That's why we patented our technology and made it available to anyone rather than rolling out "this product" or "that product" for ourselves.

We hope to sit back and watch while the industry licenses our technology and runs with some great future ideas like we describe in Exhibit C. Let us work together to implement technology that will save lives and provide added safety to all Americans.

Best regards,

Leo A. Wrobel
CEO of FailSafe Communications Inc.
Inventor of TeleSentient®
www.failsafecommunications.com
(214) 484-6805

Attachment 1

Detailed ISDN Cause Codes

Cause No. l - Unallocated (unassigned) number [Q.850]
This cause indicates that the called party cannot be reached recluses although the called party number is in a valid format. It is not currently allocated (assigned).

Cause No. 2 - No route to specified transit network (national use) [Q.850]
This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular transit network. While it does exist. does not serve the equipment which is sending this cause.

Cause No. 3 - No route to destination [Q.850]
This cause indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This cause is supported on a network dependent basis.

Cause No. 4 - send special information tone [Q.850]
This cause indicates that the called party cannot be reached for reasons that are of a long term nature and that the special information tone should be returned to the calling party.

Cause No. 5 - mis-dialed trunk prefix (national use) [Q.850]
This cause indicates the erroneous inclusion of a trunk prefix in the called party number. This number is to sniped from the dialed number being sent to the network by the customer premises equipment.

Cause No. 6 - channel unacceptable [Q.850]
This cause indicates that the channel most recently identified is not acceptable to the sending entity for use in this call.

Cause No. 7 - call awarded. being delivered in an established channel [Q.850]
This cause indicates that the user has been awarded the incoming call and that the incoming call is being connected to a channel already established to that user for similar calls (e.g. packet-mode x.25 virtual calls).

Cause No. 8 - preemption [Q.850]
This cause indicates the call is being preempted.

Cause No. 9 - preemption - circuit reserved for reuse [Q.850]
This cause indicates that the call is being preempted and the circuit is reserved for reuse by the preempting exchange.

Cause No. 10 - normal call clearing [Q.850]
This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared. Under normal situations, the source of this cause is not the network.

Cause No. 17 - user busy [Q.850]
This cause is used to indicate that the called party is unable to accept another call because the user busy condition has been encountered. This cause value may be generated by the called user or by the network. In the case of user determined user busy it is noted that the user equipment is compatible with the call.

Cause No. 18 - no user responding [Q.850]
This cause is used when a called party does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated.

Cause No. 19 - no answer from user (user alerted) [Q.850]
This cause is used when the called party has been alerted but does not respond with a connect indication within a prescribed period of time. Note - This cause is not necessarily generated by Q.931 procedures but may be generated by internal network timers.

Cause No. 20 - subscriber absent [Q.850]
This cause value is used when a mobile station has logged off. radio contact is not obtained with a mobile station or if a personal telecom user is temporarily not addressable at any user-network interface.

Cause No. 21 - call rejected [Q.850]
This cause indicates that the equipment sending this cause does not wish to accept this call. although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible. This cause may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection.

Cause No. 22 - number changed [Q.850]
This cause is returned to a calling party when the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this cause, cause no. 1, unallocated (unassigned) number shall be used.

Cause No. 26 - non-selected user clearing [Q.850]
This cause indicates that the user has not been awarded the incoming call.

Cause No. 27 - destination out of order [Q.850]
This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates that a signal message was unable to be delivered to the remote party; e.g., a physical layer or data link layer failure at the remote party or user equipment off-line.

Cause No. 28 - invalid number format (address incomplete) [Q.850]
This cause indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete.

Cause No. 29 - facilities rejected [Q.850]
Cause is returned when supplementary service requested by the user cannot be provided by the network.

Cause No. 30 - response to STATUS INQUIRY [Q.850]
This cause is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS INQUIRY.

Cause No. 31 - normal. unspecified [Q.850]
This cause is used to report a normal event only when no other cause in the normal class applies.

Cause No. 34 - no circuit/channel available [Q.850]
This cause indicates that there is no appropriate circuit/channel presently available to handle the call.

Cause No. 35 - Call Queued [Q.850]

Cause No. 38 - network out of order [Q.850]
This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time e.g., immediately re-attempting the call is not likely to be successful.

Cause No. 39 - permanent frame mode connection out-of-service [Q.850]
This cause is included in a STATUS message to indicate that a permanently established frame mode connection is out-of-service (e.g. due to equipment or section failure) (see Annex A/Q.933)

Cause No. 40 - permanent frame mode connection operational [Q.850]
This cause is included in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information. (see Annex A/Q.933]

Cause No. 41 - temporary failure [Q.850]
This cause indicates that the network is not functioning correctly and that the condition is no likely to last a long period of time; e.g., the user may wish to try another call attempt almost immediately.

Cause No. 42 - switching equipment congestion [Q.850]
This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

Cause No. 43 - access information discarded [Q.850]
This cause indicates that the network could not deliver access information to the remote user as requested. i.e., user-to-user information, low layer compatibility, high layer compatibility or sub-address as indicated in the diagnostic. It is noted that the particular type of access information discarded is optionally included in the diagnostic.

Cause No. 44 - requested circuit/channel not available [Q.850]
This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.

Cause No. 46 - precedence call blocked [Q.850]
This cause indicates that there are no predictable circuits or that the called user is busy with a call of equal or higher preventable level.

Cause No. 47 - resource unavailable, unspecified [Q.850]
This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.

Cause No. 49 - Quality of Service not available [Q.850]
This cause is used to report that the requested Quality of Service. as defined in Recommendation X.213. cannot be provided (e.g., throughput of transit delay cannot be supported).

Cause No. 50 - requested facility not subscribed [Q.850]
This cause indicates that the user has requested a supplementary service which is implemented by the equipment which generated this cause but the user is not authorized to use.

Cause No. 52 - outgoing calls barred

Cause No. 53 - outgoing calls barred within CUG [Q.850]
This cause indicates that although the calling party is a member of the CUG for the outgoing CUG call. Outgoing calls are not allowed for this member of the CUG.

Cause No. 54 - incoming calls barred

Cause No. 55 - incoming calls barred within CUG [Q.850]
This cause indicates that although the calling party is a member of the CUG for the incoming CUG call. Incoming calls are not allowed for this member of the CUG.

Cause No. 57 - bearer capability not authorized [Q.850]
This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but the user is not authorized to use.

Cause No. 58 - bearer capability not presently available [Q.850]
This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but which is not available at this time.

Cause No. 62 - inconsistency in outgoing information element. [Q.850]
This cause indicates an inconsistency in the designated outgoing access information and subscriber class

Cause No. 63 - service or option not available. unspecified [Q.850]
This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.

Cause No. 65 - bearer capability not implemented [Q.850]
This cause indicates that the equipment sending this cause does not support the bearer capability requested.

Cause No. 66 - channel type not implemented [Q.850]
This cause indicates that the equipment sending this cause does not support the channel type requested

Cause No. 69 - requested facility not implemented [Q.850]
This cause indicates that the equipment sending this cause does not support the requested supplementary services.

Cause No. 70 - only restricted digital information bearer capability is available (national use) [Q.850]
This cause indicates that the calling party has requested an unrestricted bearer service but the equipment sending this cause only supports the restricted version of the requested bearer capability.

Cause No. 79 - service or option not implemented unspecified [Q.850]
This cause is used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.

Cause No. 81 - invalid call reference value [Q.850]
This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.

Cause No. 82 - identified channel does not exist [Q.850]
This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example. if a user has subscribed to those channels on a primary rate interface numbered from l to 12 and the user equipment or the network attempts to use channels l 3 through 23, this cause is generated.

Cause No. 83 - a suspended call exists, but this call identify does not [Q.850]
This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).

Cause No. 84 - call identity in use [Q.850]
This cause indicates that the network has received a call suspended request containing a call identity (including the null call identity) which is already in use for a suspended call within the domain of interfaces over which the call might be resumed.

Cause No. 85 - no call suspended [Q.850]
This cause indicates that the network has received a call resume request containing a Call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.

Cause No. 86 - call having the requested call identity has been cleared [Q.850]
This cause indicates that the network has received a call resume request containing a Call identity information element indicating a suspended call that has in the meantime been cleared while suspended (either by network time-out or by the remote user).

Cause No. 87 - user not a member of CUG [Q.850]
This cause indicates that the called user for the incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber calling a CUG subscriber.

Cause No. 88 - incompatible destination [Q.850]
This cause indicates that the equipment sending this cause has received a request to establish a call which has low layer compatibility. high layer compatibility or other compatibility attributes (e.g., data rate) which cannot be accommodated.

Cause No. 90 - non-existent CUG [Q.850]
This cause indicates that the specified CUG does not exist.

Cause No. 91 - invalid transit network selection (national use) [Q.850]
This cause indicates that a transit network identification was received which is of an incorrect format as defined in Annex C/Q.931

Cause No. 95 - invalid message, unspecified [Q.850]
This cause is used to report an invalid message event only when no other cause in the invalid message class applies.

Cause No. 96 - mandatory information element is missing [Q.850]
This cause indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message before that message can be processed.

Cause No. 97 - message type non-existent or not implemented [Q.850]
This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined of defined but not implemented by the equipment sending this cause.

Cause No. 98 - message not compatible with call state or message type non-existent or not implemented. [Q.850]
This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state. or a STATUS message was received indicating an incompatible call state.

Cause No. 99 - Information element / parameter non-existent or not implemented [Q.850]
This cause indicates that the equipment sending this cause has received a message which includes information element(s)/parameter(s) not recognized because the information element(s)/parameter name(s) are not defined or are defined but not implemented by the equipment sending the cause. This cause indicates that the information element(s)/parameter(s) were discarded. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

Cause No. 100 - Invalid information element contents [Q.850]
This cause indicates that the equipment sending this cause has received and information element which it has implemented; however, one or more Gelds in the I.E. are coded in such a way which has not been implemented by the equipment sending this cause.

Cause No. 101 - message not compatible with call state [Q.850]
This cause indicates that a message has been received which is incompatible with the call state.

Cause No. 102 - recovery on timer expiry [Q.850]
This cause indicates that a procedure has been initiated by the expiration of a timer in association with error handling procedures.

Cause No. 103 - parameter non-existent or not implemented - passed on (national use) [Q.850]
This cause indicates that the equipment sending this cause has received a message which includes parameters not recognized because the parameters are not defined or are defined but not implemented by the equipment sending this cause. The cause indicates that the parameter(s) were ignored. In addition, if the equipment sending this cause is an intermediate point, then this cause indicates that the parameter(s) were passed unchanged.

Cause No. 110 - message with unrecognized parameter discarded [Q.850]
This cause indicates that the equipment sending this cause has discarded a received message which includes a parameter that is not recognized.

Cause No. 111 - protocol error, unspecified [Q.850]
This cause is used to report a protocol error event only when no other cause in the protocol error class applies.

Cause No. 127 - Intel-working, unspecified [Q.850]
This cause indicates that an interworking call (usually a call to 5W56 service) has ended.

Notes about Cause Codes over 128
Cause code values of 128 and higher aren't sent over the network. and aren't defined in Rec. [Q.850].

Attachment 2

FailSafe Communications Inc.

Using Intelligent Signaling Networks for 911 Alerts

A Demonstration to the
Federal Communications Commission
by Leo A. Wrobel, Inventor of TeleSentient®
and others.

Presenters

Leo A. Wrobel

CEO and Chairman of the Board

Eddie M. Pope

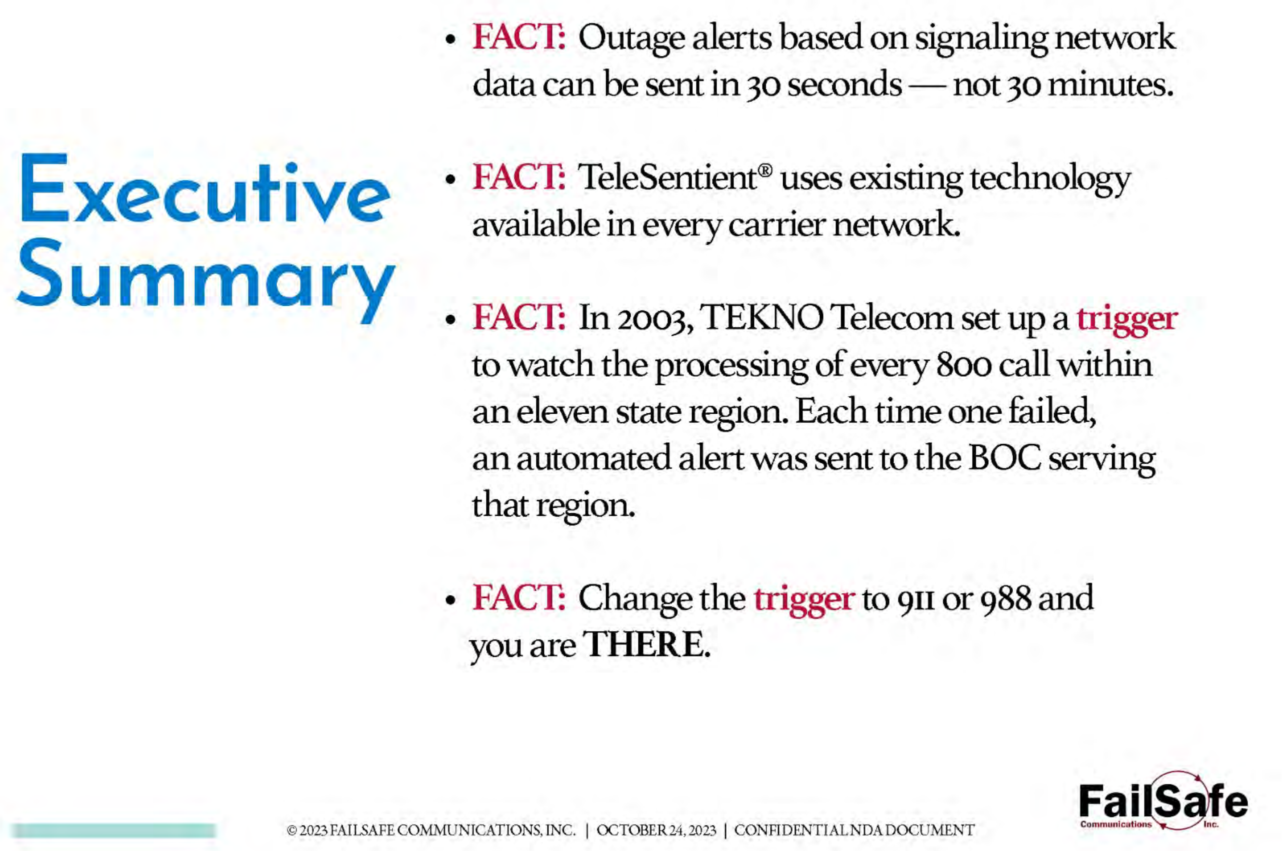
General Counsel

Philip N. Diehl

Board Member

Sam Galler

Advisor to the Board



Executive Summary

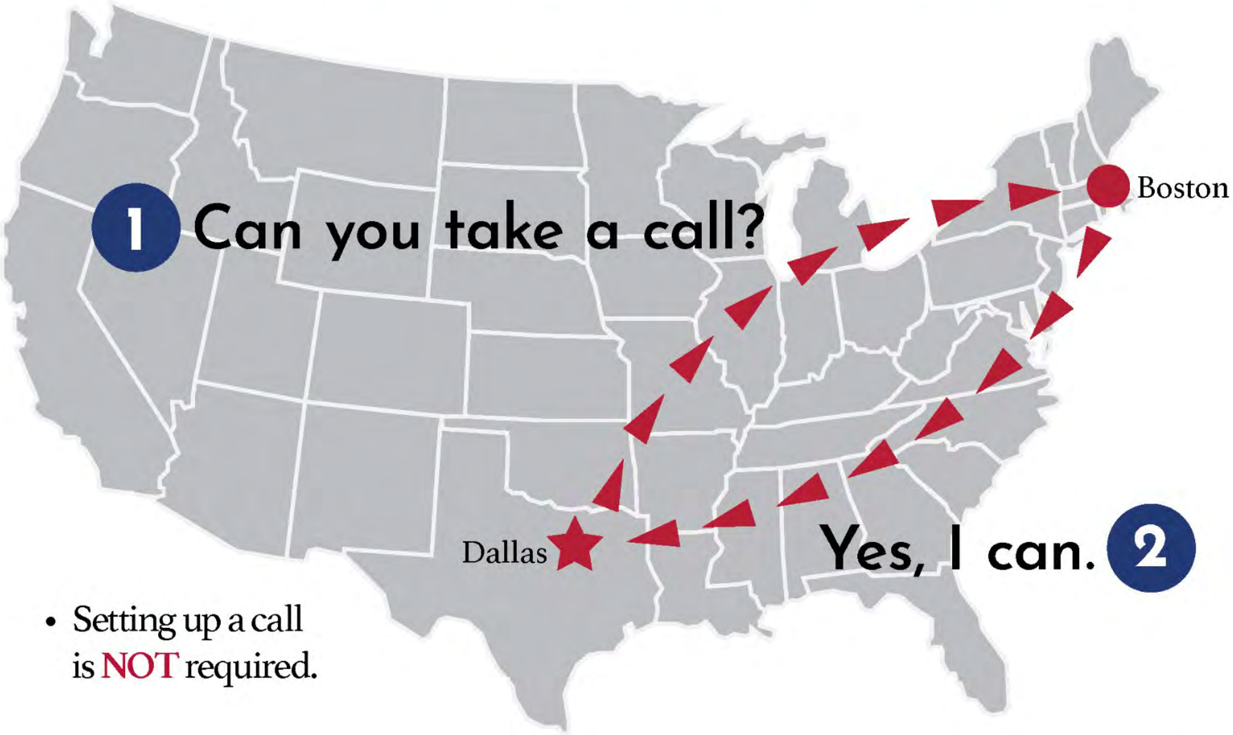
- **FACT:** Outage alerts based on signaling network data can be sent in 30 seconds — not 30 minutes.

- **FACT:** TeleSentient® uses existing technology available in every carrier network.

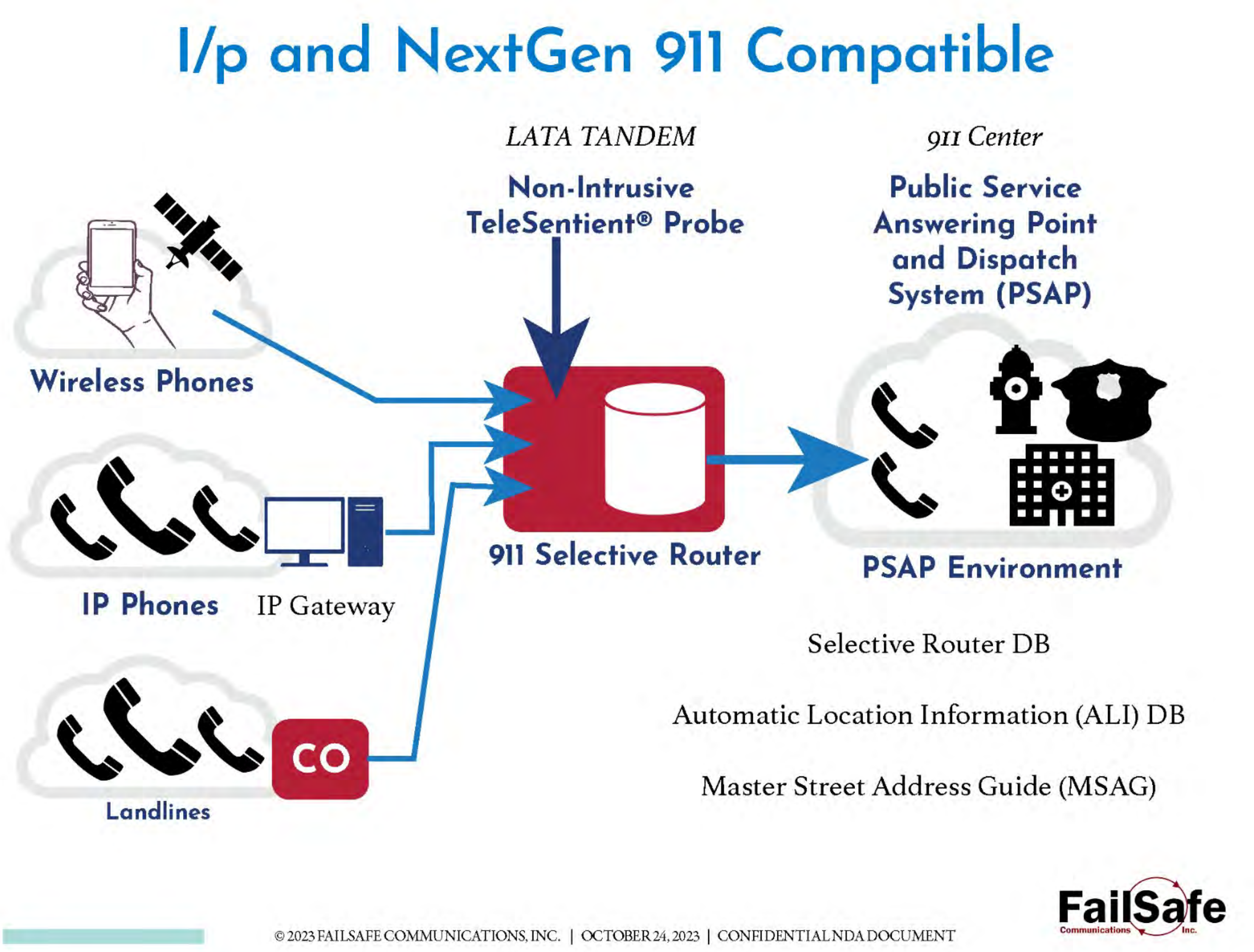
- **FACT:** In 2003, TEKNO Telecom set up a **trigger** to watch the processing of every 800 call within an eleven state region. Each time one failed, an automated alert was sent to the BOC serving that region.

- **FACT:** Change the **trigger** to 911 or 988 and you are **THERE.**

Intelligent Signaling Networks



- Setting up a call is NOT required.



I/p and NextGen 911 Compatible

LATA TANDEM

Non-Intrusive TeleSentient® Probe

911 Center

Public Service Answering Point and Dispatch System (PSAP)

Wireless Phones

IP Phones

IP Gateway

Landlines

CO

911 Selective Router

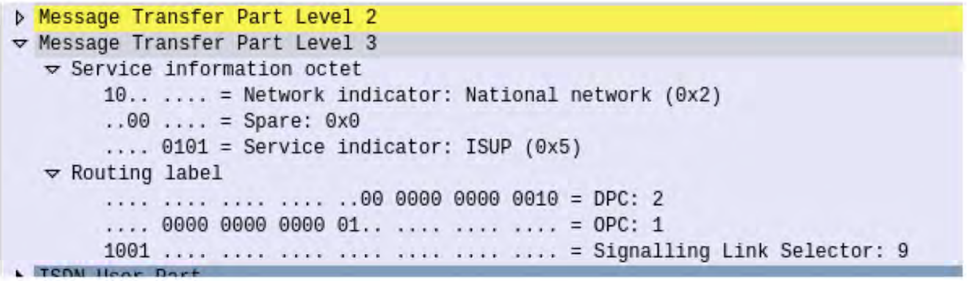
PSAP Environment

Selective Router DB

Automatic Location Information (ALI) DB

Master Street Address Guide (MSAG)

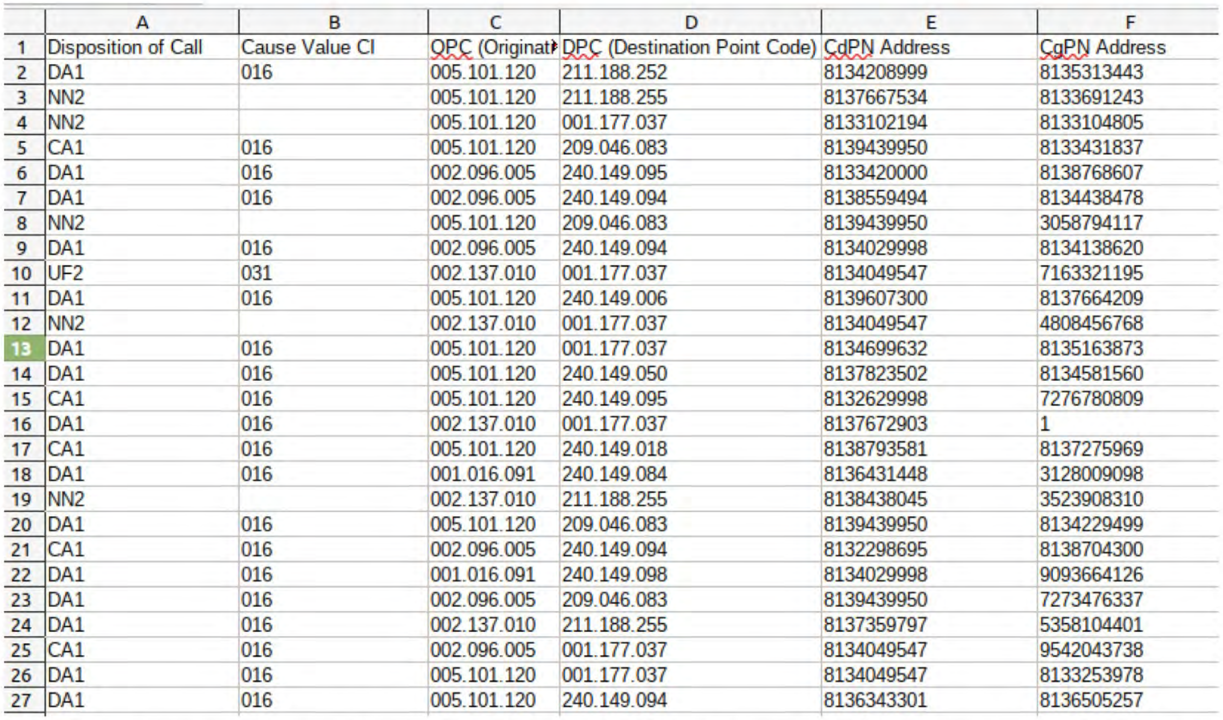
Intelligent Networks Use "Point Codes"



```
▷ Message Transfer Part Level 2
▽ Message Transfer Part Level 3
  ▽ Service information octet
        10.. .... = Network indicator: National network (0x2)
        ..00 .... = Spare: 0x0
        .... 0101 = Service indicator: ISUP (0x5)
  ▽ Routing label
        .... .... .... .... ..00 0000 0000 0010 = DPC: 2
        .... 0000 0000 0000 01.. .... .... .... = OPC: 1
        1001 .... .... .... .... .... .... .... = Signalling Link Selector: 9
▸ ISDN User Part
```

- A **Point Code** is the unique address of a SS7 Network element.
- **Point Codes** are like I/p Addresses.
- Every message sent over an SS7 network will contain an Origin **Point Code** that identifies the sender, and a Destination **Point Code** that identifies the intended recipient.

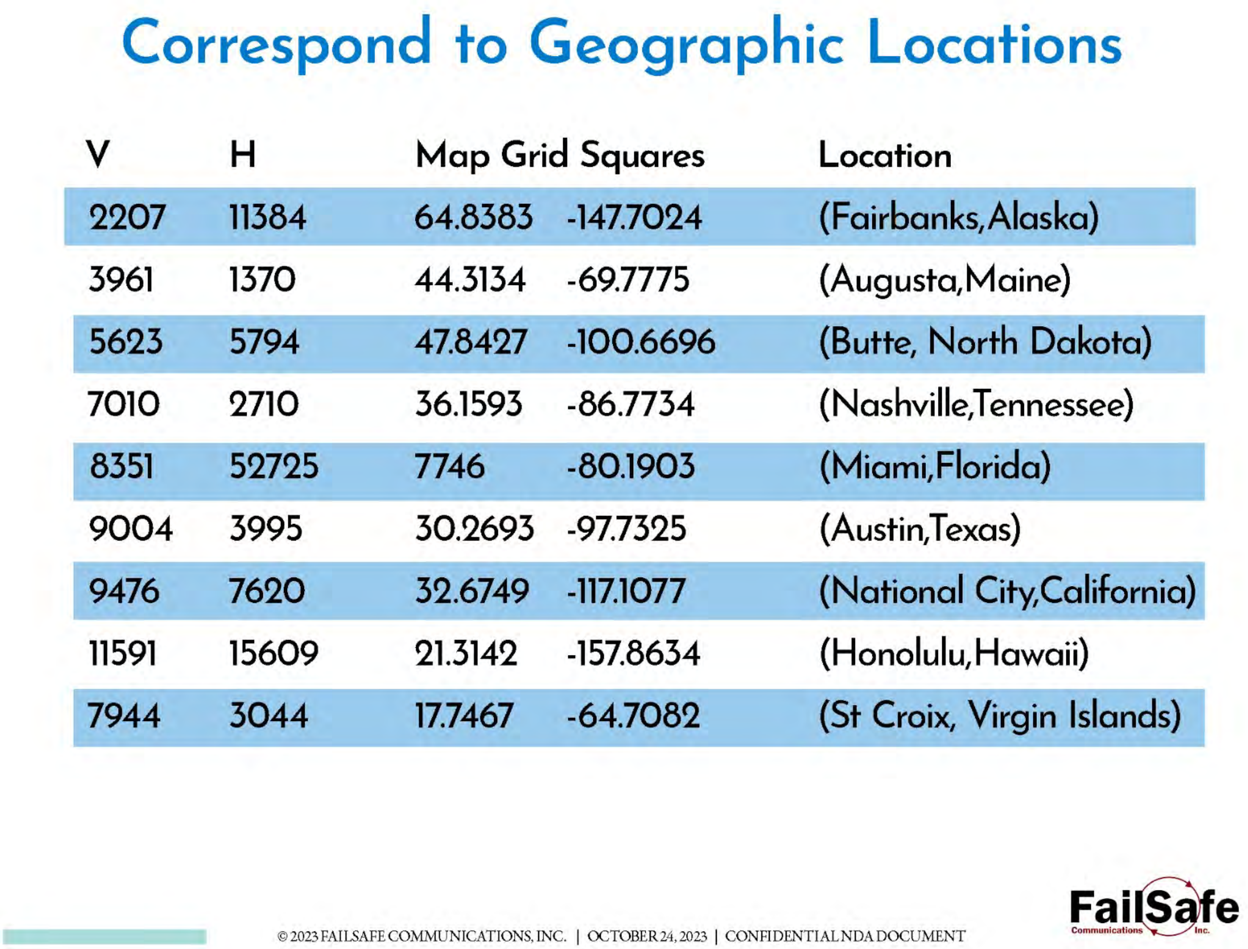
Point Codes Provide Called & Calling Numbers



	A	B	C	D	E	F
1	Disposition of Call	Cause Value CI	OPC (Originat	DPC (Destination Point Code)	CdPN Address	CgPN Address
2	DA1	016	005.101.120	211.188.252	8134208999	8135313443
3	NN2		005.101.120	211.188.255	8137667534	8133691243
4	NN2		005.101.120	001.177.037	8133102194	8133104805
5	CA1	016	005.101.120	209.046.083	8139439950	8133431837
6	DA1	016	002.096.005	240.149.095	8133420000	8138768607
7	DA1	016	002.096.005	240.149.094	8138559494	8134438478
8	NN2		005.101.120	209.046.083	8139439950	3058794117
9	DA1	016	002.096.005	240.149.094	8134029998	8134138620
10	UF2	031	002.137.010	001.177.037	8134049547	7163321195
11	DA1	016	005.101.120	240.149.006	8139607300	8137664209
12	NN2		002.137.010	001.177.037	8134049547	4808456768
13	DA1	016	005.101.120	001.177.037	8134699632	8135163873
14	DA1	016	005.101.120	240.149.050	8137823502	8134581560
15	CA1	016	005.101.120	240.149.095	8132629998	7276780809
16	DA1	016	002.137.010	001.177.037	8137672903	1
17	CA1	016	005.101.120	240.149.018	8138793581	8137275969
18	DA1	016	001.016.091	240.149.084	8136431448	3128009098
19	NN2		002.137.010	211.188.255	8138438045	3523908310
20	DA1	016	005.101.120	209.046.083	8139439950	8134229499
21	CA1	016	002.096.005	240.149.094	8132298695	8138704300
22	DA1	016	001.016.091	240.149.098	8134029998	9093664126
23	DA1	016	002.096.005	209.046.083	8139439950	7273476337
24	DA1	016	002.137.010	211.188.255	8137359797	5358104401
25	CA1	016	002.096.005	001.177.037	8134049547	9542043738
26	DA1	016	005.101.120	001.177.037	8134049547	8133253978
27	DA1	016	005.101.120	240.149.094	8136343301	8136505257

NOTE: This file was produced the day before Hurricane Ian hit Florida. We asked our folks to query the 813 area code - corresponding to Tampa, Fla.

FailSafe Communications Inc.

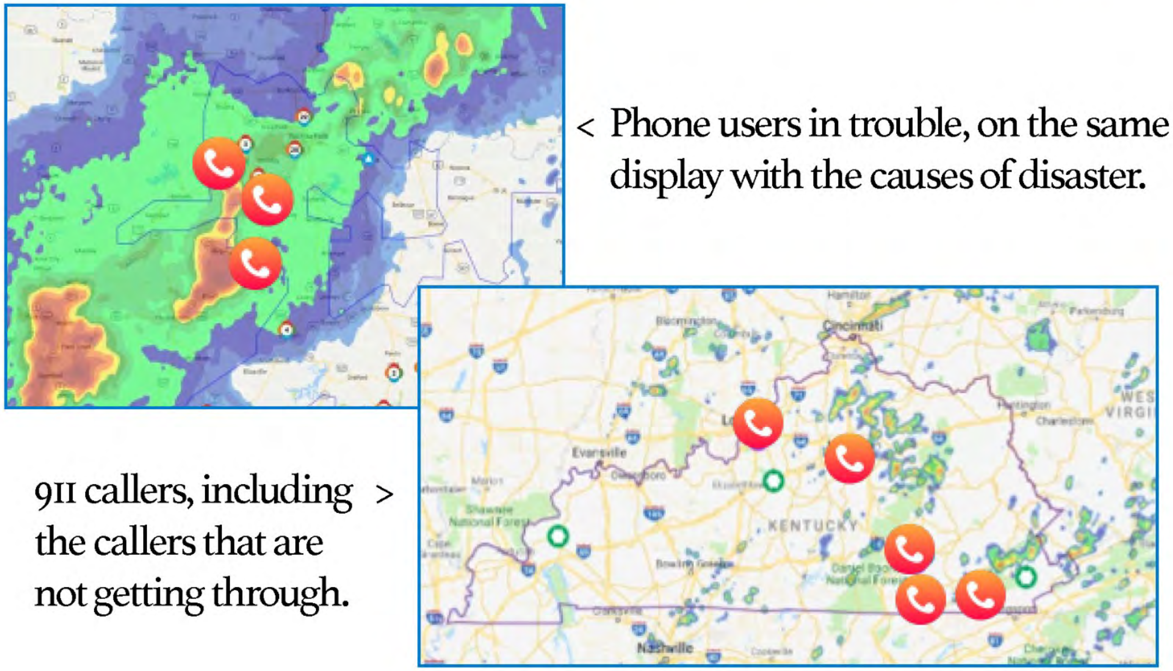


Correspond to Geographic Locations

V	H	Map Grid Squares		Location
2207	11384	64.8383	-147.7024	(Fairbanks,Alaska)
3961	1370	44.3134	-69.7775	(Augusta,Maine)
5623	5794	47.8427	-100.6696	(Butte, North Dakota)
7010	2710	36.1593	-86.7734	(Nashville,Tennessee)
8351	52725	7746	-80.1903	(Miami,Florida)
9004	3995	30.2693	-97.7325	(Austin,Texas)
9476	7620	32.6749	-117.1077	(National City,California)
11591	15609	21.3142	-157.8634	(Honolulu,Hawaii)
7944	3044	17.7467	-64.7082	(St Croix, Virgin Islands)

And Voilà!

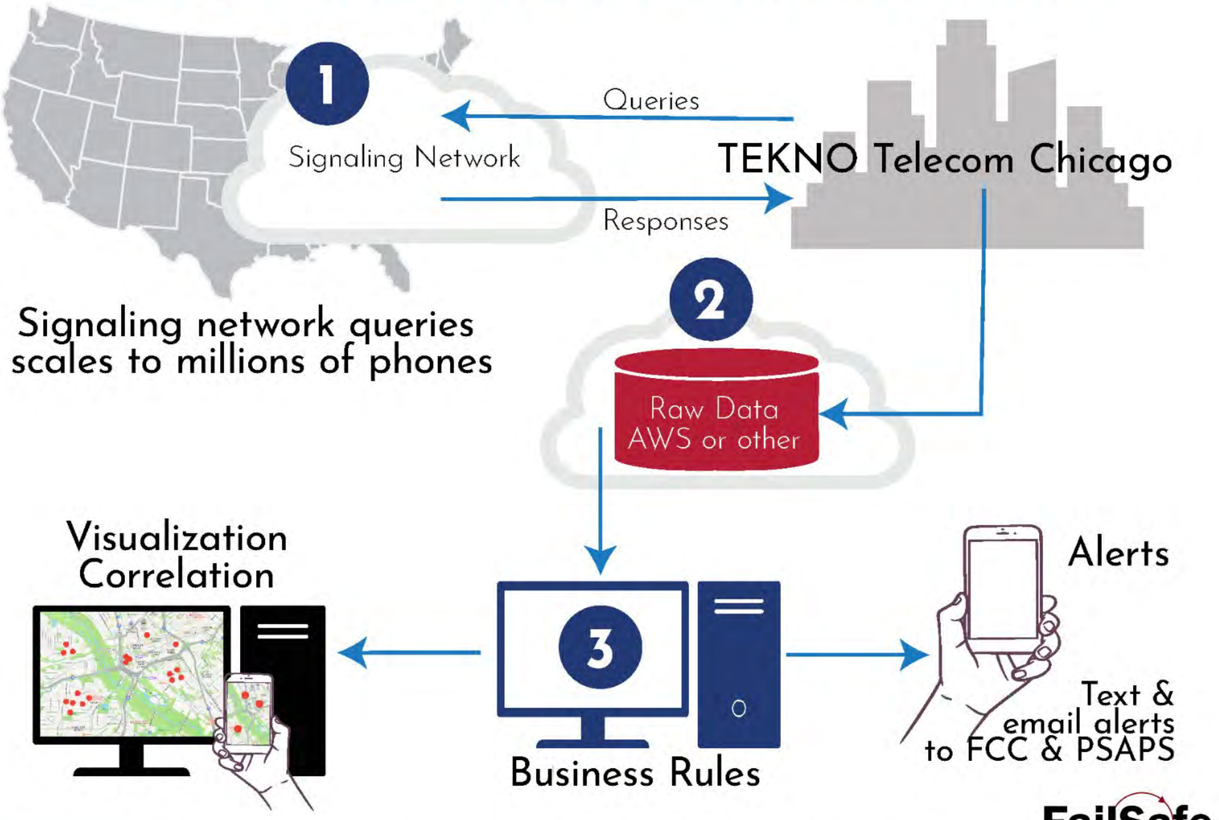
Users are Correlated with the Cause of Trouble and/or Outage



< Phone users in trouble, on the same display with the causes of disaster.

911 callers, including the callers that are not getting through. >

Using "Intelligent Networks" for Alerts



1

Signaling Network

Queries

Responses

TEKNO Telecom Chicago

Signaling network queries scales to millions of phones

2

Raw Data AWS or other

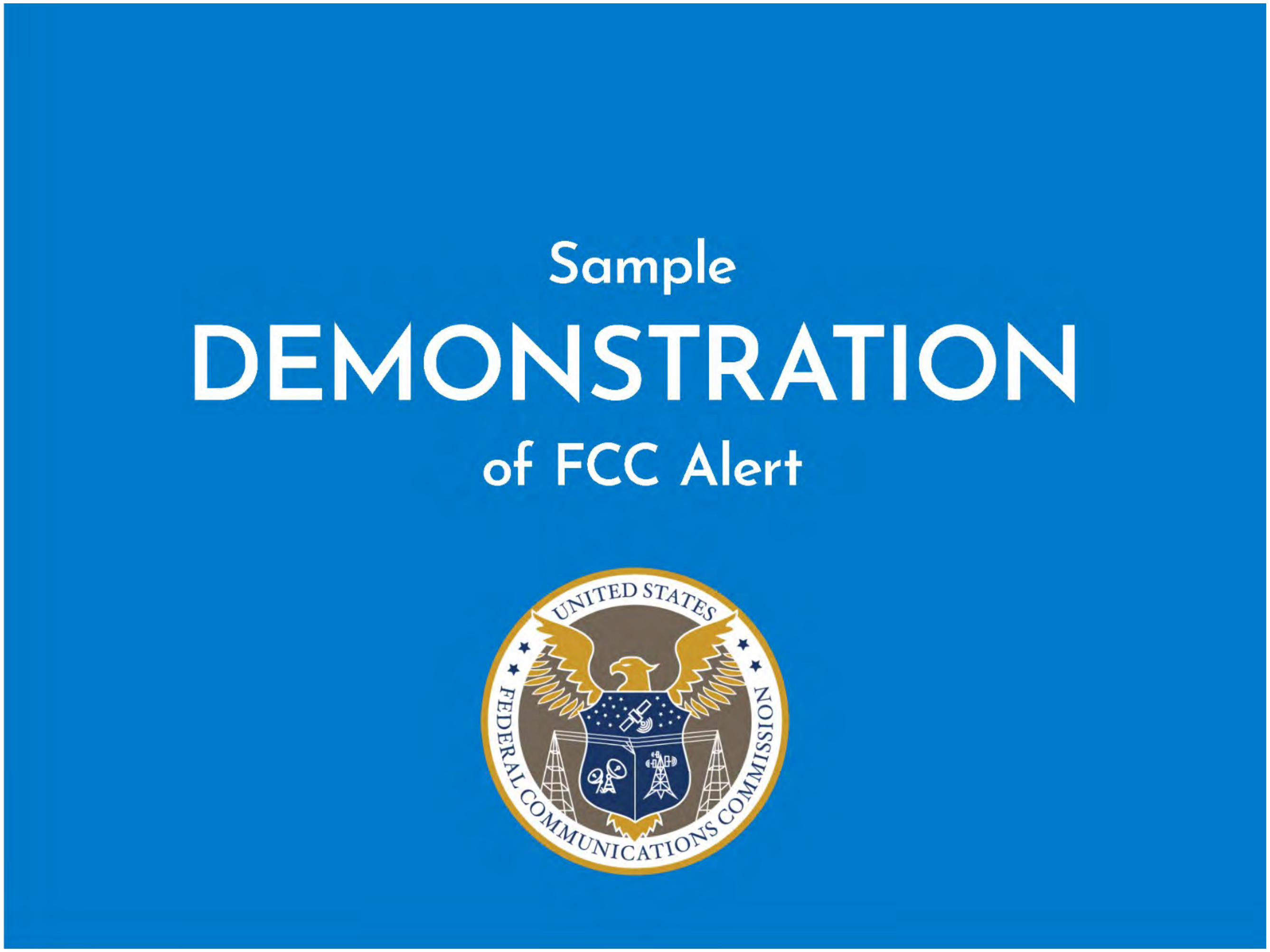
Visualization Correlation

3

Business Rules

Alerts

Text & email alerts to FCC & PSAPS



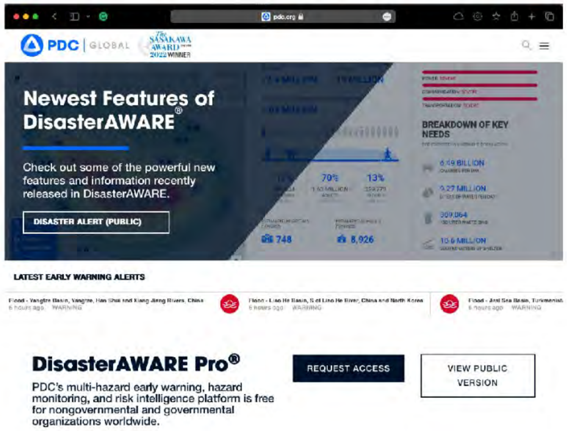
Sample

DEMONSTRATION

of FCC Alert

UNITED STATES
FEDERAL COMMUNICATIONS COMMISSION

The Pacific Disaster Center & DisasterAWARE®



Newest Features of DisasterAWARE®

Check out some of the powerful new features and information recently released in DisasterAWARE.

LATEST EARLY WARNING ALERTS

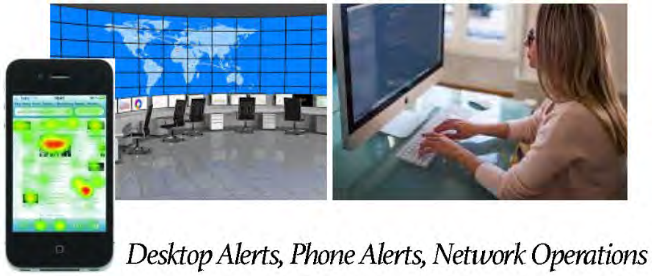
Flood - Yangtze Basin, Yangtze, Han Shui and Xiang Jiang Rivers, China
6 hours ago WARNING

Flood - Liao He Basin, S of Liao He River, China and North Korea
6 hours ago WARNING

Flood - Aral Sea Basin, Turkmenistan
6 hours ago WARNING

DisasterAWARE Pro®

PDC's multi-hazard early warning, hazard monitoring, and risk intelligence platform is free for nongovernmental and governmental organizations worldwide.

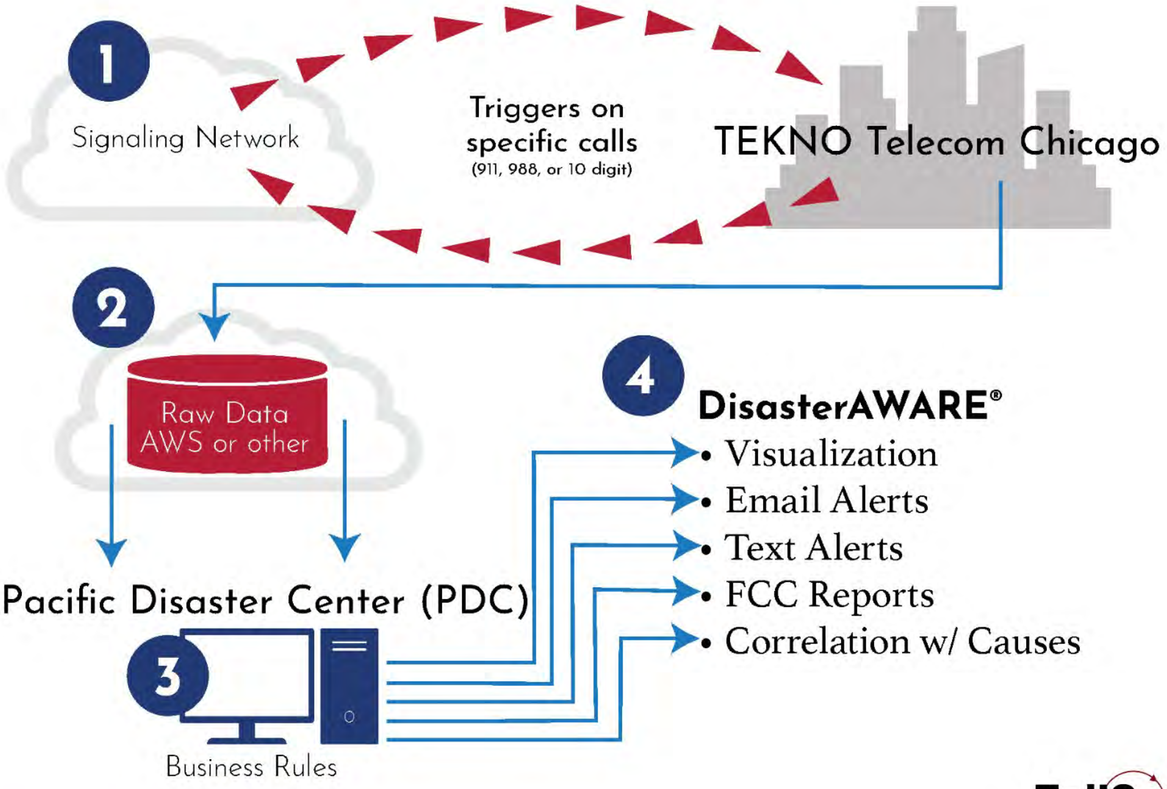


Desktop Alerts, Phone Alerts, Network Operations Center Alerts

- A $50 Million Federally Funded system that is already paid for.
- Proven compatibility with TeleSentient®.
- Scales nationwide.
- A DisasterAWARE® demonstration is forthcoming.
- www.pdc.org

FailSafe Communications Inc.

Scaling Nationwide



1 Signaling Network

Triggers on specific calls (911, 988, or 10 digit)

TEKNO Telecom Chicago

2 Raw Data AWS or other

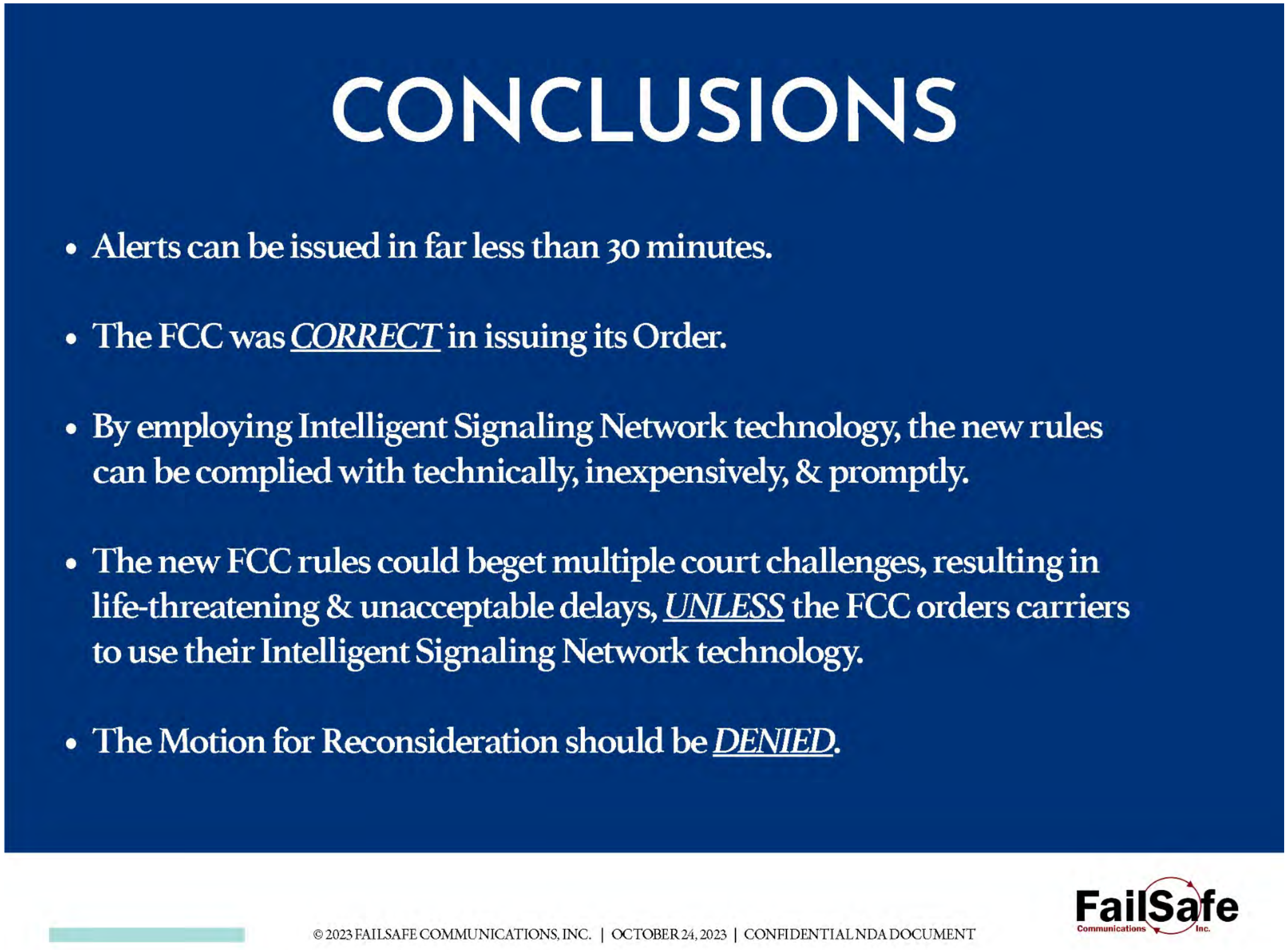
Pacific Disaster Center (PDC)

3 Business Rules

4 DisasterAWARE®

- Visualization
- Email Alerts
- Text Alerts
- FCC Reports
- Correlation w/ Causes

FailSafe Communications Inc.



CONCLUSIONS

- Alerts can be issued in far less than 30 minutes.
- The FCC was *CORRECT* in issuing its Order.
- By employing Intelligent Signaling Network technology, the new rules can be complied with technically, inexpensively, & promptly.
- The new FCC rules could beget multiple court challenges, resulting in life-threatening & unacceptable delays, *UNLESS* the FCC orders carriers to use their Intelligent Signaling Network technology.
- The Motion for Reconsideration should be *DENIED*.

FailSafe Communications Inc.
"Because Lives Are On The Line"™

Exhibit "C"

TELESENTIENT®

An Open Letter to the Industry

by

Leo A. Wrobel, CEO and Inventor

United States Patents 10,812,663, 11,582,352 and 6,748,051

Dear Colleagues,

The purpose of this letter is to encourage the industry to move beyond its current squabblers and to concentrate on its common goals, chiefly, to foster a safer America through financially prosperous organizations. It presents forward looking discussion points about things that could be developed and sold once the practice of mining Intelligent Switching Network data becomes commonplace. As part of the broad view of why we believe that the industry will embrace these ideas, we invite you to take a quick look at the opportunities that have come and gone in the telecom industry:

- Switched access used to be 50% of the revenue of a typical local phone company. Access charges are now gone. Some carriers still cling to switched tandem fees, and fight one another over fractions of a cent per minute, but clearly the bloom is off of this rose.
- Database services for 8XX and LNP are capped at fractions of a cent per minute. Like access and tandem charges, they are also in a price race toward zero.
- Another money maker for landline providers used to be the End User Common Line Charge (EUCL). The trouble is that only 25% of all telecom users have landlines today.
- Other than resale, the wireless industry offers limited opportunity to smaller players. We are not bashing AT&T, Verizon or T-Mobile, but has wireless become a zero-sum-gain? Can T-Mobile gain market share only by stealing a Verizon customer or vice versa?

At the same time, the Disaster Recovery as a Service (DRaaS) Market is expected to grow from around $10 billion this year to $26.5 billion by 2028, at a combined annual growth rate of 19.8%.[1] Set in this context, consider some other facts:

- 75 million baby boomers all getting old at the same time.
- New immigrants, many of whom live in some pretty rough neighborhoods.
- The threat of terrorism hitting us right here at home.
- Weather-related disasters are on the rise. Even Climate Change skeptics will admit that there are more people, living at greater population densities, in areas of high risk.

All of this means that the need for 911 has never been greater. At the same time though, because of these facts, the strain on 911 has never been greater either. The telecom industry has a new revenue opportunity sitting right under its nose and doesn't realize it. This is why we patented our technology and made it available to anyone rather than rolling out "this product" or "that product" ourselves. With this in mind, we invite industry and regulatory comments as part of this discussion.

[1] Market and Markets https://www.marketsandmarkets.com/Market-Reports/recovery-as-a-service-market-962.html

Our Purpose and Your Expectations Regarding This Letter

In the previous Exhibit B we showed how network providers may have everything they need on hand already to exploit a lucrative, multi-billion dollar DRaaS market. We did not discuss as much how to pay for such an effort, how to charge for such services, or how a network provider can even get started. We present some ideas here based on things network service providers already have and already do.

If you have not already done so, you may find it helpful to watch a quick 3-minute video below which describes the opportunity to network providers with a broad brush before we get into specifics.

How To Deploy and How to Fund

In this Letter we demonstrate the practical side of how an organization, large or small, can package and market these essential emergency services. There are three ways this can happen, and we discuss them all in this Letter:

- **End User Funding**
- **Industry Funding**
- **Government Funding**

Since there is no one-size-fits-all solution that covers End Users, Industry and Government, we address the pricing and deployment of a number of embodiments of this technology one at a time.

End User, Industry, and Government Options

As industry participants we worry a lot about new costs imposed by new regulations. For just a moment, let's consider a few alternatives to create new revenue that can offset those costs. The first embodiment to consider addresses a nightmare scenario for just about anyone,

"What happens when you call 911 and cannot get through?"

We present the reasons why we believe that your organization can do this, and how it can be financially successful addressing this need. One option is through End User Funding.

End User Funding

Would the public pay for an enhanced 911 service? Decide for yourself. Here is a 60 Second Video for a fictitious product called My911.plus. We *do not* offer a product called My911.plus. The video is intended only to illustrate one way that a third party might turn this technology into a profit center.

Turn on Channel 33 tonight after 11 PM. You will see a lot of commercials for VegaMatics and Ginsu knives. If someone ran a commercial for My911.plus would people pay a few cents a month to assure an overwhelmed 911 center would know they are in trouble? [2]

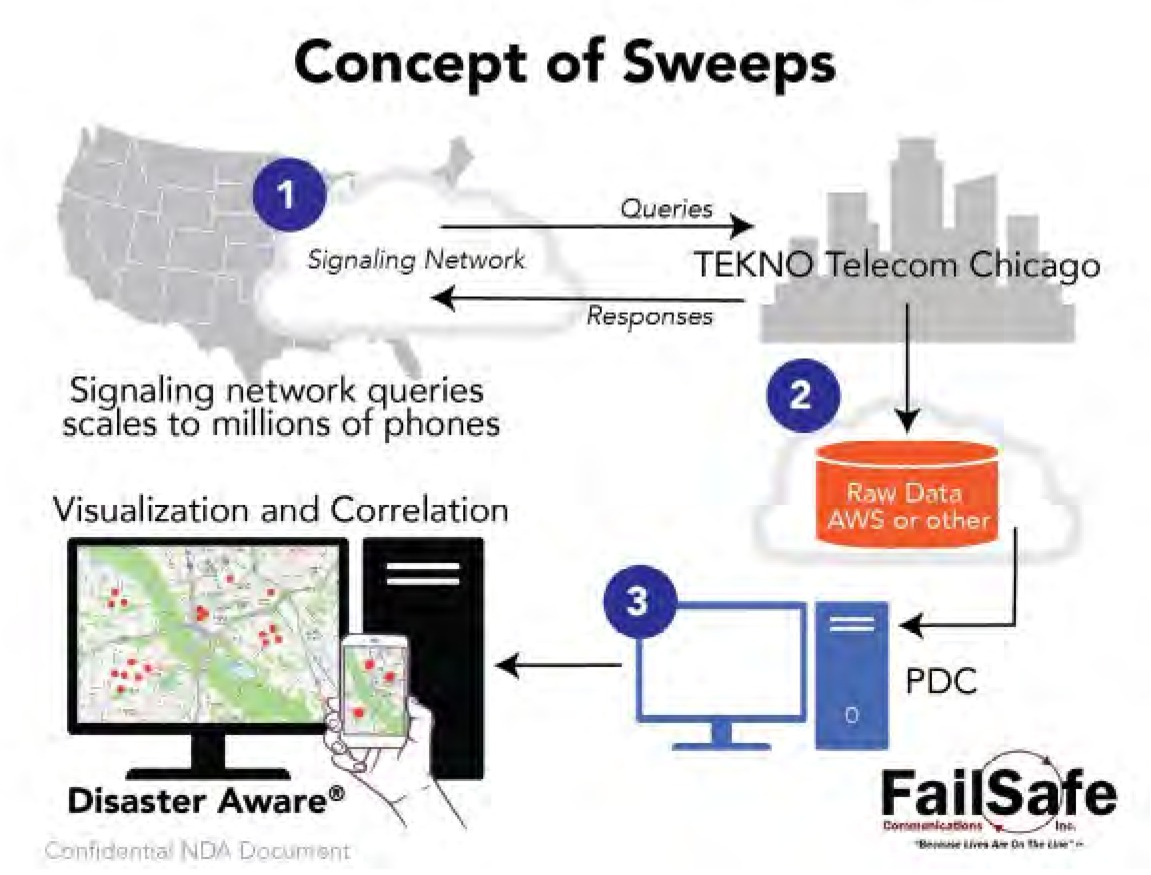
[2] Could a network provider offer this service without having to add staff? We think so. Through the Intelligent Signaling Network you already have the customer's number and location. Your IVR prompts them to dial 1 to sign up or hang up. When they dial 1 the service is added to their bill automatically.

Industry Funding

A second option might be from Industry. Would Disaster Recovery as a Service (DRaaS) providers like Everbridge, Intrado, OnSolve Rapid SOS, or other companies like to know where every disaster in the U.S. is – in real time? We believe they would. It would certainly help with their sales effort to know all the companies experiencing pain today. It's also a revenue opportunity for network service providers. Perhaps Sweeps are the answer. Sweeps are not alerts, but use similar equipment.

Sweeps

Sweeps generate a request to make a call, just as if the same end user above were dialing that call. A Sweep transfers SS7 signaling information the same way as well. It does NOT, however, extend the voice connection. Using the Intelligent Signaling Network only, TeleSentient® can determine the status of users (in service, out of service, busy, etc) unobtrusively.

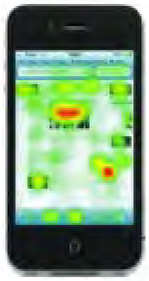

Concept of Sweeps
1
Signaling Network
Queries
Responses
TEKNO Telecom Chicago
Signaling network queries scales to millions of phones
2
Raw Data AWS or other
Visualization and Correlation
3
PDC
Disaster Aware®
Confidential NDA Document
FailSafe Communications Inc.
"Because Lives Are On The Line"™

Visualization of Sweep Data

Regulators have hypothesized that it would be useful to have data that could be easily displayed in 911 and 988 call centers on screens. When millions of Sweeps with their results are combined and displayed, a complete picture of conditions over a broad geographic area can be produced as well as updated every few minutes. Again, it is important to note that only the Intelligent Signaling Network data path is utilized. No voice call is ever set up as part of this process.

Message Automation and Protocol Simulation (MAPS™) equipment is employed for Sweeps.[3] You may already have this equipment. If not, it's available from GL Communications. Network probes for data collection and formatting are available from Tekno Telecom. For visualization and correlation with disasters, an outside provider is used such as the Pacific Disaster Center which is highlighted later in this letter.

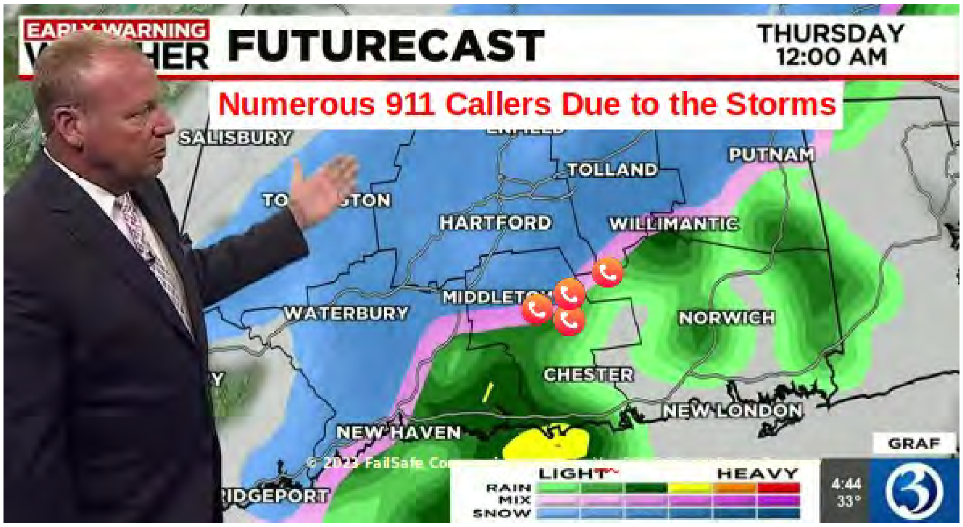
Visualization of Sweep Data



Phone Alerts

Desktop Alerts

Network Operations Center Alerts



[3] Message Automation & Protocol Simulation (MAPS™) is a protocol simulation and conformance test tool that supports a variety of protocols such as SIP, MEGACO, MGCP, SS7, ISDN, GSM, MAP, CAS, LTE, UMTS, SS7 SIGTRAN, ISDN SIGTRAN, SIP I, GSM AoIP, Diameter and others. Along with automation capability, the application gives users the unlimited ability to edit messages and control scenarios. See: www.gl.com

Government Funding

References to pricing and funding are so subjective that they can be an easy target for disputes. As a starting point for discussion we have to start somewhere. Imagine you are trying to sell a Chevrolet but the prospective buyer doesn't know if they can afford it. They would have to be given at least an estimate of the cost or there is no way they would commit to buy the car. Extra information like lease vs purchase options, financing incentives, rebates and other factors would be even better. For that reason, let's consider a few numbers, but like the rest of this report, as talking points only. The last thing we want to do is start an argument over numbers. In fact, we would like to see you, the reader, start here but provide anything you think we may have overlooked.

Government Option 1: Eligible Telecommunications Carriers and Providers (ETC/ETP) offer a discount to eligible low-income consumers on mobile or fixed voice service as well as broadband service and receive a reimbursement from the Federal Universal Service Fund. (FUSF) Since many carriers offer ETC / ETP services sponsored by the federal government, and receive subsidies on the same, do regulators have the authority to make enhanced services like those described here mandatory? Like we pointed out earlier, many live places where 911 calls are frequent. This may be one avenue of funding, and it's directed at people who need it most.

Government Option 2: Do funding alternatives exist through the Department of Homeland Security, DOD or other Agencies? We invite the industry and stakeholders to brainstorm other creative options.

Other Ideas?

What Would It Cost?

The figures below are intended as focal points for discussion and not hard estimates. They are however based on actual data and equipment costs. There is no way to predict the reaction of the industry to these costs, therefore we invite productive dialogue.

Option #1 – A Passive LATA Tandem Signaling Network Probe

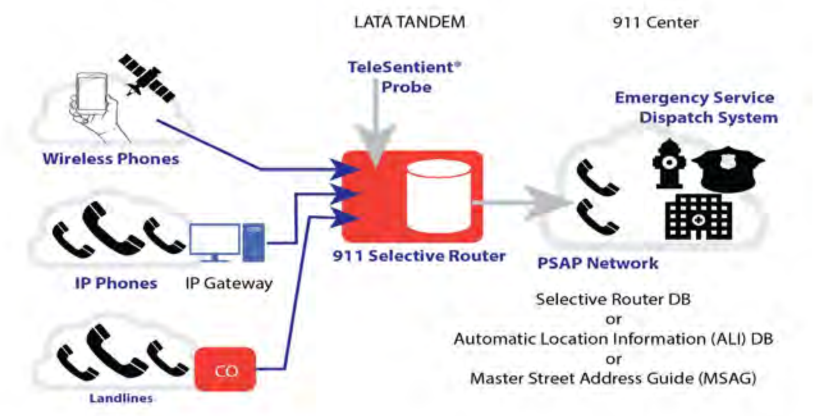
911 calls generally traverse a Selective Call Router in an incumbent LEC LATA tandem office, One method to produce alerts is to put a passive network probe in a collocation adjacent to the Selective Call Router.[4] Since we are located in the Dallas area, we made the following assumptions based on actual City of Dallas data. That data cites an average of 5000 911 calls per day and as the largest 911 center we used it to price out the probe. There are 16 more 911 entities in the Dallas suburbs. These figures would cover all of them as well since it's a LATA wide solution.

[4] Local Access Transport Area (LATA): The United States is divided geographically into 245 LATA regions. Local telephone companies are permitted to offer local or long distance telecommunications services within these regions

Rough Estimate of Cost to Offer TeleSentient® in a Single LATA

Cost of Tekno Telecom Probe and Consulting: $50,000
Number of Subscribers in D/FW LATA: 8 Million
Cost Per Line: $0.00625 per subscriber

Option #1



The carriers will not do this for free. This is another reason why the FCC may want to evaluate funding alternatives ranging from a billing surcharge, to DHS, or other federal funding alternative such as USF. Assuming the dominant carrier provided everything, and they were allowed a 400% markup (not unusual for vertical switch features) to cover their cost and the patent license fee, that would be a $0.025 surcharge per line per month. In D/FW this would generate $200,000 in month one, presumably more than justifying participation and equipment purchase by the carrier.

There is also of course the possibility of a third-party (e.g. Google, AWS, PDC, etc) to take the project on as an outgrowth or investment, assuming they had the security of a binding FCC Order.

Estimating a Nationwide Implementation Using the Same Assumptions

Once again there are Commercial and Government solutions. A nationwide implementation using these assumptions would be $50,000 × 245 tandems or $12,250,000. Equipment costs would be lower for smaller LATAs but the number of subscribers would be as well. As a point of reference, the City of Dallas just allocated $8 million for improvements to their *backup* 911 center.

a. **End User Funded:** In a scenario like the My911.plus video, the effort would be funded by voluntary end users. If such an end user was willing to pay 25 cents a month, using the Dallas LATA example of 8 million phone users, and a 10% take rate, this would generate a comparable break-even as the carrier scenario with $200,000 in revenue in month one. While this would facilitate a roll-out, it would be on a patchwork basis and create haves and have-nots based on ability to pay.

b. **Industry Funded:** If a company like Everbridge, Intrado, OnSolve, NGA911 or another company with roots in the 911 PSAP space spearheaded the effort by deploying Sweeps, one of these firms could become a dominant player in implementation of an end user solution as well. A major LEC could also take over operation, selling to all three markets including end users, industry and government. Depending on the "who" and "how" of this option, it could represent a patchwork deployment or total solution.

c. **Government Funded:** FCC, DHS, Pacific Disaster Center, or other entity operates under contract and charter from the FCC or Congress. The Pacific Disaster (PDC) is highlighted below because it has demonstrated compatibility with these technologies, is already federally funded, and can visualize and correlate disasters in its DisasterAware® system down to street level. This would represent a total solution.

A Possible Shortcut to Funding a National Implementation

The FCC has stated that it desires the means to visualize 911 and 988 outage data, and presumably desires a standardized national roll-out. This would among other things eliminate the patchwork that existed for many years while e911 (with ANI and ALI) slowly proliferated across the states. For this reason we strongly suggest they contact the Pacific Disaster Center. An overview of their technology is contained in Attachment 3.

Using PDC, 911 callers can not only be located, they can also be correlated with the causes of their call with reliable outside data. Besides being mission control for the recovery effort following the Lahaina fire, they have displayed TeleSentient® data on their $50 million DisasterAware® system that our government has already paid for. They can fast track your effort. A visit would greatly benefit the suffering people of Maui. Please consider calling or visiting them.

Option #2

There is another option is less expensive, available nationwide, does not require a LATA tandem collocation or the cooperation of the carrier, but it is highly proprietary. It can be discussed with the FCC under suitable confidentiality covenants.

Pricing Conclusions

The conclusion is that there is no conclusion. As noted above, these are just brainstorming ideas. We offer them only as a starting point for all stakeholders to join us in this dialogue.

Summary, Conclusions, and Next Steps

Imagine a National Weather Service radar image that shows not only the thunderstorm, but all 911 callers in the vicinity of the storm. For that matter, imagine a WAZE GPS application when you drive home tonight that says *"Accident ahead – many callers to 911!"* The industry is limited only by its imagine in terms of things it can sell.

The undersigned believes that with action by the FCC, it's a lay-down bet that 911 centers will sign on in droves, and services like My911.plus will be on every late-night TV channel. This would also assuage the concerns of carriers with regard to cost since the private sector would be the driving force, not the carrier. The more innovative and foresighted carriers might find a new profit center here.

It will be exciting to see where other industry experts take these concepts to increase the safety of Americans and save lives.

Best regards,

/ s /

Leo A. Wrobel
CEO of FailSafe Communications Inc.
Inventor of TeleSentient®
www.failsafecommunications.com *
(214) 484-6805

Attachment 3

The Pacific Disaster Center (PDC) is an applied research center managed by the University of Hawaii. It supports the most demanding governmental and nongovernmental organizations worldwide in helping to create a safer, more disaster resilient world. For more than 30 years, PDC has helped its partners enhance disaster management capacity, save lives, and reduce disaster losses through the application of our advanced tools and technologies, evidence-based research, and analytical information. The Inventor of TeleSentient® has worked with the PDC since 2004.

Since July 2023, the PDC has been mission control for recovery efforts after the Lahaina Maui fire.[5]

The PDC has proven feasibility of illustrating TeleSentient® data on its DisasterAWARE® platform. DisasterAWARE® is used by tens of thousands of disaster management professionals, from the senior-level decision makers to the operational practitioner. It provides global multi-hazard early warning, hazard monitoring, and risk intelligence to support rapid and effective disaster response, preparedness, recovery, and mitigation. DisasterAWARE® includes the highest resolution all-hazards impact models, advanced analytical reports, and augmented information through artificial intelligence. The system features the largest, scientifically-vetted big data catalog for disaster management decision making in the world.

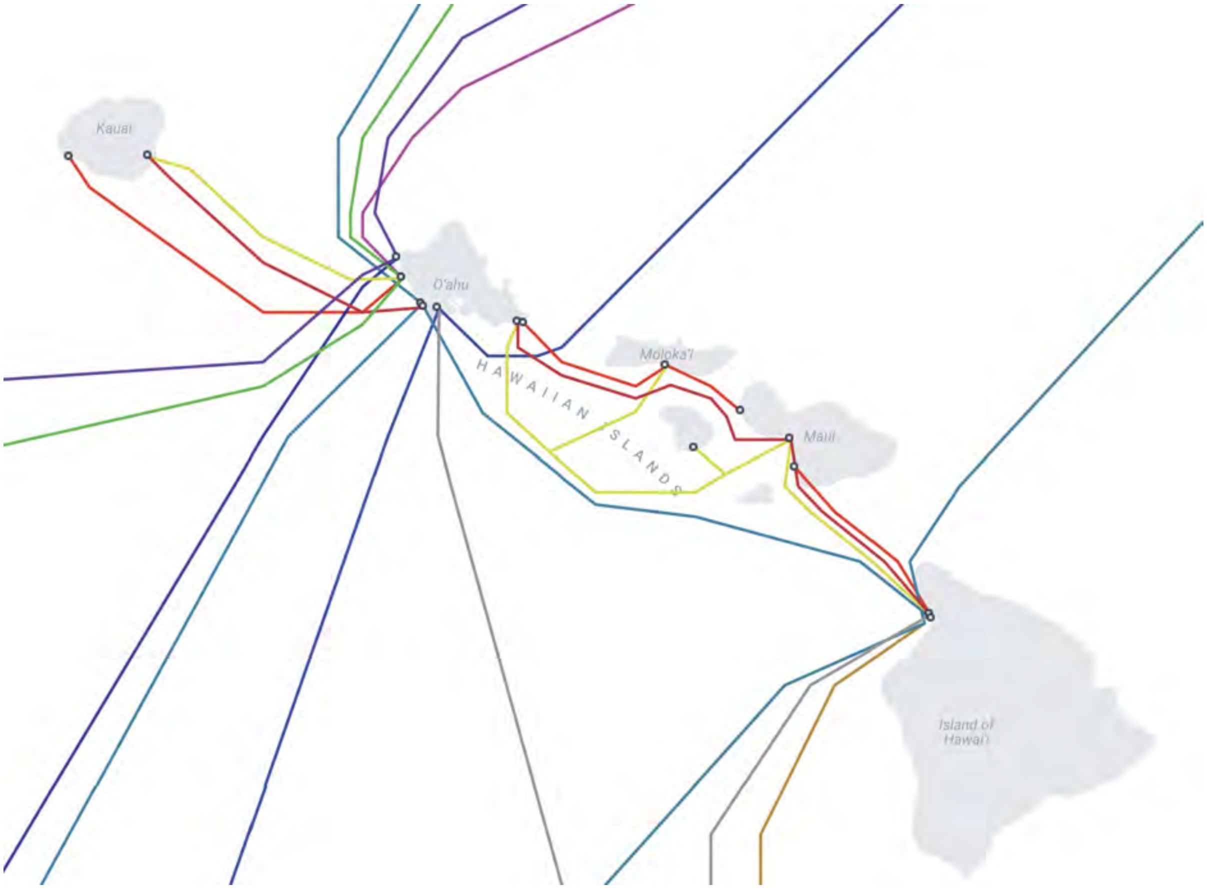
DisasterAWARE® provides near real-time analytics about impacts to population, capital, and key infrastructure for multiple hazards, calculating likely humanitarian needs down to a scale of 30 × 30 meters. DisasterAWARE® is free to disaster management practitioners and the humanitarian assistance community at disasteraware.pdc.org. In addition to offering advanced decision support technology, PDC is pioneering the scientific application of artificial intelligence for disaster risk reduction through its AI for Humanity™ program. Learn more about these innovations at pdc.org/ai-for-humanity. The Center also provides specialized research on a range of topics ranging such as national fragility, national disaster preparedness, women, peace and security, and climate change. PDC also supports disaster preparedness training and exercises.

Diagrams related to the Pacific Disaster Center concerning the ability to scale nationwide on a $50 Million federally-funded system that the United States Government has already funded. The Inventor can make appropriate introductions or arrange a Zoom call or visit. Your Agency is also in the best position to evaluate funding sources from DHS or Congress, or to make other policy decisions such as allowing carriers to include a per-line surcharge on their bills.

[5] The undersigned is a frequent traveler to Maui. He conducted an independent analysis based on the topology diagram in Attachment 2 that follows. There is a high degree of certainty that TeleSentient® would have identified unsuccessful 911 callers during and after the Lahaina fire. Thousands of unsuccessful calls in the fringe areas around the fires, and the following weeks could have been located and helped with this technology. More details in Attachment 4.

Attachment 4

We were recently asked if TeleSentient® could have helped the people of Lahaina Maui during the fire. Our response was initially “It doesn’t put out fires.” When we thought about it though, it became apparent that there were thousands of people not in the immediate vicinity of the fire. The people in the fringe areas of the fire were still calling 911 for police, fire, ambulance and other services. They didn’t know if the water was safe to drink or had no water. Of the 4000+ calls to the Lahaina 911 center on that infamous day, perhaps ten times that many were blocked, received fast busy signals, or routed to dead air. We pulled maps of undersea cable routes like the one pictured below and came to some conclusions. The results can be shared confidentially with the FCC upon request.



Source: www.submarinecablemap.com Accessed on October 24, 2023