Telephony and home alarms:

How technology change can break things that already work

Ken Short

Senior Manager – Technology Development and Strategy

Bell Canada

2017-10-17

Bell

It is a reality that telecom and alarm monitoring companies face challenges brought about by technology change

- Due to communication format configurations, VoIP-based telephone service is sometimes incompatible with home alarm systems that use a telephone line
- Consequently, customer service is negatively impacted, leaving the customer unsatisfied
- There has not always been good cooperation between Telecoms and Alarm Monitoring companies to fix issues, leading to customer dissatisfaction and frustration
- Bell is aware of the issues, has identified multiple ways of solving it, and is ready to work with you to achieve customer satisfaction

Working together, we can fix it — and drive customer satisfaction

Table of contents

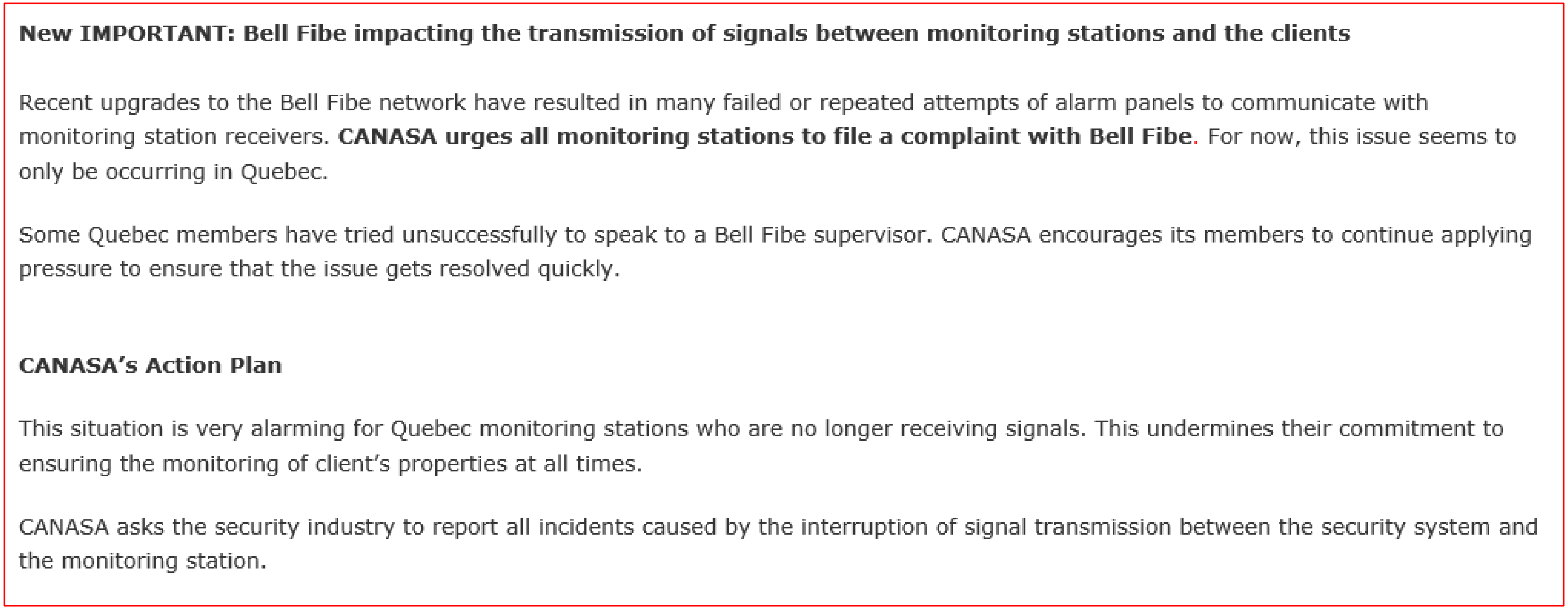
1. Technology change in the Security industry
2. Technology change in the Telecom industry
3. Understanding current problems
4. Recommend a path forward

Is there an elephant hiding in this room?

1/7/84

"Now calm down, Barbara. ... We haven't looked everywhere yet, and an elephant can't hide in here forever."

I received this on October 26, 2016



New IMPORTANT: Bell Fibe impacting the transmission of signals between monitoring stations and the clients

Recent upgrades to the Bell Fibe network have resulted in many failed or repeated attempts of alarm panels to communicate with monitoring station receivers. **CANASA urges all monitoring stations to file a complaint with Bell Fibe**. For now, this issue seems to only be occurring in Quebec.

Some Quebec members have tried unsuccessfully to speak to a Bell Fibe supervisor. CANASA encourages its members to continue applying pressure to ensure that the issue gets resolved quickly.

CANASA's Action Plan

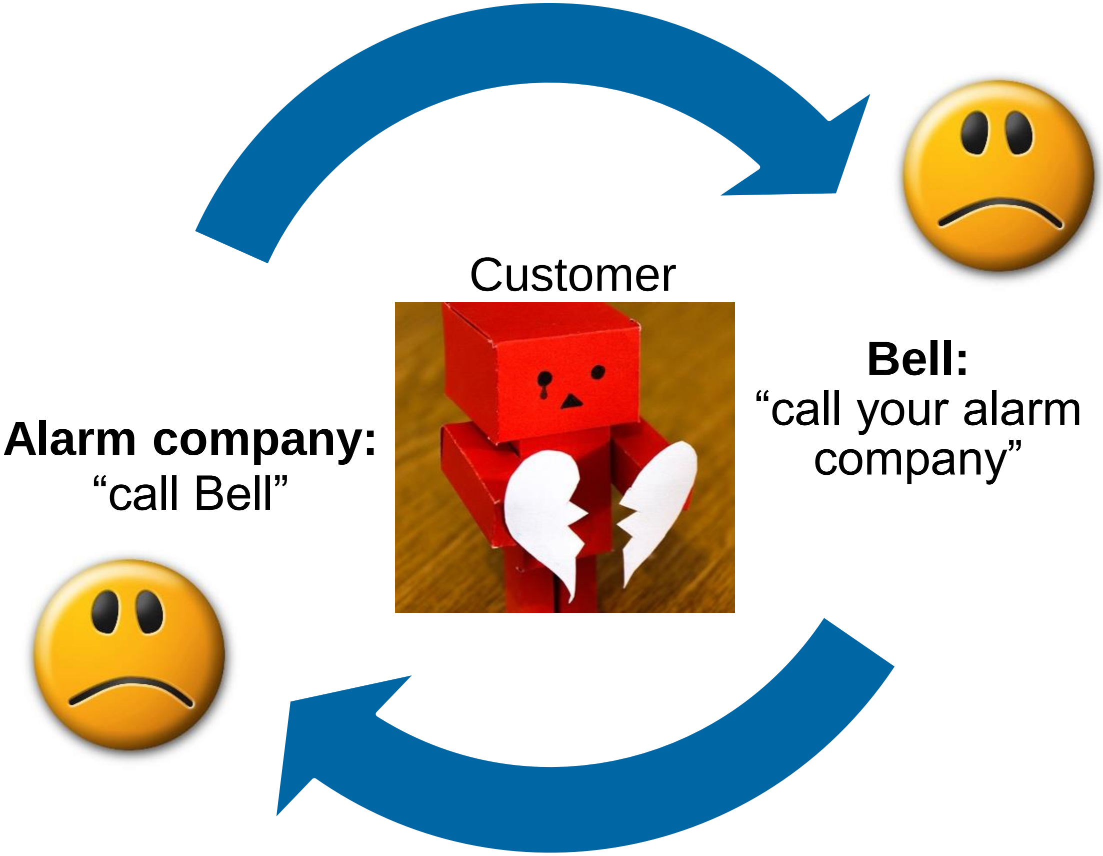
This situation is very alarming for Quebec monitoring stations who are no longer receiving signals. This undermines their commitment to ensuring the monitoring of client's properties at all times.

CANASA asks the security industry to report all incidents caused by the interruption of signal transmission between the security system and the monitoring station.

Disclosure: We at Bell know that sometimes alarm panels stop reporting once they have been converted to VoIP

Let’s talk about the elephant in the room

- When a customer has a problem with a system, it’s not a great customer experience if we just point fingers at the other provider
- In Bell, we took the October 2016 CANASA bulletin very seriously
- We have been working on an action plan that has already advanced internally
- Today we want to share our progress to date



Customer

Bell:
“call your alarm company”

Alarm company:
“call Bell”

My personal experience shows that when the Alarm company and Bell work together, we can fix customer issues quickly!

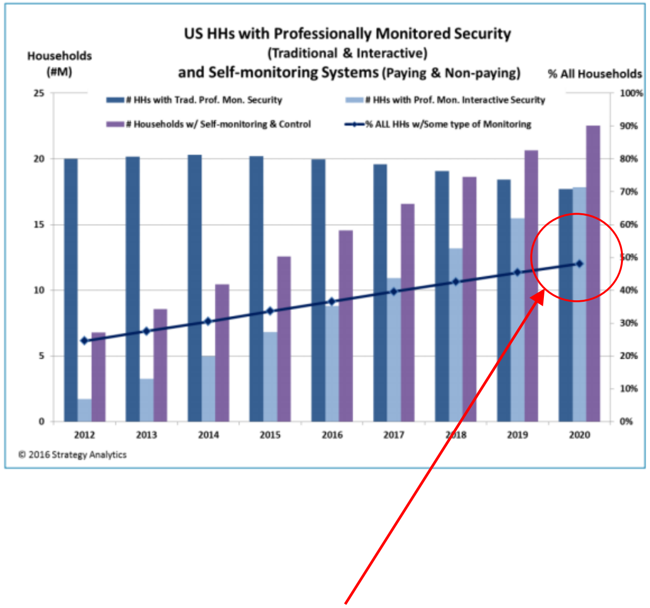
Table of contents

1. Technology change in the Security industry
2. Technology change in the Telecom industry
3. Understanding current problems
4. Recommend a path forward

Some quick research on the security industry showed that there are big changes happening in your industry due to changes in technology

- Technology disruption underway as non-traditional players enter the Industry
- “Smart Home” technologies (e.g. Zwave) and “Internet of Things” (IoT) are giving Consumers self-install/self-monitor capability
- Video monitoring is growing plus “video-verified alarms” is coming
- Cloud-based technologies (in the home and outside the home) are becoming the norm
- The “security” of providing “security” is important as apps start to be used by the consumer
- Conclusion: Security companies are being *disintermediated*

Figure 3: Market Forecast



© 2016 Strategy Analytics

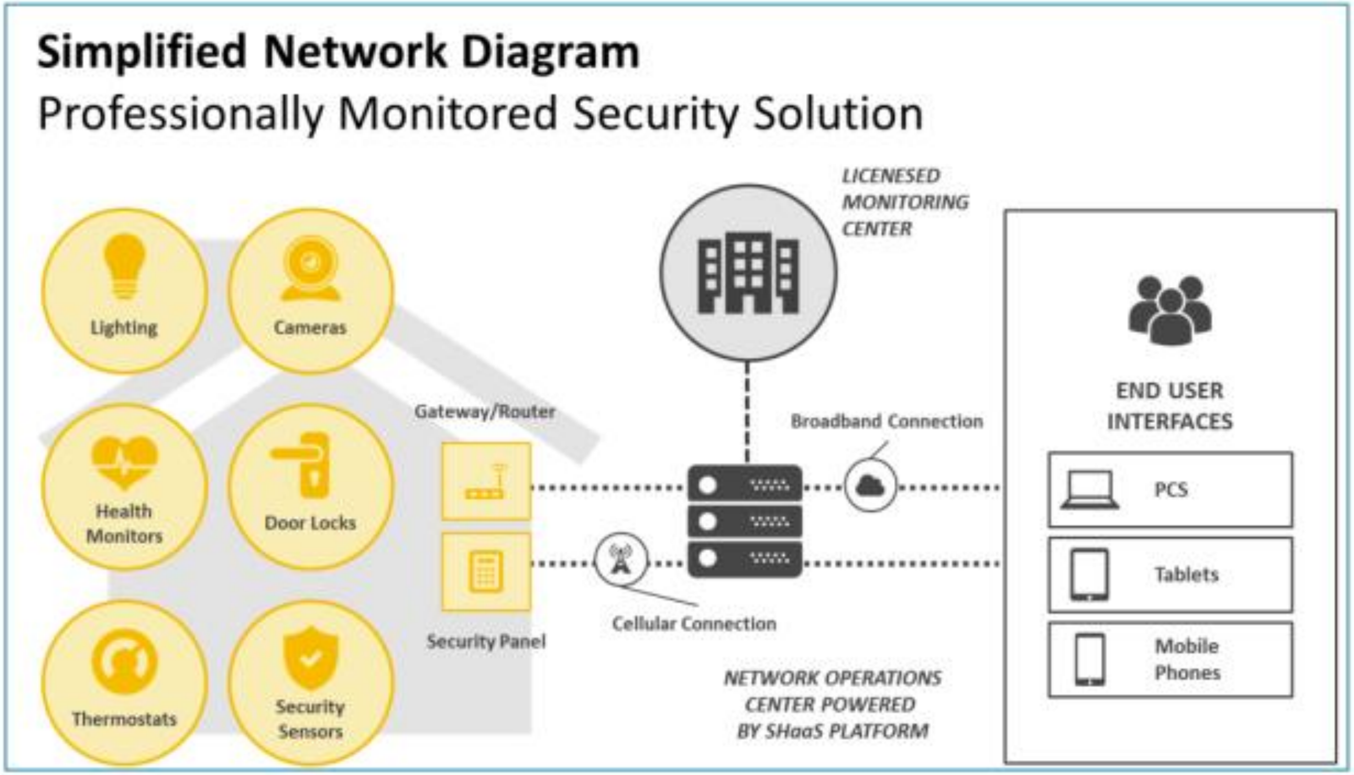
By 2020 the number of households with interactive security will edge past those with traditional security systems, and the percentage of all households with some form of monitoring system will reach nearly 50%.*

Technology changes are driven by innovators who do not usually have a stake in an existing business but who see a great opportunity in disrupting it

* Smart Home: Disrupting the Security Industry – (https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/reports/report-detail/smart-home-disrupting-the-security-industry?slid=117462&spg=1#.WdJM1ltSzRb0.7991603908750466) – p.10

A POTS line won't cut it in the smart home

Figure 1: A Typical Interactive Security System



The monitored home of the future requires broadband access

* Smart Home: Disrupting the Security Industry – (https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/reports/report-detail/smart-home-disrupting-the-security-industry?slid=117462&spg=1#.WdJM1ltSzRb0.7991603908750466) – p.3

Table of contents

1. Technology changes in the Security industry
2. Technology change in the Telecom industry
3. Understanding current problems
4. Recommend a path forward

Historically, the telephone network was not designed to carry alarm monitoring signals or other “data”

The Public Switched Telephone Network (PSTN) was designed to carry voice only

- The PSTN was built to only carry speech at a time when bandwidth was limited and therefore expensive
  - It was designed to only pass frequencies in the 200Hz – 3.3KHz; anything above or below that was deemed extraneous and was filtered out as a cost savings measure
- After more than 130 years, the original design attributes of the PSTN continue to persist even in today’s modern voice network implementation
- Today’s modern VoIP networks typically remain constrained to that ~3.3KHz range to ensure backwards compatibility with customer premise equipment

Support for data (*fax, file transfer, text, etc.*) came after and required special equipment to make it work on the voice network

- The **MoDem** (Modulator/Demodulator) was developed to transform data bits (discreet values of 1’s and 0’s) into a continuous analog signal for transmission over the PSTN
- Protocols and standards advancement enabled higher speeds (aka more data) to be crammed into a “telephone” call
  - These advancements were mostly in the domain of compression and noise reduction because noise was the key inhibitor in the early analogue PSTN
- Innovation continued until late 1990’s when the world started to move away from dial-up data communications to Internet-based protocols

Technology change for telecom started with the Internet age

In the late 1990's the Internet revolution begins

- The world gets bolted into the ".com" age and technology disruption is prevalent
- The demand for higher data communication speeds and volumes can no longer be met with dial-up data over the PSTN
- Everything is going "IP"
- In the voice domain, a shift begins to new multi-media services that the PSTN couldn't support but that IP networks can with ease

This shift to IP heralds a new era for voice

- Innovation on the PSTN stops
- VoIP requires development of special protocols to maintain voice – "real-time" by nature – quality when transmitted over IP (a not "real-time" protocol)
- It also requires the development of new devices like Media Gateways (MGW) to bridge between the old PSTN and the new VoIP networks, otherwise people couldn't call each other if they were on the different networks

VoIP brought challenges as developers looked for a balance

- The tension between new service creation and support for legacy services becomes a constant balancing act
- Modems are caught in the middle
- New network standards, required to make existing modems work on VoIP networks [ITU V.150 (Modem over IP; 2003) and ITU V.152 (Voice Band Data; 2005)], are developed
- It takes time to incorporate and fine tune the implementation of new standards in equipment

Table of contents

1. Technology changes in the Security industry
2. Technology change in the Telecom industry
3. Understanding current problems
4. Recommend a path forward

Home alarm panels have been on collision course with VoIP for a long time; however the issue is exposed only when a home converts to VoIP

Huge installed based of home alarm panels

- There is a huge base of home alarm panels with embedded technology that pre-dates the Internet age[1]
- Vast majority of panels have not been changed or updated since their initial installation

Technology enhancements didn’t address the installed base

- Developments in telecom and the alarm industry occurred but these did not address the installed base
- No economic incentive for the alarm industry to change or update the base of home alarm panels

Customer conversion to VoIP may trigger the latent problem

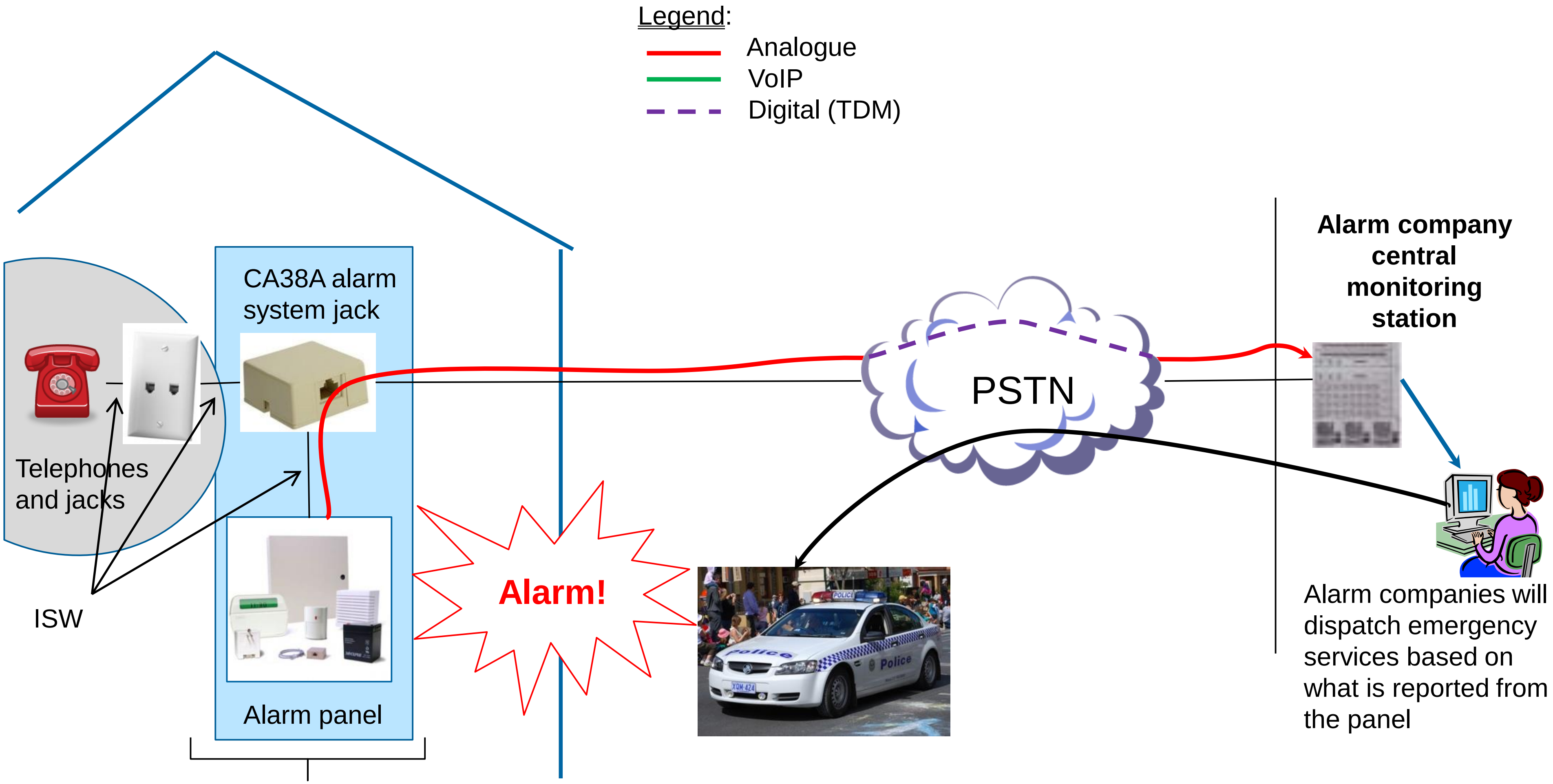
- As customers convert to Broadband Internet, their home phone service is upgraded to VoIP
- This conversion may lead to an unpleasant surprise for the customer – the alarm panel is not configured properly to work over VoIP

For too long we have only addressed this problem by “passing the buck”

[1] http://www.statisticbrain.com/home-security-alarm-system-statistics/

Animated

Traditional home alarm panels worked just fine with PSTN connections



Legend:

- 🟥 Analogue
- 🟩 VoIP
- ▬ ▬ ▬ Digital (TDM)

Alarm company central monitoring station

Alarm companies will dispatch emergency services based on what is reported from the panel

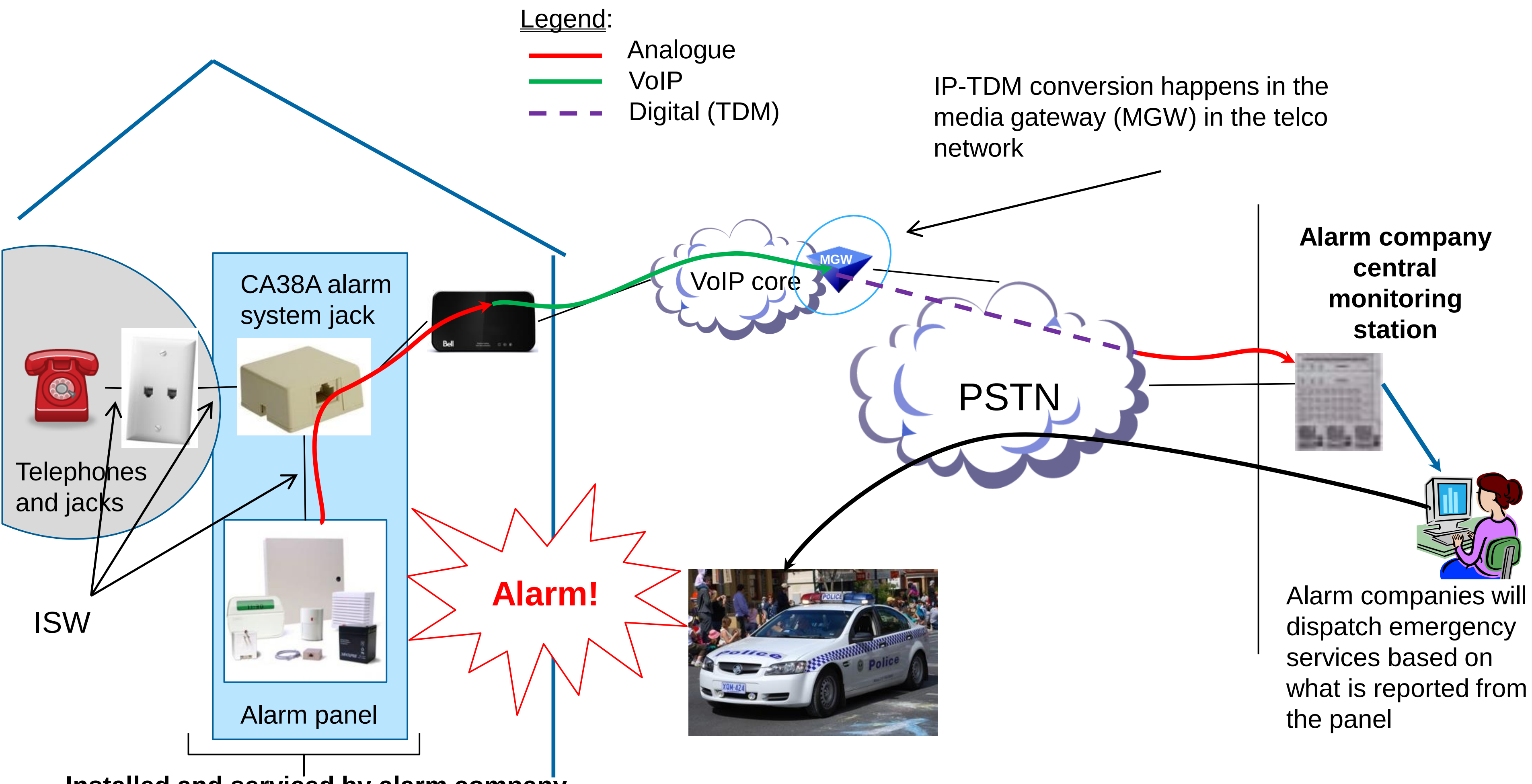
Installed and serviced by alarm company

PSTN-connected alarm systems worked well because they used communication formats optimized for the PSTN

- In an alarm/event situation, the home alarm panel seizes the telephone line and calls the central station to report the event
  - If the homeowner is on the telephone when there is an alarm, the CA38A jack enables the alarm panel to disconnect that call so that it can use the line, returning it to a usable state when finished
- The call is a low speed ***data*** call (modem to modem) over the telephone network using a single “voice” channel
  - The voice network doesn’t “know” it’s a data call until both ends are connected and there is a communication path established [*this latter point is more important when we talk about VoIP*]
- Alarm panels can use different communication formats for modem speed training and transmission as follows:
  - Security Industry Association (SIA) format (packet-based)
  - Contact ID (DTMF-based)
  - Pulse formats (similar to rotary dialing: 3x1, 3x1 extended, 3x2, 4x2, 4x3; # digits in account x # digits in the event)
  - A variety of other formats which may be proprietary to the panel or the central monitoring station

Animated

While some home alarm panels and VoIP connections may not be compatible, in reality, the incidence of failure is less than << 1% of customers



Legend:

— Analogue

— VoIP

- - - Digital (TDM)

IP-TDM conversion happens in the media gateway (MGW) in the telco network

Alarm company central monitoring station

CA38A alarm system jack

Telephones and jacks

ISW

Alarm panel

Alarm!

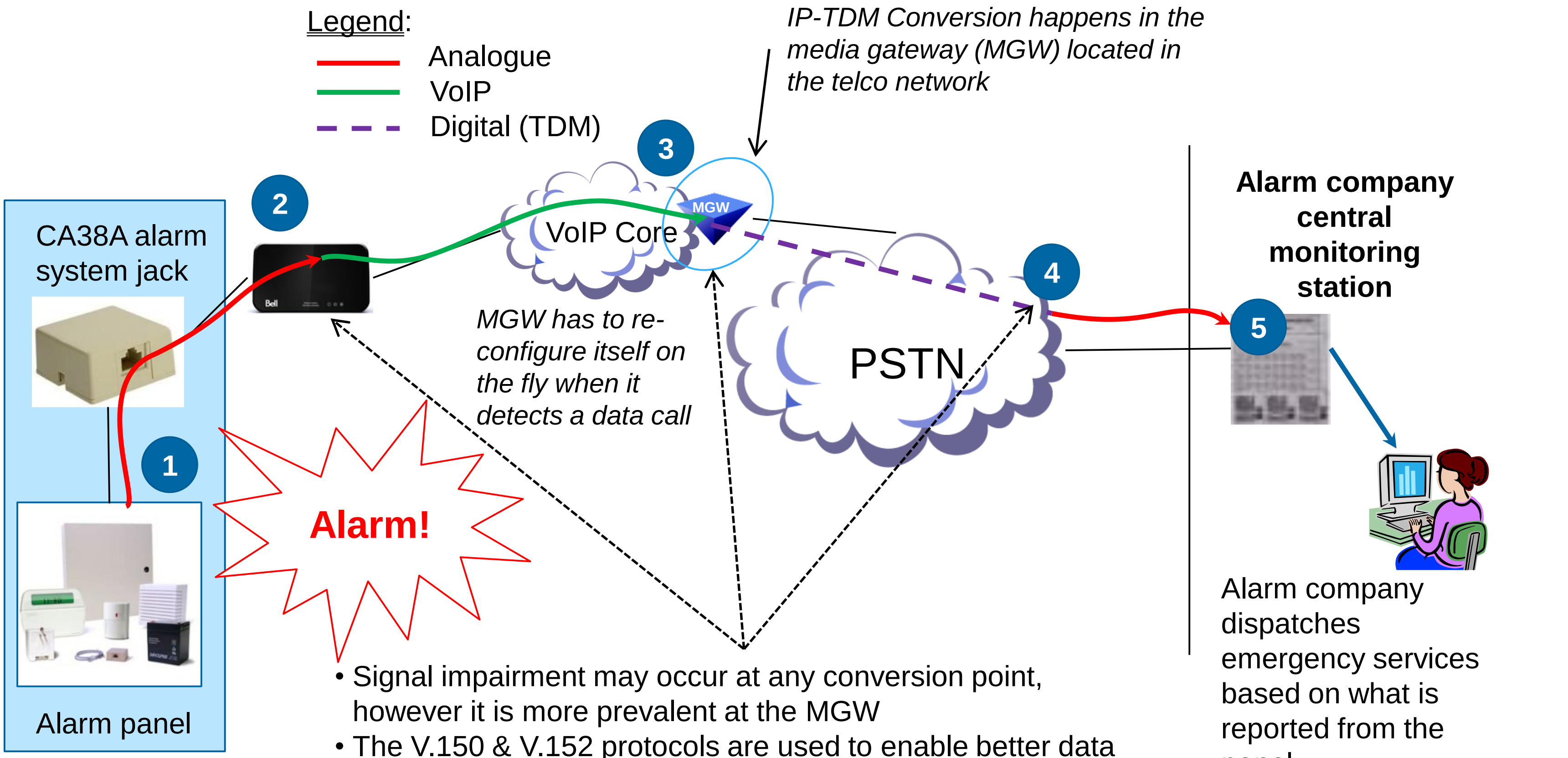
Alarm companies will dispatch emergency services based on what is reported from the panel

Installed and serviced by alarm company

The endpoints are the same however the network has changed

Animated

Signal impairments occur due to the conversion of analog signals generated by the alarm panel to/from digital signals and packetization


Legend:
Analogue
VoIP
Digital (TDM)
IP-TDM Conversion happens in the media gateway (MGW) located in the telco network
3
MGW
VoIP Core
2
Bell
CA38A alarm system jack
PSTN
4
Alarm company central monitoring station
5
MGW has to re-configure itself on the fly when it detects a data call
1
Alarm!
Alarm panel
Alarm company dispatches emergency services based on what is reported from the panel

- Signal impairment may occur at any conversion point, however it is more prevalent at the MGW
- The V.150 & V.152 protocols are used to enable better data communication via the MGW by disabling voice band functions like echo cancellation
- These are enabled once the MGW ***detects a "data" call in real time***
- Detection of the data call requires a finite period during which time the critical signal timing may be impaired
- Signal timing can also be distorted with additional delay introduced during transcoding and IP network transmission

As the alarm message traverses the VoIP network, multiple signal conversions can distort it and cause the receiver to drop the call

1. After connecting to the reporting station, the alarm panel composes the message based on the communications format. This is an analogue signal that includes the customer account number and details on the alarm event.

2. The ATA digitizes the signal at 8000 samples/second then encodes it using a standards-based codec (coder/decoder) format, called G.711, into an IP "packet." Packets are then routed in the IP core to the media gateway (MGW).

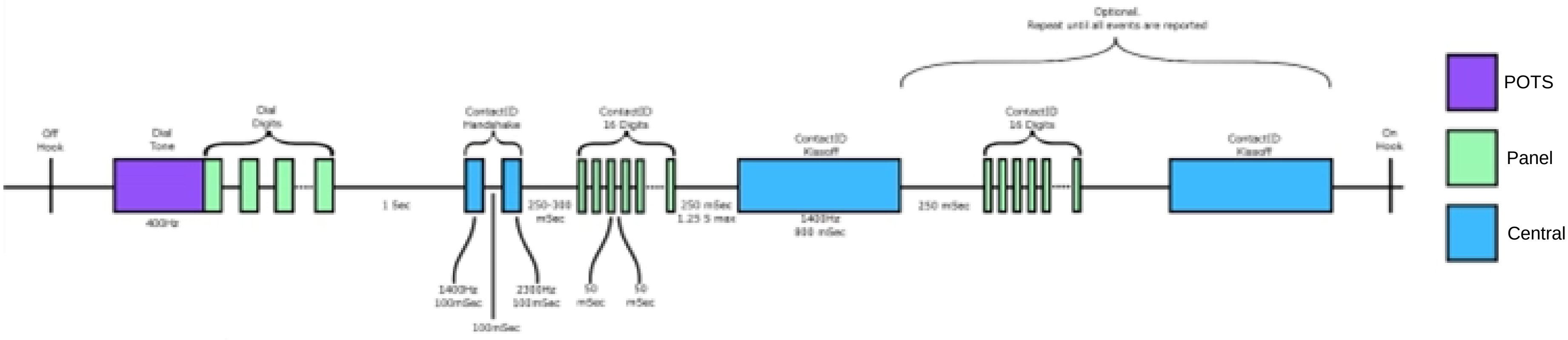
3. At the MGW, the signal is de-packetized and converted back into TDM[1] for transmission across the PSTN to the monitoring station. The extra payload required for the packet overhead may impact the inter-signal timing.

4. At the PSTN edge, the signal is converted back to analogue for transmission over the Copper network. At this point, the analogue signal is re-constructed from bits. The reconstituted signal may not exactly match the original and even slight deviations may result in misalignment or an unrecognizable signal.
   (N.B. This step may not be required if the receiver can support a digital interface).

5. The receiver interprets the signal and acts accordingly which may mean dropping the call if it cannot decipher the message.

[1] TDM = Time Division Multiplexing - the main PSTN protocol

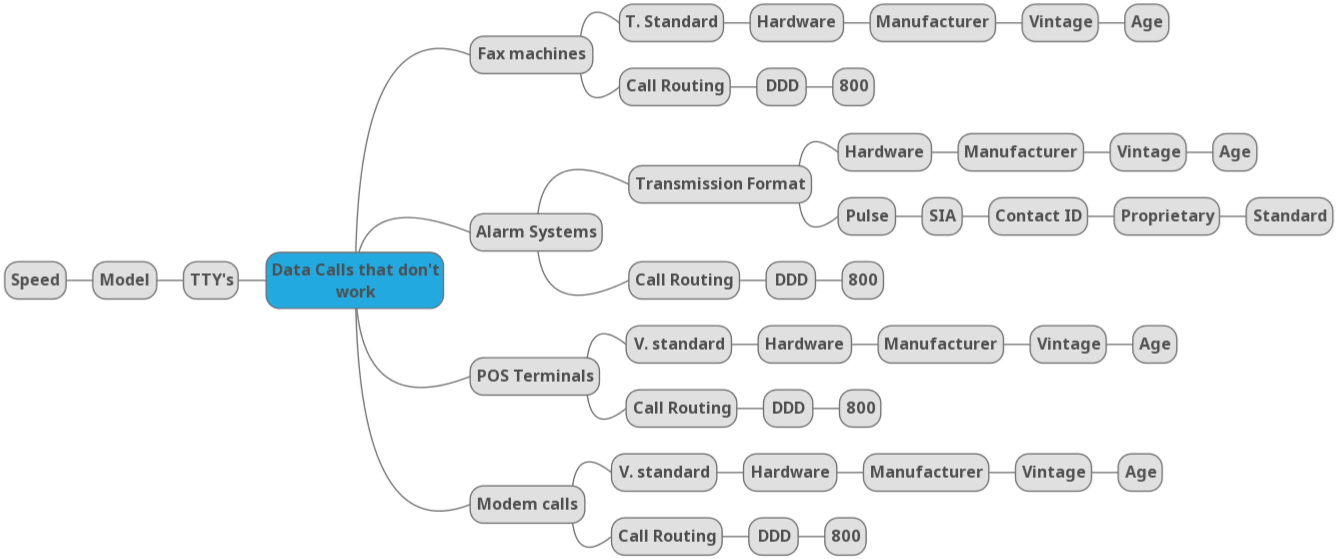
Signal distortion occurs because transmission protocols are very timing sensitive



- As shown above, the Contact ID[1] protocol (example) relies on fixed time gaps and handshake tones
- As the message sequence is sent from the alarm panel to the receiver, it must be digitized (converted from analogue to digital) and packetized, transmitted over the IP core, then de-packetized and converted back to analogue before being transmitted to the receiver
- Once the MGW (see previous slide) detects the "data" call, it switches to "data" mode by enabling modem over IP (V.150) and voice band data (V.152) to optimize the call for data transmission
- Switching modes may cause minor timing variations and/or signal impairment such that the receiver cannot properly decipher the message
- When the receiver cannot decipher the message, it drops the call, the alarm event remains unreported, and the alarm panel may not automatically recover without intervention

[1] Adapted from https://li0r.wordpress.com/contact-id-protocol/

“So, Bell, why don’t you just fix it?”



- It’s a complex problem of many variables
- Fixes or network tweaks that address one set of variables for a particular panel do not work in other cases
  - E.g. sometimes SIA works and sometimes it doesn’t
- The permutations and combinations of the above are staggering from a coding/testing viewpoint
- A lab of hardware combinations alone would be impractical
- Our equipment vendors do not have the development environments to support the permutations/combinations of 20+ year old equipment

If there were an easy fix, we would have found it by now

Table of contents

1. Technology changes in the Security industry
2. Technology change in the Telecom industry
3. Understanding current problems
4. Recommend a path forward

We are proposing to quickly get your experts connected to our experts to ensure customer satisfaction

- Dedicated email (ap.help@bell.ca) for alarm companies to reach Bell when issues occur with customer panels. Email should include the following information:
  - Customer telephone number
  - Telephone number of the monitoring station as programmed in the panel
  - Panel make and model
  - Transmission format
  - Date/Time of call failures
  - Alarm company contact name, telephone number and email
- Joint mailbox in monitored by Bell Voice Operations and Technology Development teams
- 24-hour turn around between 8am-5pm EDT
- Access to SME's who can do live call traces and packet captures at different network tap points
- Well versed in these kinds of issues
- Can re-route calls (if required)
- Can find network faults
- Internal and external contacts and processes for escalations when required

We will address all *customer* alarm system-related issues

Next Steps

Bell is committed to actively improving the situation in a timely manner

- Bell will respond to emails sent to ap.help@bell.ca and address problems
- Bell will make available to CANASA members our captive Voice lab in Ottawa for testing/verification of new equipment and/or software
- Bell will advise CANASA members of network changes that could impact alarm reporting systems
- Bell will continue to participate in the CANASA Telecom Signal Problem Working Group