Communications Outage Risk Assessment: a case study

Santa Clara County
Emergency Managers Association

21 July 2016

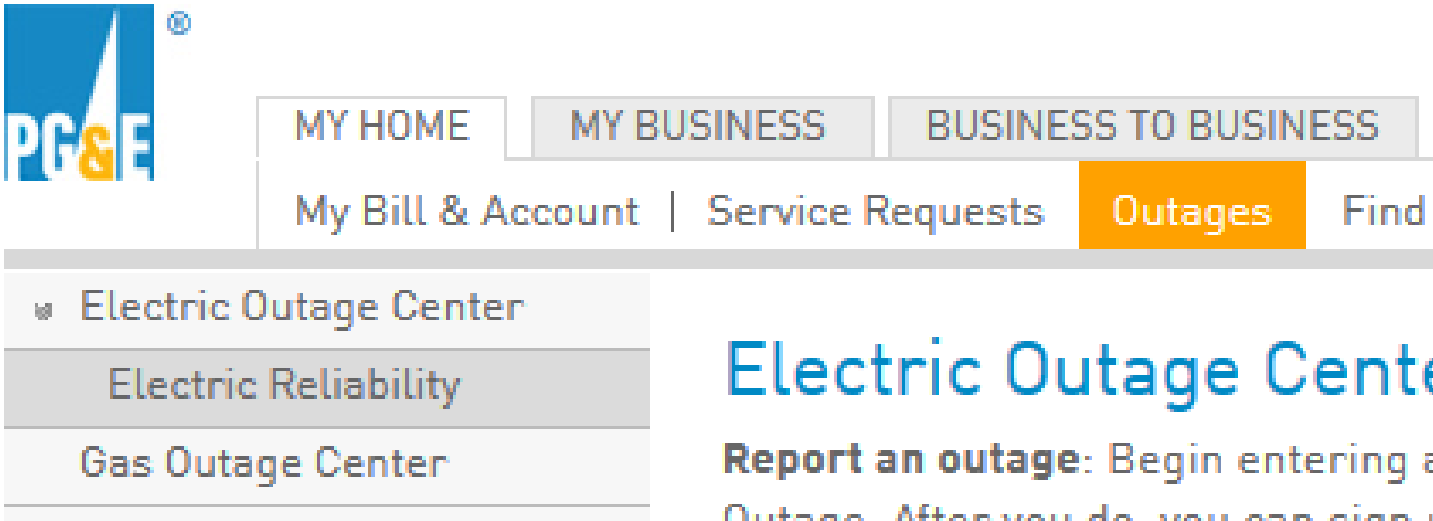
Jim Oberhofer
EC,RACES, Cupertino OES

Thursday morning, 8:00am

Bay Area power outage

All of the Bay Area woke up (late) with no power.

As people scramble to find their smartphones or battery-powered AM Radios, they learned that at 2:15am this morning, a massive power failure occurred and left most of northern California without electrical power. PG&E and CAISO issued statements saying that finding and fixing the cause of the outage is in progress.



Thursday afternoon, 1:00pm

Bay Area power outage

11 hours into the blackout.

PG&E reports that some unidentified fault is hampering them from bringing up the power grid per their usual procedures.

- The ***good news*** is that they isolated the source of the problem to the Cortina Substation, about 73 miles north of Sacramento.
- The ***bad news*** is that the cause is still unknown.
- County OES increases its activation level.

Friday morning, 8:00am

Bay Area power outage

30 hours into the blackout.

The County OES PIO issues a press release:

- Essential services remain in operation throughout most of the bay area. Some backup power systems failed.
- Water systems in a few cities lost pressure forcing boil-water advisories to be put into effect.
- Telephone networks are operational, but an increased demand left many circuits overloaded.
- Cellular service is spotty due to call volume.
- Major cellular providers are now on backup power.
- Most Commercial TV, radio stations are still on the air.

Friday afternoon, 3:00pm

Bay Area power outage

37 hours into the blackout.

County OES hosts a joint press conference with PG&E and several telephone/internet carriers. The news is not good.

- PG&E suspects a software bug or worse… a cyber-attack.
- Attempts to bring up the grid have failed; PG&E thinks this could go on for another 24 hours.
- AT&T and other carriers state their networks continue to be overloaded, long delays getting a dial tone, and some backup power systems have started to fail.
- Wireline services are working, but most field equipment backup batteries will run down tonight.

Friday afternoon, 4:00pm

Bay Area power outage

38 hours into the blackout.

The Cupertino City Manager requested RACES and CERT teams to activate Saturday *if they wake up with no telephone service at home*. The request is to do the following:

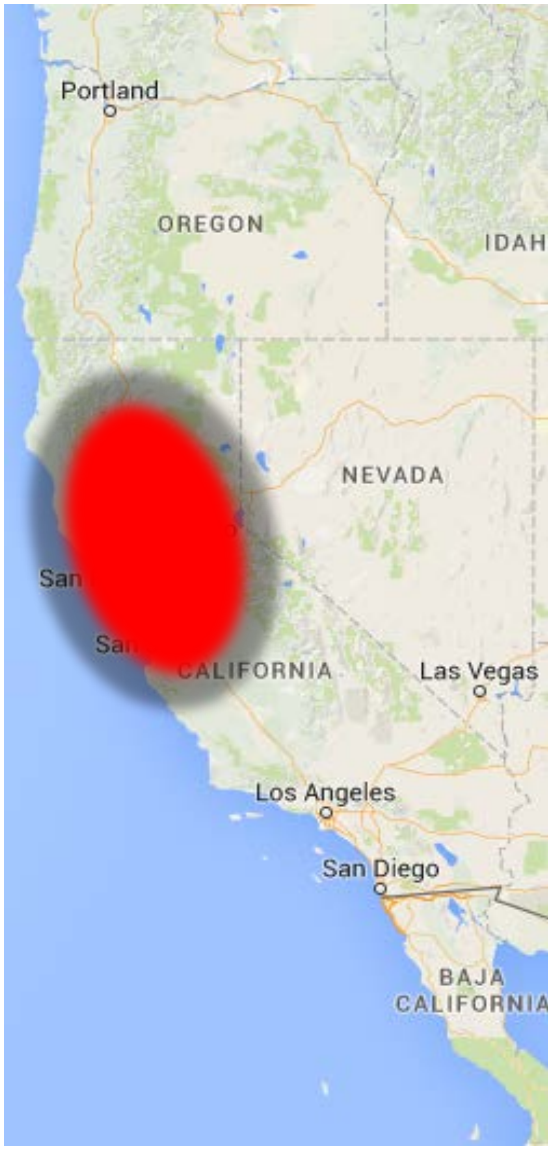
- Set up communications outreach locations throughout the City to pass on information and relay resident requests for help.
- Support the EOC.

Saturday early morning, 1:30am

Bay Area power outage

Almost 48 hours into the blackout.

- Wireline and cell phone communications fail throughout all of Santa Clara County and northern California counties.
- No dial tones were heard when picking up the telephone handset.
- Placing 911 calls is no longer possible.



Is this scenario likely?

Could this happen here?

Looking at the Risks

What's been done so far

- National Infrastructure Protection Plan (NIPP)
  - FEMA, 2006, Risk Management Framework to address pre-existing threats that may occur from natural disasters, cyber-attacks, and terrorism.

Critical Infrastructure Sectors

1. Chemical
2. Commercial Facilities
3. Communication
4. Critical Manufacturing
5. Dam
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Finance Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Pub Health
13. Information Technology
14. Nuclear Reactor, Mat'ls, Waste
15. Transportation Systems
16. Water and Wastewater

Looking at the Risks

What's been done so far

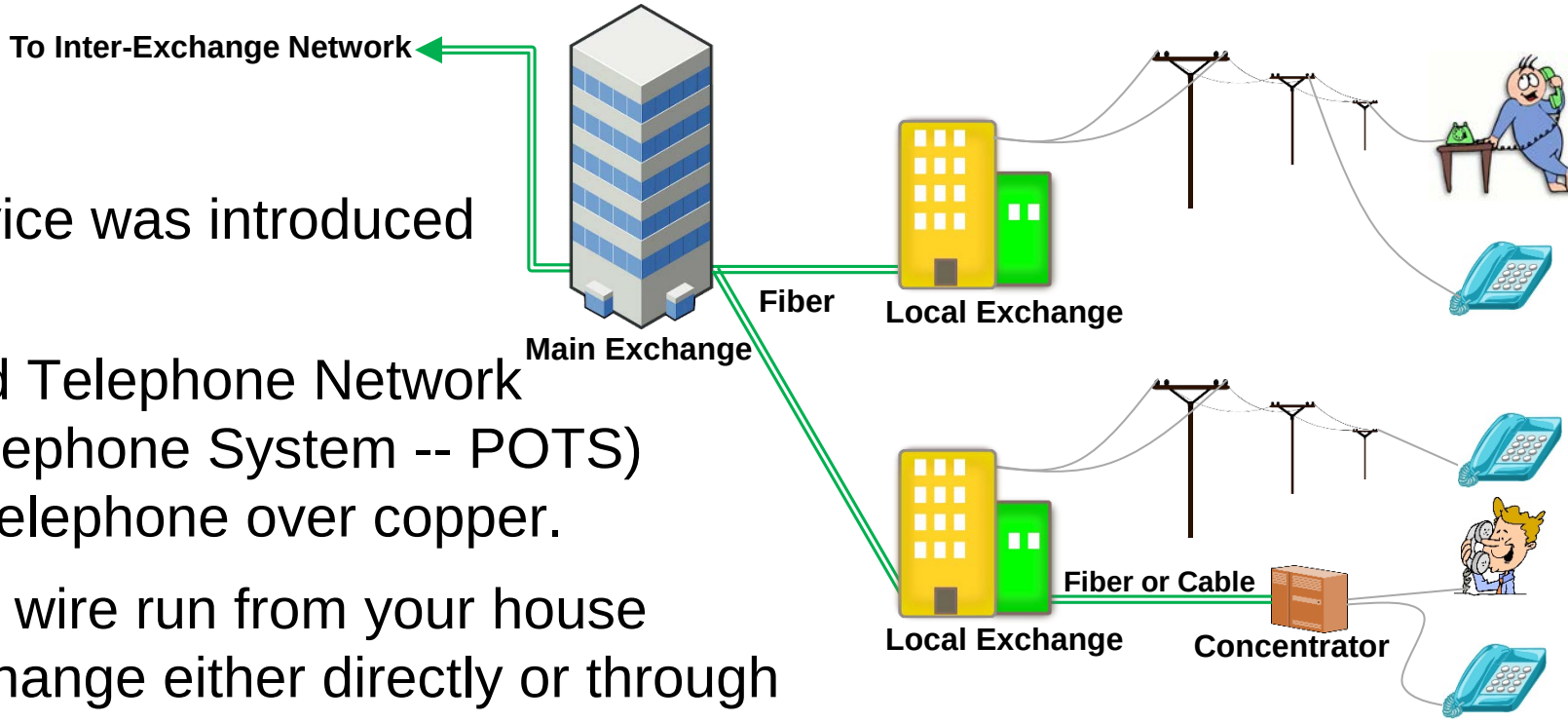
- National Infrastructure Protection Plan (NIPP)
  - Communications Sector-Specific Plan (CSSP)

An approach to a local risk assessment

1. ***What could fail?*** *(potentially impacted systems)*
   - *Telephony*
   - *Internet*
   - *Radio*
   - *Messaging*
   - *Video*
   - *others?*
2. ***What could cause a failure?*** *(impacting events vs. initiating hazards)*
   - *loss of power*
   - *loss of connectivity*
   - *system overload*
3. ***How likely is it to occur?*** *(characterize the risk)*
   - *redundancy, diversity, recoverability*
   - *probability and seriousness*
4. ***What do we do when it does occur?*** *(develop the plan, prioritize actions)*
   - *mitigations & contingencies*
   - *recommendations*

Landline Telephone Network

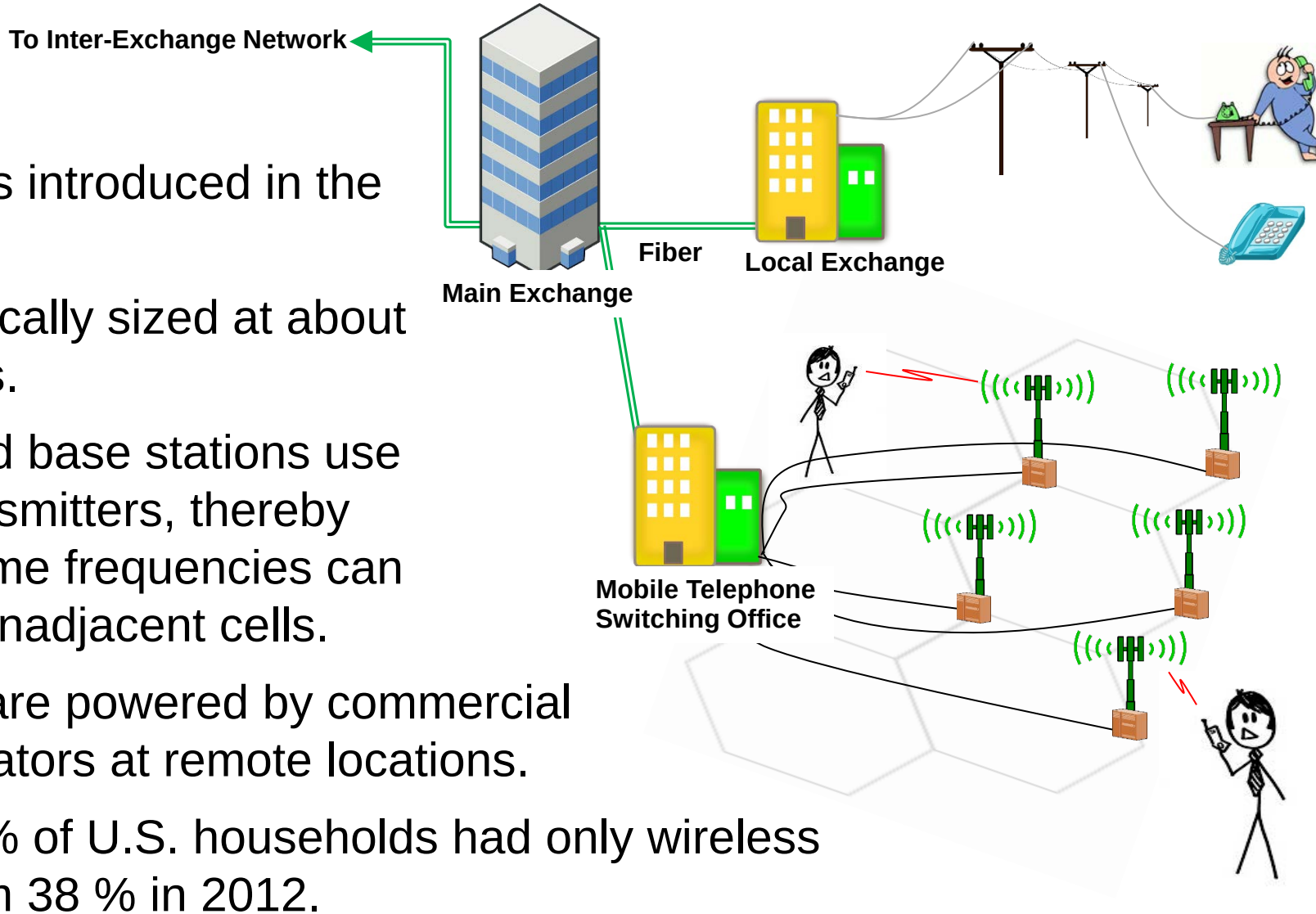
What could fail?



1. Telephone service was introduced in 1876.
2. Public Switched Telephone Network (or Plain Ol' Telephone System -- POTS) is voice-grade telephone over copper.
3. Copper pairs of wire run from your house to the local exchange either directly or through a digital concentrator.
4. Local calls are kept local; Out of area calls are switched to the Inter-exchange Network.
5. In 2013, there were 1.16 billion landline subscribers worldwide.

Cellular Telephone Network

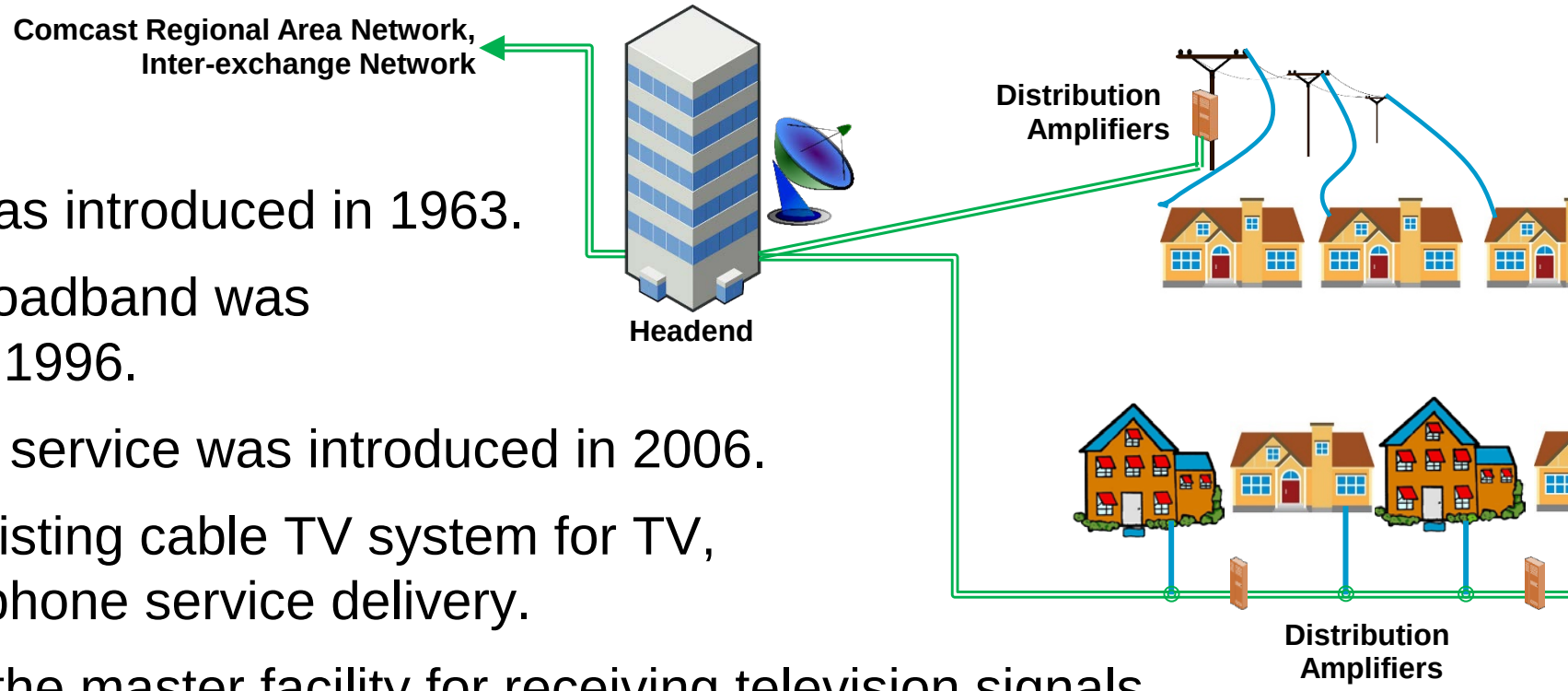
What could fail?



1. Cell service was introduced in the U.S. in 1983.
2. Each cell is typically sized at about 10 square miles.
3. Cell phones and base stations use low-power transmitters, thereby allowing the same frequencies can be reused in nonadjacent cells.
4. Most cell sites are powered by commercial power or generators at remote locations.
5. As of 2015, 48% of U.S. households had only wireless phones, up from 38 % in 2012.

Digital Telephone, Cable Data Network

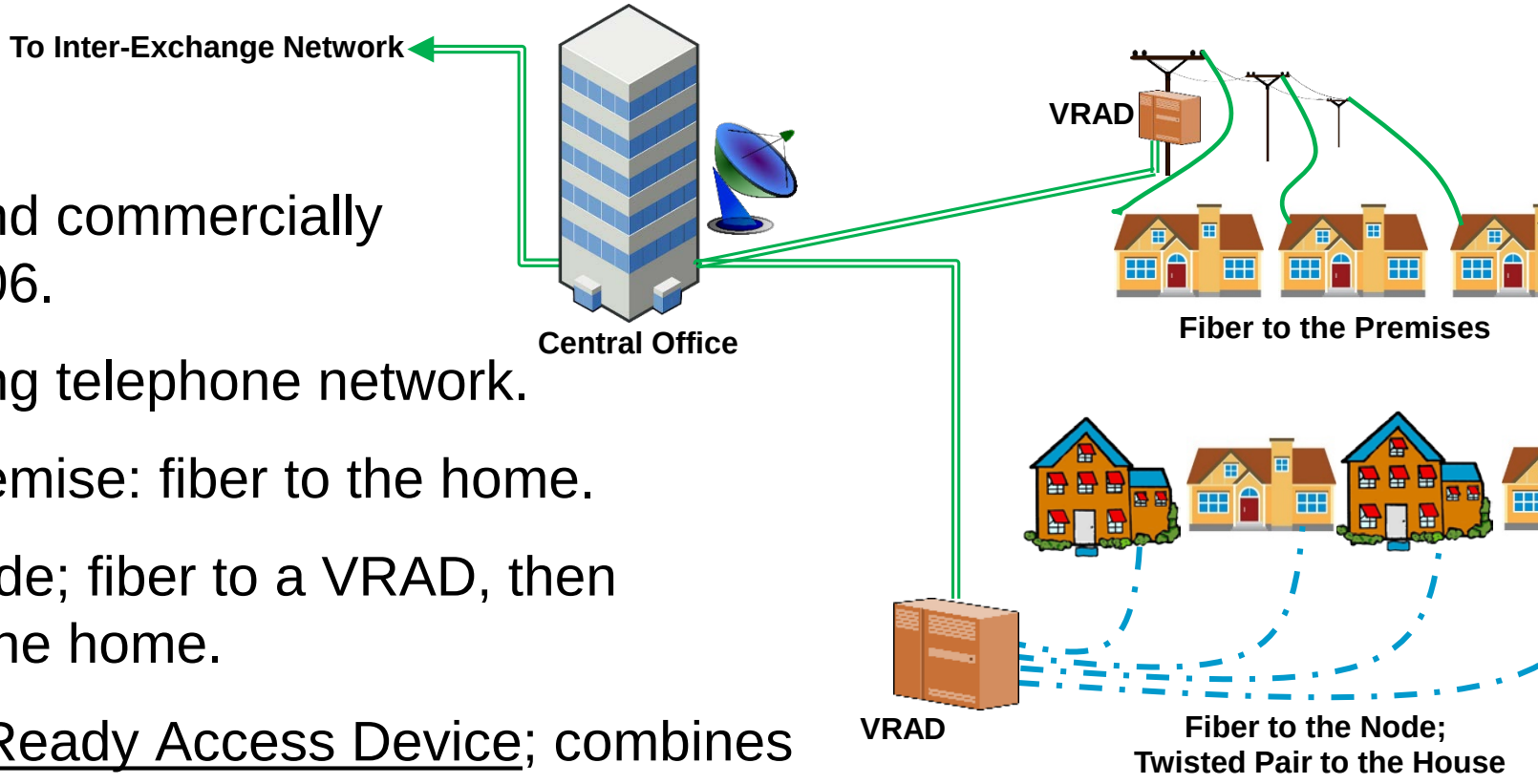
What could fail?



1. Cable TV was introduced in 1963.
2. Comcast broadband was launched in 1996.
3. VoIP phone service was introduced in 2006.
4. Uses the existing cable TV system for TV, data, VoIP phone service delivery.
5. **Headend:** the master facility for receiving television signals for processing and distribution over a cable television system.
6. **Distribution Amplifiers:** ensures a sufficient signal level down the path.
7. **Coax Splitter:** splits signal for TV, Internet, and Phone.

Digital Telephone, DSL Data Network

What could fail?



1. AT&T broadband commercially launched in 2006.
2. Uses the existing telephone network.
3. Fiber-to-the-Premise: fiber to the home.
4. Fiber-to-the-Node; fiber to a VRAD, then twisted pair to the home.
5. **VRAD**: Video Ready Access Device; combines voice and data (DSLAM) with the TV stream to the home.

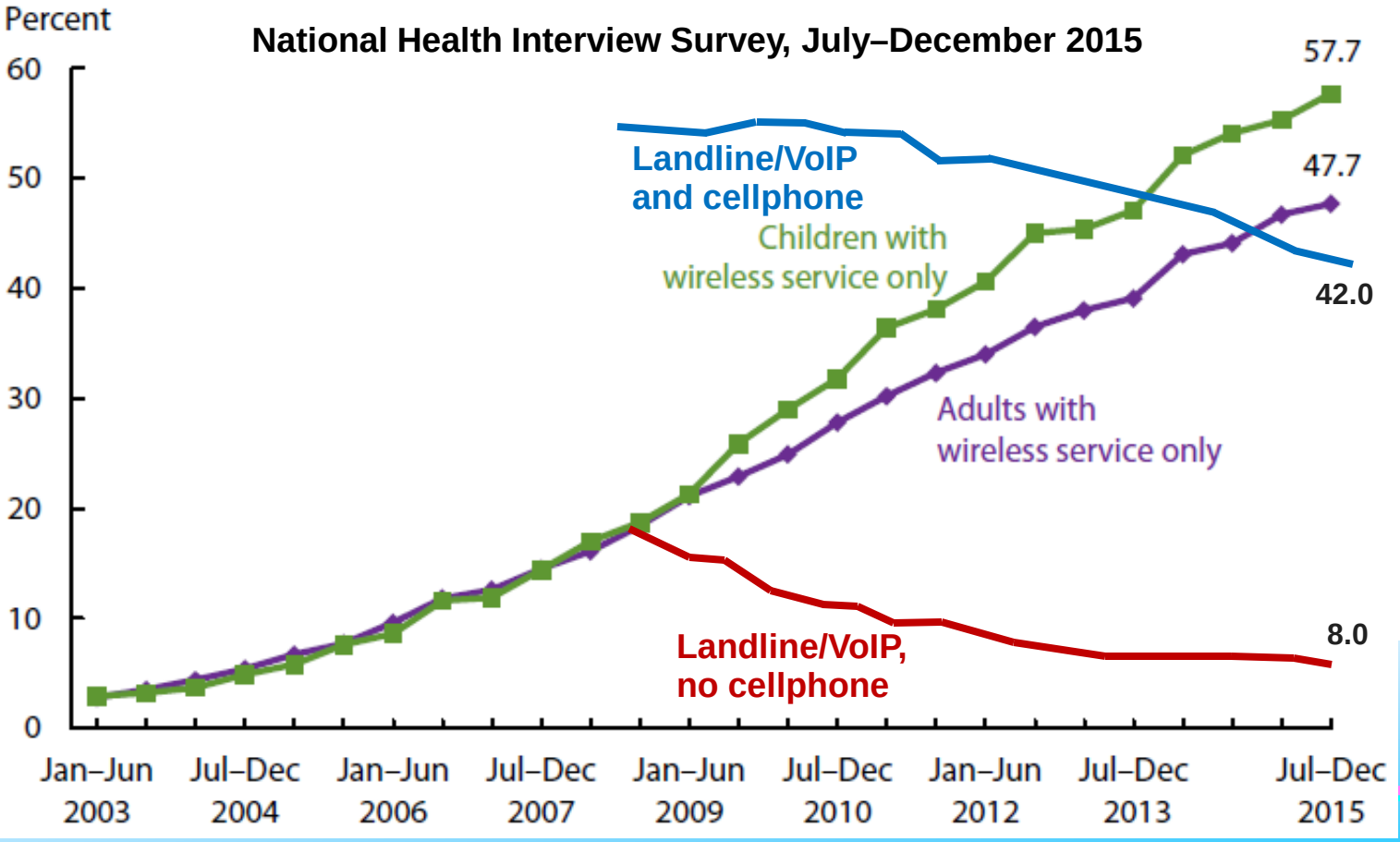
DSLAM: Digital Subscriber Line Access Multiplexer; combines end voice and data traffic into one signal; at the Central Offices or VRADs.

Telephone use… by the numbers

What could fail?

The Jan-Dec 2015 CDC/NHI Survey showed…

- nearly one-half of American homes (48.3%) had only wireless telephones.
- 7.2% have a POTS or VoIP phone only.



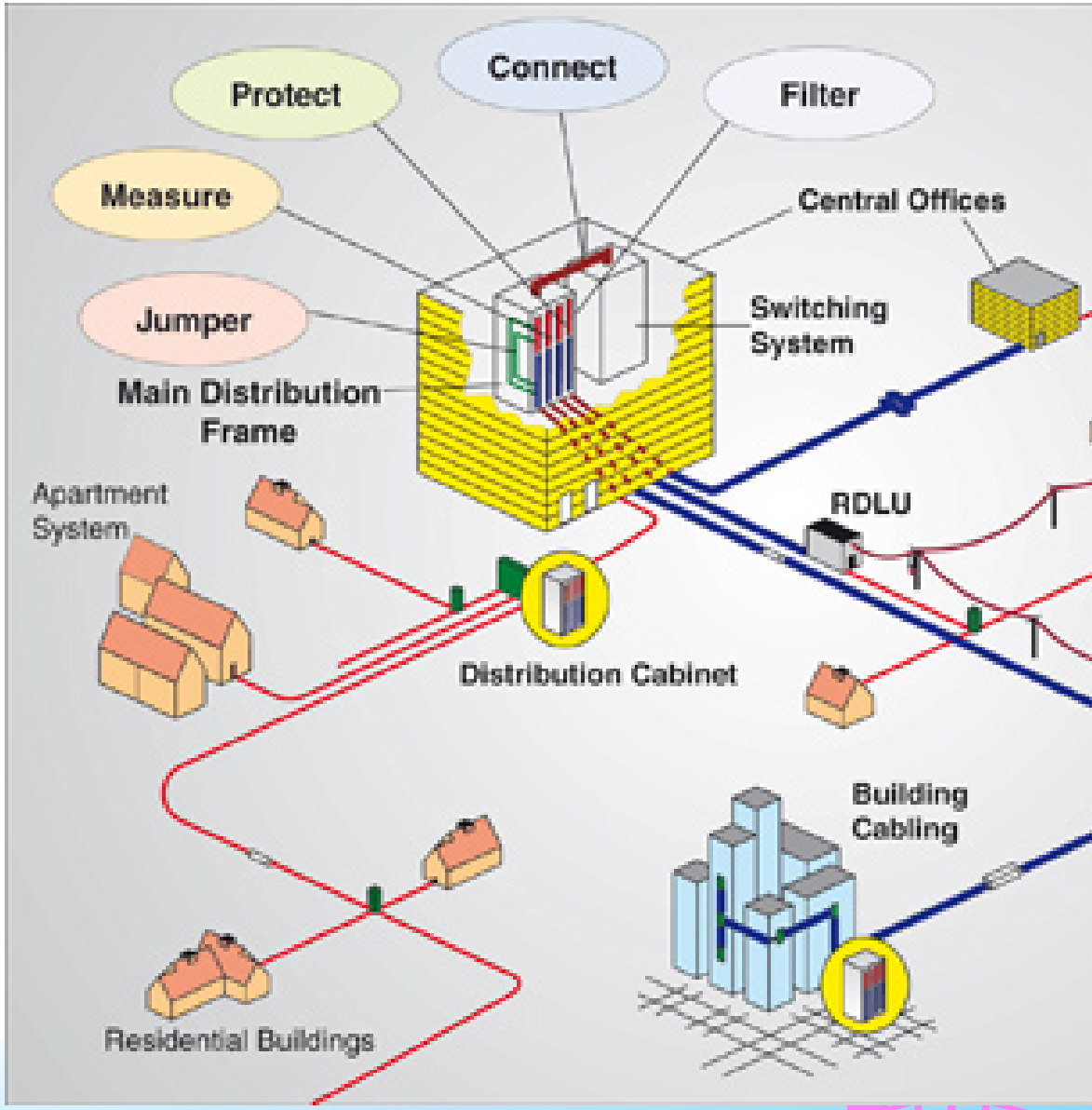
What do they all have in common?

What could fail?

1. **Everything connects together**

   … in the physical world of wire, cable, or fiber sooner or later.

   1. Wired Telephone
   2. Cellular phone
   3. AT&T, Comcast, Sprint, Verizon, other carriers



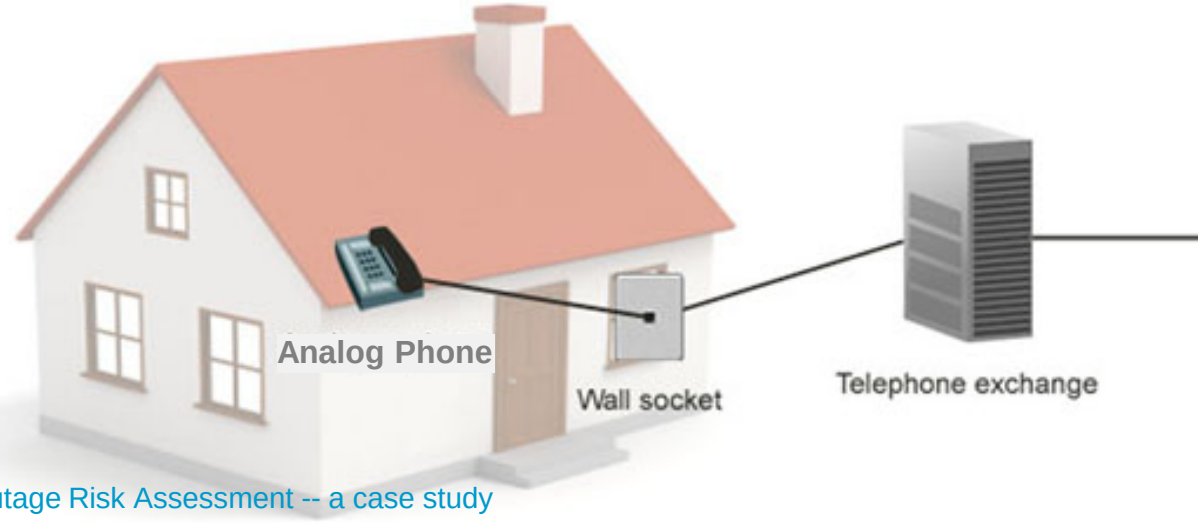
What do they all have in common?

What could fail?

2. All require power to operate

Landline Telephone Network

1. The *phone company powers your phone* with an extensive battery system with backup generators at Local Exchange offices.
2. Operates at 6 to 12 volts DC, ~30ma.
3. 90VAC for the ring signal, as provided by the Local Exchange.
4. During a power failure, wired phones will continue to work,
5. … provided at least one is a “corded” phone.



What do they all have in common?

What could fail?

2. All require power to operate

Cellular Telephone Network

1. Towers, controllers fed from commercial power.
2. Backup batteries are built into most standard power systems.
3. Batteries can last from 2 to 8 hours, depending on their configuration.
4. Generators are also used to avoid service interruption.

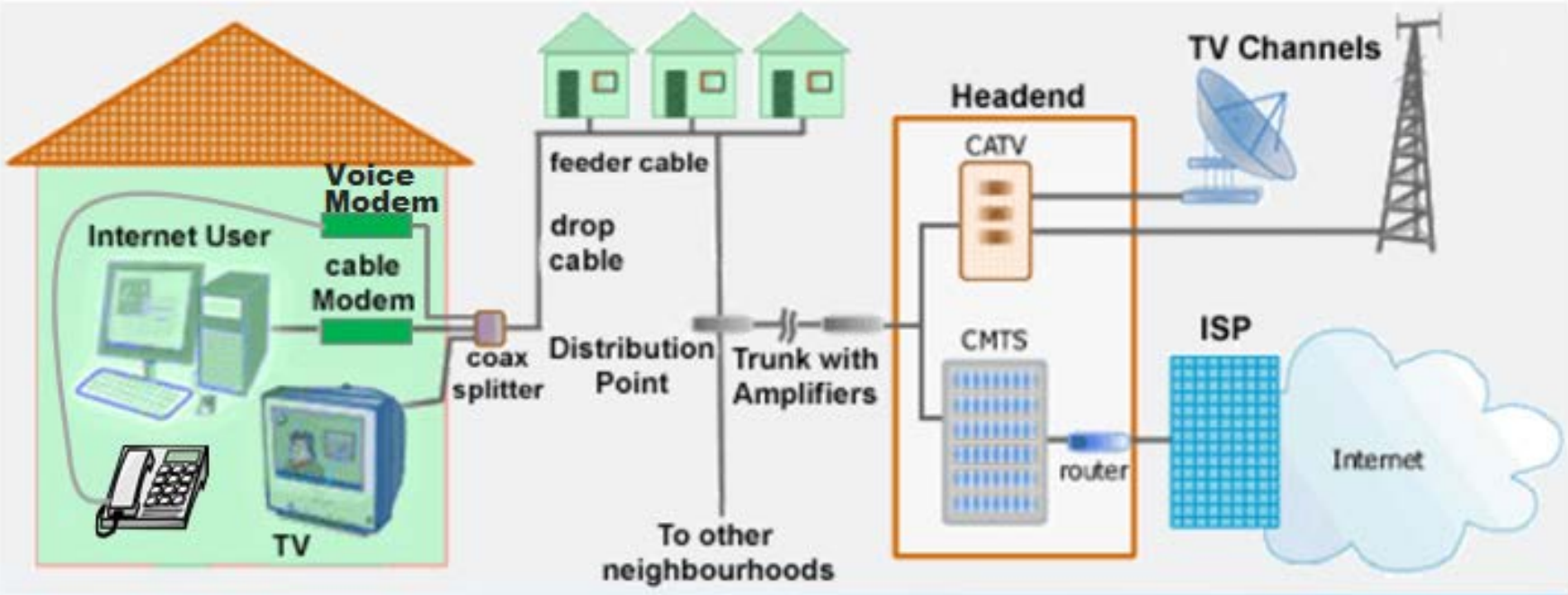
What do they all have in common?

What could fail?

2. All require power to operate

Comcast Digital Network

1. Central Office / Headend: backup generators, batteries.
2. The *voice phone modem* requires a ***backup battery*** to ensure telephone service remains operational during a power outage.

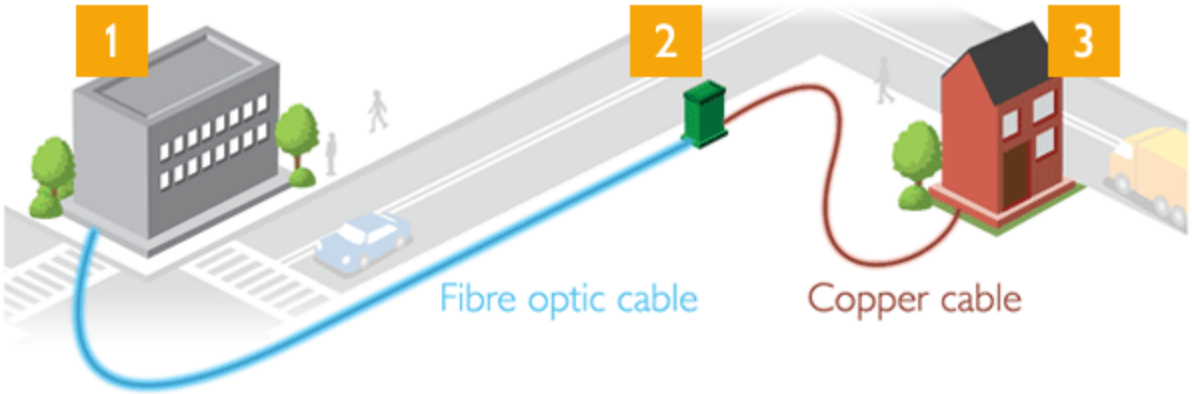


What do they all have in common?

What could fail?

2. All require power to operate

AT&T Digital Network



1. Central Office: gen & battery backup.
2. VRAD Neighborhood boxes; backup NiMH batteries, 2-4 days of power.
3. Wi-Fi Resident Gateway; with phone service, includes a Belkin 12V, 7Ah SLA.

What could cause a failure?

Impacting Events

- **Loss of Power**
  - Power failures – accidental, natural, intentional
- **Loss of Connectivity**
  - Cable breaks – accidental, natural, intentional
- **System Overload**
  - Some out-of-the-ordinary event that causes a lot of people to use the phone at the same time
- **Solar Storms, Solar Flares**

Power loss and Comm outages

What could cause a failure?

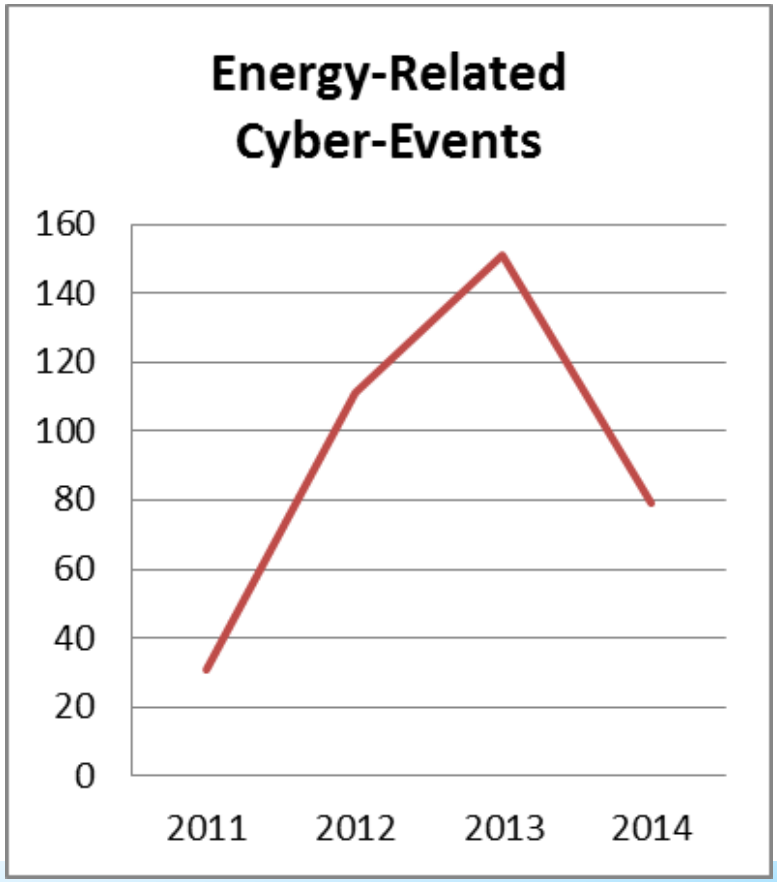
Date	Event	Duration	Impact (people)
Accidental			
November 1965	Northeast Blackout	13 hours	30,000,000
October 2003	Northeast Blackout	1-2 days	55,000,000
September 2011	Pacific Southwest	12 hours	7,000,000
Natural…			
October 1989	Loma Prieta Earthquake	2-3 days	1,400,000
January 1994	Northridge Earthquake	1 week	300,000
September 2005	Katrina	Weeks	3,900,000
Intentional…			
April 2013	Metcalf Sniper Attack	27 days	None
December 2015	Ukrainian Cyber Attack	6 hours	225,000

Power loss and Comm outages

What could cause a failure?

Intentional – Other Reports

- Parts of the U.S. power grid are attacked online or in person every 4 days.
- From 2011 to 2014: the U.S. Department of Energy received 362 reports from electric utilities of physical or cyber-attacks that interrupted power services.



Connectivity loss and Comm outages

What could cause a failure?

Date	Event	Duration	Impact (people)
Accidental			
March 2015	Arizona	12 hours	1,000's
2013	San Juan Islands, WA	10 days	1,000's
March 2012	Morgan Hill	1 day	1,000's

Connectivity loss and Comm outages

What could cause a failure?

Intentional – in the news

- ***April 2009, San Jose***
  Event: Underground fiber-optic cables were cut
  Impact: outage of landlines, cell, and Internet for 10,000's in 3 counties
- ***June 30, 2015, Sacramento***
  Event: three major fiber cables connecting the region were cut
  Impact: disrupted service to Sacramento, Rocklin; ~15 hour outage
- ***July 1, 2015, San Jose***
  Event: Break-in to an underground vault; vandals cut 3 fiber-optic cables belonging to Level 3 and Zayo.
- ***July 15, 2015, San Joaquin County***
  Event: Fiber optic line intentionally cut
  Impact: 9-1-1 outages; 10 hour outage.
- **September 3, 2015, CA North Coast**
  Event: Vandals cut AT&T fiber cable in Hopland
  Impact: disrupted Internet, landline and cellphone service.

Connectivity loss and Comm outages

What could cause a failure?

Intentional – and then the consolidated FBI report-out of even more cable cuts throughout the Bay Area

- July 6, 2014, 9:44 p.m., Berkley. Near 7th St. and Grayson St.
- July 6, 2014, 11:39 p.m., Fremont. Niles Canyon Blvd and Mission Blvd.
- July 7, 2014, 12:24 a.m., Walnut Creek. Jones Road and Iron Horse Trail.
- July 7, 2014, 12:51 a.m., Fremont. Niles Canyon Blvd. and Alameda Creek.
- July 7, 2014, 2:13 a.m., San Jose. Stockton Ave. and University Ave.
- Feb 24, 2015, 11:30 p.m., Fremont. Niles Canyon Blvd. and Mission Blvd.
- Feb 24, 2015 11:30 p.m., Fremont. Niles Canyon Blvd. and Alameda Creek.
- June 8, 2015, 11:00 p.m., Alamo. Danville Blvd. and Rudgear Road.
- June 8, 2015, 11:40 p.m., Fremont. Overacker Ave. and Mowry Ave.
- June 9, 2015, 1:38 p.m., Walnut Creek. Jones Road and Parkside Dr.


Date
of cuts
1 June 6-7, 2014 5
2 Feb. 24, 2015 2
3 June 8-9, 2015 5
4 June 30, 2015 2
Walnut Creek
Berkeley
Twitter
San Francisco
Oakland
San Francisco Bay
San Mateo
Fremont
Livermore
CALIFORNIA
Facebook
Google
Mountain View
San Jose
Apple
580
80
880
680
280
5 miles
Cut to Bits
A sabotage streak targeting northern California's Internet infrastructure is frustrating companies and cops alike. Shown here are sites of fiber optic cable vandalism identified by the FBI.
Source: FBI
THE WALL STREET JOURNAL.

Connectivity loss and Comm outages

What could cause a failure?

Other Notes

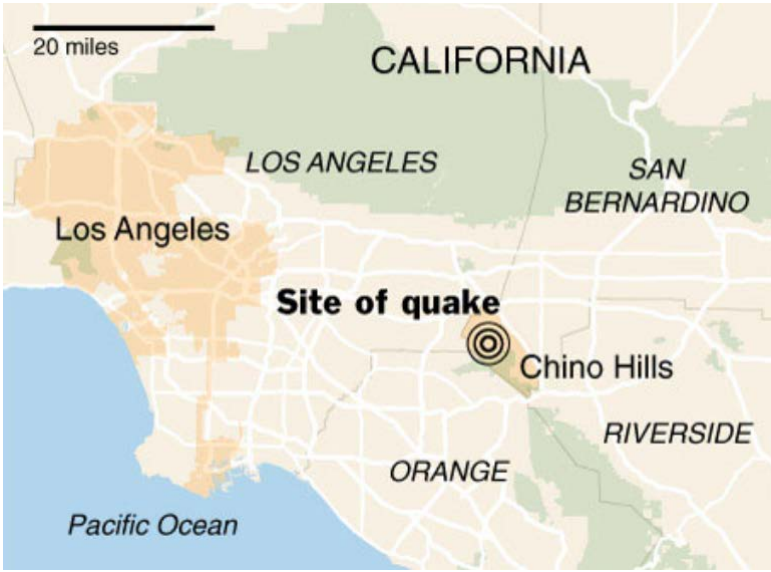
- In 1995, U.S. Commerce Dept's NIST warned that the "power of optical fiber technology is **diminishing the number of geographic transmission routes**," concentrating the flow of information and "resulting in an **increase in network vulnerability**."
- Companies deploy more than **10 million miles of fiber annually** in the U.S., **increase the risk** of damage from backhoes, trench-diggers and shovels.
- The FCC reported that outages on high-capacity fiber lines in the U.S. more than doubled from **221 in 2010 to 487 in 2014**.
- And… are these intentional cable cuts a *Test*?

System Overloads and Comm outages

What could cause a failure?

Natural *(2 examples)*

- July 30, 2008, Los Angeles.
  - 5.4 earthquake, San Bernardino County.
  - **Cell phone lines were jammed**.
  - No damage was reported to the network infrastructure.
- August 23, 2011, Washington DC.
  - 5.8 earthquake, central Virginia.
  - **Cell phone networks were jammed** in Manhattan, Washington D.C., other areas.
  - SMS could get through.
  - Major carriers reported no major problems with their network infrastructure.



Solar Storms and Comm outages

What could cause a failure?

Date	Event	Duration	Impact (people)
September 1859	Solar Storm (Carrington)	Unknown	Unknown
August 1972	Solar Flare, Illinois	Unknown	Unknown
March 1989	Solar Flare, Quebec	9 hours	6,000,000

- In 2012, NASA said the sun unleashed two massive plasma clouds that ***barely missed*** a catastrophic encounter with Earth.
  - "A direct strike could've caused widespread power outages and other damaging effects."
  - "If it had hit, we would still be picking up the pieces 2 years later."
  - NASA also cited research suggesting that there is a 12% chance of something like this happening in the next decade.

Takeaways

What could cause a failure?

- POTS will be gone within 5-10 years.
- Fewer fiber optic cable paths means wider impact when a cable break occurs.
- Intentional cable cuts are up.
- Communications is growing more dependent on distributed (versus central) power sources.
- Cyber attacks on the power grid are also increasing.
  - *The Ukraine cyber-attack pointed out the high degree of sophistication, coordination, and planning that occurred.*

Managing Communications Risks

What can we control?

- Local backup generators
- Local 2-way radio systems
- AM TIS Stations
- Ham Radio
- First responders, local staff and volunteers

What can't we control?

- Power generation and distribution
- Landline telephone network
- Cellphone network
- Digital network

This implies that we should…

apply **Mitigations** here

apply **Contingencies** here

Classifying the risks

How likely is a failure to occur?

Failure Scenarios

Verbal / Two-way, City Gov't, loss of:

1. Wireline telephone only
2. Cellular only
3. Wireline and Cellular
4. Wireline, Cellular, and Satellite
5. Radio, two-way

Verbal / Two-way, City residents, loss of:

1. Wireline telephone, Cellular is available
2. Wireline telephone, Cellular NOT available
3. Cellular when Cellular is the only home telephone service

Verbal / One-Way Broadcast, loss of:

1. Commercial Radio Broadcast
2. Cupertino TIS station
3. Commercial Television Broadcast
4. Satellite Television
5. Cupertino Television Transmission

Written / Digital Messaging, loss of:

1. Wireline Internet
2. Satellite Internet
3. Infralink Wi-Fi Internet
4. City Intranet
5. Amateur Radio Packet

… Plus one or more causes for each

Probability & Seriousness

Approach

Probability: the likelihood of an initiating hazard and impacting event to occur that has an impact on the City.

1. Incredible - Cannot believe that it could occur.
2. Improbable - So unlikely, it can be assumed the occurrence may not be experienced.
3. Remote - Unlikely, but possible to occur in the life of an item; has never occurred.
4. Occasional - Likely to occur sometime in the life of an item; has occurred at least once before.
5. Probable - Will occur in the life of an item; has occurred more than once before.
6. Frequent - Expected to occur frequently; has occurred frequently.

Seriousness: the severity of the initiating hazard and impacting event on the City (government, businesses, and residences).

1. Negligible – no measurable system impact; no impact to the city; minor injuries at worst.
2. Marginal – minor system impact; minor city impact; major injuries to one or more persons.
3. Critical –systems are damaged or destroyed; all city operations are disrupted; loss of a single life.
4. Catastrophic – uncontrolled environmental impact; multiple loss of life.

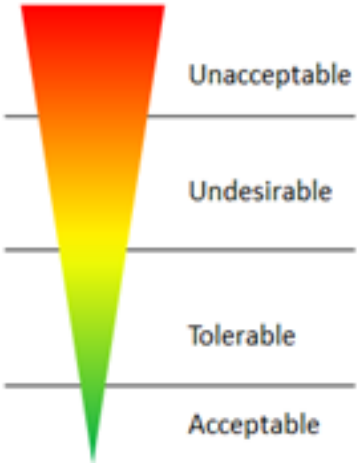
reference: *IEC 61508 Standard*; International Electrotechnical Commission

Classifying the risks

Approach

Risk Classifications provide a means for applying thresholds for taking action to address risk. For this report, the following thresholds are used.[26]

- *Class 1: Unacceptable* in any circumstance.
- *Class 2: Undesirable:* Tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained.
- *Class 3: Tolerable* if the cost of risk reduction would exceed the improvement.
- *Class 4: Acceptable* as it stands, though it may need to be monitored.



Seriousness

Probability	Negligible	Marginal	Critical	Catastrophic
Frequent	2	1	1	1
Probable	3	2	1	1
Occasional	3	3	2	1
Remote	4	3	3	2
Improbable	4	4	3	3
Incredible	4	4	4	4

Classifying the risks

How likely is a failure to occur?

1. **Tested 18 failure scenarios**
2. **Identified 43 risks for Cupertino**
   - Unacceptable: 7 (16%)
   - Undesirable: 9 (21%)
   - Tolerable: 27 (63%)
   - Acceptable: 0

Example Risk Assessment

3. Loss of Cellular when Cellular as the only home telephone service. As of 2013, 91% of surveyed adults own a cell phone. For 48% of the population, Cellular is the only phone system they have.

Failure	***Cause***	***Probability***	***Seriousness***	***Risk***	***Mitigation***	***Cont***
R19. Cell Phone battery runs out of charge (smartphone: <24 hours).	Extended power outage at home.	Occasional (4) Likely to occur	Negligible (1)	Tolerable	Ensure you have a cell phone car charger.	Not
R20. Cellular is the only phone available. Cell Towers loses power; backup batteries are exhausted (8 to 48 hours).	Extended power outage caused by natural or intentional events.	Occasional (4) Likely to occur	Critical (3)	**Undesirable**		Not Com Assis

   a. ***Impact of Loss:***
      i. Inability for residents to dial 911 to report an emergency or request help.
      ii. Inability to receive Cupertino Alert System and AlertSCC notifications.

Recommendations for Cupertino

What do we do when it does occur? – mitigations & contingencies

1.3 Recommendations for the City

1. Move the TIS station to a more secure facility, or retrofit City Hall.
2. Complete the TIS backup battery upgrade.
3. Improve the reliability of the City Hall backup generator.
4. Define the Public Information Outreach plan.
5. Define the Community Emergency Assistance Request Intake plan.
6. Complete the build-out of the Cupertino Emergency Intranet (ARKnet).
7. Perform testing of specific backup communications measures.
8. Explore other emerging technologies and means for communicating with the community during an emergency.

1.4 Recommendations for the Community

9. Public Outreach to the community:
    a. Ensure residents have a car cell-phone charger.
    b. Ensure they have at least one corded phone for home wireline telephones.
    c. Ensure every home has a portable AM/FM radio.

Some light reading

1. *Inside the Cunning, Unprecedented Hack of the Ukraine's Power Grid*, 3/3/2016, Kim Zetter, Wired
2. *American Blackout 2013*, National Geographic, 1:27 min
3. *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*, Ted Koppell, Crown Publishers

Thank you!

Questions?