

Alexander Do, UC Berkeley
Joseph Tavormina, Tavormina and Associates Inc.
Revision date: 14 Febuary 2006

PCT Communication Interface Questions and Issues

This document builds a framework with which to investigate the PCT communication interface, independent of whether it is 1-way or 2-way. The operational and functional requirements needed for this discussion are still under development; however the primary focus will be on the specific application of dispatching demand response (DR) for both emergency and economic events to PCT's. The first section of the document poses questions and raises issues in the communication interface definition and design which are universal to 1-way or 2-way systems. A 2-way network can enable the collection of additional customer data and value-added services, but presents additional issues pertaining to security and network topology; a section presenting issues specific to 2-way systems is presented following the primary framework. The purpose of this framework is to summarize a key set of critical questions and issues which need to be applied to each possible candidate solution.

The framework is a compressed version of the OSI (open systems interconnection) 7-layer reference model for open communications which has been adopted by the computing industry as a standard "thought model" for designing communications and networking systems. In this implementation, it's been reduced this to 3 layers for reasons of simplicity:

- **Application**
 Issues related to exchanging data for the PCT application, including demand response functionality and security
(amalgamating the OSI Application and Presentation layers)
- **Network**
 Issues related to topology of PCT operation and the transport of information *(in some way including OSI Session, Transport, and Network layers)*
- **Physical**
 Issues stemming from physical connection to the network *(amalgamating OSI Data Link and Physical layers)*

	OSI Model		Discussion Framework	
	Data unit	Layer		Function
Data		Application	Network process to application	Application
		Presentation	Data representation and encryption	
Segments		Session	Interhost communication	Network
		Transport	End-to-end connections and reliability	
Packets		Network	Path determination and logical addressing (IP)	
Frames		Data link	Physical addressing (MAC & LLC)	Physical
Bits		Physical	Media, signal and binary transmission	

Universal Questions and Issues for the Communication Interface

For each layer discussed, a list of questions and issues believed to be necessary in evaluating a candidate solution for 1-way communication. The questions and issues are numbered, such that analysis can be presented for each one in separate documents.

1. Application

a. **Downlink Security: What are ways in which DR data can be authenticated and possibly protected (encrypted)?**

The solution for this interface must provide some kind of mechanism to authenticate the source of the DR signal and possibly protect its contents. It is assumed that for most emergency and economic dispatches, additional security above authentication is not needed, though some utility-specific DR programs and value-added services may require confidentiality.

b. **Information Model**

A common information model for DR dispatch functionality must be developed and agreed upon by the manufacturers and distribution to ensure compatibility and minimum functionality. This information model must also be translated digitally over the communication medium through a standardized protocol.

2. Network

a. **Infrastructure, Operational, and Maintenance Costs**

Is the infrastructure necessary to support PCT receivers at the traditional location of use (on a wall inside the residence) already existing or must it be built up or expanded? What is the cost to build or expand this infrastructure? What is the cost to operate and maintain the infrastructure 24 hours/day x 7 days/week x 365 days/year, and can it be supported for the next ten years?

b. **Network Capacity**

How much data needs to be carried by the network to support DR dispatch, system health (heartbeat messages), and other data applications (clock synchronization, pricing information, etc.)?

c. **Connectivity**

The PCT should be able to determine if it is not connected to the broadcast network so that a customer can be alerted that there is a problem. One example of this is the inability to receive a heartbeat signal.

d. **Error Detection and Correction**

How are errors in data transmission detected and corrected? What is the overall strategy for error detection and correction (e.g. In 1-way applications is it OK if say 1% of the PCT's do not receive the correct data transmission? Will there be rebroadcasts and multiple attempts to communicate with all PCTs?)

e. **Membership: How could various manufactured appliances and devices establish membership?**

The PCT needs to understand its membership to parent entities to obtain a desired granularity of demand response. This membership information can be accounted for through network addressing or some kind of addressability information embedded in a universal broadcast. For this application, a membership hierarchy

which matches the topology of the electricity distribution system is desired. Title 24 requires one primary level of membership identification:

- i. With the distribution substation (by implication, membership to the distribution utility is accomplished)

Additional PCT membership properties may be desired:

- ii. With the feeder
- iii. With program enrollments (various DR and load control programs offered by the utilities and munis for economic response)
- iv. With the customer (AMI/EMCS system)

3. Physical

a. Frequency Band and Channel Plan

For a wireless system, a frequency band must be chosen within licensed (i.e. AM radio, FM radio, television, PCS communications, paging) or unlicensed (i.e. 900 MHz, 2.4 GHz, 5.8 GHz) bands. The bands will have different attenuation characteristics and sources of interference, each addressed in separate sections below. The unlicensed ISM bands for wireless communication are limited to a fixed number of channels, which must be distributed among the broadcast infrastructure in 1-way applications. Though the primary 1-way candidates already leverage existing infrastructure which has already been built to address channel plan issues, there are still questions to be answered. For example, in the FM scenario, the minimum number of carrier channels per geographic region must be considered, and then the PCT receiver must be able to identify the best channel to use.

b. Radio

i. Cost

What is the additional cost to the bill of materials (BOM) of the radio subsystem, accounting for required components and processor upgrades?

ii. Overhead

What is hardware and software burden to the PCT's core processor?

iii. Data Rate

What is the practically attainable rate of data transfer for this radio?

iv. Receive Sensitivity

The receive sensitivity specifies how faint a signal (low in power) a receiver can successfully receive a signal. The smaller the receive sensitivity the better. The receive sensitivity, combined with knowledge of the transmitter strength, path loss, and transmitting and receiving antenna gains, gives a general indication of radio range.

v. Range

What is the maximum free-space radio range (signal power falls off as R^2)? What is the practical radio range in the target environment, given sources of signal attenuation such as concrete or other building materials (signal power falls off as R^4 in urban outdoor environments, or even faster within buildings)? What is the standard deviation signal power vs. distance in the target environment?

- vi. **Power-use (accounting for duty-cycle assumptions)**
Power use will depend on network configuration as well as the receiver hardware. Under certain scenarios for powering on the receiver, what is the expected average power use for the receiver?
- c. **Antenna**
A practically realizable, inexpensive PCT antenna at the correct frequency and with the required bandwidth (including manufacturing tolerances) will be needed to make the system work. As the frequency of the signal increases, the wavelength, and consequently ideal antenna size, decreases. Another variable is the antenna gain that is needed to make the system work properly. In general gain decreases with size, from +6 dBi for a half-wavelength antenna to perhaps -10 to -20 dBi for an antenna which is a tenth of a wavelength.
- d. **Noise, Reflections, and Interference**
Sources of electromagnetic interference and signal reflections will affect the signal-to-noise ratio. Reflections of a radio transmission can lead to multiple signals arriving at the receiver with some level of multi-path delay between them. This can lead to inter-symbol interference, which can impair radio operation. However, both the FM broadcast and the IEEE802.15.4 radio systems are quite accommodating of multi-path propagation and delay spread. Common sources of electromagnetic interference, such as cordless phones, microwave ovens, Wi-Fi radio transmitters, and iPods with FM converters can also be cause for concern. A noise rejection scheme can be chosen – frequency hopping spread spectrum vs. direct sequence spread spectrum vs. ultra wideband – to improve the system performance. How will the PCT know it is experiencing radio interference, and how will it notify the user?

Additional 2-Way Specific Issues

In addition to the issues mentioned above, 2-way systems present an additional set of key questions and issues which are documented in this section.

1. Application

- c. **Uplink Security: In 2-way applications, what are the ways in which data collected from PCTs are validated and protected from malicious spoofing, are kept private and protected from data theft?**

Whereas downlink DR data represents “one-to-many” transmission of information from a single (trusted) source, uplink radio transmissions from PCTs over a mesh network represent “many-to-many” transmissions of information that may need to be validated at each point of entry into the communication network. The additional (above acknowledgement) data transmitted back to the distribution utilities, as desired to support the business cases being considered, adds considerable complexity to security and privacy issues. Privacy laws will have a considerable influence on the system design for transmission of customer use data. For example, **FERC regulation** for any controllable load amount greater than 300 MW mandates a certain level of data protection¹.

¹ ???

2. Network

f. Network Capacity for Uplink

Some solutions may be asymmetric in the data capacity for downlink vs. uplink transmission. How much data needs to be carried in 2-way (uplink as well as downlink) applications?

g. Network Topology

Is the network topology a star, a structured mesh, an ad-hoc mesh, or other? Are successful data transmissions dependent on the relay of data packets through secondary radio nodes? If so, are these nodes part of the communication infrastructure, or not? How are secondary relay nodes powered? How does the relay of data packets affect battery life?

h. Error Detection and Correction for Uplink

How are errors in data transmission detected and corrected? Are acknowledgements of correct data transmission needed (in 2-way applications)? Will the PCT make multiple attempts to transmit to the gateway?

3. Physical

e. Access Method

Is the radio access method (for 2-way applications) based on reserved capacity (e.g. time slots), or is random access based on contention (and the possibility of packet collisions) employed? How does the access method affect network capacity, overhead in data transmission, and the likelihood of successful data transmission?

f. Radio

i. Transmit Power

In a 2-way application, the radio will consume a considerable amount of power for transmission as well. Generally, the power to the transceiver in wireless nodes is held constant, while the duty cycle is adjusted to meet the power budget.

ii. Range

Given the transmit power and antenna gain, what is the maximum range for uplink transmissions?

g. Power-use (accounting for duty-cycle assumptions)

Power use will depend on network configuration as well as the receiver hardware. Under certain assumptions for data transmission, what is the expected average power use for uplink transmissions?

h. Channel Plan

How many separate non-overlapping radio channels can be used to create subnetworks (particularly in 2-way applications)? What geographic separation is needed in order for radio channels to be reused in different regions?

RDS Analysis against Communication Interface Questions and Issues – DRAFT

Alex Do, UC Berkeley

25 April 2007

Version 1.0

The information in this document, which addresses the Communication Interface Questions and Issues for the FM/RDS technology, was obtained from a combination of technical documentation and interview with industry representatives and experts.

Application

1.a. Downlink Security

Authenticated communication is not inherently provided by the RDS transport layer and a message authentication and tamper detection scheme needs to be built into the payload. The Title 24 PCT Reference Design Working Group is responsible for defining acceptable solutions for these requirements, and currently has a recommendation on proposal². A key-hashed message authentication code (HMAC) has been recommended as a solution for message authentication and tamper detection. A more detailed discussion of security issues is available in the Security section (Section 4.6) of the Reference Design document.

1.b. Information Model

An implementation of the high-level data model created by the Reference Design Working Group will have to be mapped into a digital format for use on RDS networks by the network operator or some industry alliance. The mapping should be done as efficiently as possible in regard to bit-lengths in consideration of the data rate limitations of RDS.

Network

2.a. Infrastructure, Operational, and Maintenance Costs

- Infrastructure

When discussing infrastructure, we need to consider two segments of the network: the physical, transmitting infrastructure, and the data network which delivers data to the broadcast stations.

The physical infrastructure for the RDS solution is not expected to be of significant cost to the State. RDS leverages the existing commercial FM radio infrastructure which already covers almost all populated areas of the State, possibly excepting small groups of residents in remote mountainous areas. By default, a particular FM broadcaster may not have the capability to transmit dynamic RDS data; this is enabled with the addition of a special encoding unit and wide-area connection to a data stream. According to e-Radio USA, the retrofit of a broadcaster which does not have RDS capability is estimated to cost \$10,000 to \$15,000³, though depending on existing equipment it is believed that the upgrade costs may be considerably less. Market data about the penetration of RDS among existing operators has been difficult to obtain, but a frequency scan from

² The latest version of the PCT Reference Design, which includes the PCT security strategy recommendation, can be downloaded from <http://sharepoint.californiademandresponse.org/pct/default.aspx>.

³ Rick Boland, Letter to Title 24 stakeholders titled "Questions on AM/FM Infrastructure for Title 24 Demand Response Programs," March 31, 2006.

Berkeley, CA revealed 18 Class B⁴ operators in the San Francisco Bay Area (and at least 4 more local, lower-power, Class A operators) with at least basic (static) RDS functionality, implying that physical infrastructure upgrades for the primary media markets could be largely unnecessary. Class B FM stations have FCC interference-protected service areas that generally reach up to 40 miles⁴, and in practical reception can go much farther. It has been estimated by Jackson Wang of E-Radio USA that 90% of the 594 licensed FM stations⁵ in California already have static RDS functionality. At least 22 of ClearChannel's FM stations in California already use dynamic RDS data (which is remotely managed) for sending automotive traffic information.

The existing physical infrastructure is believed to be highly robust and reliable; commercial FM transmitters are heavily secured, can withstand some types of natural disasters and have on-site redundant power generation in case of power outages. Many broadcast stations also have auxiliary transmitters which can be used if the primary transmitters fail or are undergoing maintenance. The communications link from the broadcast station to its transmitter is also built with redundancy; major transmitters are believed to have triple-redundancy, employing a T-1 line as the primary link and using microwave line-of-sight, optical line-of-sight, and satellite communications as backups.

The data network for this solution is more questionable and poses a potentially multi-million dollar cost to the state. Radio stations may not have a broadband data link to an external source, and the data will need to be managed by a central entity. The most practical solution is to hire a large data operator which can and/or has explicitly built a private network accessing a large distribution of affiliate transmitting stations. E-Radio USA is one company which has built IP-based networks which allow them to route and manage data appropriately through separately owned radio stations. Some larger radio networks, such as ClearChannel, have built up their own internal networks as well. These companies can develop a secure socket or portal connection for CA utilities or some other agency to submit DR data for transmission. The capital outlay costs for their access to the stations are expected to be factored into the operational prices quoted to the State or utilities; early order-of-magnitude estimates are listed in the next section, Operation and Maintenance.

However, the solution of contracting with a single, large operator may not be acceptable if the State would like more players to get involved, or if smaller, local stations necessary for extending coverage to remote areas are unwilling or unable to connect to a private network. In this case, the State, through some agency, may want to create an open, client-server architecture for hosting DR data so that any individual radio broadcaster or large network operator may participate. The concept is similar the architecture of the OpenADR system: a secure server hosts DR status data which is updated in realtime, and clients can be installed at any involved broadcast station which poll the server and automatically re-transmit the appropriate dispatches over RDS when necessary. In this

⁴ FCC's definition of FM Station Classes: <http://www.fcc.gov/mb/audio/fmclasses.html>. Class B is the highest power transmitting class allowed in California.

⁵ FCC's FMQ FM Radio Database Query: <http://www.fcc.gov/fcc-bin/audio/fmq.html>. Search parameters were for all full service FM licensed records in CA.

manner, a State agency could independently contract FM stations (regardless of affiliation) and equip each one with a client which links the station to a central source. This option effectively achieves the same functionality as the first strategy, but with an added benefit and complication. The benefit is that anyone would be able to participate (**note: does the CPUC have any jurisdiction in this area?**). The complication is that some particular State agency would then be charged with maintaining a *secure* network service and a number of contracts with independent station operators. This option also poses an unknown, yet significant – possibly multi-million dollar – cost to the State.

- Operation and Maintenance

The estimated costs for operation are primarily dependent on the number of stations required to support the application statewide. It is believed that data requirements (RDS utilization discussed in the following section) are so low that network access to the station is the primary driver for cost. According to industry experts, the cost of TMC/Navteq's RDS utilization (20-25% of data capacity) from a single station is in the low tens-of-thousands of dollars per year. E-Radio USA has estimated that 30 to 35 stations could be required across the state, preliminarily estimated to cost \$5 Million per year to support (this includes data and security management)⁶. The actual number of stations required must be determined through careful network planning and design; the UC Berkeley team is proposing a field experiment which can determine some of the requirements for network design.

2.b. Network Capacity

The required network capacity is expected to average less than 1% of RDS utilization annually. This has been estimated from three primary functions: dispatch, clock-synchronization, and heartbeat. The total network utilization is primarily determined by the heartbeat function due to its high frequency.

The RDS medium uses a “group” as a basic transport mechanism for data which can carry as much as 37-bits fully loaded. In our assumptions, we are using each group to carry 4-bytes of raw data and using the rest of the capacity for fragmentation overhead. The medium is capable of 11.4 groups per second, and assumptions about data requirements for the PCT application in terms of required groups is presented in this section.

Question: what are the payload impacts of HMAC and ECC encryption?

Note: HMAC sizes are currently estimated at 128 bits, or 16 bytes, or 4 additional groups in the case of RDS. It is assumed that in general 20 bytes, or 5 groups, would be sufficient for the average PCT command.

- Dispatch

The primary use for the DR signal will be to curtail loads, and it is expected that the frequency of these events is rather low (5 days per year). When a curtailment is required, it is expected that **9 to 10 groups** could be required per DR dispatch. Depending on localization requirements (for example one radio transmitter might support 20 different

⁶ Rick Boland, Letter to Title 24 stakeholders titled “Questions on AM/FM Infrastructure for Title 24 Demand Response Programs,” March 31, 2006.

load groups), multiple permutations of a dispatch message could increase network utilization. Also, to ensure reliability, re-transmission of the dispatches may be required. After accounting for the possible amount of data involved in a dispatch, these events are of such low frequency that they do not affect general network utilization requirements on an ongoing basis, though the broadcast contracts need to give these types of data priority over other data in the system queue; DR dispatches may require highest-priority network utilization for 10 to 20 minutes during critical periods to ensure reliability.

- Clock-synchronization

Clock-synchronization is required by the DR application and also serves as a non-cryptographic security measure. The update frequency will depend on the recommendations of the PCT Reference Design Working group as a result of detailed security analysis. The RDS protocol does have a built-in clock update function which many stations currently use on a frequent basis, meaning that no additional data capacity could be required. However, if any existing difference between the utility's and ISO's system time and the broadcaster's time is unacceptable, then additional network utilization of approximately **XX groups per** synchronization would be required. The number of daily updates depends on the recommendations of the PCT Reference Design Working Group's security analysis.

- Heartbeat

It is expected that this function will dominate the data capacity requirements of the network. A system "DR" heartbeat is required for two functions: so that the PCT can identify connectivity status, and so that the PCT can identify appropriate FM stations to listen to during initial setup. Frequencies of 4 to 60 times per hour have been discussed for this. Individual "3A"-type groups used as heartbeats can identify that a station supports the DR application and can also carry additional information about supported utilities or substations, allowing for station diversity within geographic areas. A heartbeat frequency of 1 group per minute represents 0.15% network utilization.

2.c. Connectivity

PCT's using RDS must scan the band to find RDS-enabled stations which are carrying DR functionality during some kind of initialization or setup phase. The receivers can identify very quickly whether or not connectivity to any stations in the band can be established by checking signal strength and RDS block statistics. To identify connectivity with DR-carrying stations, the receiver must reliably receive the heartbeat signal. This can be done with the use of "3A" ODA group identification blocks built into the RDS specification.

2.d. Error Detection and Correction

RDS natively handles some amount of error detection and correction within the protocol. Each block in the protocol consists of a 16-bit data segment and a 10-bit checkword. The checkword allows the RDS decoder to identify an error, and determine whether it is capable of 1-bit, 2-bit, or 5-bit error correction or if the data block is unrecoverable.

From the RBDS Specification⁷:

The error-protecting code has the following error-checking capabilities:

- a) Detects all single and double bit errors in a block.

⁷ National Radio Systems Committee. *United States RBDS Standard*, April 9, 1998.

b) Detects any single error burst spanning 10 bits or less.

c) Detects about 99.8% of bursts spanning 11 bits and about 99.9% of all longer bursts.

The code is also an optimal burst error correcting code and is capable of correcting any single burst of span 5 bits or less.

2.e. Membership

Membership for the 1-way RDS system is expected to be accomplished through addressing at the data layer (refer to PCT Reference Design document). The RDS specification also contains a “radio paging” function but it is not expected to be viable for DR applications. The membership function is highly dependent on the installation scenario, but it is likely that the installer or customer will need to enter an activation/registration code into the PCT which sets the utility identification code, substation code, and possibly feeder and billing codes.

Physical

3.a. Frequency Band and Channel Plan

Since RDS leverages commercial FM radio, the overall frequency band and channel issues are accounted for in FCC procedures. There are 101 channels allocated for FM transmission in the US, from 87.9 MHz to 107.9 MHz. One key question which will affect the final system design is, ‘what number and characteristics of (distance, power, antenna height above average terrain, etc.) FM stations is needed to support a given geographic region?’ Preliminary testing by UC Berkeley of RDS receivers installed at residential dwellings implies that some level of station diversity may be required for locations with poor FM reception to mitigate variations in performance within a particular site (i.e. a particular station might work well in the kitchen but not the living room). A long-term study for network planning is recommended if RDS is selected by the State as the 1-way DR standard.

3.b.i. Radio Cost

The additional BOM cost for an RDS subsystem is expected to cost less than \$3 per PCT. This includes an integrated tuner/receiver/decoder chip, a crystal, passive components, and an antenna. This budgetary pricing of an RDS chip at 1-million pieces is \$1.70⁸, and the external components are expected to total an additional \$0.20 - \$0.30 (at lower volumes, these costs are expected to be higher).

3.b.ii. Radio Overhead

The radio subsystems currently available (mentioned in 3.b.i.) tend to require a host processor which can support standard digital communication protocols such as I²C or SPI. The RDS chip itself is not expected to be a processing constraint on the host processor, as cryptographic capabilities required will dominate this requirement. NRE efforts will need to go into developing a hardware interface driver which manages the operation of the RDS chip; the software base necessary for this driver should not pose a major burden to the PCT.

3.b.iii. Radio Data Rate

⁸ Budgetary pricing from NXP for a TEA5764HN. Smaller, and therefore lower-cost, integrated receiver/decoder chips are expected to be produced by NXP and other chip-makers such as Silicon Laboratories, Comlent, and RDA in coming quarters.

The RDS system operates at 1187.5 bps, but has a large amount of overhead for error correction and radio station information. The achievable data rate, accounting for this overhead, is closer to 300 bps.

3.b.iv. Radio Receive Sensitivity

Reliable information about the required dBm (power) or dBuV (field strength) for practical RDS performance is not available. However, the UC Berkeley team is designing an experiment to determine if a statistical model for reliability under various parameters, such as field strength, location, etc.

Note: Include notes from e-Radio testing

Note: Include statistical data from prelim UCB experiment

3.b.v. Radio Range

The practically achieved range of licensed FM radio transmission ranges vastly from 1 to 100 miles and is primarily dependent upon the location and height (both relative to ground and average terrain) of the transmitting antenna and the transmitting power, but also varies with local topography from geological and manmade structures. The areas of primary interest for A/C load curtailments with PCT's, the Central Valley, have mostly flat terrain and can therefore support a large service territory. One particular station located near Fresno, KSKS, has a protected service contour extending over 70 miles in some directions⁹, yielding an approximate 15,000 sq. miles of coverage and could possibly support nearly 300,000 housing units¹⁰.

3.b.vi. Radio Power Use

The RDS chips available typically use 16 mA at 2.7 V while powered on. Title 24 requires 24VAC power available to the PCT, so good power management is only a concern when the PCT is running in battery backup mode. The PCT processor could cycle the power of the receiver if the DR dispatches are broadcast in established intervals; the RDS protocol includes a clock synchronization scheme which is accurate to the second and can be leveraged for this purpose.

3.c. Antenna

Ideally, a directional Yagi antenna at the residence oriented toward the transmitter will provide the highest signal gain and the most reliable signal. This type of antenna, however, is quite large and would cost anywhere from \$50 to \$200. Smaller antennas, such as a 54" dipole or 30" whip antenna, are *much* less expensive (on the order of tens of cents) and can be used to achieve reliable connection. However, all of these antennas are physically large compared to the PCT and would need to be connected via an external connector. A connector for an external antenna has not yet been discussed as a requirement of the PCT.

Integrated antennas which do not extend beyond the PCT enclosure have also been developed in the industry and are currently being evaluated for performance. Though internal antennas would

⁹ FCC's FMQ FM Radio Database Query entry for KSKS, FacilityID 26924:

<http://www.fcc.gov/fcc-bin/fmq?list=0&facid=26924>

¹⁰ 2005 U.S. Census Bureau data, 292,733 housing units:

<http://quickfacts.census.gov/qfd/states/06/06019.html>

have reduced gain from external antennas, existence proofs for functioning, commercially reliable, internal antennas are available in traffic information (RDS-TMC) products from Cobra¹¹ and MSN SPOT watches¹². UCB does not have performance information readily available, but the UCB site survey experiment proposed would be able to evaluate the performance and determine if these antennas are satisfactory for DR use.

Note: reference e-Radio testing data

3.d. Noise, Reflections, and Interference

Since the commercial FM radio spectrum is licensed and protected by the FCC, major sources of noise and interference are not typical. While each FM channel is separated by 200 KHz, the FCC avoids licensing stations on adjacent channels within geographic regions. Synchronized FM booster stations, translators which re-transmit the same signal on the same channel (required to operate within the service contour), can be a source of multipath interference in certain areas. Reflections of signals which cause multipath interference are also serious concern. Common FM receivers are designed with noise rejection techniques to mitigate the effects of this interference, such as switching from high-side to low-side injection.

Outside of the FM band, possible near-band sources of interference exist on both sides. On the lower end of the band, TV Channel 6 operates from 82 – 88 MHz (audio is broadcast at 87.75 MHz). The FCC manages its licensing of Channel 6 in order to protect non-commercial educational stations which are given licenses from 88.1 MHz to 91.9 MHz, but interference can occur near in regions located between competing transmitters. In California, there are only three high-power broadcasters (100 kW) on Channel 6 – KSBY in San Luis Obispo, KVIQ in Eureka, and KVIE in Sacramento. On the upper end of the FM band, near 107.9 MHz, VOR aircraft navigation systems can be a source of interference. According to Paul Harvey of Codified Electronics, there are three mitigating factors for this: that interference is localized to areas near airports, that effective radiated power (ERP) is generally less than 200 watts, and that GPS technology may eventually replace VOR.

¹¹ Cobra Nav One 4500 with TMC, <http://www.cobra.com/navone/4500page.htm>

¹² Online database of SPOT devices from SpotStop.com, <http://www.spotstop.com/price/>

Paging Analysis against Communication Interface Questions and Issues – DRAFT

Alex Do, UC Berkeley

25 April 2007

Version 1.0

The information in this document, which addresses the Communication Interface Questions and Issues for the FM/RDS technology, was obtained from a combination of technical documentation and interview with industry representatives and experts.

Application

1.a. Downlink Security

Authenticated communication is not inherently provided by the RDS transport layer and a message authentication and tamper detection scheme needs to be built into the payload. The Title 24 PCT Reference Design Working Group is responsible for defining acceptable solutions for these requirements, and currently has a recommendation on proposal¹³. A key-hashed message authentication code (HMAC) has been recommended as a solution for message authentication and tamper detection. A more detailed discussion of security issues is available in the Security section (Section 4.6) of the Reference Design document.

1.b. Information Model

An implementation of the high-level data model created by the Reference Design Working Group will have to be mapped into a digital format for use on the paging networks by the network operator or some industry alliance.

Network

2.a. Infrastructure, Operational, and Maintenance Costs

- **Infrastructure**

As with the RDS solution, we need to consider two the physical transmitting, infrastructure and the data network as separate aspects of the infrastructure.

Unlike the RDS infrastructure, the data network for paging operators is inherently built into the system design. The paging companies offer telemetry services to large clients and are experienced in offering a socket or portal-based connection for external data sources. An existence proof is Ambient Devices, which generates data about local conditions such as weather for broadcast through the paging network. NRE costs associated with developing data interfaces for the utilities or other agency/agencies are expected to be factored into the rate design for system operation.

The larger question with paging involves the physical infrastructure. There are only two national paging companies in existence, USA Mobility and American Messaging, (smaller local providers are known to exist in California but such market data has not been researched) and their coverage maps for the State are available online¹⁴. Several

¹³ The latest version of the PCT Reference Design, which includes the PCT security strategy recommendation, can be downloaded from <http://sharepoint.californiademandresponse.org/pct/default.aspx>.

¹⁴ USA Mobility's CA coverage: http://www.usamobility.com/check_coverage/index.html. American Messaging's CA coverage: http://www.americanmessaging.net/paging/coveragemaps_default.asp?service=1way.

gaps in coverage can be seen in the Central Valley.

Physical infrastructure investments could cost the State into the millions of dollars in order-of-magnitude. The cost of building out infrastructure is believed to average about \$12,000 per transmitter and is dependent primarily on the lease agreement for the installation site. It is unknown how much buildout would be required to satisfy the needs of continuing development in the Central Valley or increased density in existing service areas is required for reliability purposes. A mitigating factor in building out infrastructure is that a substantial cache of unutilized transmitting equipment is believed to exist which was previously taken out of service as a result of industry consolidation. What this means is that if the system requires infrastructure buildout, the paging companies would be able to quickly establish communication in deficient areas. If the paging companies see potential demand in developing areas, they would be willing to expand their infrastructure without cost to the State. However, the State may need to invest money to provide coverage in less populated areas.

The reliability of the overall paging infrastructure is dependent upon the site of each transmitter. A large paging network consists of a large number of distributed ground-based transmitters, which have transmission range anywhere from hundreds of yards (for example a low-power transmitter on top of a hospital) to tens of miles (for example a high-power transmitter on top of a mountain), simultaneously broadcasting the same data stream on the same paging frequency. The original signal is sent from the paging company through a redundant network connection to a satellite uplink, which is also highly reliable. A satellite relays the signal to ground-based transmitters, which translate the signal to the paging carrier's particular frequency for local transmission. The ground-based stations may be susceptible to failure if for some reason they are unable to receive the satellite signal, or more likely, lose power. The power redundancy of the transmitters is entirely dependent upon measures employed at the site, since the towers are installed at leased locations. Hospitals, for example, have backup power generation available – and paging transmitters at those locations would receive the benefit of power redundancy. Due to the “simulcast” (simultaneous broadcasting) nature of this system, individual losses of smaller ground-based transmitters would not severely affect reliability in densely populated areas. Overall, the system should be reliable except under regional catastrophes such as large natural disasters or broad power loss.

- Operation and Maintenance

Estimates of operational costs at this scale are subject to negotiation and difficult to estimate. Some information indicates that annual operational costs are could to be in the hundreds of thousands of dollars, while knowledge of utility programs similar to the PCT application indicates that annual operational costs could be in the millions of dollars. A more precise estimate will require a detailed request-for-quote (RFQ) process with the paging vendors, taking into consideration the reliability and security requirements of the system.

- Estimate based on existing rate design

In the existing rate design, a system identifier called a capcode is the dominant factor in estimating the total cost of this system. Publicly available information from the paging companies about basic volume contracts indicated that initial registration for each capcode would cost \$1 to \$2 per code, and each message sent would cost between \$0.02 to \$0.10 **per code** (cost depends on message size, time of use, and total number of codes contracted).

Capcodes are a unique registration number in the FLEX protocol which specifies the individual device address and also necessary parameters which configure when and how the device listens for messages within the TDMA frame cycle. With FLEX, individual device addressability can be inherently built into the network by using unique capcodes (FLEX can allocate up to 5-billion unique codes on a system) but presents an exceptional cost in both initial outlay and ongoing operation under the current rate design. The paging system could also be used in a more familiar broadcast mode, where a capcode is shared by a large set of devices (known as a group call) and any addressing resolution beyond the capcode is done within the data payload. Currently, PG&E is working with the national paging company American Messaging to set a system like this for their load control devices; all of the switches listen to a group capcode and cycle the air conditioners only if the message is specifically addressed to the individual switch. The paging companies are able to consider special rate designs tailored to these types of applications, but information about what new rates may look like will require a detailed discussion between CEC and the paging companies which accounts for specific details. A single PCT can also support multiple capcodes to allow layered addressability – for example a PCT may use a statewide capcode, a substation capcode, and a utility-specific program capcode to achieve membership and addressability functions.

In general, we can assume four levels of options for capcodes: a single capcode for the entire state, tens of capcodes for regions (based on climate or load topology), thousands of capcodes for substations, and millions of capcodes for individual PCT's. The use scenarios for 1-way communication on the PCT do not likely warrant the extreme costs of individual capcodes. Allow a quick cost estimate for a data budget for a PCT: 12 heartbeats per hour (every 5 minutes) for half of the day (8 AM to 8 PM to support installers), and one heartbeat per hour for the other half (at night). Rounding up to account for DR and other maintenance-related dispatches, this yields roughly 5,000 messages per year, at an approximate cost of \$100 per year per capcode. This is comparable to the existing proof-of-concept for FLEX paging in PCT's: Ambient Devices' Weather Watcher¹⁵; the cost for a year of premium service, which delivers localized weather information, is \$80 per year. On the upper end of the possible system design, if we assume 3,000 substation capcodes¹⁶, then the setup costs will be

¹⁵ <http://www.ambientdevices.com/cat/index.html>

¹⁶ This is a number which has been discussed with CA ISO as a number of distribution substations which are of interest in this context, though the full network model accounts for about 10,000 substations.

\$3,000 to \$6,000 and the annual operational costs will be \$300,000. Additional reliability, security, and liability requirements will likely increase the cost of this estimate. It may be possible to use tens of capcodes or even a single capcode, as mentioned earlier. However, it is the author's suspicion that because of the network load and reliability requirements, the cost estimates would not decrease dramatically if using less capcodes.

○ Estimates based on existing utility applications

Knowledge of existing utility applications, such as previous PCT trials and load control applications, suggests that costs could be anywhere from \$1 to \$10 per year per thermostat.

Question: is more refined anecdotal evidence available from industry experts?

2.b. Network Capacity

The required network capacity is expected to average approximately 0.1% of network utilization. As with RDS, has been estimated from three primary functions: dispatch, clock-synchronization, and heartbeat. The paging medium is roughly an order of magnitude faster than RDS, realistically capable of roughly **?,??? bits per second.**

Question: what is the realizable data rate of 3200 FLEX, accounting for overhead?

Question: what are the payload impacts of HMAC and ECC encryption?

Note: HMAC sizes are currently estimated at 128 bits, or 16 bytes and may exceed the rate estimates of what a "message" is defined as by the paging companies.

- Dispatch

When a curtailment *is* required, it is expected that a single message, or about 20 bytes, per capcode could be required per DR dispatch. These events are of such low frequency that they do not affect network utilization requirements.

- Clock-synchronization

The FLEX protocol also has a built-in clock update function which is used, meaning that no additional data capacity is required. However, if any existing difference between the utility's or ISO's system time and the broadcaster's time is unacceptable, then additional network utilization of approximately **XX messages per day** would be required, depending on the recommendations of the PCT Reference Design Working Group's security analysis.

- Heartbeat

It is expected that this function will dominate the data capacity requirements of the network. A system "DR" heartbeat is required for two functions: so that the PCT can identify connectivity status, and so that the PCT can identify appropriate FM stations to listen to during initial setup. Frequencies of 4 to 60 times per hour have been discussed for this, though the primary requirement will be driven by the installation scenario. One proposal is to issue heartbeats every five minutes between 8 AM and 8 PM, and then dramatically reduce the frequency (once per hour or less) outside of those times.

2.c. Connectivity

Due to the nature of the FLEX protocol, connectivity status to the broadcast source is built into the receiver. However, this may not mean that connectivity to a distribution utility has been

established. Though connection to the broadcast source has a high-probability implication of connection to the utility-data, there is a chance that the capcode or frequency settings can be misconfigured. In this case, use of a heartbeat signal is still recommended.

2.d. Error Detection and Correction

The FLEX protocol has a built-in error correction scheme which is similar to RDS. A check character embedded in each FLEX “word” allows for one or two-bit error correction.

2.e. Membership

Using “capcodes,” addressability to the substation-level and possibly lower (feeder, PCT) can be established at the paging transport layer. Using some type of registration process, the customer or installer can provide a capcode and/or some unique billing point address to the distribution utility so that messages intended for a particular PCT or group of PCT’s can be addressed correctly within the FLEX protocol. The PCT host processor, upon configuration, can configure its capcodes internally to listen to the properly addressed messages.

Physical

3.a. Frequency Band and Channel Plan

Similarly to RDS, FLEX paging operates on licensed frequencies above 900 MHz. The FCC licenses 49 channels (unique frequencies) around 929 and 931 MHz which are typically used for FLEX paging. Within those channels, a number are allocated specifically for national, regional, and local use to independent operators. Each operator owns the license to operate on a specific frequency, and typically FLEX receivers are pre-configured to operate on a single before purchase. Older technology required that the frequency be set in hardware (through a crystal) but newer receivers allow the receiver to set the frequency in software, allowing for possible redundancy of carriers.

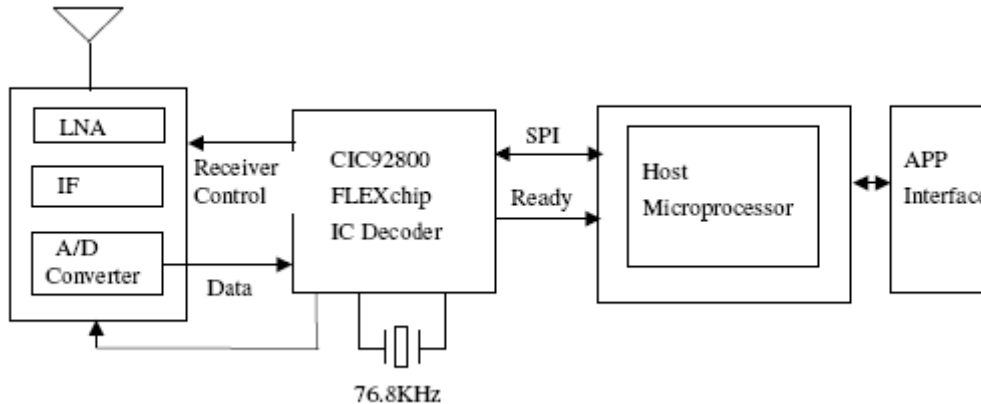
In the case of the PCT application, it must be determined how many carriers will be required for this operation. There are only two paging companies which offer statewide coverage, and each operates on a different frequency. If a single operator were supported, then the frequency could be hard-coded into the PCT before purchase and installation so that it could work statewide. However, by using multiple paging operators, the PCT, during installation or registration, would need to automatically or manually select from a pre-configured list of supported frequencies, especially those which are specific to rural regions outside the coverage of the two national operators. A generic “frequency scan” throughout all the paging channels to search for supported DR carriers would be possible but intensive because of simultaneous, multiphase transmission which is supported by FLEX. The result is that before PCT’s can be programmed for distribution and shipping, they need to know which FLEX operator(s) will be supported.

3.b.i. Radio Cost

The cost of integrating a FLEX receiver into a PCT is expected to be relatively high compared to RDS, at \$5-10 additional cost to the BOM over a regular PT. These estimates were provided by industry device designers; FLEX subsystems are proprietary and detailed estimates of the subsystem requirements are difficult to obtain without non-disclosure agreements.

3.b.ii. Radio Overhead

According to industry manufacturers, implementation of the FLEX stack is non-trivial to devices and presents a large overhead for an electronic device. The FLEX stack can either be integrated heavily at the core microprocessor or within a special FLEX decoder chip. In either scenario, the protocol and stack are proprietary so licensing costs will apply. In addition, no fully integrated solutions are known to exist on the marketplace. The block diagram below shows the architecture of components required in the system.



3.b.iii. Radio Data Rate

The FLEX protocol allows operation at multiple speeds: 1600 bps, 3200 bps, and 6400 bps. The protocol can change transmission speed on-the-fly through overhead information transmitted at the beginning of a frame. For reliable performance, the national companies typically run at 3200 bps, since bit errors are more likely to happen at higher speeds. The actual throughput is restricted by addressing and error-correcting overhead, and practically is closer to **?,??? bps**. Also, depending on the collapse value, which specifies the number of frames within a cycle that the receiver will listen to, the receive latency could be anywhere from seconds to four minutes.

Question: what is the typically available data payload within a given frame?

3.b.iv. Radio Receive Sensitivity

Information about the required dBm or dBuV for reliable performance is not available.

Question: Is any data available about field strength limitations of FLEX receivers?

3.b.v. Radio Range

The range of paging transmission is predominantly determined by the transmitter's location, power, and antenna configuration. The range can vary drastically, from hundreds of yards to 20 miles. A transmitter on top of a hospital may be configured to primarily provide penetration specifically for that building, while a transmitter on top of a mountain (such as San Bruno Mountain in the Bay Area) can reach multiple cities.

3.b.vi. Radio Power Use

It appears as though FLEX subsystems pull a comparable amount of power as RDS subsystems when they are running, estimated to be anywhere from 15 to 20 mA.

3.c. Antenna

Consumer pagers typically use a wire-loop antenna which runs the perimeter of the enclosure. Greater gain can be achieved with an external antenna, which will provide better signal-to-noise above adjacent signals. In densely populated areas, the small embedded antennas are believed to be sufficient to reliably receive a signal. Within buildings in rural areas, external antennas may be required. Around 929-931 MHz, the size of the wavelength is roughly 1/10 that of FM radio. Consequently, corresponding antenna designs for this system can be approximately 1/10 the size; a quarter-wave antenna would be about 3" long and a half-wave 6" long.

3.d. Noise, Reflections, and Interference

Commercial paging, like FM radio, operates in a licensed band. In-band sources of interference may be caused by other paging operators broadcasting on an adjacent channel, or by another paging transmitter within the network on the same channel (simulcast interference). A good receiver will be designed to reject image, adjacent channel, and spurious noise interference. Well-designed paging receivers can also use multipath signals to fill in if the direct signal is weak or absent.

Question: Are there published papers about real-world experiences with noise, reflections, and interference of paging in urban, suburban, and rural environments?

Note: TS Rappaport has written papers about 1.9 GHz PCS band issues and possibly 930 MHz paging as well.