Abstract—Digital television (DTV) provides a critical broadband broadcast resource for interoperable public safety and homeland security applications. Beyond the simplistic view of DTV as a resource for repurposed spectrum to public safety, existing DTV stations are providing megabits per second of encrypted data, including Internet Protocol (IP) video, geospatial visualization, data files, text messages, any digital media. These datacasts, not available to the public, can be targeted to one or any number of selected receivers or groups of receivers in the broadcast area with no congestion effects, unlike cellular systems; that is, DTV ensures all subscribers receive the full bandwidth available. From school security artifacts for Las Vegas police to National Mall awareness for the U.S. Park Police, DTV provides secure, nationwide coverage using existing resilient infrastructure. It is a vital element of homeland security and day-to-day public safety and service communications technology, largely underutilized nationally due to lack of awareness of its capabilities. This paper provides an introduction to DTV used for public safety and service, both for day-to-day applications as well as resilient emergency and post-disaster datacast for wide-area situational awareness and command coordination. Nominal receiver cost is $100. The paper also emphasizes the development of a datacast concept of operations (CONOPS) as arguably the highest risk element to be addressed in any successful implementation of the technology for public safety and homeland security.

Keywords—Broadband, ATSC; datacast; digital television; DTMB; DTV; DVB-T; H.264; IP video; ISDB-T; MPEG-2; MPEG-4; situational awareness; common operating picture; resilient communications; public safety communications; disaster emergency communications; WiFi; wireless communications

I. Introduction

A. Use of Digital Television

Despite initiatives like Project 25 digital land mobile radio (DLMR) and the D block former TV spectrum auctions, public safety agencies are still severely bandwidth constrained. This constraint is especially true when it comes to delivering video and large files. Most agencies have had to rely on public wireless Internet infrastructure to deliver this content. Because these services are also publicly accessible, they are subject to congestion, especially during emergencies when it is needed most. Although Wireless Priority Service (WPS) provides a form of priority for wireless voice calls for public safety, WPS does not apply to data communications. Broadcast television recently completed their digital conversion and is now capable of delivering IP payloads, encrypting content and targeting specific receivers or selected groups of receivers. These capabilities are not normally associated with broadcast television and, for the first time, allow private secure delivery of files and IP video.

Broadcast television also has many native benefits – natively multicast, large geographic coverage, professionally maintained infrastructure, redundant systems, already operational, and inexpensive receivers. These core competencies allow an unlimited number of receivers to view high-quality content with no degradation in service. Multiple stations can be deployed in each market to further increase bandwidth, coverage (if needed), and resiliency.

Public safety has begun taking advantage of this new delivery network, but it is still relatively unknown. The public television station in Las Vegas has been delivering incident response data to law enforcement for over two years. New capabilities recently adopted by the Advanced Television Systems Committee (ATSC) allow mobile reception as well as handheld receivers.

B. Need for Concept of Operations and Standard Operating Procedures

History shows that the development, planning and implementation of technology are far simpler than the integration of that technology into the human organizations intended to benefit from its use [1]. The government investigations of 9/11 [2], Katrina, and the Deepwater Horizon (i.e., Gulf of Mexico Oil Spill) [3] demonstrated the same 25 failures of leadership and planning as documented in the 1946 (seventh) investigation on U.S. preparedness for the
1941 Pearl Harbor attack [4]. In these instances, the existence of technology itself — no matter how advanced — provided no guarantees of success. It was failed human interaction with technology and the lack of coordinated and collaborative planning in the implementation of that technology that caused the same failures to be revisited time and time again. Again, the common, and often tragic, mistake is to believe that the existence of the technology itself, particularly IT and communications technology, guarantees success. History shows that nothing could be further from the truth.

This principal applies directly to DTV as an existing and deployed technology providing a critical — yet untapped — national broadband datacast resource. It remains unused arguably because of lack of awareness of federal, tribal, state and local system planners as well as potential users who think of DTV as a source for spectrum and not immediate broadband datacast. This paper was written to increase awareness of this valuable and available broadband resource.

Even if properly recognized for its potential benefit and low cost, the typical “rush to buy” mentality resulting from a vendor-driven historic market for public safety communications equipment and equipment-oriented grant programs may squander this resource. For this reason, it is important to plan best use of DTV datacast prioritized to meet the needs of local responders to support their day-to-day activities and a variety of uses during major planned events, developing emergencies, and disaster response as depicted in Fig. 1. Although arguably receiving lower priority to these safety and preparedness datacast functions, information sharing among all smart-city services, such as transportation, energy, education, etc., would be valuable.

The number of channels delivered is a local-station decision and may include one high-definition channel using 8 Mbps to 15 Mbps and/or multiple standard-definition channels using from 2.5 Mbps to 5 Mbps. The actual data rate required is driven largely by the age of the digital encoders with newer units capable of producing excellent image quality at lower data rates.¹

A. Transmission Equipment

Digital video is encoded with 1080, 720 or 480 vertical lines of resolution with an aspect ratio of either 4:3 or 16:9. Multiple streams of this MPEG-2 video are then multiplexed into a single MPEG ASI stream and sent to a high-power transmitter which typically provides metropolitan area-wide coverage as shown in Fig. 2 for WETA Washington, D.C.

![WETA DTV Signal Coverage](image)

**Figure 2.** WETA DTV Signal Coverage.

1) Fixed

Conventional digital television broadcasts require lock on the entire transport stream before data within that stream can be accessed. This allows for a very high density of bits to hertz of almost 4:1. Originally it was thought that this high density would be required to transmit a single high-definition video stream. As mentioned earlier, high definition (HD) is now being achieved with newer encoders at half this rate.

2) Mobile

A fairly recent addition to the ASTC digital television specification allows for mobile reception. See the ATSC A/153 mobile DTV standard². Mobile DTV broadcasting adds additional forward error correction at the transport layer to allow signal lock even where multipath is significant, as it would be in a moving vehicle. The tradeoff is a lower bits-to-hertz ratio that is closer to 1:1. Program streams can be mixed with both conventional and mobile occupying the same

---


transport stream. Conventional receivers ignore any mobile content, allowing both to coexist.

B. Subscriber Devices

1) Fixed

Receiving digital television signals has not changed since the early days of television. While there have been advances in antenna design, it is still possible to receive digital television signals with the same antenna that has been on some consumers’ roofs since the days before most people switched to cable. Digital receiver technology has undergone a significant transformation since the early days of digital TV. Now in their seventh generation, DTV receivers are capable of rejecting multipath that would have broken reception in the past. DTV receivers are mandated in all digital television sets, but are also built into some portable devices, and available as USB dongles (see Fig. 3) used on the laptop as shown in Fig. 4.

2) Mobile

Mobile reception, by definition, increases multipath, mandating a receiver specifically designed for mobile DTV. These are becoming available in computers, DVD players, USB dongles and cell phones.

An antenna mounted to a moving vehicle will not always be oriented toward peak gain in the direction of the transmitting antenna. Since it is impractical to ask users to continually re-orient an antenna, effective mobile reception requires an omnidirectional antenna, or at least one with small nulls. Lower antenna gain and greater multipath are impediments to reception, but are offset with additional forward error correction making reliable reception possible even in moving vehicles.

III. DATACASTING BY DIGITAL TELEVISION

Datacasting is the term used to describe the process of inserting IP packets into the payload of some MPEG transport packets in the digital television transport stream. It is short for data broadcasting. The IP packet payload can be de-encapsulated at the receiver, with content then made available to the host receive device. Content can be files, live IP video or both concurrently.

A. Spectrum

Encapsulated IP data is assigned to a specific transport stream packet identifier (ID) or process identifier (PID). Multiple PIDs can be used to identify separate datacasting streams in the same transport stream. These datacasting transport packets are part of the same transport stream that delivers television programming to TV sets. It is not a sideband or auxiliary service.

B. Transmission Equipment

Television stations are not natively capable of transmitting Internet Protocol (IP) packets in their transmission stream. As shown in Fig. 5, IP encapsulation equipment must be installed. The IP encapsulator takes in IP packets, typically from a standard Ethernet jack, inserts those packets into MPEG transport packets, and then delivers that MPEG Asynchronous Serial Interface (ASI) stream to the multiplexer, where it is combined with the other ASI streams from the digital video encoders. Null packets are added to pad the stream to the required 19.392658 Mbps as shown in Fig. 6. The equipment rack is pictured in Fig. 7.
When sending IP data over digital television signals, you get the best attributes of both. Digital television signals are natively multicast, allowing for almost infinite receive-side scalability. Because the payload is IP, it is also possible to apply IP-centric attributes like encryption and receiver targeting.

C. Subscriber Devices

1) Fixed

The basic hardware required to receive a datacast is the same as required to receive a DTV signal for the purpose of watching television programming on a TV set. An antenna and digital TV receiver and a device, which could be a computer or appliance, is used to process and render the content. A software layer to manage the IP content, decryption, targeting and content management is also required for datacasting applications.

2) Mobile

Mobile receivers can also employ encryption and conditional access. These capabilities are built into the specification to support pay-per-view content targeted to consumers. This same capability, when employed on a handheld phone or tablet, would allow public safety users to secure and control distribution of their content while on the move.

D. User interfaces

1) Datacast

Public safety data would typically be protected, so software to manage content, forward error correction and a user interface that makes it easy to manage distribution to only authorized users may also be required. Multiple customers can share bandwidth on the same station. Server controls can be implemented to allow bandwidth sharing. Content protection can be implemented to assure that data repositories are not accessible between agencies.

2) Subscriber device

While the technical capabilities are endless, solving a complex problem with complex technology does not ultimately address the needs of public safety. A graphical user interface (GUI) interface was designed to structure and organize available data. Dispatch can then pick the required elements, select targeted recipients and initiate the datacast transmission.

Receivers on the target reception list are then notified by a desktop crawl and/or pop-up notification that files have arrived and can be viewed if desired. If video is among the deliverables, a video window opens automatically showing the views determined by dispatch to be useful and actionable.

Messages, alerts, warnings, received files and other content are logged and archived. Expired alerts are moved to a
separate area for review and current alerts are listed with all relevant attachments for immediate action.

3) Reception hubs
   a) 802.11

   While mobile DTV reception on properly equipped handheld devices is easily accomplished, those devices are not currently widely available. It is also possible to extend reception of content delivered over the DTV signal by redistributing it over a private, secure WiFi connection.

   This approach allows existing WiFi-enabled devices like smartphones and tablets to display video and files within the WiFi coverage area without requiring any special equipment or adapters to receive the mobile DTV broadcast. When the WiFi service set identifier (SSID) is not broadcast and security, including MAC address registration, is used, the public cannot access the WiFi re-transmission. Even though this option requires two networks, it allows content to flow directly to the public safety officer over private, secure bandwidth that is not subject to oversubscription by unauthorized public users.

   Phased-array broadcast antennas can be used to improve WiFi coverage, lessening the chance that public access points will degrade throughput.

   b) Internet Media Gateway

   In some cases, it is useful to extend DTV datacasts outside of the DTV station’s coverage area. For example, after the initial Fukushima Daiichi nuclear power plant incidents related to the 2011 earthquake in Japan, the Tokyo Electric Power Company (TEPCO) set up a live video feed available to the public on the Internet. However, for public safety, the needs for this type of system extension are quite varied; one must consider data sensitivity, expected audience size, network security restrictions, and receiving device capabilities.

   Public safety agencies that do not have the necessary DTV datacasting receivers, but would benefit from reception, can use a gateway approach. An Internet media gateway has been developed with password-protected access to the same video stream and alerts received by the specially equipped DTV datacasting laptops. Fig. 8 illustrates the key components of the media gateway.

   The gateway first receives the visual data for retransmission via a PC that has both the DTV datacasting receiver software and encoding software for capturing the live video application from the screen. A large portion of the screen (1024x768) is digitized and compressed using an H.264 codec and then pushed to a Web server for distribution. The video is compressed into three streams at different resolutions and bandwidths to support adaptive streaming. The three rates chosen are 700-, 500-, and 300-kbps at 1024x768, 800x600, and 640x480 resolutions, respectively. All video is digitized at 15 frames per second (fps). These parameters can be adjusted as required. A single Web server has the ability to distribute any one of the streams to a few hundred clients simultaneously, given available bandwidth from the Internet. The gateway can be linked to a content delivery network (CDN) to serve extremely large audiences.

   Each viewer logs into the Web site with username/password and can then access the live datacast stream. The PC client media player constantly measures received bandwidth and automatically selects a lower bandwidth rate if the highest rate cannot be delivered consistently within the time required. There are also settings to enable a user to have DVR-like capabilities to pause or seek back in time to view earlier content.

   Though several approaches are possible for Internet streaming media distribution, this solution demonstrated the following:

   - High-resolution live screen capture — while a high-performance PC laptop is needed, the solution requires no other external video equipment or separate encoding server.

   - H.264 video — using standards-based video enables high quality and minimal degradation from the original and simplifies editing and rehosting of the content.

   - Adaptive streaming — when large audience sizes are expected or bandwidth is limited, the system automatically adjusts to deliver the best video possible to each client viewer.

   - Data encryption — by enabling digital rights management (DRM), the solution will encrypt the streaming data to prevent unauthorized access.

   - CDN compatibility — since the solution uses progressive HTTP delivery of small media fragments, the Internet’s caching infrastructure can be leveraged for delivering to large numbers of distributed users.

   Other approaches may be used based on available infrastructure. For example, if a secure regional network with support for quality of service (QoS) were to be used, a multicast IP delivery approach might be more desirable. One could select a real-time streaming protocol instead of HTTP adaptive streaming.

   Through experience with other similar projects, we know that we can easily extend the Internet media gateway solution to support smartphones with Internet access. The major platforms (e. g., iPhone® [Apple Inc.], BlackBerry™ [Research
F. Applicability to Worldwide DTV standards

a) Terrestrial Broadcast

Although the primary focus of this paper presents an evolving solution based on ATSC-based DTV standards, other global DTV standards could support these datacasts with little modification when the MPEG-2 transport stream (TS) can be used to provide encrypted, encapsulated elementary streams.

Worldwide DTV transition is well underway or complete in the U. S., Europe and parts of Asia, and ASTC is only one of several standards in use. The Digital Video Broadcasting-Terrestrial (DVB-T) standard and its enhanced version, DVB-T2, are likely to be the most widely adopted. Other standards, such as Integrated Services Digital Broadcasting-Terrestrial (ISDB-T), is deployed in Japan and South America. Digital Terrestrial Multi-media Broadcasting (DTMB) is also being deployed in China, Hong Kong, and Macau.

With all of these standards, MPEG-2 TS is supported and a unique elementary stream can be included within the transport stream that enables datacasting.

b) Handheld

There are several global DTV handheld standards for the provision of mobile video services for consumer use, and all support some form of datacasting. The key advantage of using handheld standards is that they are likely to be promulgated via low-cost, power-efficient chipsets and integrated into consumer mobile phones or other handheld devices. The modulation/coding standards employed are designed and tested for stable operation in moving vehicles. The following summarizes key characteristics:

- ATSC-M/H (mobile/handheld) – delivers 312 kbps per group with User Datagram Protocol (UDP) streaming content
- DVB-H – delivers IP datacast services multiplexed with DVB-T broadcasts. Also supports burst rates up to 2 Mbps
- One-Seg – delivers 416 kbps using one of the 13 segments of the ISDB-T broadcast
- T-DMB – delivers 128kbps of datacasting, primarily designed for web-, XML-, and image-based applications

Further study is required to determine suitability and accessibility of the available mobile handheld services and devices for public safety application.

IV. APPLICATION TO PUBLIC SAFETY AND HOMELAND SECURITY

A. Current and Trial Deployments

1) Las Vegas, Nevada, School Security

The Clark County (Las Vegas), Nevada, School District is one of the largest school districts in the country. They operate 370 schools and are responsible for over 300,000 students. They lacked the ability to distribute critical incident response data to police and emergency personnel operating in the field.
KLVX-TV, the local public television station, used their existing television signal to distribute public safety data anywhere in the Las Vegas Valley.

Response data, including school blueprints, evacuation plans, response plans, aerial views, hazardous material (HAZMAT) lists and school contact info was organized by the school and presented in a hierarchical GUI for selection and broadcast. Additionally, all the security cameras are available for selection and then inclusion in the broadcast as well.

All data is encrypted and targetable. Some information can be sent to officers, different information to administrators, and still other data to the schools.

The system was recently updated to aid with crowd control by pushing Common Alerting Protocol (CAP) files to digital signage and audio devices. This helps keep the assembled onlookers informed, out of harm’s way, and from consuming the attention of law enforcement on the scene.

2) Norfolk, Virginia, School Security

In Norfolk, Virginia, similar technology is being deployed to improve response at several institutions of higher learning. A consortium of 13 universities work together to improve campus safety.

Blueprints, crisis plans, security camera feeds and other data are being aggregated for distribution to local law enforcement and fire trucks. Since this system is being shared by multiple end users, metrics are being developed to manage content, prioritize and explore common data that improves awareness across all campuses.

3) Washington, D.C., Fourth of July Celebration

Public safety has traditionally relied on the use of commercial wireless networks for data communications in the field. Few agencies enjoyed budgetary capability to build private networks for data exchange, and most private networks that were built in the past did not provide for robust, high-speed, broadband data exchange.

The use of commercial wireless networks brought several inherent flaws. Public safety data flows were restricted by the capacity constraints of those networks. In the midst of a large-scale special event attracting tens or hundreds of thousands of persons, commercial wireless networks slow or come to a halt. In the case of a large-scale manmade incident or natural disaster, the use of the commercial wireless network by the public often spikes far above capacity levels. It’s at these times that public safety has the greatest need for bandwidth. Bandwidth-consumptive applications such as video are crucial to command and control, and sense-and-respond capabilities must be provided to incident commanders both on the scene and at remote command centers.

Additionally, public safety data needs for situational awareness tools or sense-and-respond capabilities are often held hostage to the availability of supporting infrastructure such as the electrical grid or other network systems that provide backhaul for wireless communication cells or nodes. An electrical grid outage or an unplanned incident with the infrastructure backbone can quickly eliminate the ability to port critical situational awareness tools to incident commanders within a scene.

During the second half of 2010, the United States Park Police handled four large-scale special events, each attracting from 100,000 to several hundred thousand participants in and around the National Mall and National Memorials. At each of these four special events, the United States Park Police utilized commercial wireless networks to provide situational awareness and command and control tools to incident commanders within the special events. In three of the special events, the ability to port these tools over the commercial wireless networks failed as crowds grew and use of personal cellular devices and smartphones increased. In the fourth event, the United States Park Police lost capability due to an incident at a construction site in which fiber feeds for all local cells was accidentally cut.

To support situational awareness during the 2011 Fourth of July celebration on the National Mall and along the Potomac River, the United States Park Police deployed a datacasting solution to push video and alerts across disciplines and jurisdictions and across all levels of government. Fifteen agencies were able to receive relevant video feeds from the United States Park Police during the event, with the ability to transmit to dozens more agencies had an incident occurred.

A limited amount of video interoperability had been achieved at very low levels during special events in the past. Secure video interoperability during the 2011 Fourth of July celebration was unprecedented in terms of scope, reach, and ease of accessibility, and brought situational awareness among involved and impacted agencies to a new level.

B. Evolving Concept of Operations

The integration of DTV datacast into public safety, public service, and homeland security activities requires that CONOPS be developed prior to implementation – a step often ignored in civilian system planning to the detriment of the public as well as responder subscribers. This integration will be based upon existing functional standards from the Project 25 land mobile radio (LMR) standard service set in the Statement of Requirements (SoR) (5).

1) Definition and Importance

A CONOPS document is depicted in Fig. 9 as the critical explanation of the need for a new capability that fills the gap between strategic planning and systems engineering to implement the envisaged new capability. In the figure, the letter-annotated elements define the following steps:

Strategic planning – provides the documented and vetted mid-term and long-term direction for a group of systems and system users to best achieve their purpose and objectives – often employing business case analysis to develop alternatives to strategic needs (e.g., alternative capabilities or improvements), vet them, and recommend a specific alternative at the inception of CONOPS development

a. Purpose and background – this initial portion of the CONOPS document defines its content and summarizes its need and value, presenting the high-level environment and problem to be addressed by the CONOPS...
AS-IS operations and systems – this critical part of the CONOPS describes the current (AS-IS) capability in terms of operational environment, operational and system architecture, and the user organizations and characteristics

b. Need for change – this portion of the CONOPS describes the problem or issues with the current capability and explains why a new system concept must be developed and implemented to correct the problem and mitigate or eliminate the issues

c. Proposed system concept – this section is the heart of the CONOPS document, describing the operational and system architecture and providing the interaction of all user groups with the new capability in its operating environment (note the feedback path labeled)

d. Operational scenarios – describes day-to-day and special or unforeseen environments or events for which the new capability is proposed to correct one or more operational/logistical problems or mitigate/eliminate a performance/cost issue; normally these scenarios will be identified in collaborative strategic planning

e. Concept analysis – provides analytic or simulation-based performance assessment to demonstrate that the expected problems or issues will be adequately addressed by the proposed capability

f. Expected impacts – forecasts the likely affects on the environment, support systems, users and other organizations and people, which result from implementation of the new capability

g. Systems engineering – the detailed process for creating the new capability, beginning with the development of detailed user requirements through design and test disciplines to deployment, operational test and user acceptance/usage

h. Fast prototyping to support development – this feedforward and feedback path shows that concept development is often aided by the trial of one or more components or subsystems considered for the new system concept; this is often known as “fast prototype” i. User standard operating procedures (SOPs) are developed for the individual agencies interoperating as defined by the CONOPS, and the SOPs define the activities of individuals and agency staff integrated with this CONOPS – all involved agencies have their SOPs also integrated with the same CONOPS

The CONOPS document provides the transition from high-level strategic planning to the establishment of user needs and expectations, prior to the development of detailed requirements and system specifications as the standard front-end of best-practices-based systems engineering. Enterprise architecture views are an important component of this transition, providing standards-based visualization of operational, system, and technical standard “slices” of the overall capability architecture. Systems planning and implementation require these components. Without these components, there is the risk of poorly justified and little-used – yet often expensive – system enhancements.

2) Functional capabilities

One-way datacast can be configured to provide functional information-sharing capability – albeit in datacast (talkout) mode – analogous to the Project 25 functional requirements. In this context, we will relate the LMR concept of a radio “call” to that of a datacast “push.” Of course, two-way communications requires an independent transmission path from datacast subscribers to the datacast generation point (talkback). The analogous Project 25 functional requirements are as follows (from P-25 SoR 2.1.2) [5]:

- Group push – comparable to P-25 group calls, in which a digitally designated, or targeted, subset of all datacast subscribers can receive specific datacasts (SoR 2.1.2.1/2)
- Private push – analogous to private calls in P-25(SoR 2.1.2.3/4)
- Public switched telephone network (PSTN) push – audio from telephone interconnect pushed as voice packets over datacast (SoR 2.1.2.5/6)
- Voice encryption control – targeted datacast audio packet encryption control (SoR 2.1.2.9/10)
- Preprogrammed data message push – preprogrammed data messages (SoR 2.1.2.11/12)
- Subscriber tracking – possible through multiple DTV station transmission to cover statewide or multi-state regions and subscriber Global Positioning System (GPS)-location talk back (SoR 2.1.2.13/14)
- Dynamic subscriber regrouping – controlled by datacast source-merge control software (SoR 2.1.2.15/16)
- Emergency alarm – handled by broadcast facilities (SoR 2.1.2.17/18)
- Source ID transmission – datacast identifying the source of pushed information (SoR 2.1.2.19/20)
o **Test messaging** – Transmitted from DTV source and merge control point, inherent part of the datacast (SoR 2.1.2.21)

o **Broadcast push** – a one-way single transmission (datacast) to all (merged) push groups (SoR 2.1.2.22)

o **Subscriber authentication** – implemented by a specific datacast query from the data merge point to a subscriber and then reporting the subscriber-authenticated ID back to the merge point via different media (SoR 2.1.2.23)

o **Announcement group push** – datacast to a group of push groups, an announcement group (SoR 2.1.2.24)

o **Emergency push** – emergency alerting to all groups with priority and, perhaps, preemption over other datacasts (SoR 2.1.2.25)

o **Subscriber check** – same approach as a datacast authentication, but initiated by a push subscriber through talkback media (SoR 2.1.2.26)

o **Unit de-authorization** – removal of one or more specific subscriber units from datacast targeting (SoR 2.1.2.27)

o **Busy-channel lockout** – not relevant as datacast does not produce multi-subscriber interference (SoR 2.1.2.28)

o **Unmute control** - receivers operating in the Untargeted Push mode are configured to not include Push Group ID in their decision to unmute for a received push (SoR 2.1.2.29)

o **Digital carrier squelch mode** – reception of any authorized DTV signal (SoR 2.1.2.30)

o **System-wide group push** – datacast to all subscribers (SoR 2.1.2.31/32)

o **Datacast site control** – specific DTV transmitter sites are selectable, inherent in Web/network distribution of merged datacasts (SoR 2.1.2.33)

o **System-wide group push (all-group push)** – datacast to all subscribers through all participating DTV stations (SoR 2.1.2.34)

o **Surveillance mode** – datacast push produces minimal or no audio output while still permitting talkback (SoR 2.1.2.35)

Other supplementary services analogous to P-25 include

- **Encryption** – end-to-end encryption of content as appropriate to the datacast

- **Priority push** – at least five priority levels [ (2) ]
  - **Emergency:** Priority Level 1. Immediate datacast stream access for exclusive use in “safety-of-life” situations

- **Mission:** Priority Level 2. Situations of increased risk, such as high-speed chases, exchanges of gunfire, and major fires may require activation of this mission priority. Once activated, this precedence level must remain in effect until a dispatcher restores normal operation, that is, regularly assigned precedence levels. Only the emergency access (Priority 1) takes precedence over this mission-level priority.

- **Command:** Priority Level 3. The executive (command) or supervisory personnel have this third priority level, which also may incorporate privacy features. The specifications state that subscriber devices used by command or supervisory personnel may be assigned this Priority 3 level for their normal operating mode. This optional capability is suggested because many command personnel may require this added precedence for higher reliability channel assignments as they provide direction for those under their authority.

- **Operational:** Priority Level 4. This priority level is intended for public safety subscribers in systems used to support non-public safety or administrative functions. In this way, a public safety subscriber would preempt a non-public safety subscriber as a matter of course during day-to-day operations, not otherwise considered Level 3 or above.

- **Routine:** Priority Level 5. This lowest priority level is intended for non-public safety or administrative users in public safety systems for their routine operations.
  - **Preemptive priority push** – if higher priority datacasts than the current transmission arrive at the merge point, the higher-priority datacast should begin within 0.5 seconds from this arrival, preempting other datacasts of lower priority
  - **Push interrupt** – capability to interrupt a queued datacast within 0.5 seconds of its transmission to include higher-priority information
  - **Discrete listening** – a subscriber may monitor all authorized push groups and have the capability or recording for subsequent viewing as well as database updating, all authorized DTV receptions, though no interaction with the merge source is expected
  - **Actuation push** – a targeted datacast prompting subscriber devices linked to datacast sources, such as sensors or video cameras, to actuate an action, such as operating a video camera pan-tilt-zoom controls.

These functional requirements mimic the operational capabilities defined for Project 25 in public safety and emergency response.

3) **Routine, Event, Discipline, Core, Dynamic, and Alert**
Standard (interoperable) operational definitions for datacast composition include the following datacast pushes as private, group, or multi-group pushes:

- **Routine** – Datacast providing moment-to-moment or day-to-day conditions or incidents
- **Event** – Datacast providing predetermined elements of a given event or incident, like type (e.g., tornado, wildfire, explosion, etc.), location (e.g., map location, affected area, floor plans, local critical infrastructure, etc.), video (e.g., live, recorded, thermal, smart, etc.), etc.
- **Discipline** – Discipline-specific information, either routine- or event-related, defined for each public safety or service-related discipline, including federal, tribal, state, county and municipal
- **Core** – Basic content of any type of datacast, such as time, targeted group(s), etc.
- **Dynamic** – Predetermined type and data fields which may be included depending on the datacast purpose, but not included in the core datacast set
- **Special** – Datacast including alerts (e.g., private, group, multi-group, all-group pushes), status, etc.
- **Common** – Datacast common to two or more push groups

These datacast descriptors can be strung together, such as

- **Routine_Discipline_Core** – a moment-to-moment or day-to-day transmission for a specific public safety or service discipline, such as traffic video on a commute period on a typical workday for the transportation discipline or the number of beds in each hospital for the emergency medical services discipline
- **Event_Discipline_Core** – Datacast makeup regarding an event for a specific discipline, like floor plans for school security police
- **Event_Discipline_Dynamic** – Changing datacast content for a specific discipline as situational awareness evolves, such as a fire discipline datacast merge adding area air-quality maps given suspected HAZMAT release

V. SUMMARY AND RECOMMENDATIONS

DTV datacast presents a viable broadband delivery mechanism for day-to-day as well as safety-of-life, critical public safety; emergency preparedness/response; and disaster response information. Resilient infrastructure to support these broadcasts exists nationwide, and equipment to support receiver targeting and encryption is available today. It does not limit the number of engaged subscribers in any geographic area. It does not use existing public safety spectrum and can mimic many functions of Project 25 LMR. Public safety and homeland security agencies should evaluate DTV capabilities for their responders and other stakeholders.

ACKNOWLEDGMENTS

Mark O’Brien would like to thank WETA Public Television & Radio, Winegard Company, and West Pond Technologies.

Robert Desourdis thanks John DiSalvo, former P-25 User Requirements Chairman, for his review, Wayne Quick supporting SpectraRep for his edits, and Roz Reece of SAIC for her quality review of this document.

REFERENCES