NIST Special Publication 1500-15

Strategic Roadmap for Interoperable Public Safety Video Analytics

Diane Simpson
Michelle Brennan
Susan Gomperts

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-15

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1500-15

Strategic Roadmap for Interoperable Public Safety Video Analytics

Diane Simpson
Michelle Brennan*
Information Access Division
Information Technology Laboratory

Susan Gomperts
The MITRE Corporation
McLean, Virginia

**Former contractor; all work for this publication was done while under contract with NIST*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-15

April 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1500-15
Natl. Inst. Stand. Technol. Spec. Publ. 1500-15, 63 pages (April 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-15

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

The Public Safety Communications Research (PSCR) Division is the primary federal laboratory conducting research, development, testing, and evaluation for public safety communications technologies. It is housed within the Communications Technology Laboratory (CTL) at the National Institute of Standards and Technology (NIST). It addresses the research and development (R&D) necessary for critical features identified by public safety entities beyond the current generation of broadband technology. PSCR conducts internal research across key public safety technology areas, otherwise known as research portfolios including applied analytics for multi-modal real time data in conjunction with the Information Technology Laboratory.

Executive Summary

The public safety community requires robust, scalable and interoperable technologies to assist effectively with real-time capabilities to support situational awareness and conduct post-event analysis. With the rapid growth of video in the public safety domain, the strategic incorporation of next-generation video analytics into public safety systems and workflows is fundamental to harnessing the value of these data sources. Successful insertion will hinge on the interoperability of data and systems.

NIST gathered input from diverse public safety video analytic stakeholder communities to provide insight into technical and organizational interoperability concerns through two workshops.

These engagements identified five primary themes that encompass the challenges to achieving video analytic interoperability and aligned these to the public safety community widely adopted SAFECOM Interoperability Continuum: Standards/Best Practices, Collaboration/Outreach, Education/Training, Technology/R&D and Policy [1]. The Continuum's five elements serve as the focus areas for analysis of gaps between current and desired future outcomes.

The *Strategic Roadmap for Interoperable Public Safety Video Analytics* identifies issues surrounding the difficulties faced by public safety in moving from interoperability that occurs by chance to institutionalized interoperability where evolutions across all five elements contribute to organic interoperability.

The *Strategic Roadmap for Interoperable Public Safety Video Analytics* establishes a foundation by describing the functional video analytic workflow and interoperability considerations in Section 2 and by describing the current public safety video analytics environments and key takeaways in Section 3, along with a sample set gaps and challenges associated with achieving

interoperability, desired outcomes, and recommended steps to move toward the future environment. The sample roadmaps are not comprehensive and are provided as a tool for framing strategic planning around the problem sets. Public Safety video analytics leaders and stakeholders are responsible for further discussions and decisions on the actual gaps and activities to be addressed and will need to determine lead organizations responsible for specific products/outcomes.

Purpose

This roadmap is intended to inspire both federal administrators responsible for public safety grants and investments, and public safety operations decision-makers at local, tribal, state, and regional jurisdiction levels to understand, plan appropriately, and make investments in all of the elements that support interoperable video operations. We hope to increase focus on the international video standards impacting public safety and encourage industry to consider public safety needs proactively in those efforts. In doing so, we also hope to drive research and development on interoperable solutions which will add to public safety ability to monitor, maintain, and control their video surveillance systems (VSS); improve the flow and dynamic prioritization of emergency video data within networks; enhance data quality; and support unbiased analysis in order to triage, visualize, and alert first responders. This roadmap may also serve as a mechanism to spark discourse and debate on governance mechanisms as well as the legal and societal concerns related to rights and privacy which may encourage the development of policies, standard operating procedures based on best practices, public safety community partnerships, or laws that ensure emergency responders utilize video and video analytics in ways that positively impact their communities and save lives.

Abstract

Since 9/11, the Department of Homeland Security has provided over $16 billion dollars in grant assistance to secure cities and non-profit organizations against terrorist and disaster incidents. In order to meet the threat demands, public safety organizations have increasingly invested in video surveillance systems to increase their patrol footprint and monitor major transportation areas. Many cities now have hundreds to thousands of public safety and transportation infrastructure cameras; larger cities have tens of thousands of these cameras. Public safety now faces a growing diversity of video data sources, and these volumes of data are increasingly vital to public safety operations. However, analysis of video data to support real-time operations largely relies on manual processes and non-security related, impractical physically isolated architectures. The purpose of this publication is to chart a path forward to guide public safety related agencies and individual public safety departments in their transition from a state of interoperability that occurs by chance to a state of institutionalized interoperability which incorporates the next-generation of video analytics through measured steps and broad stakeholder informed decision making.

Key words

Data sharing; emergency management; governance; information sharing; best practices; interoperability; public safety; video analytics

Audience

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

This report is primarily intended for national and regional level public safety technology communications technology thought leaders, and public safety video analytics stakeholders.

Acknowledgements

The authors wish to thank all contributors to this publication, including the participants in the workshops and other interactive sessions and the individuals and organizations from the public and private sectors who provided comments on the preliminary ideas. We thank the membership and leadership of the Video Quality in Public Safety community whose hard work and dedication in identifying standards and best practices provided a solid springboard for this research and roadmap.

Additionally, the authors thank and acknowledge the following people and organizations for their support to this publication:

Federal Advisors: Cuong Luu, Program Manager, Office for Interoperability and Compatibility - First Responders Group, Science and Technology Directorate, Department of Homeland Security; Dereck Orr, Chief, NIST Communication Technology Lab Public Safety Communications Division, and John Garofolo, Workshop Chair, NIST Information Technology Laboratory

Technical Editors: James Horan, NIST Information Technology Laboratory; Sam Ray, NIST Communications Technology Laboratory

Organizational Contributors: Kaitie Karavai, NIST Information Technology Laboratory; John Contestabile, Vivian Wong, and Marjorie Fioravante, Johns Hopkins University - Applied Physics Lab

Second Workshop Sponsors: DHS Office for Interoperability and Compatibility (OIC) - First Responders Group, Science and Technology Directorate; NIST Communications Technology Laboratory, Information Technology Laboratory, and Johns Hopkins University - Applied Physics Lab

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Table of Contents

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

List of Tables

List of Figures

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Acronyms

ACE	Analytic Container Environment
AES	Advanced Encryption Standard
APCO	Association of Public-Safety Communications Officials
API	Application Programming Interface
ATC	Area Technology Centers
CAD	Computer-aided Design
CAP	Common Alerting Protocol
COG	Council of Governments
CoI	Community of Interest
COP	Common Operating Picture
CJIS	Criminal Justice Information Services
CSIM	Converged Security Information Management
DMC	Digital Multimedia Content
DNS	Domain Name Service
DHS	Department of Homeland Security
DME	Digital Media Evidence
EMS	Emergency Medical Services
FEMA	Federal Emergency Management Agency
HDCCTV	High Definition Closed Circuit Television
HIMMS	Health Information and Management Systems Society
HL7	Health Level 7
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
IPTC	International Press Telecommunications Council
ISO	International Standards Organization
JSON	JavaScript Object Notation
LEVA	Law Enforcement & Emergency Services Video Association International, Inc.
LMR	Land Mobile Radio
LPR	License Plate Recognition
LTE	Long Term Evolution
MPEG	Motion Picture Experts Group
NCSWIC	National Council of Statewide Interoperability Coordinators
NG911	Next Generation 911
NIEM	National Information Exchange Model
NIJ	National Institute of Justice
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology

NITRD	Networking and Information Technology Research and Development
NPSTC	National Public Safety Telecommunications Council
OIC	Office for Interoperability and Compatibility
ONVIF	Open Network Video Interface Forum
OSI	Open Systems Interconnection
PTZ	Pan Tilt Zoom
PVMD	Photo and Video Meta Data
P2P	Peer to Peer
PSCR	Public Safety Communications Research
PSIM	Public Safety Information Management
R&D	Research and Development
RDT&E	Research Development Test and Evaluation
RAT	Radio Access Technology
ROC	Regional Operating Center
RTSP	Rapid Spanning Tree Protocol
S&T	Science and Technology Directorate
SCC	Standards Coordinating Council
SDK	Software Development Kit
SOAP	Simple Object Access Protocol
SoS	Systems of Systems
TCP/IP	Transmission Control Protocol/Internet Protocol
VAPS	Video Analytics in Public Safety
VIA	Video and Image Analytics
VMS	Video Management System
VQiPS	Video Quality in Public Safety
WSDL	Web Services Description Language
XML	Extensible Markup Language
XMP	Extensible Metadata Platform

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

1. Introduction

Since 9/11 the Department of Homeland Security (DHS) has provided over $16 billion dollars in grant assistance to secure cities, critical infrastructure, and non-profit organizations against terrorist and disaster incidents [2].

To meet these and other threat demands, public safety organizations–law enforcement, fire and rescue, and emergency medical services—have increasingly invested in video surveillance systems (VSS) to increase their patrol footprint and monitor major transportation areas. Many cities now have hundreds to thousands of public safety and transportation infrastructure cameras; larger cities have tens of thousands of these cameras. These departments now face a growing volume and diversity of video data sources which are increasingly vital to public safety operations [3].

Many public safety departments struggle with how to balance the benefit to public welfare brought by video with the challenges of managing the data and associated systems. Though the application of video for operations varies from city to city and department to department, most public safety offices believe video analysis can assist in answering three strategic questions:

- How can we respond faster to the public's needs?
- How can we more effectively deploy our resources?
- How can we intervene to mitigate outcomes that negatively impact people's lives before loss of life or property occurs? [3]

Those leaders who have effectively utilized their video systems to assist with these operational challenges continue to add cameras on the streets. For the video operations units and the organizations that support the information technology and communications systems streaming the video from these cameras, their challenge is not in making the data relevant to operations, but in keeping the data flowing and meeting the demand. Video data is bulky, impacting transmission and storage in ways that audio and text data do not. Video Operations units, public safety information technology professionals, and the vendors that support them struggle with network bandwidth, backend systems, support agreements, and manpower levels that do not scale to meet the volume, velocity, and variety of data. Support agreements can be limited to single camera types, systems, or training, adding another layer of complexity when trying to troubleshoot an already complex video enterprise network.

The analysis of live streaming public safety video data is manually intensive and often carries with it a psychological toll that is just now being understood. Video operators may monitor a dozen or more cameras simultaneously and on multiple screens and different proprietary video management systems. Real-time video operations units are unique, homegrown efforts, often created and sustained by grant funding. Staffing varies by jurisdiction; some are staffed by police officers, others by communications professionals, video analysts with backgrounds in forensics, transportation officials or a combination of each.

The key to managing the amount of incoming video data and lightening the burden on the limited number of video operators lies in applying the next generation of analytics, such as computer vision and network analysis tools, to help manage the video workflow. NIST IR 8164 defines video analytics as the "application of computer vision that leverages information and knowledge

from video content to address a particular applied information processing need [3]." Successful insertion of these analytics, however, depends on secure, stable networks and components that can receive, interpret, and transmit data freely. It requires interoperability.

1.1. Roadmap Development Approach

The need for the public safety focus on video analytics began in 2014 and arose out of the White House Office of Science and Technology Policy (OSTP) National Science and Technology Committee (NSTC) Networking and Information Technology Research Directorate (NITRD) federal cross agency coordination and collaboration on Video and Image Analytics. Informed by these collaborations, the roadmap development design incorporated a multi-year mixed-methods approach which included two workshop events, discussions with subject matter experts, and literature research.

Under the sponsorship of the longstanding DHS S&T-led Video Quality in Public Safety working group, PSCR held two 2-day workshops between 2016 and 2018 to bring together stakeholders with vested interest in the use of video analytics in public safety operations. The objectives of these workshops were to:

(1) establish a public safety video analytics community,

(2) foster cross-community education and strategic cross-cutting discussion regarding R&D, measurement, standards, technical education and outreach, and collaboration, and

(3) conduct discussions to shape the development of a roadmap for future collaboration activities and standards that promote video analytics interoperability input from the Video Analytics in Public Safety (VAPS) community.

The 2016 workshop utilized panel discussions to obtain perspectives from public safety and transportation video professionals; social considerations groups; academia; human factors, human-computer interaction, and visualization researchers; industry; and collaborative partnerships between public safety and research teams. Breakout groups in 2016 addressed technology related needs and issues, best practices, and collaborations and coordination. *NIST IR 8164 First Workshop on Video Analytics in Public Safety* summarizes finding from this workshop [3].

The format for the second workshop, held in 2018, also incorporated panel discussions which reviewed takeaways from the first workshop and highlighted current perspectives from academia, industry leaders in video analytics research and development and video management systems, standards and collaborations organizations, and public safety operations and systems. An open question and answer period followed each panel session to allow for elaboration on issues relevant to the participants. The format also included a one-hour session that leveraged a modified nominal group approach to ascertain challenges and gaps, grouped around five themes identified by workshop leaders based on the first day's panel discussions. Themes included policy/governance, procedures/best practices/standards, technology/R&D, collaboration/outreach, and education/training. Another open question and answer period elicited stakeholders' requirements and recommendations for the roadmap. Stakeholders articulated requirements that the roadmap should address:

- Applicable and actionable—not a "one size fits all" approach

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

- Adaptable to emerging ecosystem approaches and challenges
- Inform industry-driven standards development
- Promote video data security and integrity

Notes from the workshops containing non-attributed participant and panel comments, as well as recommendations and findings were dissected from the *2016 Public Safety Analytics R&D Roadmap* and August 2016 *PSCR Analytics Summit Report*. Using a qualitative coding approach, sections of narrative data were examined, labeled and aligned them through an iterative process to the various functional components of the video analytics workflow identified during the first workshop (Figure 1) and to the five themes identified on day one of the second workshop. Qualitative coding is a process of labeling narrative data in order to group, examine, and manipulate it into meaningful ways. Unlike software coding in computer science, it is a process of reducing and reconfiguring data for sensemaking. Data was also qualitatively coded into the five elements of the SAFECOM Interoperability Continuum to provide a consistent format for the public safety audience.

Analysis was followed by a literature review on the most recent research on public safety video analytics to incorporate findings from *NISTIR 8255 Interoperability of real-time public safety data: Challenges and possible future states*, RAND's *Using Video Analytics and Sensor Fusion in Law Enforcement*, and National Public Safety Telecommunications Council's *Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes*. Additional research was conducted to supplement detail on standards and organizations relevant to the gaps and challenges articulated by the stakeholders.

Public safety information technology offices provide network and computer support, augmented by video systems contract staff, are responsible for the acquisition and maintenance of video networks and systems. Throughout the paper, the term technical video operations staff is utilized to describe this role to delineate video technology as a specialized area apart from the broader range of IT support needs.

1.2. Roadmap Structure

The remainder of this publication is organized into the following major sections and appendixes:

- Section 2 describes and defines functional components within the video data workflow.
- Section 3 describes the current state of interoperability, aligned to the elements of the DHS SAFECOM Interoperability Continuum. The continuum elements are broken into subsections which describe the influences and standards impacting interoperability, and highlights key takeaways concerning public safety's gaps and challenges. The subsections are:
  - 3.1 Governance
  - 3.2 Standard Operating Procedures
  - 3.3 Technology - To elaborate on the technologies and standards impacting video operations and analytics, the Technology subsection is further divided into four levels of interoperability: Foundational, Structural, Semantic, and Organizational.
  - 3.4 Training and Exercises

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

  - 3.5 Usage
- At the end of each subsection a sample roadmap is provided which contains gaps, desired outcomes and activities that could be taken to improve interoperability. Activities are laid out in three stages. Sample roadmaps are submitted as a potentially useful tool for framing future discussions and decisions on actual steps and measures needed to address video interoperability for each element.
- Appendix A provides additional detail on public safety video analytics stakeholder groups.

1.3. Transitioning the Interoperability Focus to Enhance Video Analytics

The Institute of Electrical and Electronics Engineers defines interoperability as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged [4]."

In public safety, communications interoperability refers to the ability of emergency responders to communicate on demand, in real time, when needed, and as authorized, resulting in an effective shared understanding and situational awareness among the responders and the command structure [5]. This DHS definition does not preclude video interoperability, but other federal partner definitions have narrowed the opportunity for needed enhancements to improve the flow of data by limiting their efforts on specific network types. For example, the Federal Communications Commission adopted the definition in Section 90.7 of the Commission's rules as "[a]n essential communications link within public safety and public service *wireless* communications systems which permits units from two or more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results."

The problem is that current public safety video operations units leverage a combination of network and broadcast approaches to include municipal dark fiber, commercial ethernet, and wireless networks to capture, transmit, and broadcast video data. The monumental effort of developing a 5G broadband wireless network to improve communications between first responders has raised awareness on interoperability, but it left public safety video operations units behind and increasingly reliant on network architectures that are ill-equipped to meet the video quality requirements for the continued expansion of video sources and the use of video analytics. Additionally, video data quality efforts and advanced LTE communications design processes to accommodate video have leaned towards forensic use cases—situations in which the video is saved and is capable of playback. Other real-time monitoring use cases focus on social media video [6, 7]. In order to apply analytics to the video workflow, public safety must pivot its focus.

Analytics refers to the scientific process of transforming data into insight for making better decisions. Video Analytics (VA) leverage information and knowledge from video data content to address a specific applied information processing need. Video analytics is a quickly emerging application area focused on automating the manual tasks of monitoring live streams of video, streamlining video communications and storage, providing timely alerts, and making the task of searching enormous archives of video manageable [3]. Video analytics applications typically address information needs for the following “W” questions:

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

- Who (people detection and identification);
- What (object, activity, event, behavior, and relationship analysis);
- Where (frame space, 3D space, and world map space); and
- When (date/day, time-of-day, time-of-year) [3].

Video analytics can be applied to retrospective analysis of archives (search, triage, forensic investigation), real-time analysis of live video streams (situational awareness, triage and alerting), and predictive analyses leveraging both live video streams and archives as well as data from other domains (event/activity prediction, anomaly detection) [3]. This paper focuses on real-time video analysis in support of public safety operations, while recognizing that improvements in interoperability will also impact forensic and predictive analysis.

2. Video Data Workflow

Large-scale distributed video surveillance systems usually comprise many video sources distributed over a vast area, transmitting live video streams to a central location for monitoring and processing [8]. As system size and diversity grow, complexity increases, as does the probability for inconsistency, unreliability and unresponsiveness. The design and implementation of distributed real-time systems present essential challenges to ensuring that these complicated systems function as required [8].

To comprehend any complex system, it is necessary to decompose it into component parts and functions. The current DHS VQiPS guidance offers a framework for video surveillance systems that is component-focused, providing a system view into the video components and environmental factors considered when determining camera placement. [9] It includes lighting/environment, Digital Multimedia Content (DMC) Source, physical infrastructure, logical infrastructure, control analysis, video management system (VMS), systems integration, storage, and display [9]. This approach does not adequately provide an understanding of the video data workflow to inform troubleshooting the complex systems and subsystems in today's public safety video operations programs. Figure 1 lays out the basic functional components related to the flow of video data through an end-to-end public safety video analysis framework.

Figure 1. Functional Components of the Video Analytics Workflow

This functional workflow is not strictly linear; for example, an alert could be generated earlier in the workflow as analytics and edge computing capabilities mature. RAND's report offers a different sample workflow based on a passive monitoring model which is triggered by a positive detection of an object or event by a video analytic, as well as several considerations for the business case for real time video analytics [10]. Regardless of the order, interoperability between each function is essential to achieve the full range of public safety missions.

In this section, steps in the data workflow are defined and expand upon. Relevant supporting terms and definitions are also incorporated in order to generate a common understanding for public safety officials not directly familiar with video operations technologies.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

2.1. Capture

Capture includes the access to, collection, and ingestion of DMC sources from video devices. These can be publicly or privately owned and fixed or mobile.

Digital Multimedia Content (DMC), also known as digital video, IP video content, or DME, refers to digital data representing audio content, video content, metadata information, location-based information, relevant IP addresses, recording time, system time, and any other information attached to a digital file. DMC may be compressed or uncompressed and may also be referred to as original, copied, local, or virtual [9].

2.2. Transmission/Communication and Broadcasting/Distribution

Transmission/Communication and Broadcasting/Distribution are considered together, because for both workflow components, video quality can be greatly impacted by the method(s) employed, data interoperability, security and privacy considerations which need to be incorporated into the process.

Transmission/Communication is the movement of information across communication channels or networks. Video quality can be impacted by the transmission method(s) employed [8]. Poor video transmission can introduce significant and unpredictable visual artifacts such as jitter, dropped frames and jagged edges.

Broadcasting is the manner of transmitting video data in a one-to-many model, intended for more than one recipient and not limited to one-to-one communication channels [11].

Datacasting is a broadcasting method that allows distribution of computer-generated digital content within the unused bandwidth of the public television digital transmission stream. This data receives a specific transport packet ID (PID) for identification by public safety digital television receivers. The data can be encrypted using the 256-bit Advanced Encryption Standard (AES) and tagged using the Common Alerting Protocol (CAP) standard. The approach leverages the resilience of public broadcast television as a distribution mechanism and offers 97% nationwide coverage, making this a viable solution for rural areas. During the 2012 Superstorm Sandy it was mostly unaffected due to back up power and redundant systems, while cell and public safety radio services were compromised due to flooding [12]. Datacasting has been successfully employed for one-to-many data distribution via

Distribution is the process by which organizations identify and disseminate the right information to the right individuals at the right time. Mechanisms to distribute public safety video vary depending on data handling policies and procedures and may be comprised of manual or technical means, or a combination of both.

2.3. Encoding and Compression

Video encoding is the process of compressing and potentially changing the format of video content, sometimes even changing an analog source to a digital one for the purpose of consuming less space, thereby improving the efficiency of transmission, storage, or use. The choice of encoding format is driven by the target destination and use [13]. For example, different encodings may be used for mobile device playback (e.g., phone) versus storage in a data management system.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Video codecs are video compression standards implemented through software or hardware applications. Each codec is comprised of an encoder, to compress the video, and a decoder, to recreate an approximation of the video for playback. The name "codec" comes from a merging of these two concepts into a single word: enCOder and DECoder. Example video codecs include H.264, VP8, RV40 and many other standards or later versions of these codecs, like VP9. Although these standards are tied to the video stream, videos are often bundled with an audio stream which can have its own compression standard [13].

Transcoding is the process of changing one video format to another.

Compression "is an algorithmic sequence of operations designed to reduce redundancy in a data source, so that the data may be transported within a prescribed communication network. This can be achieved in a number of ways: reducing color nuances within the image; reducing the color resolution with respect to the prevailing light intensity; removing small, invisible parts of the picture; and by disregarding the parts of the picture that remain unchanged from the previous frame. All of these techniques are based on the way the human brain and eyes work together to form images. As a result, these subtle reductions account for a significant reduction in file size and lower bit rate yet have little or no adverse effects on the visual quality [13]." Compressing data leads to a tradeoff between transmission data rate, data quality, and latency [13]. Compression is typically a lossy process that eliminates spatio-temporal details and redundancies from the video to reduce its size. An approximation of the original is generated upon decompression for playback. As more compression is applied, more data is thrown out, and the approximation looks less like the original.

Containers are used to encapsulate everything in transit from the device or from data storage during retrieval. Containers can contain video, associated audio, and metadata. MKV (Matroska Video), WMV (Windows Media Video), AVCHD (Advanced Video Coding, High Definition), and MP4 are common examples of digital container formats. Containers store metadata and bytes from a codec in a way that compatible applications can play back content, but they do not define how to encode and decode the video data [13].

Considerations: Encoding and decoding should be compatible for all data, structured and unstructured, including camera position, time, geospatial, subject, event, audio, video, video quality, and derived analytics. They must also support how the operator needs to interact with the video (e.g., rewind, fast forward, frame-by-frame playback) at the necessary data rates. Compression efficiency is influenced by the video content. For example, compression rates will be different for data from a moving camera than from a fixed camera and can influence the resulting quality. Improvements to video compression best practices and implementation will drive toward optimal compression for particular uses/operations and content and optimization of video for both human and analytic consumption.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

2.4. Alerting, Triage, Forensics

Alerting, triage and forensics are addressed together, because they are different uses of metadata and analytics derived from video. The objective of video analytic interoperability is to enable the application of analytics at any point in the workflow, giving a user the ability to receive an alert, triage the data or forensically examine the data in support of real-time operations from any point in the system. Definitions for alerting, triage and forensics use are below:

- An *alert* is a notice initiated to make someone aware of something, such as an event or other condition based on prescribed rules or thresholds [13].
- *Triage* and real-time processing of real-time video data is a critical technology enabler for improving the speed and effectiveness of emergency response. Public safety will need analytic solutions that can process high-velocity volumes of big data quickly, so that they can react to changing response conditions in real time [7].
- *Forensics* enables real-time application of video analytics to retrospective, forensic analysis of archived data [3].

2.5. User Experience/Visualization

User Experience relates to user's perceptions and responses that result from the use and/or anticipated use of a system, product or service. Factors such as brand image, presentation, functionality, system performance, interactive behavior, and assistive capabilities of a system, product or related service can impact the user experience. A user's internal and physical state resulting from prior experiences, attitudes, skills, abilities and personality can also influence the experience with a product or system [12].

Visualization is the process of representing data graphically and interacting with these representations in order to gain insight into the data. Traditionally, computer graphics have provided a powerful mechanism for creating, manipulating, and interacting with these representations.

> *Considerations:* Public safety's focus alert generation currently centers on communications from public safety to the public. Interoperability for this is achieved through the Common Alerting Protocol (CAP) standard, which allows Federal, state, local, tribal, and territorial alerting authorities to send mass alerts to multiple outlets via the Integrated Public Warning and Alert System (IPAWS). IPAWS leverages and provides the ability to alert the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and other public alerting systems via a single interface [53].

Usability is the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use [14].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

User interface includes all components of an interactive system (software or hardware) that provide information and controls for the user to accomplish specific tasks with the interactive system.

> *Considerations:* According to one blog, data storage often exceeds 30% of the cost of an entire video surveillance solution [52]. In public safety literature, legal and policy requirements for data retention and continuity of operations considerations have driven data storage requirements, and these vary between jurisdictions. Stakeholders report that requirements range between two and ten years. Public safety video operations planners must monitor changes in these retention requirements, but they should consider the number and resolution of cameras, video duration, codecs, and data retrieval, as well as the impact of

2.6. User Access

User Access refers to User Access Management (UAM) or Identity Access Management (IAM) processes which enable access to, and grant permission levels for, a user to read, write, edit, or delete information within a network or application.

2.7. Data Management/Data Storage

Data management includes stream/multi-stream management, data optimization, smart transcoding for preserving bandwidth for data on the move, and quality analysis for optimizing data for use by humans and analytics. The process of managing these is also referred to as data wrangling. Management of video data sources requires optimal management of the video, video indices and associated data (e.g., audio, metadata) to support the intended use which can include video presentation, playback, editing, conferencing, education, and processing.

Data storage describes how information is kept and may be retrieved later. Video data may be stored temporarily using random access memory or saved to hard drives or solid-state drives either locally or in the cloud that is at a centralized public safety or commercial data center. Present recommended best practices for VSS network security usually place devices like IP video well behind corporate firewalls. Data storage requirements increase as data quality increases. Higher resolution and lower compression rates require increased storage capacity.

3. Interoperability Model for Video Analytics

Executive level public safety stakeholders need a consistent and familiar model to frame video analytics interoperability issues. The DHS SAFECOM Interoperability Continuum was created as a path for achieving interoperable voice and data communications for first responders. This current Continuum offers a balanced framework for articulating gaps and challenges identified by public safety stakeholders [1]. SAFECOM identifies interoperability as a multi-dimensional challenge and suggests regions should consider five independent elements to evaluate and optimize communications interoperability. The five areas are governance, standard operating

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

procedures, technology training and exercises, and usage, as shown in Figure 2. Adjustments have been made to the continuum's governance element to describe necessary support structures outlined in Section 3.1.5. Also, the technology continuum removes voice elements narrowing the focus to data. Video is considered as a subset of data; therefore, it remains appropriate within the continuum. However, dedicated efforts specifically focused on the video subset will be required across all five elements to realize interoperable video analytics outcomes.

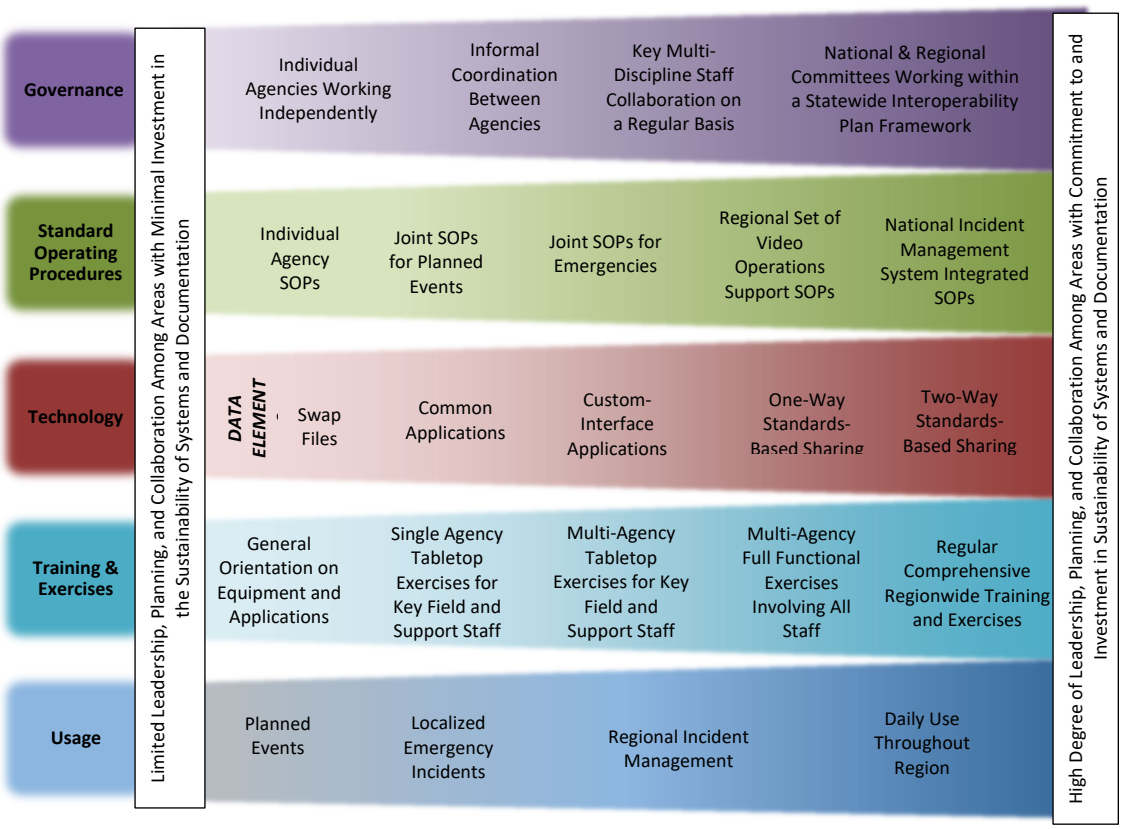

Figure 2. Adapted Video Analytics Interoperability Continuum

This section describes the current state for each element and identifies additional stakeholders, standards, and models that can influence the public safety video analytics community. This is followed by key takeaways. Each element concludes with a matrix which enumerates needs and desired outcomes and lays forth a potential three-phase roadmap to reach the desired state.

- **Phase 1: Laying the Interoperability Foundation.** Activities in this phase establish the basis for successive phases by defining how the community researches, develops, uses, and trains for the adoption of video analytics.
- **Phase 2: Moving Toward Shared Practices and Standards.** In Phase 2, best practices and standards are identified or developed to improve data sharing and interoperability.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

- **Phase 3: Implementing Common Practices and Interoperable Components.** Phase 3 realizes the practical implementation of activities through technology adoption, standards codification, and exercises.

The Public Safety Video Analytics community is responsible for development of the products and accomplishment of outcomes identified in this roadmap. The community will need to determine the approaches and organizations involved with specific product/outcome completion.

3.1. Governance

Governance is a broad term that describes the oversight and management of activities or businesses. Although it can encompass many things, in its simplest form it defines the rights and responsibilities of various stakeholders, sets the process for decision-making, and establishes checks and balances. Governance operating models and frameworks help boards and managers implement policies, best practices, and job responsibilities [15].

The Public Safety Video Analytics community initially grew out of a Federal Networking and Information Technology Research and Development (NITRD) Video and Image Analytics (VIA) Working Group deep dive into public safety video analysis. A multi-agency partnership arose through those efforts and led to the VAPS community. The community, comprised of representatives from the stakeholders identified in Appendix A, is informal and loosely organized around events and workshops sponsored by the DHS Science and Technology (S&T) Directorate Office for Interoperability and Compatibility Technology Center (OIC-TC). Until October 2019, OIC-TC funded the Video Quality in Public Safety (VQiPS) program in conjunction with Johns Hopkins Applied Physics Laboratory and the NIST Public Safety Communications Research Program's Video Analytics in Public Safety (VAPS) programs.

3.1.1. National Level

Multiple national level organizations exist with the authority, mission, and ability to guide and influence the maturation of video operations and video analytics for public safety. Some have already initiated research, workshops, or subcommittees to identify emerging issues in video for public safety. Below organizations with active or recent efforts in public safety video are listed, followed by potential stakeholders not already directly engaged.

- **Video Quality in Public Safety (VQiPS).** DHS S&T's VQiPS initiative has provided information and support to first responders so they can articulate their video quality needs and buy the best products to fit their unique needs. VQiPS has also documented policy considerations for agencies in the process of establishing or implementing recently established video systems. VQiPS quality efforts have not yet extended to computer vision technology or the full range of analytic interoperability needs for video operations.
- **National Institute of Justice (NIJ).** The U.S. Department of Justice's research and evaluation agency improves knowledge and understanding of crime and justice issues through multi-disciplinary research and evidence-based knowledge. In 2017, NIJ's sponsored research on the use of video analytics and sensor fusion for law enforcement built upon NISTIR 6184 by identifying four business use cases, innovation needs and a near term investment roadmap [10].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

- **National Public Safety Telecommunications Council (NPSTC).** NPSTC is a practitioner driven organization comprised of fifteen public safety organizations, state, and local government representatives, as well as federal representatives, which focuses on improving public safety communications and interoperability. With participation from users, technology developers and other experts, NPSTC evaluates capabilities and provides advocacy for public safety through reports, white papers, and public comments to government authorities.
  - Video Technology Advisory Group (VTAG), which falls under the Technology and Broadband Committee, serves as an intermediary between the VQiPS and VAPS efforts and the broader community of public safety users and technology developers by making available news, information, materials, and meeting schedules.
  - Interoperability Committee promotes the elements of the SAFECOM Interoperability Continuum and leads five working groups which identify and review issues, make recommendations and create standards to improve interoperability of communications. The Interoperability Committee's working groups currently include Channel Naming for LTE, Communications Unit Training, Cross Border Communications between the United States and Canada, Emergency Medical Services, Project 25 (P25) Standards for Land Mobile Radio (LMR), and Radio Interoperability Best Practices.
  - Internet of Things (IOT) Working Group, which also falls under the Technology and Broadcast Committee, examines specific the current state of IOT and identifies specific areas and issues which should be brought to the NPSTC Governing Board for review. The working group's June 2019 report identifies eight use cases for the application of IOT devices and analysis of IOT generated data, including a variety of video types [16].
- **NIST PSCR Public Safety Innovation Accelerator Video Analytics Research and Development Grant Awards.** NIST PSCR Analytics Portfolio stimulated R&D in video analytics key technology need areas and increased community collaboration between grant award winners and public safety departments. This research has also led to two informal two-day meetings to compare progress and build relationships for future research collaborations. These two- and three-year grants will terminate in June 2020.
- **DHS Federal Emergency Management Agency (FEMA).** FEMA manages the National Incident Management System (NIMS) which defines a comprehensive approach for jurisdictions and organizations to work together to share resources, integrate tactics, and act collaboratively to save lives, stabilize the incident, and protect property and the environment. NIMS key principles of interoperability; reliability, scalability and portability; resilience and redundancy; and security align closely with VAPS stakeholder technical issues and data collection from public safety video is already incorporated in the NIMS plan. FEMA develops and delivers training to support the implementation of NIMS [17].
- **Association of Public-Safety Communications Officials.** (APCO) is an international organization which provides public safety communications expertise,

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

professional development, technical assistance, advocacy, and standards. APCO is also an American National Standards Institute (ANSI)-accredited Standards Developer (ASD) that reviews and develops operational, technical and training standards for public safety communications. APCO has voting membership on the NPSTC Governing Board.

- **National Council of Statewide Interoperability Coordinators (NCSWIC).** Sponsored by DHS Cybersecurity and Infrastructure Security Agency (CISA), Statewide Interoperability Coordinators (SWIC) from **56** states and territories play a critical role in organizing and executing interoperability efforts in all the states and territories. The NCSWIC maintains three working committees: (1) Planning, Training, and Exercise, (2) Funding and Sustainment, and (3) Technology Policy. The latter promotes the use of technologies, resources, and processes related to emergency communications and interoperability and works with Federal partners to further various technologies within the emergency communications ecosystem (e.g., Next Generation 911 (NG911), alerts and warnings) [18]. NCSWIC also has voting membership on the NPSTC Governing Board.
- **Federal Communications Commission Public Safety and Homeland Security Bureau (PSHSB).** PSHSB serves as the FCC primary expert on public safety and homeland security matters and promotes public access to reliable 911, emergency alerting, and first responder communications. PSHSB develops and implements policies, consistent with the FCC statutory authority, to address issues related to network reliability, resiliency, security, and interoperability; public alerts and warnings; and public safety communications, including spectrum management and interference resolution.

Occupied with the rollout of NG911 and FirstNet, only a few organizations have recognized the potential impact of the impeding explosion of video analytics technologies on public safety. Fortunately, in the near term the emphasis on communications interoperability makes some players strategically poised to take on leading roles in future public safety video analytics discussions as interest and funding permit. For example, the U.S. Fire Administration Strategic Plan for Fiscal Years 2019–2023 recognizes the need to enhance fire and EMS ability to identify, prevent, prepare, and mitigate community risks and encourage data driven decision-making and information sharing as strategic objectives. Interoperable video analytics has a role to play in supporting both objectives [19].

3.1.2. Regional and Local Level

Stakeholders note that overcoming organizational constraints and operational inertia is equally difficult to navigating technical challenges. They described a high level of difficulty in navigating local budgeting, acquisition, and approval processes across departments, mission areas and jurisdictions that precludes them from making joint decisions on systems architecture purchases and leveraging their collective buying power to obtain favorable pricing and influence vendor development. The inability to align video efforts within a jurisdiction gives rise to unplanned redundancies such as multiple cameras (police, public works, transportation, and major events) on the same pole with similar angles, different video communications networks and video management systems in multiple operations units, silos of video data, shortfalls in technical and training support, and increased cost to the taxpayer.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Stakeholders identified currently employed mitigations. First, they cited the development of consolidated shared systems and the appointment of a single department as the lead for video operations. This approach is driven by budget constraints in small to midsize communities. The second method was the collocation of disparate video operations in county or regional operations centers.

Only one approach noted during the workshop highlighted a strong governance mechanism with broad sharing of video data, from the Metropolitan Washington Council of Governments (COG), an independent, nonprofit association with a membership of 300 elected officials from 24 local governments, the Maryland and Virginia state legislatures, and U.S. Congress. COG is supported by financial contributions from its member governments, federal and state grants and contracts, and donations from foundations and the private sector. Under the guidance of the COG Board of Governors, which sets plans, priorities, and policies, the COG addresses transregional needs for transportation, environment, community, homeland security and public safety through numerous committees. Committees are chaired by, and membership is comprised of, local government officials. COG-funded staff members support committee administrative needs with data analysis, strategic policy development, meeting coordination and scheduling, and research support. The COG staff and Chief Contracting Officer committee enable the collective purchasing of items and services through their Cooperative Purchasing Program, reducing costs for jurisdictions through economies of scale. [20]

Through the COG supporting framework, public safety officials in the National Capital Region (NCR) are able to exchange data through the National Capital Region Interoperable Communications Infrastructure (NCR ICI), also known as NCRnet—a private, high-speed fiber optic network interconnecting 24 regional jurisdictions and municipalities as well as the Metropolitan Washington Council of Governments (COG). The network is primarily comprised of dedicated fiber optic strands, with limited use of leased wavelengths where dedicated strands are not currently available. Network links typically operate at Ethernet speeds of either 10 or 1 gigabit per second [21]. The COG CIO committee oversees and guides technical development and security, while the Homeland Security Executive Council sets funding priorities and determines public safety and emergency response objectives and goals. NCRnet offers Identity and Access Management Services for federated login to regional applications and a Data Exchange Hub which provides a set of standards and methodology that form a “template” for building and implementing public safety applications that translate data between different systems and regional sources. This common vocabulary and structure facilitates improved situational awareness in the region and eases future growth of sharing of CAD, GIS, law enforcement, and other data [22].

3.1.3. Economic Challenges

NISTIR 8255 identifies economic challenges related to interoperability in the current environment, observing that the selection of interoperable and non-interoperable products essentially becomes a cost-benefit analysis between financial and efficiency constraints [23]. Video analytics stakeholders’ inputs echo this point, noting that demands to expand geographical coverage and performance often outweigh lifecycle costs for training, routine maintenance, technical support, and necessary upgrades to maintain compatibility between cameras and devices, data storage and management, or analytics.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

As public safety struggles for influence and support to have its needs met by the $52.31 billion global surveillance system market, it is also unrepresented in industry dominated standard organizations and forums [24]. The 2018 workshop planning efforts identified a sole standards group focused on video surveillance. Open Network Video Interface Forum (ONVIF) is an international forum open to manufacturers, software developers, consultants, system integrators, end users and other interest groups which aims to standardize how IP products within the video surveillance industry communicate with each other. ONVIF focuses standardizing the network interface (i.e. network layer) of network video products which does not support all necessary interoperability functions across the video analytics workflow [25]. Full voting membership in ONVIF is $20,000 annually, a price beyond the budgets of most public safety organizations and the small to mid-sized VMS companies that support them [26]. ONVIF partners with the International Electrotechnical Commission (IEC) Technical Committee 79/Working Group 12 to identify public safety interoperability requirements and set ISO standards. Awareness of VAPS efforts have generated interest and invitations from the IEC to participate in teleconferenced working group meetings, attend annual face-to-face events, and nominate a deciding member to an upcoming ISO standard development effort. However, current governance and funding mechanisms are not agile enough to realize representation within a single fiscal year. Responsibility, authority, and capacity to represent US public safety interests in the international standards community are not yet aligned and codified.

3.1.4. Key Takeaways for Governance

- Although many stakeholder organizations have roles to play in the advancement of video analytics, the community is in need of an authoritative body with the mission and funding to coordinate national and state level activities that could eventually lead to interoperable technologies and standards, common best practices, and professionalized staff to support emerging real-time video analytics.

- Continuing coordination and research funding at the national level is required to maintain and update quality guidelines and spearhead new interoperable video technologies and analytics.

- Adoption of local governance models could improve relationships amongst public and private partners, address unplanned redundant systems, and achieve cost savings for departments and taxpayers.

3.1.5. Governance Roadmap

There is a deep, persistent need for governance forums and mechanisms at local, regional, and national levels that can bridge the divides between the public safety mission areas and drive toward common resilient video architectures that support interoperable data for real time and forensic public safety operations. Drawing upon issues across the five elements in Section 3, Table 1 identifies a sample set of challenges, desired outcomes for governance mechanisms and suggests activities in a phased approach that could assist the public safety video analytics community in addressing them.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Table 1. Potential Elements for a Future Governance Roadmap

Area	Challenges and Gaps	Desired Outcomes	Phase 1	Phase 2	Phase 3
GOV-1	Video Quality Guidelines do not address interoperability needs for inclusion of video analytics in the workflow.	Public safety organizations (such as VQiPS) publish detailed guidelines that address the technical considerations and standards needed to ensure analytic performance and interoperability of data for public safety workflows.	Socialize proposed guideline updates	Review, draft, and update with considerations and best practice information.	Review, draft, and update based on research outcomes and standards recommendations.
GOV-2	Need to improve relationships between stakeholders within a jurisdiction.	A local governance model facilitates a mutually respectful environment for professional to exchange perspectives on mission needs and facilitates the development of best practices.	Identify opportunities for collaboration; research and engage community and regional governance models and organizations that collaboratively address cross jurisdictional issues; identify models suitable for jurisdiction.	Identify potential member partners and champions; develop business plan; design implementation plan; identify gaps and needs; identify risks and mitigations; garner funding and support.	Implement business plan; expand membership.
GOV-3	Challenges in navigating difficult budget, acquisition, and approval processes to enable collective decision making for video architecture and components	Local and regional governance models facilitate consensus of Chief Information Officers and administrators on technology insertion and enable collective purchasing to lower joint costs.			Expand local and regional governance forums to include an acquisition element; establish policies and procedures for joint requirements development and source selection.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

	giving rise to unplanned redundant components.				
GOV-4	Need for an overarching governance body and infrastructure to support national events to unit stakeholder, conduct outreach, or set agenda to address issues across the police, fire, EMS, and communications sectors.	The Public Safety Video Operations community has a federal champion and single focal point that facilitates intra- and interagency relationships and coordinates stakeholder engagements to solve gaps in public safety video communications.	Identify lead government agency to spearhead video interoperability efforts with stakeholders and across federal stakeholder agencies; develop and maintain online forum for information exchanges; create organizational structure to govern and support annual events and ongoing working groups that prioritize and address SOP, technology, training, and usage needs; coordinate and track annual budget; identify contracts, grants, challenges, and other mechanisms to fill video analytic interoperability gaps.	Conduct outreach to encourage inclusion of video into national level strategic planning efforts; hold meetings and workshops to facilitate stakeholder evaluation and adoption of SOPs, technology standards, training curriculum requirements, and use cases; maintain online forum, governance and support structure; coordinate and track annual budget; identify contracts, grants, challenges, and other mechanisms to fill video analytic interoperability gaps.	Monitor progress; continue cross agency collaboration; hold annual meeting; maintain online forum, governance and support structure; coordinate and track annual budget; identify contracts, grants, challenges, and other mechanisms to fill video analytic interoperability gaps.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

GOV -5	Need for a forum for ongoing constructive discourse on societal concerns.	Governance mechanisms foster and maintain dialog with the community, garnering insight on community expectations, and transparency into the privacy controls utilized by public safety.	Identify venues to maintain community engagement at local and regional levels; include societal concerns topics and panel discussions at national level meetings; identify and fund privacy related RDT&E.	Discuss privacy related R&D findings in public forums and elicit feedback; evaluate and acquire validated privacy solutions.	Maintain community engagement on societal issues.
GOV -6	Need for ongoing industry and standards organization engagement.	Governance mechanisms serve as the public safety focal point to identify government and industry leaders to carry forth requirements in industry led and dominated standards forums; and provide updates on standards relevant to public safety video operations.	Identify immediate standards development efforts impacting public safety; nominate delegates to participate in standards development; engage public safety vendors participating in standards organizations.	Include a standards presentation and invite standards committee members to participate in public safety technology panels at national events.	Ongoing.

3.2. Standard Operating Procedures

The public safety community is rich in policy and procedure development. Legal and policy concerns around video necessitate guidance and documentation for handling of video data, and these, along with increasing privacy concerns, drive current procedures for the management of video data systems. Guidance documents from VQiPS on system considerations are not intended as policy documents or standard operating procedures, so it appears to most stakeholders that individual agencies have generated their own [11]. Stakeholders anecdotally addressed procedures during workshop discussions as they relate to login and access, privacy management and data release, and data handling of digital media evidence [27]. Despite these stakeholders' concerns over standards and best practices in video analytics, interoperability ranked as their second highest need.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Most Stakeholders articulated that the operational tempo of daily missions generates fragmentation amongst the community and entrenchment in technologies and operating practices without the opportunity to make informed upgrades and changes. Stakeholders indicated that DHS-sponsored video quality and video analysis related workshops have done much to improve their understanding of best practices and have informed current standard operating procedures. Participants in the two-day 2018 VAPS event remained focused on increasing their understanding of standards and best practices for technical interoperability in their own ecosystems, before expanding to multi-jurisdictional or regional level standard operating procedures for video analytics interoperability.

Other participants cited the need to improve relationships and standard operating procedures within their jurisdictions to overcome data sharing obstacles and constraints arising from governance and political decisions. Along these lines, one stakeholder noted that responsibility for video operations and analysis for planned events such as large sporting events and festivals can fall under a different city department than those for daily public safety missions.

However, some regions with multiple jurisdictions that frequently need to exchange information and data have made progress in exchanging procedures and jointly adopting technologies. Examples include collocation of personnel and video systems at county and state fusion centers in Raleigh-Durham, North Carolina; the National Capital Region Metropolitan Washington Council of Governments; and Los Angeles County efforts to develop requirements for the construction of the 5G LTE network.

The exchange of video data is based on data sharing agreements which require multiple levels of legal review and coordination. Public safety video operations managers cited a need for additional insight on generating and maintaining agreements. NISTIR 8255 addresses critical elements for data sharing policies including data definitions, data management, data ownership, data access, data security practices, data integration, data retention, data redaction, and data policy consistency [23].

An organization that has relevance and authority for network best practices but has not yet been involved in VAPS forums is the FCC Communications Security, Reliability, and Interoperability Council (CSRIC). CSRIC is an advisory council with the responsibility for making recommendations to the commission to promote the security, reliability, and resiliency of the nation's communications systems. Under the current charter which runs through March 2021, CSRIC will focus its recommendations on a range of public safety and homeland security-related communications matters, including these topics: (1) the reliability of communications systems and infrastructure; (2) 911, Enhanced 911 (E911), and NG911; (3) emergency alerting; and (4) national security/emergency preparedness (NS/EP) communications, including law enforcement access to communications [28].

CSRIC recommendations lead to prioritized best practices including those for network interoperability for public safety and government, as well as for service providers, network operators, equipment suppliers, and property managers. Best practices are made available online and are searchable by topic and industry sector with filters for network types, industry roles, and keywords. CSRIC best practices address requirements applicable to maintenance and security of interoperable video networks and align to the current best practices described by video operations personnel. While neither video analytics nor video interoperability are specifically

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

addressed in CSRIC current best practices, they can provide a starting point for the development of a best practice baseline and overall approach for the public safety video analytics community.

An example of CSRIC work is *Best Practice 11-9-0803* which encourages network operators, service providers, public safety and equipment suppliers to continue to participate in the development of standards for traffic management to promote interoperability and assist in meeting end user quality of service needs. Ranked as an important requirement by CSRIC, in the video analytics community this may be ranked as a critical requirement for two reasons. First, collaboration in this area does not currently exist. More importantly, second, is the VAPS community's gap in establishing end user quality of service requirements for the various elements of the video data workflow.

Other best practice needs cited by stakeholder's center on alerting, privacy controls such as more robust de-identification mechanisms for video data, and data management. Sponsored participation in collaborative meetings that facilitate understanding of current operating procedures employed and generate consensus best practice improvements in these areas was of high concern to stakeholders. Consensus on the best practices and identification of needs will drive baseline requirements for policies and procedures as well as identify gaps for technology research, development and investment.

3.2.1. Key Takeaways for Standard Operating Procedures

- Although frameworks, forums, and resources for common standard operating procedures and practices relevant to video operations are available, knowledge of those outside of previous DHS S&T VQiPS efforts remains relatively unknown to stakeholders that participated in VAPS events.
- Exchange of best practices and development of common operating procedures which are necessary to steer technical, training, or other areas require time and resource commitments by experienced public safety video experts.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

3.2.2. Standard Operating Procedures Roadmap

The development of standard operating procedures and best practices are considered critical for enabling training and technical activities in phases two and three. Table 2 offers a starting place for leaders and stakeholder to further identify and discuss the challenges of the public safety video analytics community in creating standard operating procedures. Challenges and gaps are followed by desired outcomes, and suggested activities that could be taken to develop and sustain a community of practice.

Table 2. Potential Elements for a Future Standard Operating Procedures Roadmap

ID	Challenges and Gaps	Desired Outcomes	Phase 1	Phase 2	Phase 3
SOP-1	Best practice development.	Community best practices inform training and technology requirements.	Identify and nominate one individual to participate in national level governance committee; support attendance and participation.	Ongoing.	Ongoing.
SOP-2	FCC standards and best practices address some, but not all of public safety video network needs.	FCC standards encompass video network requirements and best practices for maintenance, patching, and troubleshooting.	Review and adopt applicable CSRIC best practices; define and identify gaps.	Collect research findings and community best practices.	Finalize research findings and community best practices; gain community consensus on best practices and standards; present findings to CSRIC for recommendation to FCC.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

SOP-3	Video operations leads seek insight on developing and maintaining data sharing agreements.	Data sharing agreements enable sharing across public safety and its partners and provide the technical insight necessary to facilitate and maintain the flow of data.	Review NISTIR 8255 and current agreements; incorporate criteria into new agreements.	Update expiring agreements and review agreements annually with partners to identify changes.	Ongoing.
SOP-4	Privacy and de-identification best practices.	Best practices are employed across public safety to maintain the privacy of individuals and entities captured in video images and metadata.	Identify manual and computer processes in practice, current research, review NIST Privacy Framework V1.0 [29], and document recommendations; document findings on privacy and de-identification best practices; socialize and update local policies.	Monitor and participate in evaluation of new privacy and de-identification technologies; update best practices.	Ongoing.
SOP-5	Video data management best practices.	Best practices for annotating, tagging, storing, and retrieving data provide ready access to aggregate and analyze data, ensure the chain of custody of data throughout a variety of use cases and workflows.	Identify policies and best practices for raw (gold copy) and processed video data; document findings; update local policies.	Monitor and participate in evaluation of new privacy technologies; update best practices.	Ongoing.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

SOP-6	Alert best practices.	Best practices and streamlined workflows accelerate alert notifications for video operators, first responders, and the public; and ensure logging of events for future reference and retrieval.	Identify current best practices and workflows; envision future computer aided workflows and event logging requirements.	Monitor and participate in evaluation of new privacy technologies; update best practices.	Ongoing.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

3.3. Technology

In the last 20 years, the industry supporting video monitoring technologies has made marked advancements – especially with regard to video quality and transmission. Video resolution has improved dramatically with current security cameras typically supporting resolutions well exceeding HDTV standards. During this time, communications technology has also rapidly evolved to support fiber optic and high-speed wireless and cellular network communications. Likewise, the cost of data storage has dramatically plummeted due to both hardware advances and the creation of Cloud-based data storage systems. Despite the plethora of new technologies from other industries which have supported marked improvements in systems to support security video streaming, the interoperability of the systems to support public safety use and sharing of video resources has lagged. This can be partially attributed to the growth of the video monitoring industry largely from security camera manufacturers. This section explores the current state for public safety in terms of the interoperability for public safety video monitoring and analysis technologies.

To describe the current state of technology, this document adapts the interoperability model developed by Healthcare Information and Management Systems Society, Inc. (HIMSS) for healthcare information systems. HIMSS is the global advisor and thought leader organization which drives interoperable data exchange for patient healthcare [30]. The HIMSS model contains interoperability *subtype*s: (1) foundational, (2) structural, (3) semantic, and (4) organizational. This model is readily extended to other technology domains. These subtypes are adapted to the public safety video monitoring and analysis domain for their ability to provide an understandable approach for relating the often-overlooked technical interoperability challenges at the physical, transport, and application levels.

3.3.1. Foundational

Foundational interoperability develops the building blocks of information and interconnectivity requirements needed to exchange information between disparate video devices in the field and analysis systems.

DMC sources, specifically VSS cameras, and Video Management Systems (VMS), are the most recognized hardware components networks. However, switches, routers, encryption devices, virtual private networks, servers, client terminals, and monitors all make up the backbone of

video operations networks. Foundational interoperability rests on the physical connectivity of these devices through copper, fiber, ethernet, or wireless networks, as well as the routing protocols that control the flow and direction of information through the networks. It also includes the authentication and authorization of these devices based on IP or MAC addresses through a directory services server which then allows them to communicate and relay data.

Maintaining video interoperability in the current environment is complex. Jurisdictions may receive data directly from hundreds of cameras. Additionally, they may receive and integrate video data from two or more subnetworks and transmit images back to scene responders via another. For example, a potential fire at a dock may be captured by a camera on the port authority's local area network. A data sharing agreement between the port authority and the regional operations center (ROC) has allowed ROC personnel to access and monitor port cameras on a subnet of the local police video network. Video operators at the ROC spot the fire and contact dispatch personnel. Meanwhile, operators isolate a few seconds of video frames and email the footage to dispatch, who then push the video clip to the responding fire chief's wireless mobile device. Alternatively, some organizations are exfiltrating data from their PSIMs to other video systems that allow mobile devices to subscribe to video feeds inside public safety firewalls.

Public safety stakeholders describe a host of physical issues impacting the video networks such as the lack of surge protection or electrical grounding, camera mounts weakened by water, viewing on low quality monitors, and data uplink paths being interrupted by other city services.

Cameras in the current environment differ in age, resolution, and purpose. These range from traditional high definition closed-circuit television (HDCCTV) cameras to newly emerging Internet of Things devices such as doorbell cameras and video from live streaming social media applications from mobile devices. Video devices vary in terms of resolution ranging from standard definition (720x480 pixels) to newer 4K (3840x2160 pixels) and between 5 and 30 frames per second. Best practice for public safety video operations currently recommends high definition cameras [9].

Routing protocols at different layers of connectivity facilitate the flow and direction of video data through these networks. Two primary network transport models, the Transmission Control Protocol/Internet Protocol (TCP/IP) and the Open Systems Interconnection (OSI) are employed as frameworks for routing. The United States Department of Defense-developed TCP/IP model has four layers: link, transport, internet, and application. It assumes that physical specifications exist and that a working network infrastructure is in place for the protocols to work. Preferred in Europe, the OSI model is a seven-layer model for networking that includes a physical layer at its base. Failure to plan for the physical layer in video networks can inhibit interoperability and create artifacts that impact the performance of video analytics.

Routing protocols facilitate addressing of devices and network performance monitoring, and they determine the direction in which the information moves through the network (distance vector, shortest path, or a hybrid combination). The emergence of new protocols and heterogenous networks over the last decade is enabling devices on the networks to use multiple ports for routing and receiving data. These protocols are giving rise to new peer to peer (P2P) devices and new options for public safety to build resiliency through self-healing and mesh networks.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Adoption of protocols such as such as the Rapid Spanning Tree Protocol (RSTP) can provide a needed bridge at the application layer which will allow for data sharing.

3.3.2. Structural

Structural interoperability describes the video information exchange format designed to sustain data quality and meaning and to preserve operational purpose. This topic encompasses the encoding, decoding, and transcoding functions associated with transmission and broadcast, as well as quality factors such as resolution, frame rates per second, bit rates, and pixels per foot.

Public safety video operations engineers face a staggering number of structural interoperability issues. For example, investments made to upgrade cameras to HD to improve interoperability with a new VMS employing a video analytic may be of little value if HDMI cables are not utilized or the human-in-the-loop operator who must verify an alert views it on a VGA monitor. The variety of cameras employed by public safety today generate video data in different formats, resolutions, and at different rates (e.g., 30 frame per second, 5 frames per second), and piecemeal video systems can have multiple device types. These often vary in type, age and version, and many are not replaced or upgraded until end of life. A new higher resolution camera from a less expensive vendor may be incompatible and unable to be viewed on the VMS, even when viewed on an equivalent high-resolution screen. The VQiPS group has documented best practices and considerations for ensuring interoperability; however, the diversity of approaches in video encoding remains a challenge.

Sira, a UK-based company in the VSS industry specializing in transcoding video formats into a common viewer, notes that in the video surveillance industry there a several thousand variations of video formats, with only some of the companies offering export options for their proprietary code wrapped in AVI or other container formats [31]. Containers are used to encapsulate everything in data storage. MKV (Matroska Video), MOV (short for MOVie), AVI (Audio Video Interleave) and other file types are examples of these container formats. Containers store metadata and bytes from a codec in a way that allows compatible applications to play back content, but they do not define how to encode and decode the video data [13]. To highlight the issue, in 2013 Sira surveyed CCTV manufacturers, distributors, and installers regarding transcoded export formats in current DVRs. Manufacturers may support multiple formats; therefore, the percentages exceed 100% in Table 3.

Table 3. Results of Sira Study on Supported Video Export Formats for DVRs [30].

H.264 (MPEG-4 part 10)	72.2%
MPEG-4 part 2	50.0%
JPEG	27.8%
MPEG-2	27.8%
JPEG 2000	13.9%
Formats not listed	19.4%

Around the same time as the Sira survey, industry organizations jointly developed the High Efficiency Video Coding (HVEC) or H.265 or MPEG-H Part 2 video compression standard. Offering 25-50% better data compression supporting improved video quality at similar bit rates to H.264 and resolutions up to 8K UHD. Despite improved performance offered by HVEC,

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

H.264 remains the most used codec over the last consecutive years, but a recent survey of video developers by Bitmovin indicates that developers will lean towards H.265 over the upcoming year. [32]

While the use of containers and transcoding from proprietary collection device formats to VMS may alleviate transmission issues, it is not without additional cost and does not solve all interoperability challenges. The datacasting distribution approach has an advantage in the broadcast industry's full adoption of the MPEG standard.

Beyond the complexities of encoding, decoding, and transcoding, stakeholders also noted that interoperability breaks, even in homogenous proprietary systems, as vendors introduce new functionality in upgrades. The ability to patch all devices in a timely fashion while maintaining daily operations can be a contributing factor to the breakdown; however, often new devices may contain new variants of old code that appear compatible on the surface at purchase but fail to transmit seamlessly upon implementation. To compound the matter, upgrades to devices in the field frequently require manual upload at the device location, which is manpower and time consuming and may require multiple trips to troubleshoot. This problem is further explored as an obstacle to usage in Section 3.5.1.

Shah et. al highlight an additional structural challenge related to the current impacts of transmission caps and bandwidth on video quality based on lessons learned from Houston and Baltimore video architectures [33]. Insertion of communications and network monitoring analytics are being adapted to improve monitoring of video ecosystems for data packet loss as an aspect of monitoring structural interoperability.

Industry has responded to this need with the development of Converged Security Information Management (CSIM) systems which can be utilized to monitor network performance data, as well as video data from multiple VMSs. CSIMs are applications which include a data process to transcode data from various VMSs and present it in a single proprietary user interface. With respect to technology, this is a stride forward for public safety, but for financially and manpower strapped public safety video operations units, it also adds another layer of applications to learn, manage, and support.

3.3.3. Semantic

Semantic interoperability provides for common underlying models and codification of data, including the use of data elements with standardized definitions from public safety taxonomies and coding vocabularies, providing shared understanding and meaning for system interpretation and analysis to public safety video operators and decision makers.

Already vendor offerings are beginning to include object and behavior analytics such as abandoned bag, weapons detection, and other types of recognition algorithms of value to public safety. Insertion of analytics within capture devices would enable them to start or stop recording based on prescribed events or rules (e.g., gunshot, emergency call). This insertion is referred to as edge detection or analytics at the edge. It moves identification of incidents away from operations centers and human video operators and changes their role to one of verification.

As the public safety community adopts these analytics into the video workflow, it is necessary to understand that semantic interoperability depends on foundational and structural interoperability.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

More importantly, for video data to be useful for public safety video analytics it must be of high quality and possess the metadata necessary to retrieve it to support operations and train new models. Finally, semantic interoperability requires a shared understanding of data.

3.3.3.1. Factor 1: Data Quality

DHS's Video Quality in Public Safety Working Group defines video quality as "the ability of the emergency response agency to use the required video to perform the purpose intended." The current guidance requires video quality that enables the viewer successfully to recognize a specific element of interest within an incident scene at a certain discrimination level. In the present state, visual acuity research measurement, or studies based on a human operator's ability to view and understand the images being presented, is at the core of data quality [9].

Cognitive research suggests that humans are temporally resistant to variations in frame rates. Human interpretation capability does not decline when boundary data is lost, if the loss occurs at very low frame rates [34]. Humans may require less stringent foundational and structural technical requirements to interpret and alert first responders on incidents than do the emerging algorithms. On the other hand, human ability to interpret actual events may be confronted with a variety of biases and heuristics such as availability heuristic (in which people judge likelihood by how easily examples spring to mind), the anchoring heuristic (in which people stick with initial impressions), framing effects (in which people make different decisions depending on how information is presented), and premature closure (in which several alternatives are not pursued).

Blockiness originates from block-based encoding and results in an annoying impairment in decoded images and video frames at low bit rates [35]. Blockiness and pixellation can occur at higher frame rates (bandwidth) with high motion and/or errors due to communications channel issues. Research thus far indicates that peak signal-to-noise ratio (PSNR)[1] and blockiness show a direct relationship to algorithm performance for tested algorithms [33]. For machine interpretation, a new level of research is developing to understand the data quality requirements necessary to mimic human interpretation.

3.3.3.2. Factor 2: Metadata

Generation of metadata is an essential part of data curation and retrieval. There are two distinct types of metadata. First is the data which is embedded in the video related to the format of the data and describes the structural interoperability aspects addressed in the prior section. The second is data outside the video in a data asset management (DAM) system. The latter type of metadata contains three categories: administrative, descriptive, and rights.

In the current state, the bulk of administrative metadata is generated at point of capture, encoded, possibly wrapped in an AVI container, and transmitted to an operations center. This metadata usually includes the date, time, unique camera ID number, and location. If an edge analytic is applied, automated annotation may also include start and stop times for the incident and type of alert identified in the video segment. Currently, however, descriptive, semantic data for events is manually entered once a video operator identifies an incident and most often added before a copy of the video is sent for further review, archive, or evidence. A video operator's annotation will

[1] PSNR is the ratio between maximum possible power of a signal and the power of a corrupting noise that affects the fidelity of its representation.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

generally include a narrative description, an incident code or violation type, and his or her identity, precinct, or other jurisdictional information as part of the administrative data.

Multiple freeware, shareware, and proprietary video metadata editing software choices exist with read, write, edit, or delete functionality, and support for one or more of the leading video metadata standards. Primarily influenced by the film or news industry, current leading standards include the Extensible Metadata Platform (XMP) (ISO 16684-1:2012 part 1 & ISO 16684-2:2014 part 2), and International Press Telecommunications Council (IPTC) NewsML-G2[2] and Ninjs. IPTC also provides a Video Metadata Hub which includes recommendations for four layers of metadata (approximate values):

- 20 properties describing what can be seen and heard in the video
- 15 properties providing rights-related information
- 15 properties for administrative purposes
- 25 properties covering technical characteristics
- 15 structures of properties which are used for properties listed above [36],

Video Metadata Hub recommended properties have been mapped to four metadata schemas used by industry camera producers, as well as, NewsML-G2, XMP, IPTC's PVMD JSON, MPEG 7, PBCore 2.1, Schema.org, and the European Broadcasting Union's EBUCore. Camera industry generated metadata schemas vary, but for the most part they contain limited administrative and editorial data properties, structural technical properties (frame rates, codecs, formats, etc.), and camera information such as brand, model, and serial number. Location information to include latitude and longitude is also included on some camera schemas [37]. Descriptive metadata fields which could be used to describe public safety incidents are extremely limited.

The EBUCore metadata schema, combined with EBU's Class Conceptual Data Model (CCDM), provides a framework for descriptive and technical metadata for use in service orientated architectures and audiovisual ontologies for semantic web and linked data developments. The CCDM is an ontology which describes media industry business objects, i.e., media programs, specials, and their relationships to the various process phases from commission to delivery. Although they fall short of serving public safety needs, the maturity of such models and frameworks can offer a valuable reference for developers seeking to integrate traditional public safety reference data with video data in order to retrieve and consolidate video metadata and files from other video operations for analysis, or they can lead to seamless regional alerting from video [38].

Public safety is making inroads to common schemas through efforts such as the Association of Public-Safety Communications Officials' (APCO) newly adopted standard for *Next Generation 911 Emergency Incident Data Document*. This resource provides standardized, industry-neutral National Information Exchange Model (NIEM) conformant (XML-based) specifications for exchanging emergency incident information between agencies and regions. APCO's *Public*

[2] NewsML-G2 is an XML-based container for exchanging text, photo, graphic, video, audio, or other media type, and it allows exchange of full or partial news and event information. Ninjs standardizes the representation of news in JSON, providing a lightweight, easy-to-parse, data interchange format.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Safety Communications Incident Types for Data Exchange hold promise for semantic interoperability.

NIEM brings together a variety of domains ranging from agriculture to emergency management for the purpose of translating emergency incident information between information systems [39]. A manual review of NIEM's emergency management domain nametypes, properties, types, and facets were conducted to determine its current ability to aid in the interchange of video data between systems. At present, the emergency management domain does not contain relevant terms and definitions applicable to video; however, a keyword search of other domain areas, such as CBRN, biometrics, and intelligence, identified imagery terminology that could be adopted as a starting point for building a schema to facilitate the exchange of video metadata.

The OASIS Common Alerting Protocol (CAP) provides a standard format for alerts, enabling interoperable data exchange of alerts from public safety communications officials through the Integrated Public Alert and Warning System (IPAWS). No evidence suggests that the community is prepared for sending accompanied video through this system, and a future state where automated dynamic routing of alerts from cameras or other devices at the edge has not been envisioned.

3.3.3.3. Factor 3: Shared Understanding

Overcoming foundational and structural interoperability issues to produce optimal data quality for machine interpretation still may not provide semantic interoperability with results similar to those of humans. Semantic interoperability requires shared understanding. In the current state where video is manually reviewed, usually in an operations center, there exists opportunity for second review by one or more operators who are familiar with local procedures, protocols, and lexicon. Additionally, operators in large metropolitan area with multiple cameras usually can view an incident from multiple camera angles prior to alerting communications or first responders near the incident location. Seth Stoughton's work on interpretation of incidents based upon single viewpoints from body worn cameras highlights how camera perspective bias can impact interpretation of events [40]. This raises a continued need for video operators as critical participants in the process and the need for research analytics that correctly identify incidents and generate alerts based on multiple perspectives and media sources.

3.3.4. Organizational

Technical organizational interoperability relates to end users' access to, and interaction with, the data. The HIMSS model employed in this paper includes governance, policy, societal, legal and organizational considerations to facilitate the secure, seamless and timely communication of data within and between entities and organizations. Many of these areas are already addressed in other sections of this paper. For this roadmap, considerations are confined to technical controls applied at a field level to the data through processing, transformation, and loading of video data and metadata, as well as user access and authentication. The organizational interoperability subtypes are expanded further to add those analytic interoperability workflow components that present video data in a meaningful and intuitive way that meets organizational missions. This expansion includes user visualization and user experience, as they enable the functionality necessary to act on video data.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

3.3.4.1. Security

Cybersecurity is a foremost concern for most organizations with sensitive data. Cybersecurity addresses security of networks, hardware, software, and user access to data via these components. As such, it can impact multiple levels of interoperability. It is included here at the organizational level for ease of presentation to the reader.

Stakeholders at the 2018 workshop noted that architecture designs for emerging video management systems and many of the IoT device cameras on the networks have no defined cybersecurity controls [41]. This trend is evidenced in a recent survey of edge analytics platforms by Zhang et. al, which identifies 12 emerging architectures, only one of which contains a directory services component [41]. Directory services were initiated as part of an OSI initiative for common network standards and to improve recognition and interoperability of multiple vendor devices on a network. The commonly employed Lightweight Directory Access Protocol (LDAP) is based on the X.500 directory-information services, using the TCP/IP stack and an X.500 Directory Access Protocol (DAP) string-encoding scheme on the Internet. Vendors in the public safety video marketplace, most of which have historically been small to midsize companies, have touted proprietary architectures built upon proprietary encoding and metadata formats as an enhanced security feature to fill this gap.

At the user level, attribute, role, and policy-based controls can ensure that the right video data is seen by those individuals with the need to know and ability to act. Voss and Anderson address this need and the potential for the Trustmark Framework to serve as an applicable solution. [23] Guidance on establishing and maintaining user accounts and permissions are detailed in NIST Special Publication SP 800-63 Digital Identity Guidelines, a four-volume series which covers general guidance, enrolling and proofing of identity, authentication and lifecycle management, and federations and assertions [42]. A challenge in this area is that use cases and workflows spanning the full range of video data from point of acquisition by a camera to its use as evidence in decision making tools, legal proceedings, or insurance claim investigations have yet to be fully described and documented.

Additional attention to ensure vendor development of secure video systems and IOT devices is warranted. The NIST Framework for Improving Critical Infrastructure Cybersecurity provides a guide for cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes [43].

3.3.4.2. User Visualization

Operations centers usually maintain walls of monitors streaming live footage from the VMS. Most VMS's also offer desktop visualizations that allow filtering and selection of multiple cameras for viewing on single or multiple screens. Newer advancements provide geospatial selection of cameras from maps or live earth video management with layers for traffic and integration of other public sector sensors. Newer VMS's now leverage metadata to provide the end user with a variety of filters such as location or time to narrow the number of video feeds.

3.3.4.3. User Experience

Operational needs drive requirements for the user experience/visualization of video, analytics and other data that support human decision and understanding. Utilization and optimization of

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

diverse and dynamic sources of data for real-time situation analysis within the fabric of complex communications networks presents a big data challenge that is unprecedented in other domains. At the present time, operators struggle to visualize camera position and perspective, understand geospatial context and narrative time sequence, insert overlays onto 3D surfaces, and integrate social media input with the content.

PSCR has conducted communications usability studies on law enforcement, fire, EMS, and communications (dispatch) communities through its Voices of First Responders series [44]. Video operations perspectives have not been formally captured outside of the Video Analytics for Public Safety effort.

3.3.4.4. Other

Organizations must consider the implications of the technologies they adopt and the privacy controls necessary to prevent unintended consequences for the citizens they are sworn to protect and serve. Until the necessary foundational, structural, and semantic technology needs can be addressed, public safety must ensure privacy through encryption, robust cybersecurity, and redaction. Debate persists on quality of video redaction methods utilized in forensics; meanwhile, applications for real-time redaction are entering the market. Privacy-protecting solutions that provide situational awareness to public safety operations include cryptographic obscuration, encryption, redaction of sensitive data, and new research efforts in differential privacy.

3.3.5. Key Takeaways for Technology

- In the absence of quality and service level requirements, industry driven solutions add layers of systems and expenses with limited incremental progress in video interoperability for public safety.

- A definable, measurable level of quality needs to be understood to ensure that video can be created and utilized both for human and machine analysis tasks and that has implications for the flow of data from collection device to storage, analytics, and display.

- As public safety video operations explore insertion of analytics, the current and desired future state workflows should be documented to outline the lifecycle of video data needs, users, and roles and determinations made on which should be automated and which require human interaction and decision making.

- Building blocks for public safety focused ontology to support metadata storage and data exchange exist, but additional research and collaboration must take place to evolve these for video in order to exchange data and analyze video archives.

- Neither human nor machine bias are not well understood or measured in public safety video data or outcomes but could have potentially sweeping impacts on operations and public perceptions of first responders.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

3.3.6. Technology Roadmap

A principle driver for employing video analytics is to automatically extract content relevant to an information need or decision-making process. Another key role of video analytics is the ability to contribute to a reduction in bandwidth needs, for example, where analytic processing is deployed to the edge, reducing the amount of data required to transmit and store. A lack of video analytic interoperability obstructs capabilities such as these and constrains the value proposition of enterprise-wide analytic workflows. Investment in technical interoperability solutions will democratize advancement of video analytic workflows and reduce the risk of negatively impacting public safety operations when new video analytic capabilities or data sources are added to the system. Common interoperability processes and interfaces throughout the video analysis ecosystem will enable much faster integration between systems and ensure data is moved and handled responsibly throughout the workflow.

Table 3 identifies some of the sample technology challenges and gaps facing the public safety video analytics community and the desired future state outcomes to enable stable interoperable video operations architectures that support validated analytics. Suggested activities to achieve that architecture are laid forth in a three phased approach. Phase 2 activities may incorporate findings from Standard Operating Procedures Phase 1 activities.

Table 4. Potential Elements for a Future Technology Roadmap

ID	Gaps and Challenges	Desired Outcomes	Phase 1	Phase 2	Phase 3
TECH - 1	Gap in video analytics quality of service requirements.	Measured and community agreed-upon end user quality of service needs support public safety video communications networks.	Fund gap research and evaluations of foundational and structural technical needs required for optimized performance video quality analytics.	Research findings describe technical needs for video analytics; draft quality of service needs.	Include quality of services needs in acquisition documents for video network and systems requirements and submit to NSRIC.
TECH - 2	Need to qualify and quantify variances in human and machine video quality requirements.	Measurement science drives service requirements for both human and computer workflows.	Continue and advance research on video quality measurement; identify test data; support standards definition for video quality.	Fund grants, challenges, or other opportunities for comparative evaluation visual acuity and machine vision; publish and present findings to public safety community.	

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

TECH - 3	Need to establish a first level baseline of video analytics algorithms.	Community agreed upon set of algorithms to support NIMS.	Identify applicable national level use cases.	Sponsor grants or challenges to fill algorithm gaps not already supported by industry; develop testbed for evaluation of approaches; publish findings.	
TECH - 4	Need to expand the baseline of video analytics algorithms.	Prioritized second tier algorithms to support local and regional needs.	Identify and prioritize incidents, objects, or behaviors for algorithm development and adoption.	Sponsor grants or challenges to fill algorithm gaps not already supported by industry; develop testbed for evaluation of approaches; publish findings.	Review and update semi-annually.
TECH - 5	Need to establish a baseline for video redaction and privacy preserving technologies.	Measurement and evaluation ensure video redaction and privacy techniques maximize protection of PII and limit risk for reidentification.	Sponsor research measurement of video redaction and privacy methods; conduct research on current tools and approaches to preserving privacy; collect data for testing.	Leverage best practices identified gaps and needs to target grants or challenges; develop testbed for evaluation of approaches; publish findings.	Continued monitoring and evaluation new methods based on societal and legal requirements.
TECH - 6	Need to develop and maintain a video data taxonomy.	An agreed-upon video data taxonomy classifies data into categories and subcategories and supports standardized metadata and shared understanding of incidents.	Review NIEM and APCO NG911 Emergency Incident Data; define specific content, data elements, and values for video.	Leverage best practices identified gaps and needs to identify additional taxonomy requirements for data management. Determine approach, draft, coordinate draft, and publish.	Review and update semi-annually.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

TECH - 7	Need to accelerate video alerting in support of real-time operations.	Embedded video analytics throughout the workflow alert on-scene first responders of incidents, and changes in safety conditions and incident evolution.	Test and measure video quality of datacasting and LTE-delivered live streaming video on VMS and mobile devices.	Leverage best practices identified gaps and needs to fund grants or challenges to develop lightweight video analytic applications for handheld devices; identify, test, and evaluate deployment of lightweight analytics on handheld devices; identify hardware performance requirements; document and publish findings; conduct technology demonstrations.	Acquire and deploy applications.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

3.4. Training and Exercises

In public safety, most professional training is either provided through a state or county training academy, as is the case with police and fire, or through a professional accreditation program, such as the National Registry of Emergency Medical Technicians (NREMT) or APCO International's training and instructor certification program for public safety communications professionals.

The Federal Emergency Management Agency (FEMA) Directorate of Preparedness serves as the national focal point for the development and delivery of emergency management training in support of state, local, territorial, and tribal government officials. Their training focus encompasses government personnel and over one million volunteer firefighters who comprise approximately 65% of the fire response capacity nationwide, and the volunteer EMS providers that provide the majority of coverage to one third of the States [45], [46]. FEMA's Emergency Management Institute (EMI) located in Emmitsburg, Maryland trains over two million students annually across America through residential and online programs and in partnership with emergency management training systems, colleges and universities. EMI is accredited by the International Association for Continuing Education and Training (IACET) and the American Council on Education (ACE). EMI training supports the implementation of the NIMS, the National Response Framework (NRF), the National Disaster Recovery Framework (NDRF), and the National Preparedness Goal (NPG) by conveying necessary knowledge and skills to improve the nation's capability [47].

EMI's current curriculum does not specifically address video operations or video analytics. Courses that could support video operations include the following:

- E0142: Situational Awareness (Pilot Course—Registration by Invitation Only)
- E0143: Advanced Situational Awareness and Common Operating Picture
- E0548: Continuity of Operations (COOP) Program Managers Course
- E0550: Continuity of Operations (COOP) Planning

The Law Enforcement & Emergency Services Video Association International, Inc. (LEVA) offers forensic video analysis training and two levels of certification. LEVA is a 501(c)(3) nonprofit corporation which offers membership and courses to military members, public safety, criminal justice, or legal industry employees and individuals with professional, educational organizational affiliations with the public safety sector. The first level is a Certified Video Technician which is targeted to those with a single year of experience processing video and still imagery, while the second level is designed for those with two or more years of experience in video and still imagery evidence processing, analysis, and court testimony on video or imagery evidence [48]. LEVA does not support video analytics training for real-time situational awareness, although some information on video annotation and processing may be helpful to video operations personnel. Unlike NREMT or EMI, LEVA's certification programs are not approved by an accrediting body.

At present, training for real time video operations throughout the public safety community happens at a local or jurisdictional level. Presenters at the 2019 DHS Video Quality in Public Safety Annual Meeting highlighted mandatory training in cybersecurity and data handling for video operations personnel prior to assuming watch standing assignments, but training on video networks, systems, and analysis in real time is not well organized in the community.

VMS and VSS vendors attempt to step into the gap with training and certification programs for their systems. These are marketed separately to individuals and to departments in conjunction with system installation and upgrade packages, and courses may be free or available at an additional fee to individuals and video operations units. Access to the latter (paid) training opportunities is highly dependent upon public safety organization budgets.

In some cases, novel partnerships between public safety and higher education seek to fill training gaps. For example, Chicago PD has partnered with the University of Chicago to provide public safety practitioners access to innovative technology within Area Technology Centers (ATC) Digital data management, processing and production capabilities provide the ability to create a redacted video narrative, push videos to YouTube for public information and awareness and improve the quality of the digital media (e.g., through super resolution processing). Practitioners receive 40 hours of training before operating any of the technologies in the ATC. However, this example too demonstrates the public safety community's focus on the application of video to support Public Information Officers' distribution of information to the public rather than to accelerate or enable first responders.

In the current state, video analytics training lacks consistency and focuses on organizational policies and procedures, and domain-specific (e.g., emergency services, law enforcement) processes and elements causing variance in approaches and quality across organizations and jurisdictions. Vendor training programs can reinforce stovepipes and solutions which lack

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

interoperability. Differences in levels of expertise and experience results in varying interpretations of objects and events and a not well understood variance in skill levels for handling and processing video data for real time public safety missions. The national level public safety training community has yet to broach training for real-time video operations and implementation of video analytics. Insertion of these topics into the workstream, particularly alerting functions, may generate confusion for communications professionals and first responders trained in established CAP curricula.

3.4.1. Key Takeaways for Training

- Across the five SAFECOM elements the need for three roles emerge as necessary to support daily video operations: technical support, video operator/analyst, and leader/manager.
- Access to training is limited, industry led, and forensics focused causing inconsistencies and gaps in real-time public safety video operations and analysis.
- While professional certification programs exist for IT network specialists video operations for public safety is a niche field that varies from computer networking, online video, and broadcast media and may warrant additional specialized training in order to achieve interoperability.
- Development of public safety led professional or privately led accredited programs for public safety video operations staff would be on par with training standards for other first responders and public safety communications professionals.
- Use and handling of video, along with a basic understanding of the video operations and analytic process could ease first responders' and communications professionals' adoption of this data modality and be incorporated into current curricula.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

3.4.2. Training Roadmap

Training of public safety operators has not kept pace with the escalation of video analytic technology, and this gap in training will greatly impact the ability of public safety operators to leverage these advancements. The public safety community must strive toward a common level of practice and professionalization for video operators through an accredited program of instruction. Credentialing establishes standards of professional knowledge, skills, and abilities, advances the profession, and helps to protect and assure the public that standards of practice are met. Although there is a deep need for technical proficiency, it is not required for all video operations or IT personnel, therefore training curriculum design should be designed role based. Certification and training programs should address multiple skill levels for roles including video analyst, video technical operations, and video operations manager. Exercises and training which incorporate the use of video data should also extend to critical players in the current and future video data workflows. Suggested activities to address this need are presented in Table 5.

Table 5. Potential Elements for a Future Training Roadmap

ID	Challenges and Gaps	Desired Outcomes	Short Term	Mid Term	Long Term
TRAIN-1	Need for technology focused training to strengthen all technical interoperability levels.	Video operations technical staff possess the knowledge, skills, and ability to deploy, maintain, troubleshoot interoperability issues, and make recommendations for a range video devices, networks, and systems to support mission operations. Video operations staff possess a high level of knowledge on community technology guidelines, best practices, and standards.	Leverage community workshops to raise digital media acumen and knowledge of video analytic technology; identify and document baseline requirements for training program.	Draft curriculum-based best practices and standards; obtain consensus; initiate new curricula; run pilot course; elicit and document perceptions and feedback from participants; determine training modality.	Advertise and adjust course volume to meet demand; identify and train additional trainers as necessary; offer courses.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

TRAIN-2	Need for real-time video operator and video analytics focused training.	Video analytic operators possess the knowledge, skills, and abilities to monitor live-streaming video, validate and process alerts generated from video analytics, adhere to best practices and policies for secure data handling, data storage, and privacy; understand and take measures mitigate analytic bias, and leverage the applications of a variety of analytics to support mission operations. Video operations staff possess familiarity and knowledge of community guidelines, best practices, and standards.	Leverage community workshops to raise digital media acumen and knowledge of video analytic technology; identify and document baseline requirements for training program.	Draft curriculum based best practices and standards; obtain consensus; initiate new curricula; run pilot course; elicit and document perceptions and feedback from participants; determine training modality.	Advertise and adjust course volume to meet demand; identify and train additional trainers as necessary; offer courses.
TRAIN-3	Need for real-time video operations center management training.	Video operations center leaders are familiar with all levels of video analytics technology, information sharing agreements, data handling, privacy technologies and constraints, video quality guidelines, analytic bias in human and machine	Leverage community workshops to raise digital media acumen and knowledge of video analytic technology; identify and document baseline requirements for training program.	Draft curriculum-based best practices and standards; obtain consensus; initiate new curricula; run pilot course; elicit and document perceptions and feedback from participants; determine	Advertise and adjust course volume to meet demand; identify and train additional trainers as necessary; offer courses.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

		interpretation, and nationally adopted best practices to ensure the interoperability of the public safety video lifecycle.		training modality.	
TRAIN-4	Need for communications professional training to incorporate video-based alerts into dispatch workflows.	Public safety communications professionals possess the knowledge skills and abilities to receive, process, and log video generated alerts in PSIMS and generate alerts to first responders and the public.	Identify opportunities in current curricula to introduce video operations concepts, workflows, and future video analytic possibilities; draft and propose changes; obtain consensus; initiate new curriculum; run pilot course; elicit and document perceptions and feedback from first responders.	Draft and propose curriculum changes based on alerting best practices; obtain consensus; initiate new curriculum; run pilot course; elicit and document perceptions and feedback from public safety communications professionals.	Include video analytic generated alerts in tabletop exercises; adjust curricula as necessary; train communications professionals.
TRAIN-5	Need to incorporate video analytics training into first responders' courses.	On scene first responders possess the knowledge, skills, and abilities to monitor live stream video on handheld devices and interpret alerts derived from video analytics to support real-time decision making.	Identify opportunities in current curricula to introduce video operations concepts, workflows, and future video analytic possibilities.	Draft and propose curriculum changes; obtain consensus; initiate new curriculum; run pilot course; elicit and document perceptions and feedback from first responders.	Include video analytic enabled devices in tabletop exercises; train first responders on handheld video analytic applications; test usage of video analytic enabled devices in live exercises.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

TRAIN-6	Need for accessible training platforms that deliver community accepted online and classroom training, and certification programs.	Public safety video operations are supported by a baseline of community driven professional education programs that address the range operational needs.	Identify and involve organizations with the responsibility and authority lead training efforts; identify potential opportunities for certification program.	Develop a digital training library, training toolkit and micro-training workflows based on best practices; identify necessary classroom-based courses and initiate curriculum development; pilot courses; elicit feedback.	Maintain online courses; continually review and update training courses; submit accreditation package.

3.5. Usage

SAFECOM's Interoperability Continuum for usage sets forth a model of continuous improvement of the communications flow from individual planned events to the ability to exchange information freely and without technical or semantic barriers at a national level for major threats and disasters. This section details the use of video operations and analytics for events, looks into the approaches and challenges around sharing data within the local level, then notes stakeholder use cases and concerns for scaling to regional and national levels.

Adoption of video to support unique events such as festivals, concerts, and sporting events is commonplace. The *Interoperable Communications for Planned Events* guide developed by the NCSWIC already called out the integral value of video cameras in substituting a single picture for many words and providing a common view of events during the Superbowl. This guide assists community authorities in planning and coordinating events before, during and after activities and offers best practices and checklists to ensure interoperable voice and data communications for events [5].

Insertion of object detection algorithms and other video analytics is eased when homogeneous networks and systems are employed. New cameras and systems are, in some cases, designed and installed specifically for an event [5]. Stakeholders noted that major events and the activities leading up to those events are often augmented by deployable public safety-owned cameras and systems reserved for events, and in some cases by new systems [49].

The implementation and upgrade of state-of-the-art video surveillance systems and the insertion of video analytics at sports arenas, concert venues, and other events on the low scale of SAFECOM's continuum can also be attributed to corporate risk management practices. Major event venues owned by private industry, along with some critical infrastructure locations such as hospitals, select and purchase their own systems based on a positive cost benefit analysis. For private industry, video analytics can offset the recurring costs of manned guards, real-time monitoring centers, as well as supporting decisions on pedestrian traffic flow to support marketing and sales [50].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

While events can drive adoption, for public safety the cost benefit ratio of video surveillance is realized in increased situational awareness and officer safety. Whether implemented in support of major events, critical infrastructure protection or through federal grant programs and private partnerships, cities have quickly found value in transitioning video surveillance technology to support localized emergencies and daily local use. In an NIJ sponsored workshop held by RAND, public safety stakeholders identified real-time monitoring to detect crimes and major incidents as the highest priority use case for video analytics and signal fusion for law enforcement [10]. RAND's research details use cases, considerations, and priorities for investment. Rather than repeat these, this section explores other previously unidentified gaps and challenges that may stall data sharing and the implementation of analytics at a regional and national level.

3.5.1. Video Data Sharing Approaches and Obstacles

Approaches to sharing data either require partnership between public and private entities with existing video networks or collaborating with partners to collectively acquire the same systems. The first approach is fraught with the difficulty of overcoming the foundational and structural technical interoperability challenges described in Sections 3.3.1 and 3.3.2 The latter approach is confronted by organizational challenges such as difficulty in defining roles and responsibilities for project management, acquisition, operation and maintenance; unlike or competing requirements; financial constraints (varying budgets, approval chains, and acquisition procedures); and long lead times to implementation.

Ingesting video from disparate systems using a data sharing partnership approach can accelerate a regional video common operating picture, but coverage from each subsystem can be intermittent. In most cases, integrated systems software is updated every one to two years, and these updates break the video streams from the subsystems. Although it occurs with less frequency, changes in a system's software development kit (SDK) can also disrupt integrations.

Stakeholders who have adopted a data sharing partnership approach to connect city law enforcement PSIM to partners' VMSs indicate that restoring video connectivity takes time. Rarely are public safety partners notified of changes in video subsystems and depending on their support team's experience with the jurisdiction's video network, a significant time may be spent troubleshooting a lost stream before identifying the software update issue. One stakeholder noted a minimum of four months and an average of six months for their VMS vendor to develop and update connectors. This is followed by a period to validate and test the new connector in a test environment to resolve bugs, and another month for the vendor to do a final review and roll out the update for the new connection. Updates then must be made on each client terminal in the operations center and typically involve removal and update to the SDK and Active-X controllers for the integrated subsystem. Stakeholders have noted ongoing disruptions to subsystems lasting 10 months.

An alternative method of directly accessing data from a partner's cameras is less viable, due to limited network bandwidth which prohibits streaming from the camera to a second or third VMS outside the original network. A third method, which involves placement of public safety *routers* within the network, must overcome cybersecurity risk management practices which bar the insertion of externally owned or managed hardware within a network. In cases where routers are approved, the related physical security procedures for the network usually make maintenance

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

and upgrades cumbersome. Personnel unfamiliar with the partnership agreement may challenge physical access to equipment, policies and procedures enabling the agreement, and updates to document their existence and maintenance may be overlooked in the network security package's Plan of Action and Milestones (POAM).

A final approach to video data sharing is datacasting, which is cited above in Sections 2 and 3. While this approach offers a hardened, resilient, solution that accommodates live streaming of 4K high quality data with limited latency to operations centers as well as mobile LTE devices, it also has limitations. Bidirectional data flow can only be achieved through the installation of broadcast transmitters and receivers at both ends of the signal, and the ability to prioritize incoming video data streams is limited. Quality of video received through datacasting tests has yet to be measured or evaluated for use in video analytics, and video streams have not been integrated into VMS (to our knowledge).

3.5.2. Use Cases for Sharing and Using Video Data and Video Analytics

Stakeholders' data sharing priorities centered on use cases for surge support during events in both densely populated jurisdictions and in sparsely populated jurisdictions where major annual events raise populations and overwhelm available manpower coverage. Stakeholders explored alternative concepts such as "sister city" collaborations which would allow for remote transregional surge support and continuity of operations coverage from similarly demographic cities to assist with manpower intensive events such as major sporting events and riots, or catastrophic environmental disasters. In these use cases, video analytics would support remote alerting and monitoring of events by out of county or out of state video operators who would then provide alert notifications back to first responders in the immediate region of those events.

While public safety mission owners seek to expand usage and enable cross jurisdictional access to video data, not all stakeholders are in agreement with the use of video surveillance and the analytics being applied to this data modality, there is push back against video monitoring in some communities [51]. RAND's use cases for video analytics envision a future where computer vision driven alerts at the edge eliminate the need for continuous real time streaming data [10]. From a technology perspective, that future reduces bandwidth and storage requirements. For the public, depending on their perspective, such a future could limit the monitoring of law-abiding citizens or remove incident identification out of the hands of human operators.

Even attendees at the 2019 Video Quality in Public Safety Stakeholders meeting acknowledged that there exists a pressing need for public debate on the usage of video and video analytics for monitoring both public and public safety activities. Future debate topics could encompass both public safety and privately-owned fixed video monitoring and recording devices and mobile devices such as body worn, dashboard, and drone mounted cameras.

3.5.3. Key Takeaways for Usage

- Initiating and maintaining data sharing between homogenous video networks and systems within a local jurisdiction is administratively and technically time consuming.
- Network architecture change notifications impacting the flow of data to partners are seldom coordinated and result in outages and unplanned technical support costs.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

- Datacasting may appear to sidestep technical and administrative difficulties, but its utility in supporting or utilizing the next generation of analytics remains unexplored.
- The development of safeguards and use cases for interoperable analytics hinges on understanding public concerns and ascertaining the level of comfort and trust for these devices and the analytics that will be applied to them.

3.5.4. Usage Roadmap

Interoperability issues and societal concerns challenge the scaling of video operations networks beyond local and regional use cases and levels. The first four challenges and gaps listed in **Error! Reference source not found.** (USE-1 through USE-4) reflect pressing interoperability issues and offer practical recommendations for addressing them at the local level. The last two challenges and gaps (USE-4 and USE-5) capture public safety perspectives and needs for sharing video data beyond the local and regional level to support local level operations. A measured approach and open dialog with the public on the role and need for interoperable video capabilities in local communities is warranted to balance privacy and societal concerns for security. Focusing future discussions around defined use cases relevant to the National Incident Management System goals could serve a starting point for community debate on designing these continuity of operations plans. The utilization specific video analytics in support of those operations is beyond the scope of this roadmap.

Table 6. Potential Elements for a Future Usage Roadmap

ID	Challenges and Gaps	Desired Outcomes	Phase 1	Phase 2	Phase 3
USE - 1	Software and hardware upgrades in partner networks occur without notification, resulting in prolonged coverage gaps and increased manpower troubleshooting issues.	Informal and formal coordination mechanism and analytics ensure public safety organizations are cognizant of scheduled maintenance upgrades and unplanned outages in partner subnetworks.	Organize informal, reoccurring engagements of video system administrators to improve communications.	Identify and implement a secure online shared forum for posting alert notifications for outages and changes; adjust information sharing agreements to address informal and formal communications regarding outages and upgrades.	Identify requirements for network analytics to automate alerts for outages and changes in network and subnetworks; adjust information sharing agreements to address automated alerts.
USE - 2	Long lead times to develop, test, validate, and implement connecting software solutions.	Common service level requirements and best practices adoption drives service level	Evaluate risk; negotiate pricing and support levels for routine vs. expedited services; plan for and secure funds for critical coverage areas and	Review and update contracts and Service Level Agreements with vendors based on community best practices.	

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

		requirements in vendor contracts.	times; identify and evaluate COOP plans.		
USE - 3	Partner's limited network bandwidth is prohibitive to streaming video to more than one network.	Robust, secure, resilient, self-healing networks support streaming video data to multiple VMS.	Identify alternative approaches and backup approaches, such as datacasting.		
USE - 4	Approval of and access to embedded public safety hardware on a partner network are difficult and cumbersome.		Organize informal reoccurring engagements of video system administrators to improve communications.		
USE - 5	Use cases for alerts from employed video analytics.	Alerts generated by public safety video analytics enable a seamless alerting workflow to first responders and public.	Identify and document dataflow of video-based alerts; identify and document use cases for video analytic generated alerts; identify and document alert types and prioritization levels for local, regional, and national broadcast.		
USE - 7	Major events and disasters challenge can overwhelm networks and manpower.	Use cases, information sharing agreements, common training curriculum, and public dialogue enable new approaches and plans for maintaining	Organize workshop event focused on continuity of operations for video operations; identify and document desired future state, alternative approaches, challenges, gaps, constraints, etc.; publish findings;	Identify use cases; develop business plan; define and refine scope; identify funding mechanisms; garner support.	Develop test plan; test and measure results; elicit broad stakeholder feedback; evaluate findings for approval.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

		scaled continuous operations support.	elicit feedback from policy, legal, and public communities.		

4. Conclusion

As video data sources become more prolific, technology capabilities rapidly transform, and the public demand for transparency, privacy, and responsiveness increases, many jurisdictions are being crushed under the weight of the video data they are collecting and are constrained by the technologies they employ. Many jurisdictions have approved money to buy cameras, but the gaps in technical interoperability and supporting capabilities necessary to make the data perform within current workflows prevent them from easily achieving the desired outcomes within their budgets.

Despite the increasing urgency for public safety video operators to apply analytic solutions to assist in the management of the increasing amount of real-time video, insertion of some video analytics into the workstream could result in less than optimal outcomes. Successful implementation of the next generation of analytics must be built upon a standardized, extensible, scalable architecture designed for visual digital information. These should assure data quality, take into consideration the lifecycle of public safety video needs, readily exchange useful information with other systems, and permit capability improvements while maintaining operations. As the public safety community moves to improve data analysis and management tools, the research community needs to improve the data and tools that support development and evaluation of technologies to ensure that future public safety video capabilities can achieve the desired outcomes.

Not only are tools and solutions are needed that permit public safety to develop cost-effective real-time video analytic solutions that the public safety organizations can control and maintain, but also there is a need for training to create a common level of practices amongst the video operations workforce and to engage first responders and communications professionals in training and exercises that will improve the video data workflow in meaningful ways for daily operations.

In order to effect all of these changes, there is a pressing need for strong governance models at the national and local levels—coordinated activities in R&D and measurement, development of standard operating procedures, training, and continuity of operations plans to ensure usage for major incidents and daily operations. Governance mechanisms can facilitate further discourse with all stakeholders on the use cases for video analytics within and beyond their communities and ensure balanced, measured and secure approaches to meeting public safety needs for interoperability while ensuring the public's need for increased safety, transparency, and privacy.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

5. References

[1] Department of Homeland Security (2014) *Interoperability Continuum A tool for improving emergency response communications and interoperability.* https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2_1.pdf

[2] USASpending.gov (2019) *Advanced Search*. Available at: https://www.usaspending.gov/#/search/416a0ca636f4eb301a0472eaceff8b36.

[3] Garofolo J, Garfinkel S, Schwartz R (2017) First Workshop on Video Analytics in Public Safety. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (NISTIR) - 8164, January 19, 2017 https://www.nist.gov/publications/first-workshop-video-analytics-public-safety

[4] The Institute of Electrical and Electronic Engineers (IEEE), IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, New York, NY: The Institute of Electrical and Electronic Engineers (IEEE), 1990.

[5] Department of Homeland Security (2020) *Interoperable Communications for Planned Events*. Available at: https://www.dhs.gov/sites/default/files/publications/interoperablecommunicationsforplannedevents_0.pdf.

[6] National Public Safety Telecommunications Council (2012) *Use Cases & Requirements for Public Safety Multimedia Emergency Services (MMES), Rev C* Available at: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2597&file=Use_Cases_Rqmts_PS_MMES_Report_revC_121106.pdf.

[7] U.S. Department of Homeland Security (2015) *Advanced Communications Video Over LTE: Video Design Improvement Process HSHQPM-15-X-0012*. Available at: https://www.dhs.gov/sites/default/files/publications/VQiPS_Video-Design-Improvement-Process-Memo_Report_Final_Draft_v5-508.pdf.

[8] Räty, T (2010). Survey on Contemporary Remote Surveillance Systems for Public Safety. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on. 40. 493 - 515. 10.1109/TSMCC.2010.2042446.

[9] U.S. Department of Homeland Security Science and Technology (2013) Digital Video Quality Handbook, Washington, D.C.

[10] Hollywood J, Vermeer M, Woods D, Goodison S, Jackson, B (2018) Using Video Analytics and Sensor Fusion in Law Enforcement: Building a Research Agenda That Includes Business Cases, Privacy and Civil Rights Protections, and Needs for Innovation. 10.7249/RR2619.

[11] U.S. Department of Homeland Security (2016) "*VQiPS - Policy Considerations for the Use of Video in Public Safety*" Available at: https://www.dhs.gov/sites/default/files/publications/Policy_Considerations_for_the_Use_of_Video_in_Public_Safety_Final_v5.pdf.

[12] Desourdis J, O'Brien M, McCoskey J, Wyglinski A (2019) *Meet the All Hazards Consortium...* Available at:

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

https://www.ahcusa.org/uploads/2/1/9/8/21985670/national_distribution_whitepaper.pdf.

[13] A. Romero, IBM Watson Media (2018) "What is Video Encoding? Codecs and Compression Techniques" Available at: https://blog.video.ibm.com/streaming-video-tips/what-is-video-encoding-codecs-compression-techniques/.

[14] International Standards Organization (2019) *ISO 9241-210:2019(en) Ergonomics of human-system interaction — Part 210: Human-centered design for interactive systems.* Available at: https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-2:v1:en.

[15] Deloitte., The Wall Street Journal (2013) *The Role and Benefits of a Corporate Governance Framework*. Available at: https://deloitte.wsj.com/riskandcompliance/tag/governance/?mod=readmoreabout.

[16] NPSTC Technology and Broadband Committee Public Safety Internet of Things Working Group (2019) *Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes.* Available at: http://www.npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Report_190616.pdf

[17] DHS Federal Emergency Management Agency (2017) National Incident Management System. Available at: https://www.fema.gov/media-library/assets/documents/148019.

[18] Department of Homeland Security (2020) NCSWIC Committees. Available at: https://www.dhs.gov/safecom/ncswiccommittees.

[19] U.S. Fire Administration, FEMA (2019) A Prepared and Resilient Fire and Emergency Medical Services, Strategic Plan Fiscal Years 2019-2023. Available at: https://www.usfa.fema.gov/downloads/pdf/publications/strategic_plan_2019-2023.pdf

[20] Metropolitan Washington Council of Governments (2020) NCR Homeland Security Executive Committee (HSEC) Available at: https://www.mwcog.org/committees/hsec/.

[21] TekSynap (2010) NATIONAL CAPITAL REGION NETWORK (NCRNET). Available at: https://www.teksynap.com/contracts/national-capital-region-network/

[22] National Capital Region Interoperable Communications Infrastructure, Fairfax County Department of Information Technology (2020) ICI Services. Available at: https://ncrnet.us/about/.

[23] Voss B, Anderson E (2019) Interoperability of real-time public safety data: Challenges and possible future states. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (NISTIR) - 8255, June 19, 2019. https://doi.org/10.6028/NIST.IR.8255

[24] Mordor Intelligence (2020) VIDEO SURVEILLANCE SYSTEM MARKET - GROWTH, TRENDS, AND FORECAST (2020 - 2025). Available at: https://www.mordorintelligence.com/industry-reports/global-video-surveillance-market-industry.

[25] ONVIF (2020) Our Mission. Available at: https://www.onvif.org/about/mission/.

[26] ONVIF (2018) Membership Levels. Available at: https://www.onvif.org/join-us/membership-levels/.

[27] S. Hood, Interviewee, *Director CitiWatch.* [Interview]. 3 April 2019.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

[28] Federal Communications Commission (2020) Communications Security, Reliability, and Interoperability Council VII. Available at: https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii.

[29] National Institute of Standards and Technology (2020) Privacy Framework. Available at: https://www.nist.gov/privacy-framework/privacy-framework.

[30] HIMSS (2019) Who We Are. Available at: https://www.himss.org/library/interoperability-standards/what-is.

[31] SiraView, Security News Desk (2013) Opinion: CCTV evidence and the need for a universal viewer. Available at: https://securitynewsdesk.com/opinion-cctv-evidence-and-the-need-for-a-universal-viewer/.

[32] Bitmovin (2019) Video Developer Report 2019. Available at: https://cdn2.hubspot.net/hubfs/3411032/Bitmovin%20Magazine/Video%20Developer%20Report%202019/bitmovin-video-developer-report-2019.pdf.

[33] Shah S, Mantini P, Stroup S, Weldon T (2019) Video Analytic based Alerting in Public Safety. Public Safety Communications Research 2019 (National Institute of Standards and Technology PSCR, Chicago, IL), pp 1-46. https://www.nist.gov/system/files/documents/2019/11/01/public_safety_video_analytics_and_workflow_to_enable_the_end_user_-_lessons_learned_compressed_1.pdf

[34] Kosie, J & Baldwin, D (2019) Attentional profiles linked to event segmentation are robust to missing information. Cognitive Research: Principles and Implications. 4. 10.1186/s41235-019-0157-4.

[35] Zhu K, Li C, Asari V, Saupe D (2015) No-Reference Video Quality Assessment Based on Artifact Measurement and Statistical Analysis. Circuits and Systems for Video Technology, IEEE Transactions on. 25. 533-546. 10.1109/TCSVT.2014.2363737.

[36] International Press Telecommunications Council (2018) IPTC Video Metadata Hub Recommendation 1.2, Available at: https://iptc.org/standards/video-metadata-hub/recommendation/.

[37] International Press Communications Council (2018) IPTC Video Metadata Hub - Recommendation 1.2 / all Mappings. Available at: https://iptc.org/std/videometadatahub/recommendation/IPTC-VideoMetadataHub-mapping-Rec_1.2.html.

[38] European Broadcasting Union (EBU) (2019) Metadata Specifications. Available at: https://tech.ebu.ch/docs/tech/tech3351.pdf.

[39] National Information Exchange Model (2019) Emergency Management. Available at: https://www.niem.gov/communities/emergency-management.

[40] Williams T, Thomas J, Jacoby S, Cave D (2016) The New York Times, Police Body Cameras: What Do You See? Available at: https://www.nytimes.com/interactive/2016/04/01/us/police-bodycam-video.html.

[41] Zhang Q, Sun H, Wu X, Zhong H (2019) Edge Video Analytics for Public Safety: A Review. Proceedings of the IEEE. PP. 1-22. 10.1109/JPROC.2019.2925910.

[42] National Institute of Standards and Technology (2017) Digital Identity Guidelines: Now Available. Available at: https://pages.nist.gov/800-63-3/.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

[43] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[44] National Institute of Standards and Technology (2020) User Interface/ User Experience Publications. Available at: https://www.nist.gov/ctl/pscr/user-interface-user-experience-publications.

[45] B. E. G. S. National Fire Protection Association (2019) U.S. fire department profile. Available at: https://www.nfpa.org/News-and-Research/Data-research-and-tools/Emergency-Responders/US-fire-department-profile.

[46] National Highway Traffic Safety Administration (2011) EMS System Demographics. 2011 National EMS Assessment Research Note. (National Highway Traffic Safety Administration, Washington, DC), Report No. DOT HS 812 041. https://www.ems.gov/pdf/National_EMS_Assessment_Demographics_2011.pdf

[47] Federal Emergency Management Agency (2020) Emergency Management Institute Mission. Available at: https://training.fema.gov/emi.aspx.

[48] Law Enforcement & Emergency Services Video Association International, Inc. (2020) Welcome to LEVA International, Inc.. Available at: https://www.leva.org/.

[49] Callaghan P, MinnPost (2018) Technology developed for Super Bowl LII has created an expansive new capability for police surveillance. Available at: https://www.minnpost.com/politics-policy/2018/04/technology-developed-super-bowl-lii-has-created-expansive-new-capability-pol/.

[50] Richmond T, Security InfoWatch (2019) Making the Case for Security: Benefits vs. Costs. Available at: https://www.securityinfowatch.com/security-executives/protective-operations-guard-services/article/21068909/making-the-case-for-security-benefits-vs-costs.

[51] Kwet M, The Intercept (2020) The Rise of Smart Camera Networks, and Why We Should Ban Them. Available: https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/.

[52] International Organization for Standards (2015) ISO/IEC/IEEE 15288:2015 [ISO/IEC/IEEE 15288:2015, ISO/IEC/IEEE 15288:2015]. Available at: https://www.iso.org/standard/63711.html.

[53] Fagan J, NetApp Blog (2018) Five Things You Didn't Know About Video Surveillance Data Storage. Available at: https://blog.netapp.com/five-things-you-didnt-know-about-video-surveillance-data-storage/.

[54] Federal Emergency Management Agency (2019) Integrated Public Alert & Warning System. Available at: https://www.fema.gov/integrated-public-alert-warning-system.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

Appendix A: Public Safety Video Analytics Stakeholders

There is a complex combination of government organizations, industry, academic organizations, standards organizations, and social science and legal communities with a right, share claim or interest in public safety video analytics systems and its possession of characteristics that meet their needs and expectations [3]. **Error! Reference source not found.** depicts the Public Safety Video Analytics community, which is comprised of the following stakeholders:

- **County, City, Local and Tribal Agencies** are public safety first responders such as fire, law enforcement and emergency medical services (EMS), as well as transportation services. These organizations use video analytics to assist with emergency response and law enforcement efforts. They require access to both real-time and stored video analytics information.
- **State Agencies** include state law enforcement organizations and state agencies, like regional operations centers, involved with transportation, critical infrastructure, and emergency services. These agencies use video analytics for investigative purposes and to monitor infrastructure resources and emergency response efforts.
- **Federal Agencies** include federal law enforcement, intelligence and military organizations that capture and share video information for mission operations. These organizations coordinate and share video information and analytics with state, county, city, local and tribal agencies to support public safety and law enforcement programs and operations. Federal R&D organizations conduct research, issue research grants related to video analytics and focus on projects that benefit the wider community through enhanced technical capabilities, such as new algorithms, new cutting-edge technologies, etc.
- **Non-profit Organizations** offer membership to and represent fire, police, emergency management, and public safety communications professionals' interests by maintaining awareness of relevant public policy issues and provide training, certification, and, in some cases set standards.
- **Advisory Councils** sponsored by government organizations recommend and review necessary policies, standards, and research efforts to promote commonality of practice and interoperability of technology for public safety.
- **General Public** citizens and businesses have an increasing variety of devices ranging from sophisticated surveillance systems to cell phones that capture valuable safety and security video information. The public increasingly shares information to the community via social media and directly with public safety officials through agreements or following incidents. As these devices grow in number, the need for policies and technologies supporting privacy protection increases.
- **Academic Organizations** look for cutting edge research topics that will have an impact, lead to potential funding paths, and will result in quality publications.

These organizations conduct research related to video analytics, focusing on projects in specific fields of research such as machine learning, artificial intelligence, and advanced visualization methods, which enhance the capabilities of video analytics.

Figure 3. Public Safety Stakeholders

- **Standards Organizations** are led by industry and include participation of experts from industry and government. They lead the development and maintenance of interoperability standards based on the needs identified by participants. The standards organizations can be leveraged for community engagement, coordination of proposed interoperability standards, and development of reference standards implementations.
- **Industry** responds to consumer demands, product marketability and strategic corporate partnerships or investments that result in strong marketplace presence and profitability. Industry develops and maintains video systems, applications, and devices, bringing new technologies and capabilities to video surveillance. Interoperability equalizes opportunities across industry organizations of different sizes.
- **Social Science and Legal Community** stakeholders are advisors to the public safety video analytics community to ensure that video interoperability addresses security and privacy to preserve public trust. This community raises awareness of privacy concerns and legal aspects involved with capture and use of video surveillance information.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1500-15