DataBridge^{7} Traffic Policy Function

Digital Intelligence

BAE SYSTEMS

The challenge of traffic control in Lawful Interception

Modern Lawful Interception environments are in receipt of large volumes of network traffic, much of which may fall at the margins of a given authorisation's intended scope. As services increasingly rely on shared infrastructure, dynamic IP addressing and high-bandwidth applications, it becomes difficult for authorities to precisely control which traffic is delivered, excluded, or acted upon, while still maintaining auditability and standards compliance.

Existing Lawful Interception solutions often lack the ability to:

- Express fine-grained, policy-based traffic selection in a standardised way
- Transparently align operational behaviour with ETSI-defined standards
- Allow authorised users to refine scope using objective criteria (such as IP ranges) without ad-hoc filtering or manual intervention
- Maintain a clear, auditable linkage between lawful authorisation, policy intent and delivery behaviour

As a result, LEAs and LEMFs face increased operational complexity, unnecessary data handling and reduced clarity around how traffic control can be executed in practice.

Case example - LEMF resource burdens from intercepted low intelligence/high bandwidth traffic

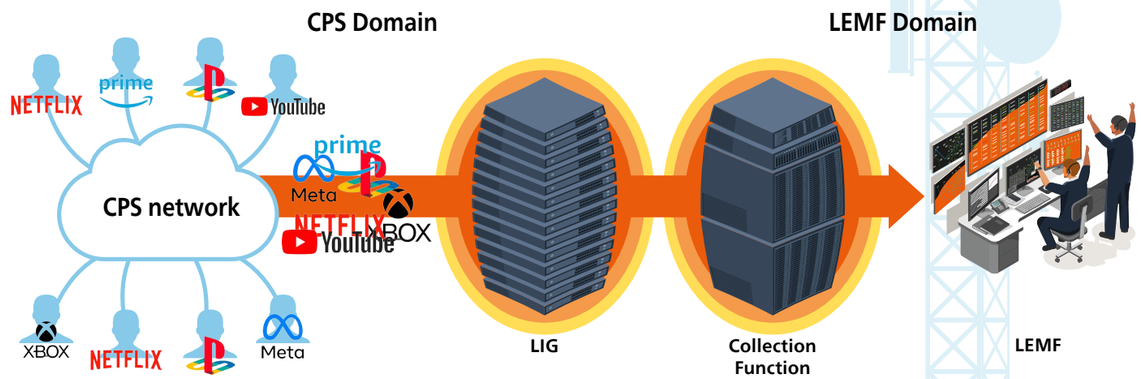
In a typical Lawful Interception operation, a Law Enforcement Monitoring Facility (LEMF) is tasked with monitoring a subject whose communications span messaging applications, web services and general internet usage. Once interception is activated, the LEMF begins receiving all associated IP traffic that falls within the scope of the lawful authorisation. Almost immediately, Collection Function Systems can become flooded with high-bandwidth application traffic — such as video streaming, media downloads, software updates and background cloud services. While technically within scope, this traffic delivers little to no intelligence value for the investigation.

The impact is felt across multiple layers of the operation:

- **Network saturation:** Continuous delivery of large video and media streams consumes significant bandwidth between the CSP and the LEMF, increasing the risk of congestion and packet loss for higher-value traffic.
- **Resource constraints:** Monitoring platforms spend disproportionate compute and indexing resources processing traffic that will never be reviewed or acted upon.
- **Infrastructure strain:** Storage systems and processing platforms must scale to handle data volumes that far exceed investigative needs, driving up operational and infrastructure costs.
- **Operational inflexibility:** Adjusting what traffic is delivered often requires reconfiguration, re-tasking or CSP intervention, introducing delays and additional operational overhead.
- **Analyst inefficiency:** Intelligence analysts are forced to sift through large quantities of irrelevant traffic to locate meaningful communications, slowing investigations and increasing the risk of missing critical signals.

As encrypted protocols and bandwidth-intensive applications become the norm, this imbalance continues to grow. The LEMF receives more data, but less usable intelligence, reducing overall effectiveness and increasing cost and complexity.

This case highlights a fundamental challenge facing modern Lawful Interception operations. Without fine-grained, standards-based control over intercepted IP traffic, LEMFs can quickly become overwhelmed by volume rather than empowered by insight.



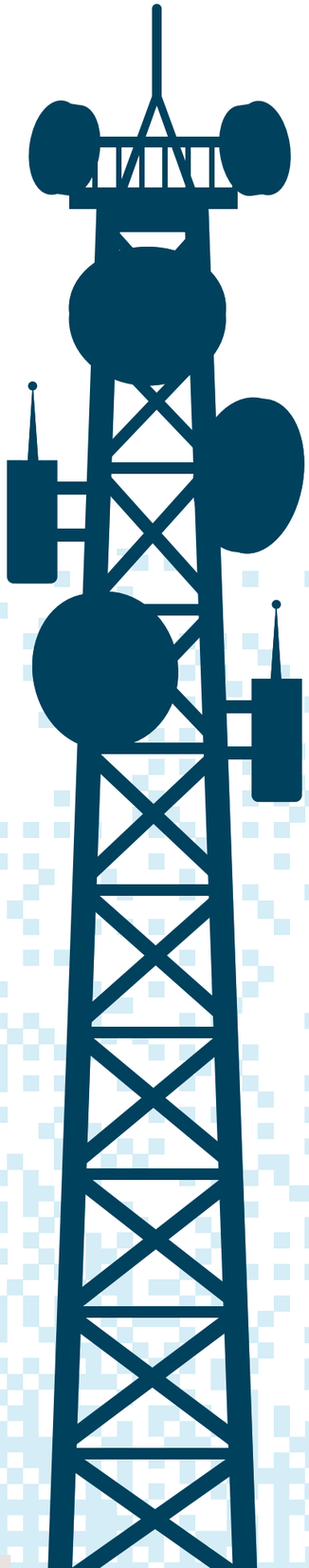
ETSI standardises traffic control

ETSI TS 103.120 addresses the challenge of precise traffic control by introducing Traffic Policy and Traffic Rule Objects as standardised, machine-readable constructs for expressing lawful scope. These objects allow LEAs and other authorised entities to define, in a transparent and auditable manner, which traffic is in scope, which traffic is excluded and what actions apply - using objective criteria such as identifiers, directions and IP-based attributes.

By separating intent from technical execution, ETSI provides a common policy language that:

- Enables fine-grained scoping without ad-hoc filtering
- Ensures consistency across vendors and implementations
- Maintains a clear audit trail linking authorisation to enforcement

Traffic Policy and Rule Objects provide a policy-driven approach to lawful interception, allowing scope to be precisely defined before traffic is delivered. Furthermore, the ETSI TS 103.120 HI-1 object linkage framework enables LEAs to react to traffic collection on a multi-surveillance basis. Traffic Policies can be dynamically linked and updated for one or more Task Objects without the need to re-provision and alter the Task Object itself, with policies taking effect immediately.



Traffic Policy and Rule technical attributes

Traffic Policy and Traffic Rule Objects possess the following attributes as defined by ETSI TS 103.120:

LITaskObject:

- **List of Traffic Policy References -** a priority ordered list of Traffic Policy Object references associated with this LITaskObject

Traffic Policy Object:

- **Traffic Policy Name -** a human readable name to be attributed to the Traffic Policy. For example, the Traffic Policy Name may capture the context of the policy, e.g., 'YouTubeUndelivered'.
- **Traffic Rules -** a priority ordered list of Traffic Rule Object references associated with this Traffic Policy Object.

Traffic Rule Object:

- **Criteria -** a list of rule criteria all of which must match for this rule to take effect. For example, IP-based criteria may include source/destination IP address ranges.
- **Action -** an action taken to associated data traffic when defined criteria is matched and the rule is in effect. For example, generate PDSRs.
- **Action Parameters -** specific parameters that are applicable to the action taken.

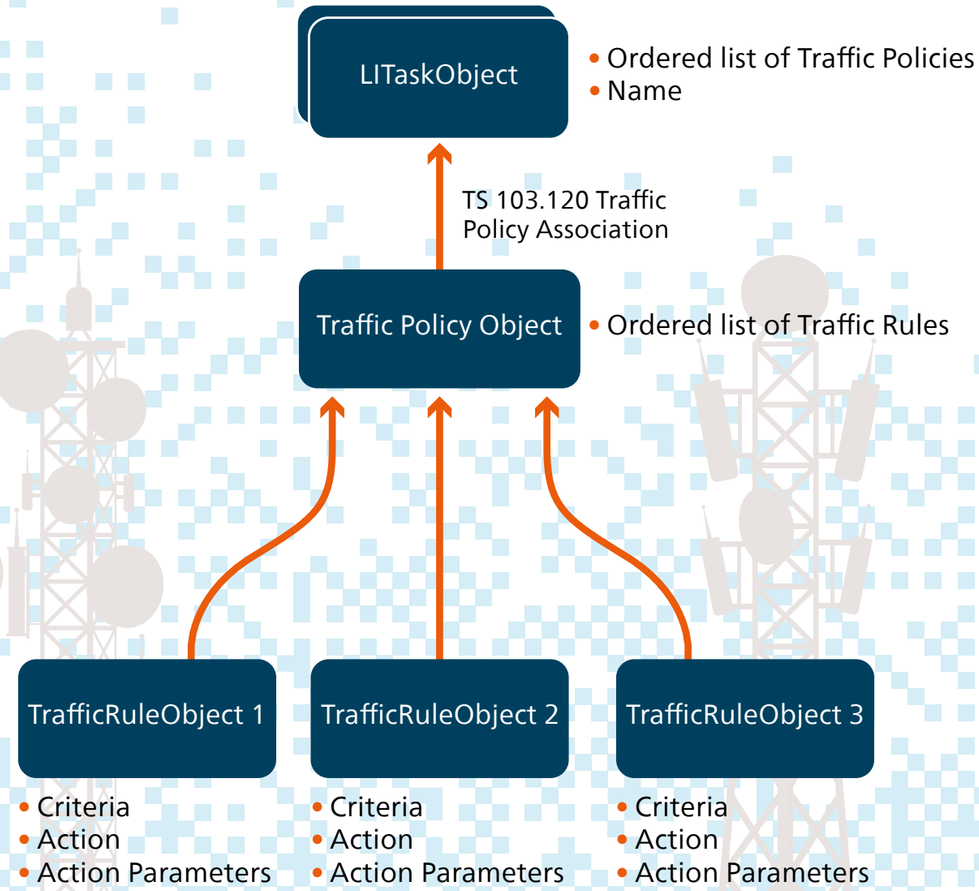


***Figure 1**: ETSI TS 103 120 Traffic Policy Associations*

Introducing DataBridge[7] Traffic Policy Function capability

DataBridge[7] Traffic Policy Function (TPF) operationalises the ETSI standard by providing a complete, standards-based implementation that spans both the control plane and the data plane.

On the control and administration plane, DataBridge[7] exposes an eWarrantry API aligned with ETSI TS 103.120, allowing Traffic Policy Objects and Traffic Rule Objects to be created, managed, and administered using ETSI defined objects and dictionaries. LEAs are enabled to define policy intent once, using standardised constructs, without vendor-specific extensions or proprietary rule models. In addition to management over ETSI TS 103.120 API, Traffic Policy and Traffic Rule Objects can be created and managed via the WMS web UI, enabling existing web-based organisational workflows to continue seamlessly.

On the data plane, DataBridge[7] TPF applies these ETSI-defined traffic policies in real time to intercepted traffic, ensuring that delivery behaviour precisely reflects the configured policy. Traffic matching defined criteria is delivered, excluded, or otherwise actioned exactly as specified, with no discretionary interpretation or manual intervention.

Together, this enables:

- Consistent enforcement of lawful scope at scale
- Reduced operational complexity and unnecessary data handling
- Clear traceability between policy definition and traffic handling
- A future-proof architecture grounded in ETSI standards

DataBridge[7] ETSI eWarrantry API, WMS Web UI and TPF operate hand in hand to deliver full end-to-end traffic control capability as part of the holistic DataBridge[7] product. Furthermore, DataBridge[7] provides full operational management of these functions via DataBridge[7] ADMF services which include DataBridge[7] Statistics (DBStats) UI and DataBridge[7] Architect Configuration UI - as well as Alarming, Orchestration, Logging and Auditing capability.

As per the core LI solution, DataBridge[7] MDF supports a variety vendor technologies in all communication domains including fixed line broadband, PSTN voice, GPRS, GSM, UMTS, LTE, NR and satellite. DataBridge[7] TPF supports ingest and processing of standardised ETSI TS 103 221-2 data transmitted over LI_X2/LI_X3 as well as legacy proprietary vendor-specific X2/X3 protocols.

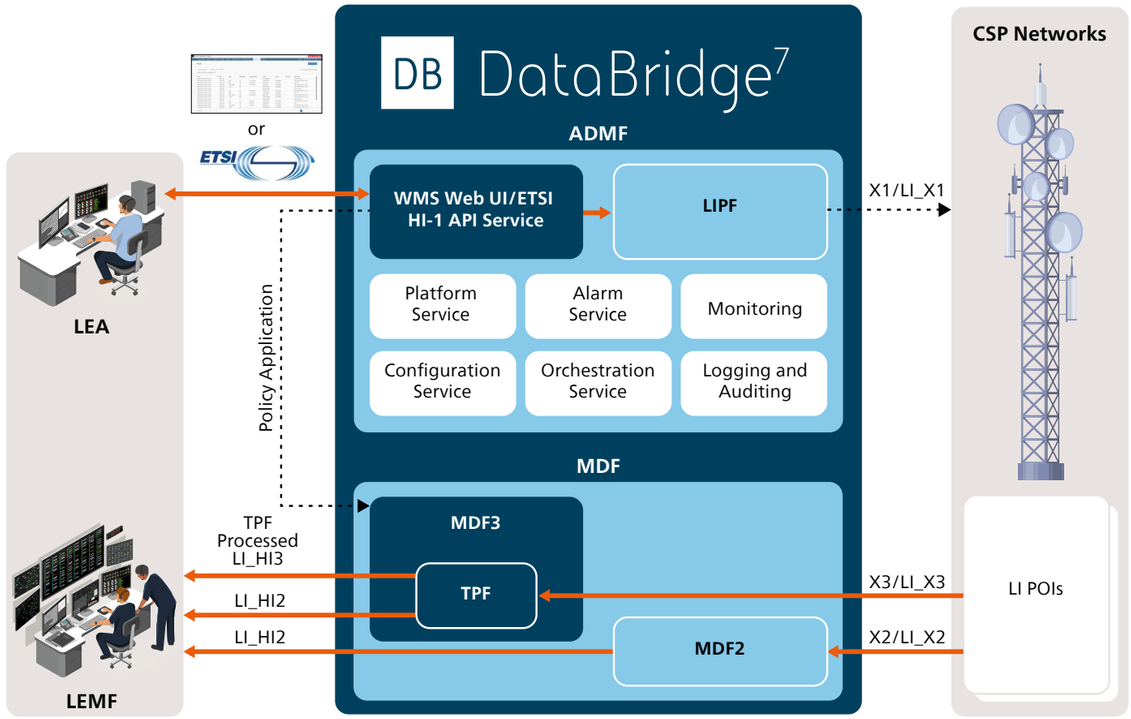
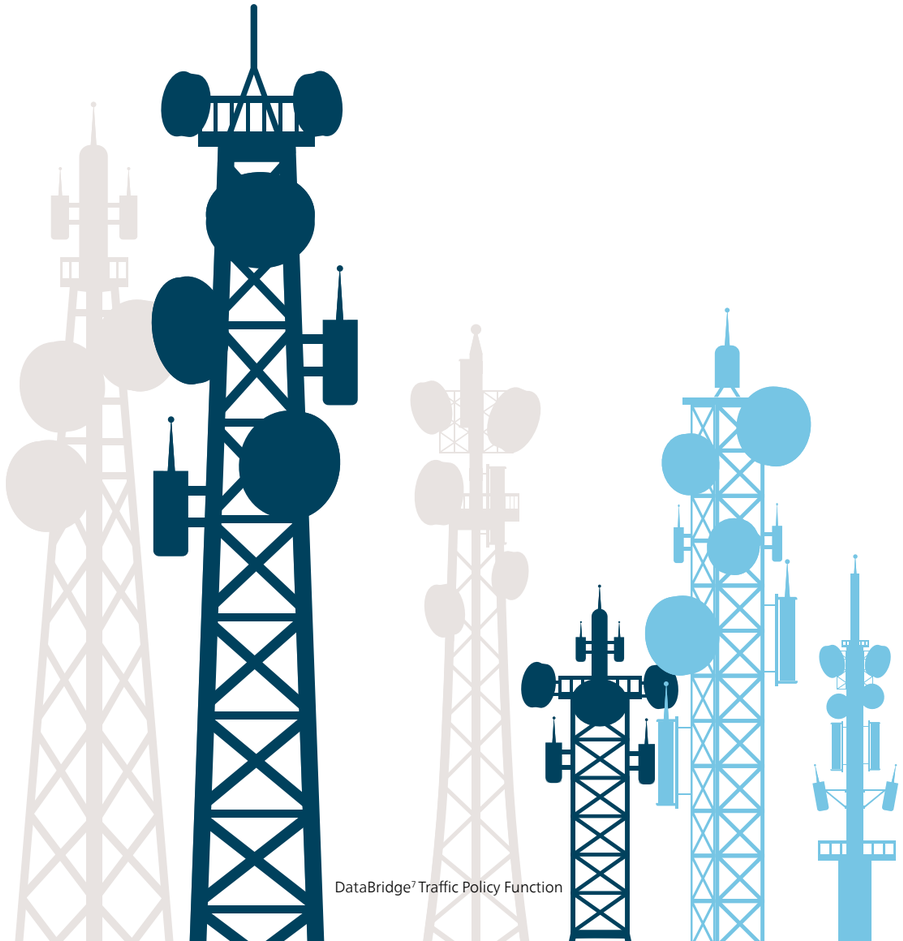


Figure 2: *Combined DataBridge[7] Architecture with Traffic Policy Function*



Combined LI or standalone/tactical deployments

DataBridge[7] supports both combined TPF and MDF deployments, as well as a standalone solution that can ingest and apply Traffic Policies to mediated HI data from a third-party Lawful Interception Gateway (LIG). BAE Systems understands that in many CSP and LEMF environments, administration and provisioning of the core LIG may need to be performed separately from administration of any HI data 'post-processing/mediation' system. This could be due to a pre-existing LIG and CSP already possessing an established administration workflow, or due to strict separation requirements between mediation and post-mediation processing. DataBridge[7] has been built with flexible deployment models in mind and can support a wide range of architectures.

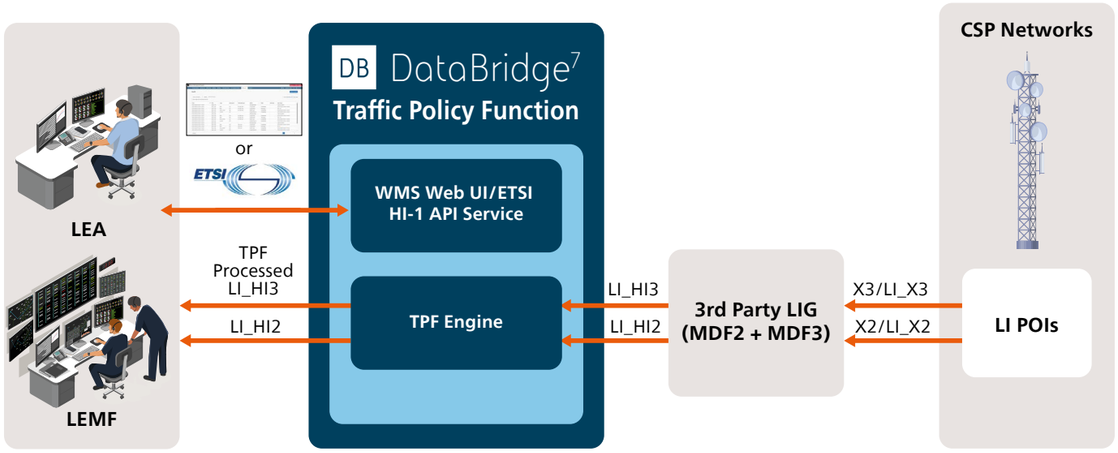


Figure 3: *Standalone DataBridge[7] Traffic Policy Function with 3rd party LIG*

When deployed as a tactical solution, DataBridge[7] TPF supports ingestion and processing of a variety of standardised input protocol including:

- ETSI TS 102.232-3 for mediated HI data sourced from the fixed line broadband domain
- ETSI TS 102.232-4 for mediated HI data sourced from L2 services
- ETSI TS 102.232-7 for mediated HI data sourced from the mobility domain

Action capability

DataBridge[7] TPF supports the following Traffic Rule Actions as defined by ETSI TS 103.120:

- **PDSR:** Intercepted traffic that matches the Criteria of a Traffic Rule possessing the 'PDSR' Action attribute shall be discarded and PDSRs (Packet Data Summary Reports) corresponding to the discarded traffic shall be generated.
- **PDHR:** Intercepted traffic that matches the Criteria of a Traffic Rule possessing the 'PDHR' Action attribute shall be discarded and PDHRs (Packet Data Header Reports) corresponding to the discarded traffic shall be generated.
- **NotDelivered:** Intercepted traffic that matches the Criteria of a Traffic Rule possessing the 'NotDelivered' Action attribute shall be discarded and no further packet data reporting shall be generated.
- **Delivered:** Intercepted traffic that matches the Criteria of a Traffic Rule possessing the 'Delivered' Action attribute shall be forward to the LEMF, while other Intercepted traffic not matching the criteria of the Traffic Rule shall be discarded.
- **Truncate:** Intercepted traffic that matches the Criteria of a Traffic Rule possessing the 'Truncate' Action attribute shall be truncated in accordance with the Truncate Action Parameters defined within the Traffic Rule.

Traffic Criteria support

DataBridge[7] supports the following Traffic Criteria (as defined by ETSI TS 103.120) that can be matched to intercepted traffic for application of Traffic Policies:

- **IP Policy Criteria:** Includes IP network-based criteria including IP transport protocol (TCP/UDP), source IP range, source port range, destination IP range and destination port range. In addition, DataBridge[7] TPF supports 'BothDirections' boolean for matching on either source or destination IP network criteria.
- **Mobile Access Policy Criteria:** Includes mobile network based criteria such as APN (Access Point Name) and DNN (Data Network Name) Identifiers.
- **Ethernet Policy Criteria:** Includes layer 2 ethernet-based criteria including source MAC address, destination MAC address and VLAN. In addition, DataBridge[7] TPF supports 'BothDirections' boolean for matching on either source or destination ethernet criteria.

Additional capability

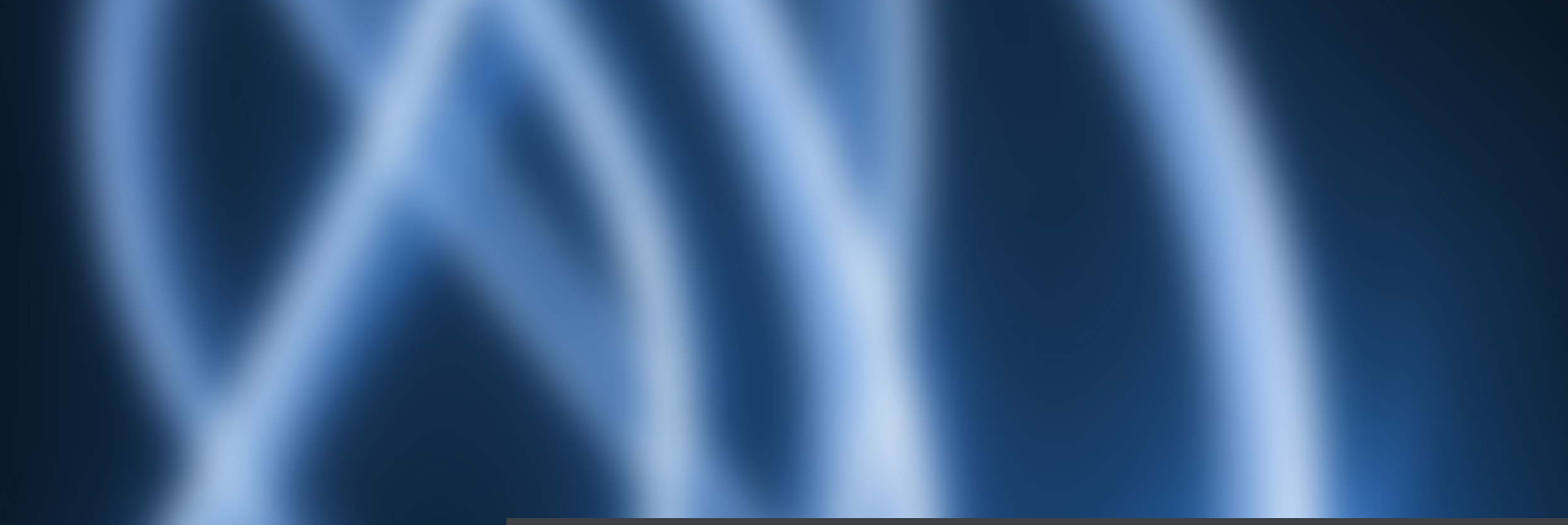
In addition to ETSI based traffic policy provisioning, DataBridge[7] also provides the following traffic control capability:

- **Global filtering:** Using local configuration instead of per-surveillance provisioning attributes, DataBridge[7] supports traffic control on a global basis for all provisioned surveillances.
- **DPI based content filtering:** DataBridge[7] supports content filtering by means of application layer level filtering using deep packet inspection.

Traffic Policy monitoring - DBStats

DataBridge[7] DBStats provides real-time and retained granular statistics to keep system operators informed of all Traffic Policy and LI activity over a desired period range. DataBridge[7] DBStats provides the following Traffic Policy related statistics and visualisations:

- Real-time and historical count of surveillances with Traffic Policies associated
- Real-time and historical count of total bytes/PDUs dropped due to Traffic Policy application
- Graphical view of bytes/PDUs dropped per surveillance due to Traffic Policy application
- Graphical view of PDSR/PDHR bytes/PDUs generated per surveillance due to Traffic Policy application
- Graphical view of bytes/PDUs dropped per Traffic Rule criteria and per surveillance/LEMF



We are Digital Intelligence

Digital Intelligence is home to over 4,700 digital, cyber and intelligence experts across 16 countries. We operate at the cutting edge of digital innovation and at the heart of organisations that keep vital infrastructure running, national security protected and armed forces prepared.

Our teams provide advanced digital capability, products and solutions that weave together digital threads of data so that customers get the vital insight they need – from the fine detail to the bigger picture, providing the power of perspective to confidently make the critical decisions that keep our societies safe and able to thrive.

Digital Intelligence is part of BAE Systems and has a rich heritage in helping to defend nations and businesses around the world from advanced threats. Whether on land, in the air, at sea, in space or cyberspace, we're your digital mission partner, with you every step of the journey.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS