sttp
Streaming Telemetry Transport Protocol

Version: 0.0.20 - June 28, 2017

Status: Initial Development

Abstract: This specification defines a publish-subscribe data transfer protocol that has been optimized for exchanging streaming time series style data, such as synchrophasor data that is used in the electric power industry, over Internet Protocol (IP). The protocol supports transferring both real-time and historical time series data at full or down-sampled resolutions. Protocol benefits are realized at scale when multiplexing very large numbers of time series data points at high speed, such as, hundreds of times per second per data point.

Disclaimer

License

Table of Contents

Introduction

Use of synchrophasors by U.S. utilities continues to grow following the jump start provided by the Smart Grid Investment Grants. Even so, the dominant method to exchange synchrophasor data remains the IEEE C37.118-2005 [1] protocol that was designed for and continues to be the preferred solution for substation-to-control room communications. It achieves its advantages through use of an ordered set (a frame) of information that is associated with a specific measurement time. When IEEE C37.118 is used for PDC-to-PDC communication or for PDC-to-Application communication, large data frames are typically distributed to multiple systems. To address the challenges presented by these large frame sizes, many utilities implement purpose-built networks for synchrophasor data only. Even with these purpose-built networks, large frame sizes result in an increased probability of UDP frame loss, or in the case of TCP, increased communication latency. In addition, IEEE C37.118 has only prescriptive methods for the management of measurement metadata which is well-suited for substation-to-control-center use but which becomes difficult to manage as this metadata spans analytic solutions and is used by multiple configuration owners in a wide-area context.

To address these issues, the Advanced Synchrophasor Protocol (ASP) Project was proposed to DOE in response to FOA-1492. In this project proposal, the argument was made for a new protocol that overcomes the limitations of IEEE C37.118 for large-scale synchrophasor data system deployments. The new protocol proposed leveraged the successful design elements of the secure Gateway Exchange Protocol (GEP) that was originally developed by the Grid Protection Alliance (GPA) as part of the SIEGate project (DE-OE-536).

On May 1, 2017, a DOE grant (DE-OE-859) was awarded to GPA and the other 25 collaborators on ASP Project (see Contributors section) to develop: (1) a detailed definition of new publish-subscribe protocol, now called the Streaming Time-series Transport Protocol (STTP) and (2) software to support it including production-grade implementations of STTP API's in multiple development platforms along with a collection of tools to test and validate the new protocol.

Scope of this Document

The purpose of this document is to define STTP and to include, as appendices, descriptions as to how to use its supporting software tools. This STTP specification is focused on effective "streaming data" delivery of which synchrophasor data is a very important use case.

In the Overview section of this specification, high-level features and the business value of STTP are presented. The balance of the sections of the specification provide the details of protocol design.

Appendix A - STTP API Reference provides instructions to enable software developers to integrate and use of STTP within other software systems.

Appendix B - IEEE C37.118 Mapping provides a detailed look at the process of transforming IEEE C37.118 into STTP as well as creating IEEE C37.118 streams from STTP.

While the format and structure of this document, established to facilitate collaboration, is different than that used by standards bodies, it is hoped that the content within this document can meet all the information requirements needed to enable repackaging of this specification into draft standard formats.

Definitions and Nomenclature

🚧 Please add liberally to this section as terms are introduced in the spec

Definition of Key Terms

The words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119 [3].

ℹ️ All the terms below are hyperlinked to a key source for the definition or to a reference where more information is available.

Term	Definition
data point	A measurement on a single member of a statistical population.
frame	
measurement	
phasor	A complex equivalent of a simple cosine wave quantity such that the complex modulus is the cosine wave amplitude and the complex angle (in polar form) is the cosine wave phase angle.
publish/subscribe	A messaging pattern where senders of messages, called publishers, do not program the messages to be sent directly to specific receivers, called subscribers, but instead characterize published messages into classes without knowledge of which subscribers, if any, there may be.
signal	
synchrophasor	A phasor calculated from data samples using a standard time signal as the reference for the measurement. Synchronized phasors from remote sites have a defined common phase relationship.
time series	A series of data points indexed in time order, most commonly measured as a sequence taken at successive equally spaced points in time.
term	definition

Acronyms

Term	Definition
API	Application Program Interface
DOE	United States Department of Energy
DDS	Data Distribution Service
GEP	Gateway Exchange Protocol
GPA	Grid Protection Alliance, Inc.
GUID	Globally Unique Identifer
IP	Internet Protocol
MTU	Maximum Transmission Unit
PDC	Phasor Data Concentrator

PMU	Phasor Measurement Unit
STTP	Streaming Telemetry Transport Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
ZeroMQ	Brokerless Messaging Queuing and Distribution Library

Document Conventions

Markdown notes in combination with the Github Emogi images are used as callouts. The standard callouts are:

> ℹ️ This is a call out in the spec to provide background, instruction or additional information
>
> ⚠️ This note use used to highlight important or critical information.
>
> 🚧 A informal note to document authors to facilitate specification development
>
> 🍅 ❓ (author's initials): May be used by anyone to toss out questions and comments that are temporal. These may be inserted at any point in any of the markdown documents. These questions will preserved as they are migrated to the QuestionsSummary.md file from time-to-time.

Code blocks are shown as:

```
public function void DisplayHelloWorld()
{
    Console.WriteLine("Hello world!");
}
```

Code is also shown `inline` as well.

Protocol Overview

> 🚧 Purpose of protocol, fundamentals of how it works (command and data) - include sub-section titles (4# items) as needed
>
> Describe what protocol is and is not - how it could operate with ZeroMQ, DDS, etc. as a transport layer - how it is different than thrift, protobuf, etc., i.e., atomized approach to native-type data vs serializing and deserializing data structures - why this has benefit at scale (i.e., very large structures)

Data transport requires the use of a command channel using TCP/IP for reliable delivery of important commands. Optionally a secondary data channel can be established using UDP/IP for the transport of data that can tolerate loss. When no secondary UDP/IP is used, both commands and data will share use of the TCP/IP channel for communications.

> 🍅❓ JRC: *The question has been raised if a UDP only transport should be allowed? In this mode, any critical commands and responses would basically be sent over UDP. Thought would need to be given to commands and/or responses that never arrive and the consequences thereof.*

more

> ℹ️ Although not precluded from use over other data transports, the design of this protocol is targeted and optimized for use over Internet Protocol, specifically TCP/IP and UDP/IP. Even so, since the command/response implementation and data packet distribution of the STTP protocol is fairly simple, it is expected that commonly available middleware data transport layers, such as ZeroMQ or Data Distribution Service (DDS), could easily support and transmit data using the STTP protocol should any of the messaging distribution and management benefits of these transport layers be useful to a particular deployment environment. However, these types of deployments are outside the scope of this documentation. If needed, STTP integrations with middleware layers should be added as reference implementation repositories to the STTP organizational site.

Protocol Feature Summary

> 🚧 This is the protocol promotional section that includes a bulleted list of the "value points" for the protocol

- Perform at high volume / large scale
- Minimize data losses (e.g., over UDP)
- Lower bandwidth requirements (e.g., over TCP)
- Optimized for the performant delivery of individual data points
- Automated exchange of metadata (no centralized registry required)
- Detect and expose communication issues
- Security and availability features that enable use on critical systems to support critical operations
- Publish/subscribe at data point level
- API implemented in multiple languages on multiple platforms

Business case

At the conclusion of the STTP project in April 2019, the new STTP will be a well-tested, thoroughly vetted, production-grade protocol that will be supported by project team vendors. An open source tool suite for STTP will be developed as part of the project (see Appendix A) that will include a test harness that will allow utilities and vendors outside the project to test and validate STTP in their systems and API's.

STTP offers both short-term cost savings and strategic value in that it is:

Intrinsically More Robust with Less Data Loss

- By design, STTP packet sizes are small and are optimized for network MTU size reducing fragmentation which results in more efficient TCP performance and less overall data loss with UDP.

- STTP puts significantly less stress on network routing equipment and facilitates mixing of streaming data traffic and other general network communications. With STTP, purpose built networks are not required to reliably support very large phasor data streams.

Security Centric

- STTP has been built using a "security first" design approach. Authentication to establish a "connection" with other parties requires a "certificate". While public certificate providers can be used, it is recommended that symmetric certificates be exchanged out-of-band to avoid the risk and cost of management of public keys.

- Best-practice encryption is natively available in STTP but not required given the common practice to manage encryption at the network layer.

Reduces First Cost

- GEP has been measured [5] to have less than half the band width requirements of IEEE C37.118 [1] when used with TCP and simple methods for lossless compression. With the compression, a single signal or measurement point (i.e., an identifier, timestamp, value and quality code) requires only 2.5 bytes. By comparison, IEEE C37.118 requires 4.5 bytes per measurement on average.

- The signal-based GEP protocol incorporates Pub/Sub data exchange methods so that unnecessary data points need not be exchanged â€" thereby further reducing overall bandwidth requirements as compared to IEEE C37.118.

Reduces Operating Cost

- GEP automatically exchanges and synchronizes measurement level meta-data using a GUID as the key value to allow the self-initialization and integration of rich meta-data with points from multiple connected synchrophasor networks. This eliminates the need to map measurements to a pre-defined set identifiers and dispenses with the cost and hassles of synchronization of individual utility configuration with a centralized registry.

- Permissions for data subscriptions can be grouped and filtered using expressions to assure that only the signals that are authorized are shared (for example, all phasors from a specified substation) while the set of points available is dynamically adjusted as PMUs come and go without the need for point-by-point administrator approval.

An Enabling Technology

- It's possible that a protocol like STTP which allows secure, low-latency, high-volume data exchange among utilities at low cost can be a major factor in driving rapid change in the industry. New forms of inter-utility interaction will be possible. New approaches for providing utility information services will be possible.

Built Upon A Proven Approach

- STTP will enhance the successful design elements of the Gateway Exchange Protocol (GEP) as a foundation and improve upon it.

- GEP is in n production use by Dominion, Entergy, MISO, PeakRC, TVA, FP&L, Southern Company and others.

Design Philosophies

- Minimize external libraries and dependencies for reference implementations
- Keep portability in mind with all protocol design work
- Target smallest possible API functionality - specialized use cases will be handled by example
- Set design mantra to be "keep it simple" *as possible*

Data Point Structure

🚧 Lead with paragraph on purpose / value of the section - (1) what is a data point structure and (2) why have a data point structure / value? Next paragraph would be contents of section...

... this section includes:

- Identification - maps to 128-bit Guid, transport mapping should be small
- Timestamp (required? could simply be a auto-incrementing counter)
- Value - multiple native types supports
- Flags - standardize minimal set of simple flags, complex state can be new data point

Data Point Value Types

- Null
- Byte
- Int16
- Int32
- Int64
- UInt16
- UInt32
- UInt64
- Decimal
- Double
- Single
- DateTime (need some thought on proper encoding, perhaps options)
- TimeSpan (Tick level resolution, or better, would be ideal)
- Char (2-byte Unicode)
- Bool
- Guid
- String (encoding support for UTF-16, UTF-8, ANSI and ASCII)
- Byte[]

🚧 Need to determine safe maximum upper limit of per-packet strings and byte[] data, especially since implementation could simply *span* multiple data points to collate a larger string or buffer back together.

🍅❓ *Should API automatically handle collation of larger data types, e.g., strings and buffers?*

Commands and Responses

🚧 Purpose of command/response structure, fundamentals of how it works, why it is needed

Commands

All commands must be sent over the command channel.

Code	Command	Source	Description
0x00	Set Operational Modes	Subscriber	Defines desired set of operational modes.
0x01	Metadata Refresh	Subscriber	Requests publisher send updated metadata.
0x02	Subscribe	Subscriber	Defines desired set of data points to begin receiving.
0x03	Unsubscribe	Subscriber	Requests publisher terminate current subscription.
0x0n	etc.		
0xFF	NoOp	Any	Periodic message to allow validation of connectivity.

Set Operational Modes Command

This must be the first command sent after a successful connection - the command must be sent before any other commands or responses are exchanged so that the "ground-rules" for the communications session can be established. The rule for this operational mode negotiation is that once these modes have been established, they will not change for the lifetime of the connection.

The subscriber must send the command and the publisher must await its reception. If the publisher does not receive the command in a timely fashion (time interval controlled by configuration), it will disconnect the subscriber.

> ℹ️ In modes of operations where the publisher is initiating the connection, the publisher will still be waiting for subscriber to initiate communications with a `Set Operational Modes` command.

- Wire Format: Binary
- Requested operational mode negotiations
  - String encoding
  - Compression modes
  - UDP data channel usage / port

Metadata Refresh Command

- Wire Format: Binary
  - Includes current metadata version number

Subscribe Command

- Wire Format: Binary
  - Includes metadata expression and/or individual Guids for desired data points

Unsubscribe Command

- Wire Format: Binary

NoOp Command

No operation keep-alive ping. It is possible for the command channel to remain quiet for some time if most data is being transmitted over the data channel, this command allows a periodic test of client connectivity.

- Wire Format: Binary

Responses

Responses are sent over a designated channel based on the nature of the response.

Code	Response	Source	Channel	Description
0x80	Succeeded	Publisher	Command	Command request succeeded. Response details follow.
0x81	Failed	Publisher	Command	Command request failed. Response error details follow.
0x82	Data Point Packet	Any	Data	Response contains data points.
0x83	Signal Mapping	Any	Command	Response contains data point Guid to run-time ID mappings.
0x8n	etc.			

ℹ️ For the response table above, when a response is destined for the data channel, it should be understood that a connection can be established where both the command and data channel use the same TCP connection.

Succeeded Response

- Wire Format: Binary (header)
  - Base wire format includes *in-response-to* command code
  - Can include response that is specific to source command:

Succeeded Response for Metadata Refresh

- Wire Format: String + Binary
  - Includes response message with stats like size, number of tables etc.
  - Includes temporal data point ID for "chunked" metadata responses
  - Includes number of metadata data points to be expected

Succeeded Response for Subscribe

Subscriber will need to wait for

- Wire Format: String + Binary
  - Includes response message with stats like number of actual points subscribed, count may not match requested points due to rights or points may no longer exist, etc.
  - Includes temporal data point ID for "chunked" signal mapping responses
  - Includes number of signal mapping data points to be expected

Succeeded Response for Unsubscribe

- Wire Format: String

- Includes message as to successful unsubscribe with stats like connection time

Failed Response

- Wire Format: String + Binary (header)
  - Base wire format includes *in-response-to* command code
  - Includes error message as why command request failed
  - Can include response that is specific to source command:

Failed Response for Set Operational Modes

Failed responses to operational modes usually indicate lack of support by publisher. Failure response should include, per failed operational mode option, what options the publisher supports so that the operational modes can be re-negotiated by resending operational modes with a set of *supported* options.

- Wire Format: Binary
  - Includes operational mode that failed followed by available operational mode options

Data Point Packet Response

- Wire Format: Binary
  - Includes a byte flag indicating content, e.g.:
  - Data compression mode, if any
  - Total data points in packet
  - Includes serialized data points

ℹ️ The data point packet is technically classified as a response to a `subscribe` command. However, unlike most responses that operate as a sole response to a parent command, data-packet responses will continue to flow for available measurements until an `unsubscribe` command is issued.

Signal Mapping Response

- Wire Format: Binary
  - Includes a mapping of data point Guids to run-time signal IDs
  - Includes per data point ownership state, rights and delivery characteristic details

Data Point Characteristics

- Priority (e.g., control over data delivery priority)
- Reliability (e.g., must be sent over TCP channel)
- Verification (e.g., notification of successful transport)
- Exception (e.g., delivery on change)
- Resolution (e.g., down-sampling)

Metadata

- Wire Format: Tabular XML format (XML) - highly compressible
- Primary data point identifier is Guid (describe)
- Extensibility
- Rights based content restriction

Dataset Contents

- Minimum required dataset for STTP operation
- Industry specific dataset extensions (outside scope of this doc)

Dataset Filtering

- Format of expressions that work against metadata
  - SQL style expressions
  - Regex style expressions
- Application of expressions
  - Metadata reduction
  - Data point access security

Dataset Versioning

- Versioned
- Difference based publication

Dataset Serialization

- Serialization for transport
  - Packet based publication using temporal data point
  - Publisher reduction by access rights and diff-version
  - Subscriber reduction by filter expression
- Serialization to local repository
  - Merging considerations
  - Conflict resolution
  - Ownership control

Compression

- Types of compression
  - Stateful data compression (TCP)
  - Per-packet data compression (UDP)
  - Metadata compression (GZip)
- Compression algorithm extensibility
  - Negotiating desired compression algorithm

Security

- Access control list (ACL) security is always on

Encrypted Communications

- Transport layer security (TLS) over TCP command channel
- UDP data channel traffic secured via AES keys exchanged over TCL command channel

Strong Identity Validation

- X.509 certificates
- Self-signed certificates

Publisher Initiated Security Considerations

How does publisher initiated connection, to cross security zones in desired direction, affect identity validation and TLS?

Access Control Lists

- Allow/deny for specific points (data point explicit)
- Allow/deny for group with specific points (group explicit)
- Allow/deny for filter expression (filter implicit)
- Allow/deny for group with filter expression (group implicit)

Expression based Access Control

- Expressions can be used to define filters and groups
- How do filters work against extensible metadata, missing columns?

Access Control Precedence

- (1) Data Point Explicit
- (2) Group Explicit
- (3) Filter Implicit
- (4) Group Implicit

References and Notes

1. IEEE Standard C37.118, Standard for Synchrophasors for Power Systems
2. The MIT Open Source Software License
3. RFC 2119, Current Best Practice Scott Bradner, Harvard University, 1997
4. STTP Repositories on GitHub, Various specification documents and reference implementations.
5. New Technology Value, Phasor Gateway, Peak Reliability, September 2016, Task 7 Data Delivery Efficiency Improvements, DE-OE-701.

Contributors

The following individuals actively participated in the development of this standard.

- J. Ritchie Carroll, GPA
- F. Russell Robertson, GPA
- Stephen C. Wills, GPA

ASP Project Participants

Project Collaborators	Project Financial Partner	Vendor	Utility	Demonstration Host
Bonneville Power Administration	♦		♦	
Bridge Energy Group				
Dominion Energy	♦		♦	EPG
Electric Power Group	♦	♦		
Electric Power Research Institute				
ERCOT			♦	
Grid Protection Alliance (Prime)	♦	♦		
ISO New England			♦	
MehtaTech		♦		
Oklahoma Gas & Electric	♦		♦	WSU
OSIsoft		♦		
Peak Reliability			♦	
PingThings		♦		
PJM Interconnection			♦	EPG
Southern California Edison			♦	
San Diego Gas & Electric	♦		♦	WSU
Schweitzer Engineering Laboratories	♦	♦		
Southern Company Services			♦	
Southwest Power Pool	♦		♦	WSU
Space-Time Insight		♦		
Trudnowski & Donnelly Consulting Engineers		♦		
Utilicast	♦	♦		
Tennessee Valley Authority	♦		♦	WSU
University of Southern California				
V&R Energy		♦		
Washington State University	♦	♦		
26	11	11	12	6

Specification Copyright Statement

Major Version History

Version	Date	Notes
0.1	TBD, 2017	Initial draft for validation of use of markdown
0.0	June 15, 2017	Specification template

Appendix A - STTP API Reference

appendix body

appendix body

> 💡 Links to language specific auto-generated XML code comment based API documentation would be useful.

Appendix B - IEEE C37.118 Mapping

appendix body

appendix body

Specification Development To-Do List

- ☑ Determine the location for posting images (June 18, 2017)
- ☑ Create script to automate markdown merge (June 19, 2017)
- ☐ Sample item 3 (date)