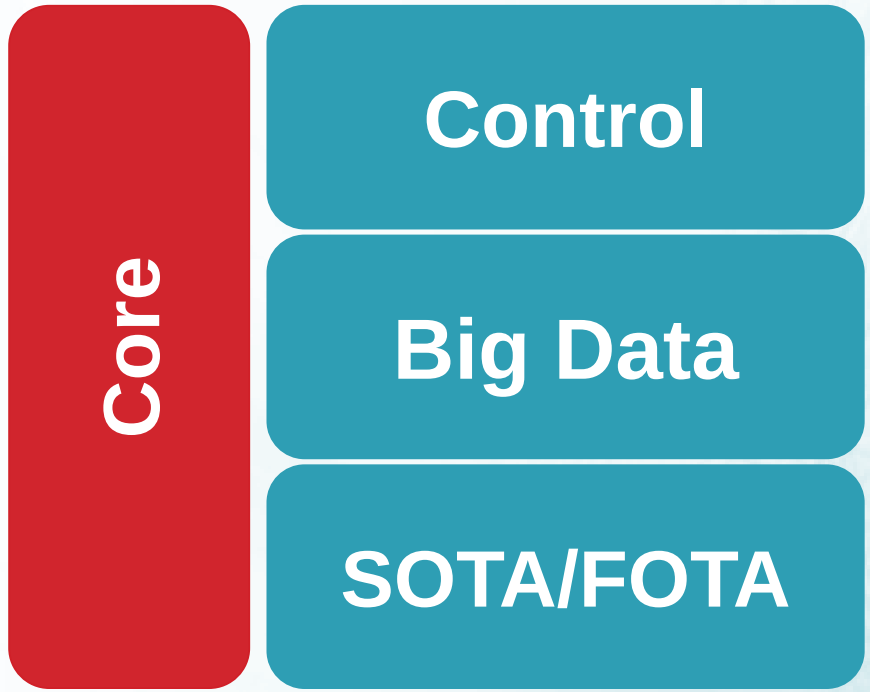
Remote Vehicle Interaction

May 11, 2017 | Project Update

Rudolf J Streif

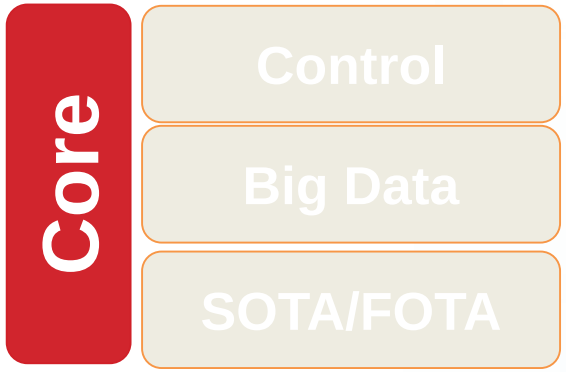
Networking Expert Group Lead, GENIVI Alliance

RVI Core Enabling Three Macro Use Cases



GENIVI®

RVI Core



Connectivity

- Utilize a wide array of data links to set up communication to and from vehicle, either with cloud backend or peer-to-peer.
- Provide encryption for secrecy, non-repudiation, replay attacks, MITM, etc.
- Work with OMA, IEEE, W3C, and other organizations for standardization and integration with existing communication standards.

Authentication

- Prove the identity of the communicating parties.
- Use best-of-breed open source technologies to drive peer-to-peer reviewed security.

Authorization

- Prove to communicating parties the right to discover and to invoke their services.
- Prove to communicating parties the right to publish and advertise services.

Service Discovery

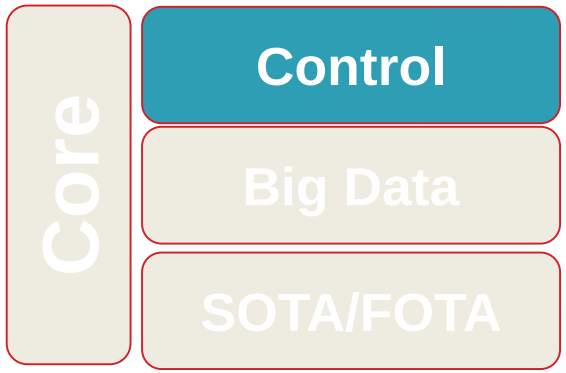
- Announce services to communicating parties.

Service Invocation

- Invoke services and report the result over data links with changing QoS.
- Support retry and store & forward of service invocations to manage transient transport.

GENIVI®

RVI Control



Vehicle Integration

- Utilize GENIVI Networking Expert Group components to integrate with vehicle buses.
- Implement W3C APIs and signal standards to provide access to vehicle information and control vehicle functions.

Service Protocol

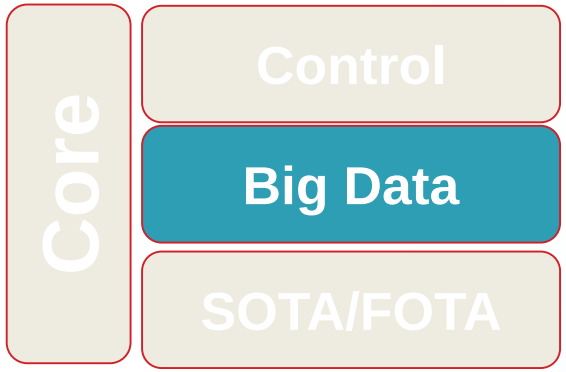
- Define vehicle control protocols between vehicle and remote entities such as cloud-based services, mobile devices, home automation gateways, etc.

Web Services

- Utilize W3C-based standards to define web services for remote interaction from web browsers and web runtimes.

GENIVI®

RVI Big Data



Data Collection

- Integrate with GENIVI components to harvest data infotainment and headunit data.
- Integrate with AUTOSAR components to collect data from ECUs and sensors.
- Utilize dynamically OTA-loadable code agents to securely collect, filter and preprocess data on-board.

Data Transmission

- Define, specify, standardize and implement secure transmission protocols for vehicle data to the cloud.

Data Reporting

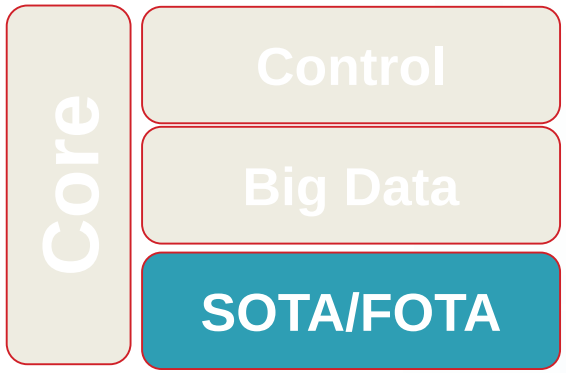
- Specify and implement in-vehicle reporting services.

Data Analytics

- Big Data cloud services for data ingestion, storage and access.
- Real-time and batch processing pipelines.
- Based on best-of-breed big data technologies such as Apache Hadoop, Ambari, Spark, NiFi, etc.

GENIVI®

RVI SOTA / FOTA



SOTA Client and Software Management

- Specify, define, standardize and implement SOTA client for receiving software update images.
- Specify, define, standardize and implement Software Management (SWM) to manage software updates on the headunit and other ECUs.
- Standardize and implement protocols for notification and transport.

SOTA Server

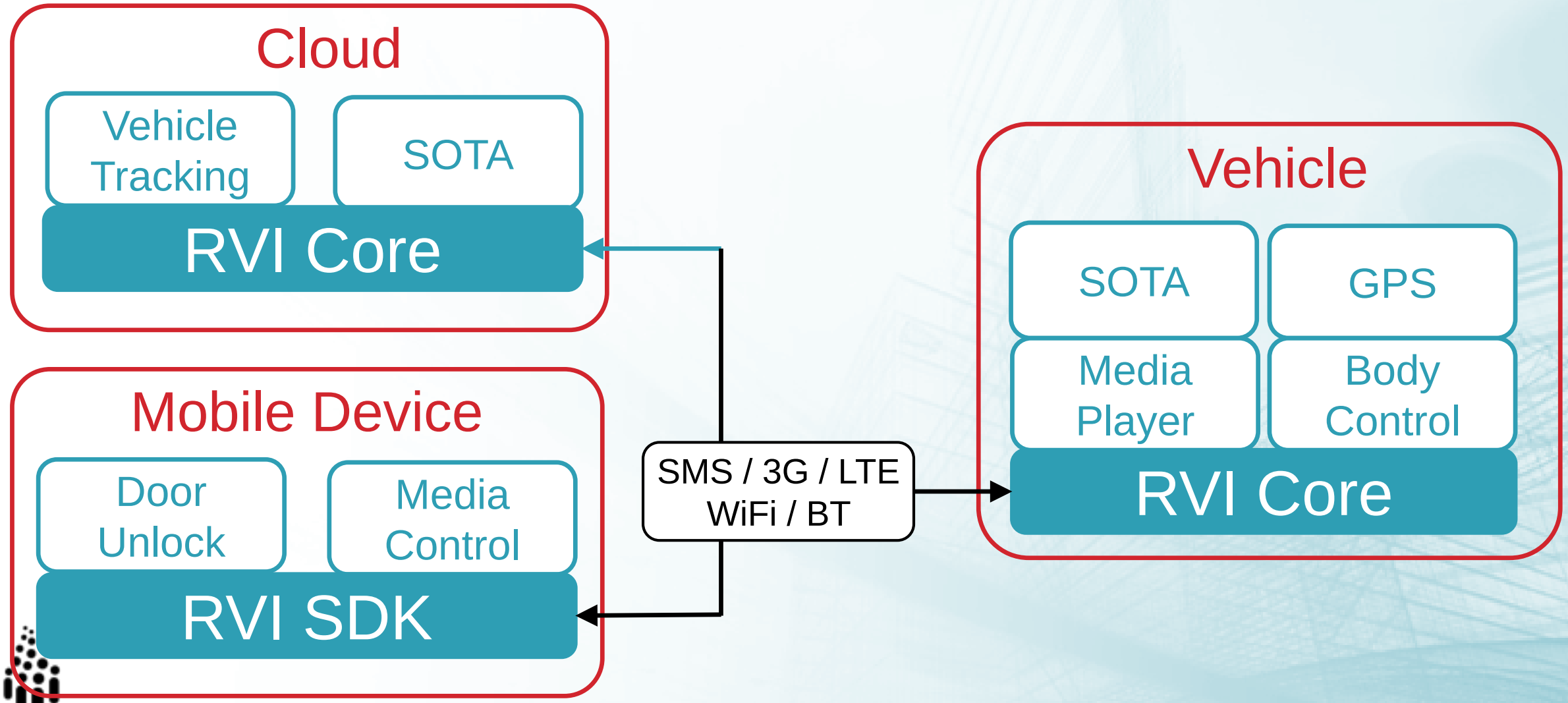
- Define requirements for server backend supporting large-scale SOTA campaigns to thousands of vehicles.
- Define integration points with enterprise software systems.
- Implement SOTA server with database and user frontend for campaign management and reporting.

Industry Integration and Adoption

- Collaborate with vendors and open source projects to foster adoption.

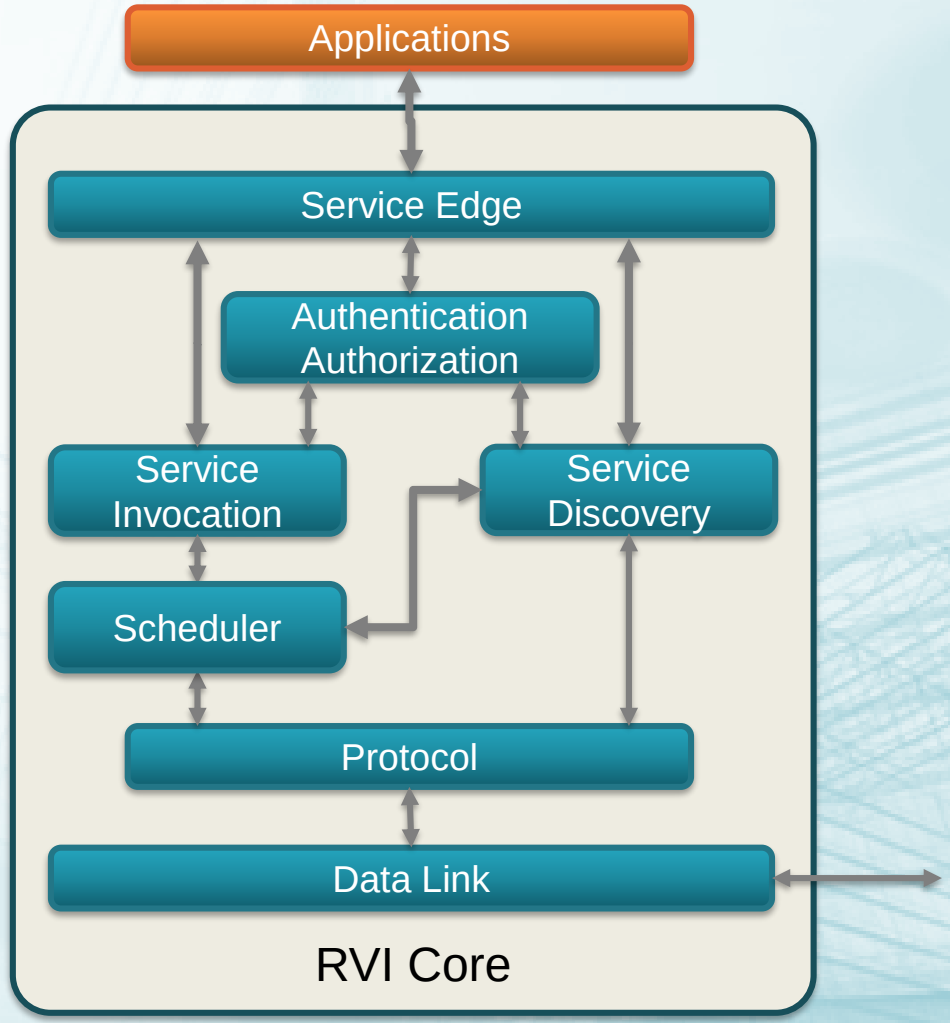
GENIVI®

RVI Schematics



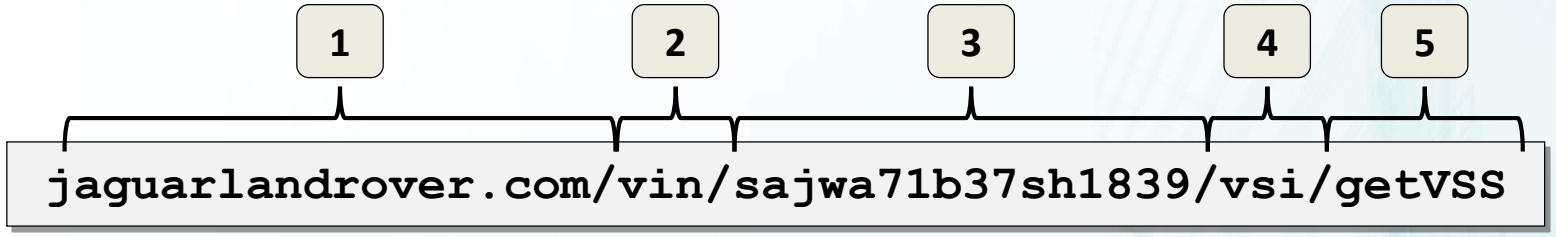
RVI Core

- **Service Edge**
  - Manages traffic from and to application.
- **Authentication / Authorization**
  - Manages certificates that allow applications to discover and invoke services.
- **Service Discovery**
  - Identifies and locates local and remote services.
- **Service Invocation**
  - Receives and dispatches local and remote service calls.
- **Scheduler**
  - Stores and forwards messages for unavailable destinations.
- **Protocol**
  - Encodes and decodes messages.
- **Data Link**
  - Controls data transmission to other RVI nodes.



GENIVI®

RVI Service Addressing



#	Name	Description
1	Organization	Specifies a sub-section hosted by a specific entity
2	VIN sub-tree	Specifies sub section for all vehicles
3	VIN	Vehicle Identification Number
4	Service Domain	Domain of service
5	Service Command	Service command within the service domain

GENIVI®

RVI Security

- TLS-protected Internode Communication
  - Prevent replay attacks.
  - Prevent man-in-the-middle attacks.
- Certificate-based Node Authentication and Service Authorization
  - Certificates, signed by a trusted provisioning system, attest application identity and grant access to services.
- Self-carried application authentication and service authorization
  - A Node presents its certificates to another node to authenticate itself and provide its service authorization. No connection to a server is required.
  - Each certificate carries the node’s public key. Nodes sign all messages with their private key.

GENIVI®

RVI Project Progress

- RVI C Library
  - Native RVI communication protocol.
  - Small footprint for embedded devices.
- End-to-End Provisioning
  - Connecting users to keys and credentials.
  - X.509 certificate creation, signing and management.
  - Self-provisioning with identity setup and dynamic assignment of authorizations.
- Security Audit by GENIVI Security Team
  - Thread models and attack vector analysis.

GENIVI®

Thank you!

Weekly Networking Expert Group Call

Mondays 0800 PT / 1700 CET

https://genivi.webex.com/genivi/j.php?MTID=mdb9482b92015e5cb7386c1a65e32a887

Meeting number: 579 975 193

Mailing List

https://mail.genivi.org/sympa/info/eg-nw

GENIVI®

