



# Software Management

Thursday 4/28 14:00 – 16:00

Arthur T. Taylor  
CTO – ATS

Contributor – Systems Infrastructure EG

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 ([CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/))

GENIVI is a registered trademark of the GENIVI Alliance in the USA and other countries

Copyright © GENIVI Alliance 2016

## **SOTA / SCOTA / FOTA / OTA**

- Delivering updates to vehicles in the field, over the internet
- Urgent requirement for existing and future IVI systems
- Non-differentiating feature - has to work

## **Existing solutions**

- Red Bend (Harman) - feature-rich, fully proprietary
- CarSync (Arynga) - Part of Arynga's proprietary server-side software suite, open source client
- OMA DM / FUMO - Open Standard - complex, some parts available as open source
- The Update Framework [1] - designed to overlay on existing solutions
- "Roll your own" - time consuming, insecure
- JLR commissioned end-to-end open source solution

1. <http://theupdateframework.com>

## **SOTA / SCOTA / FOTA / OTA**

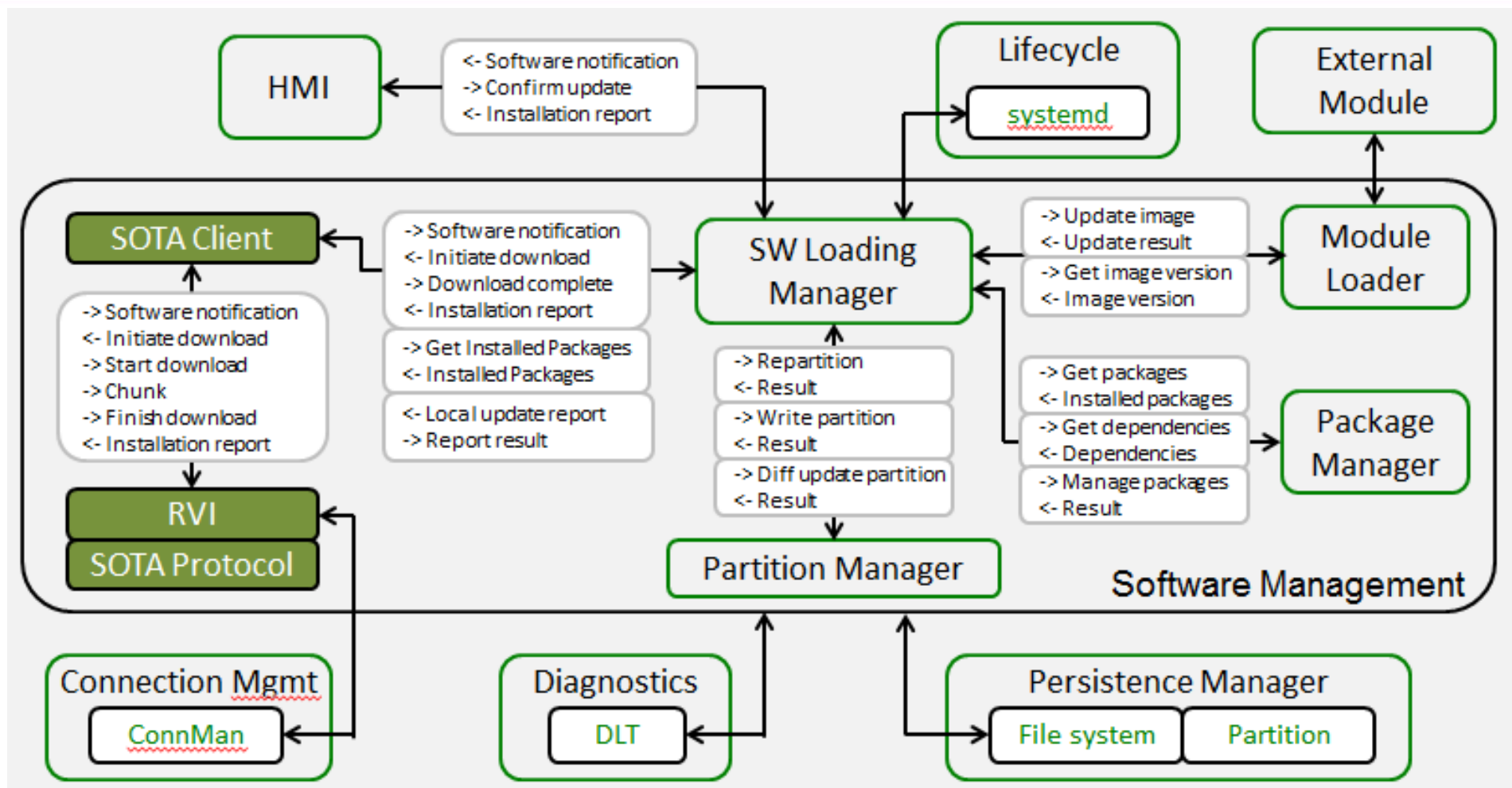
- Delivering updates to vehicles in the field, over the internet
- Urgent requirement for existing and future IVI systems
- Non-differentiating feature - has to work

## **Existing solutions**

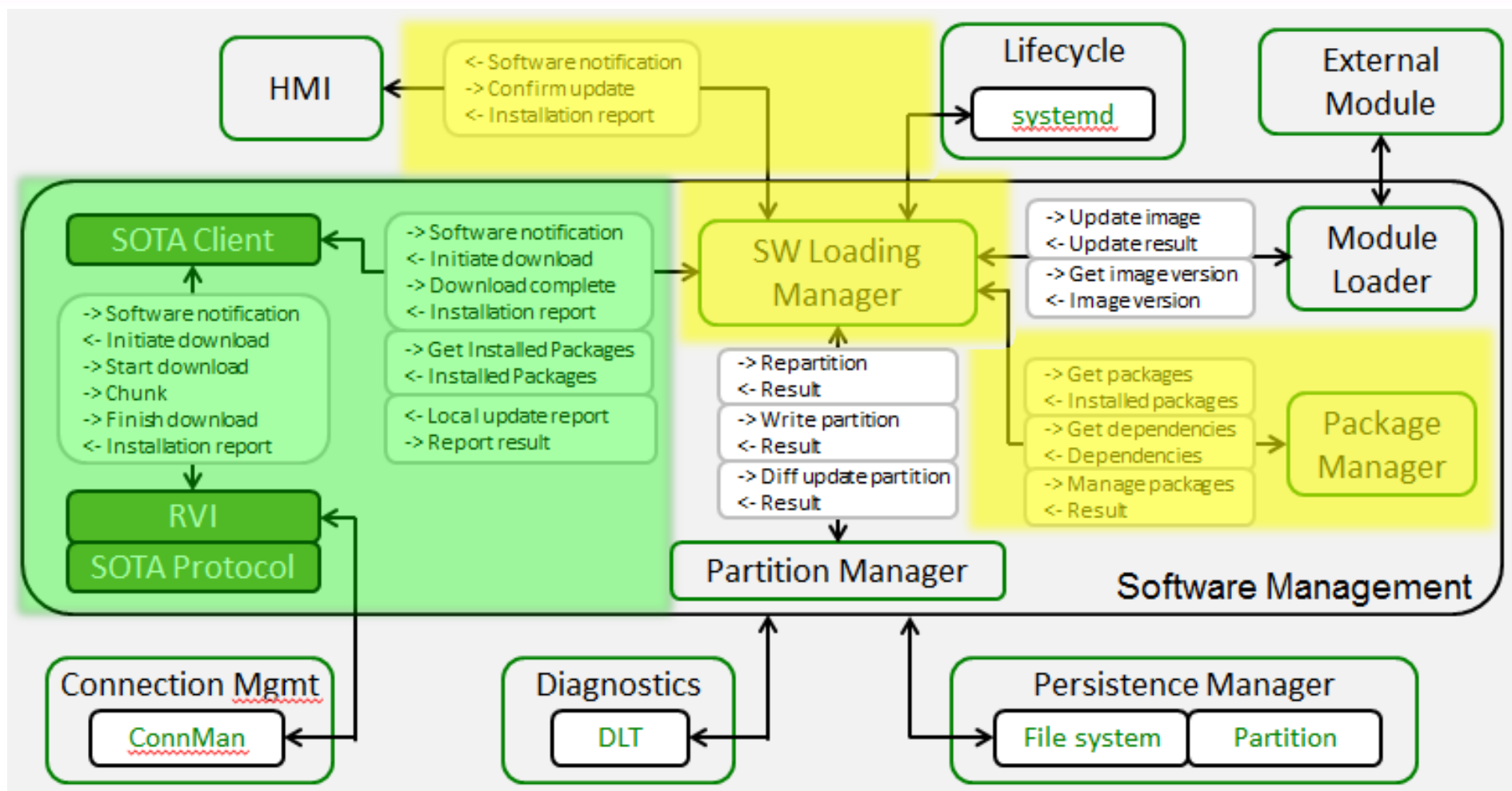
- Red Bend (Harman) - feature-rich, fully proprietary
- CarSync (Arynga) - Part of Arynga's proprietary server-side software suite, open source client
- OMA DM / FUMO - Open Standard - complex, some parts available as open source
- The Update Framework [1] - designed to overlay on existing solutions
- "Roll your own" - time consuming, insecure
- JLR commissioned end-to-end open source solution
- **OTA Plus – ATS commercially ready OTA solution based on GENIVI SOTA**

1. <http://theupdateframework.com>

# SOTA - PROJECT BACKGROUND

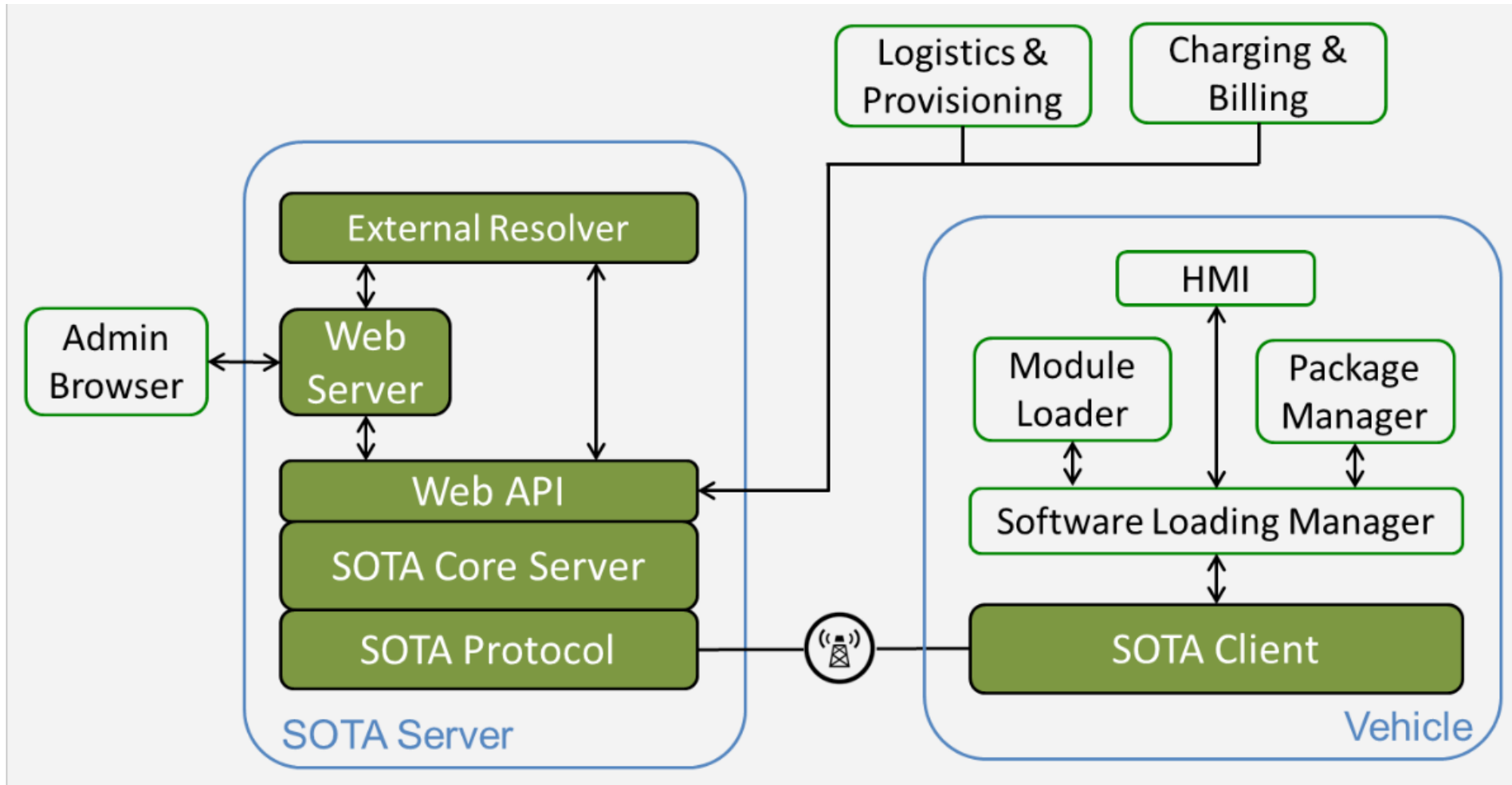


# SOTA - PROJECT BACKGROUND





# SOTA - PROJECT BACKGROUND



# SOTA - FEATURES

- Package upload
- Software / Firmware / Hardware inventory management by VIN
- Package installation campaign management
  - Filtering
  - Scheduling
  - Tracking
- Package download and installation
  - Reliable delivery by RVI
  - Interface with Software Loading Manager / local package manager
  - Success / Failure reporting to the server



# LIVE DEMO!



# SOTA CORE - ROADMAP

- Multi-tenant, multi-user support
- Standardisation of SOTA Web API with W3C
- HTTPS Transport support
- OAuth2 / SSO integration
- Configuration Management
- File Upload
- Migration to [github.com/genivi](https://github.com/genivi)
- Implementation of Security recommendations from UPTANE / AutoTUF

# SOTA CORE - SECURITY

What do these companies have in common?



# SOTA CORE - SECURITY

They all had a publicly disclosed software update hack!



## Repository compromise impact

- [SourceForge mirror distributed malware](#).
- Attackers [impersonate](#) Microsoft Windows Update to spread Flame **malware**.
- [RubyGems compromised](#) with RCE.
- Opera users **automatically installed malware** signed by **compromised** key.
- [Node Packaged Modules compromised](#).
- **Attacks** on software updaters have massive impact
  - E.g. South Korea faced **765 million dollars** in damages.

## Why Are Software Updaters Important?

- Run as root
- Update / change software!
  - Goal of most attacks
- Traditional defenses are ineffective
  - Firewalls / IDSes do not protect against these attacks
- Ubiquitous
- An attack often appears benign
  - Can look like a software repository misconfiguration



## Possible Attacks on Software Updates

- Malicious package
  - Crash / DoS / Arbitrary Code execution
- Version attacks
  - Downgrade to vulnerable version
- Metadata attacks
  - Change signatures, add bad dependencies
- Key Compromise
  - TLS root key, code signing key



## Path to failure...

- Have everyone build their own “secure” updater



– the problem is subtle



## 2010: The Update Framework (TUF)

- TUF is a **secure** software update **framework**.
- Built using some ideas from Thandy.
- Developed by security researchers from NYU
- **Best practices** to protect users from security attacks.
- **Plug-and-play** (like TLS).



[“Survivable Key Compromise in Software Update Systems” \(CCS 2010\).](#)

## 2010: The Update Framework (TUF)

- Standard mitigations and best-practices
- Resilient to Key Compromise
  - Multi-party signatures
  - Roles / Delegation
- Equivocation
  - Detect "back-doored" packages



## 2016: UPTANE / AutoTUF

- NYU / UMich collaboration, funded by DHS
- Including leading players
  - OEM, Tier 1, OTA Vendors
- GENIVI SOTA will align with UPTANE



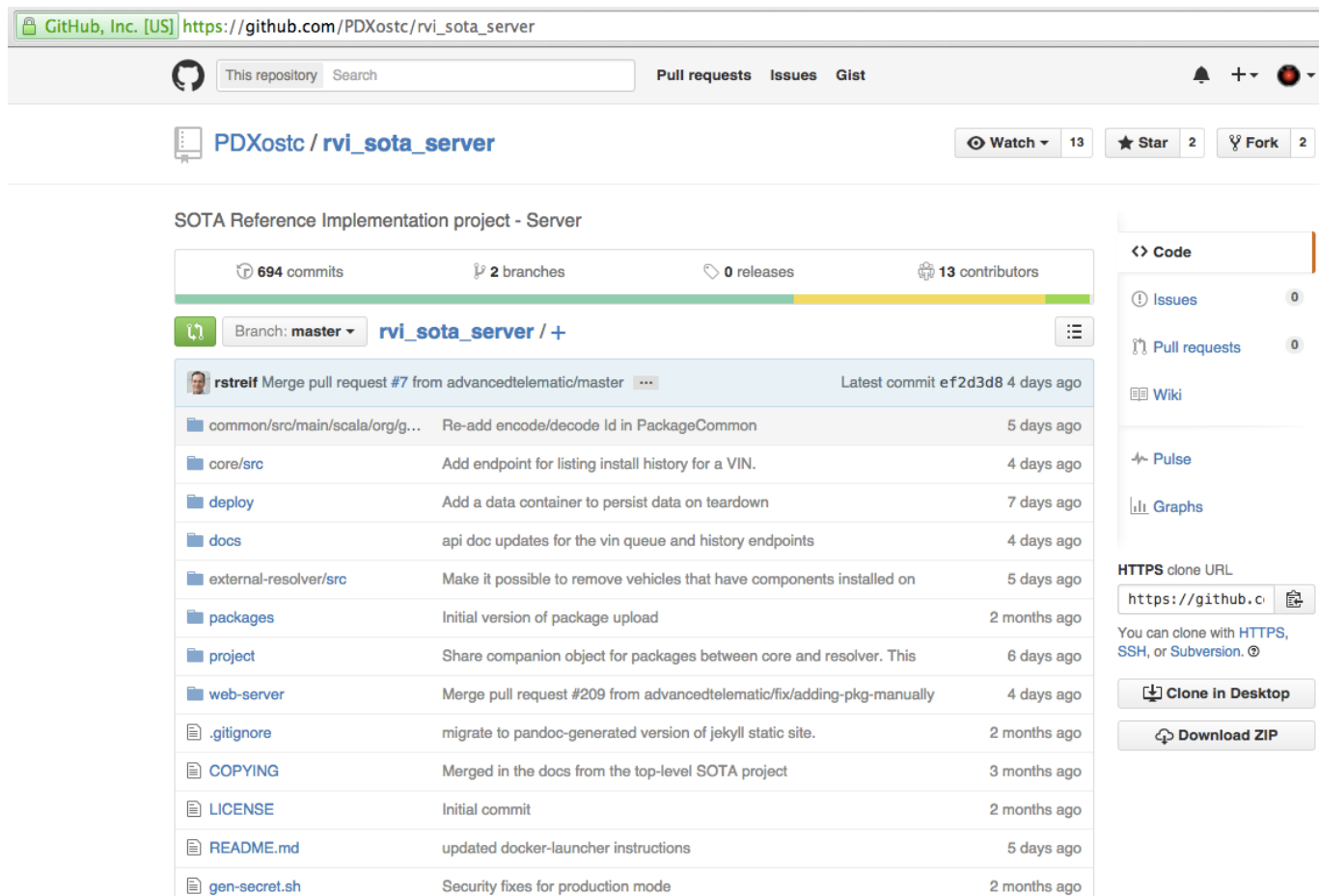
# SOTA CLIENT - ROADMAP

- Integration with GENIVI Development Platform
- Integration with AGL / Open IVI
- Support for generic Linux platforms (32-/64-bit RPM/Deb)
- Support for Binary Diffs
- Signature Validation
- Security hardening
- C/C++ implementation?

# SOTA – WHAT WE PROVIDE

- **Server-side**
  - Server implemented in Scala
  - Deployment scripts / instructions for AWS, Docker and developer machines
  - Complete Design, Architectural and API documentation
  - Complete test suite
- **Client-side**
  - Client implemented in Rust
  - Build / installation scripts for GDP
  - Complete test suite
  - Integration with GENIVI Software Loading Manager

# OPEN SOURCE!

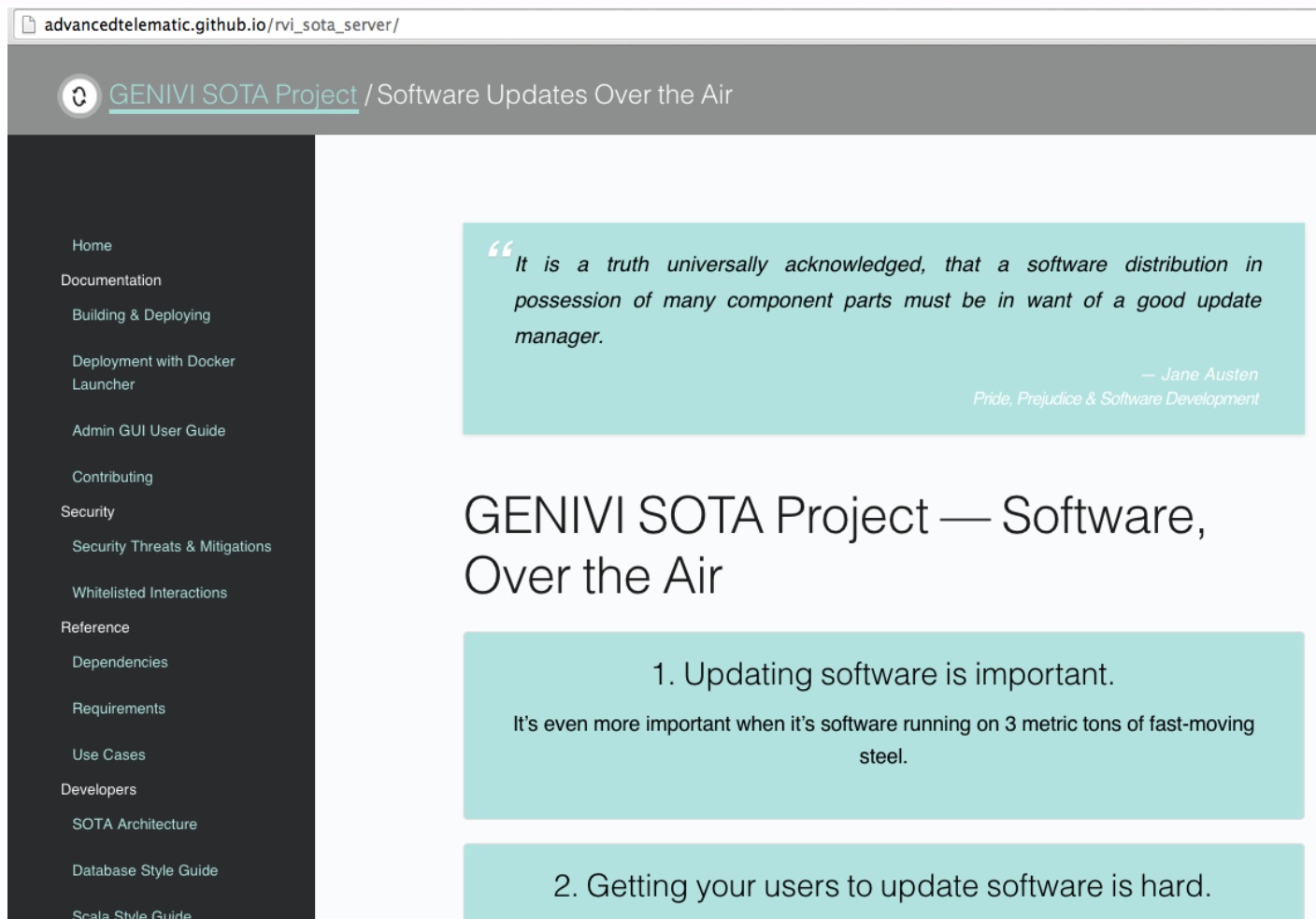


The screenshot shows the GitHub repository page for PDXostc / rvi\_sota\_server. The repository is titled "SOTA Reference Implementation project - Server" and has 694 commits, 2 branches, 0 releases, and 13 contributors. The current branch is master. A table of recent commits is visible, including a merge pull request by rstreif and several other commits by advancedtelematic. The repository is licensed under MPL v.2.

Commit	Description	Time
ef2d3d8	Latest commit	4 days ago
ef2d3d8	Merge pull request #7 from advancedtelematic/master	4 days ago
ef2d3d8	Re-add encode/decode Id in PackageCommon	5 days ago
ef2d3d8	Add endpoint for listing install history for a VIN.	4 days ago
ef2d3d8	Add a data container to persist data on teardown	7 days ago
ef2d3d8	api doc updates for the vin queue and history endpoints	4 days ago
ef2d3d8	Make it possible to remove vehicles that have components installed on	5 days ago
ef2d3d8	Initial version of package upload	2 months ago
ef2d3d8	Share companion object for packages between core and resolver. This	6 days ago
ef2d3d8	Merge pull request #209 from advancedtelematic/fix/adding-pkg-manually	4 days ago
ef2d3d8	migrate to pandoc-generated version of jekyll static site.	2 months ago
ef2d3d8	Merged in the docs from the top-level SOTA project	3 months ago
ef2d3d8	Initial commit	2 months ago
ef2d3d8	updated docker-launcher instructions	5 days ago
ef2d3d8	Security fixes for production mode	2 months ago

**All software  
available  
under MPL v.2!**

# OPEN SOURCE!



The screenshot shows a web browser window with the URL `advancedtelematic.github.io/rvi_sota_server/`. The page title is "GENIVI SOTA Project / Software Updates Over the Air". A dark sidebar on the left contains a navigation menu with the following items: Home, Documentation, Building & Deploying, Deployment with Docker Launcher, Admin GUI User Guide, Contributing, Security, Security Threats & Mitigations, Whitelisted Interactions, Reference, Dependencies, Requirements, Use Cases, Developers, SOTA Architecture, Database Style Guide, and Scala Style Guide. The main content area features a quote in a light blue box: "It is a truth universally acknowledged, that a software distribution in possession of many component parts must be in want of a good update manager." attributed to Jane Austen from *Pride, Prejudice & Software Development*. Below this is the main heading "GENIVI SOTA Project — Software, Over the Air". Two more light blue boxes contain numbered points: "1. Updating software is important. It's even more important when it's software running on 3 metric tons of fast-moving steel." and "2. Getting your users to update software is hard."



# GET INVOLVED!

## Github

[https://github.com/genivi/rvi\\_sota\\_server](https://github.com/genivi/rvi_sota_server)



[https://github.com/genivi/rvi\\_sota\\_client](https://github.com/genivi/rvi_sota_client)



## Mailing lists – GENIVI Projects

# TRY IT OUT!

- Launching this summer: SaaS version of OTA Plus
- Based on GENIVI SOTA
- Minimise develop/build/test/deploy cycle
- Allow engineers to focus on differentiating value
- Support for any GENIVI SOTA Client device

# SNEAK PREVIEW


Search by ID or name 


Zelda\_Test


112.314.134.04

● Device synchronized

Packages

Search package


Status All
Sort by A > Z

 Click on the package you want to install and select its version to add it to the queue. X

A	
Automatic Multifunction Sports Suspension Steering Feedback...	<span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">v 3.561 installed</span>
Anti-Lock Breaking System	● v 1.52 queued <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">Uninstalled</span>
Aureum_LED_Headlights	<span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">v 3.561 installed</span>
Alternate_Route_Calculation	● v 3.579 queued <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">v 3.561 installed</span>
Anti-Lock Breaking System (41.2213_Systems_Diagnostics.pdk...	<span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">Uninstalled</span>
Anti-Theft Sensoric Suite	● v 2.594 queued <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">Uninstalled</span>
Anti-Skidding Brake Microvariation	<span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">2.301 installed</span>
Aureum_LED_Smart_Headlights	<span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">1.07 installed</span>
Alternate_Route_Calculation	not compatible with device <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">Uninstalled</span>

10 compatible, 4 installed, 0 broken, 4 queued

Queue Hide History

 The installation of the queued packages will start automatically when you connect to your device. X

Bluetooth Package	v 3.561	<span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">retry</span>	<span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">log</span>	<span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 5px;">cancel</span>	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">↑</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">↓</span>
-------------------	---------	---	---	--	--

Bluetooth Driver v 3.561 Log  
Terminated due to Error:

```
#!/bin/bash
# Needed variable: ERRORDB
# Optional variables: ERROROUTPUT, SQLITE3_EXECUTABLE,
ERROR_CLEANUP_ACTION, ERROR_ENVIRONMENT_VARIABLES

if [ -z $ERROROUTPUT ];then
  ERROROUTPUT=/var/tmp/$$.err
fi
if [ -e $SQLITE3_EXECUTABLE ];then
  SQLITE3_EXECUTABLE="which sqlite3"
fi
# The settings file for SQLite3:
ERROR_INIT_SQLITE=/var/tmp/$$.init.sql
# For convenience, a function to create the settings for SQLite3:
function Error_Create_Init_File
{
  cat > $ERROR_INIT_SQLITE <<'ERROR_SQLITE_SETTINGS'
  .bail ON
  .echo OFF
  PRAGMA foreign_keys = TRUE;
  ERROR_SQLITE_SETTINGS
}
# Create the database:
if [ -z $ERRORDB ] ;then
  echo "Runtime Error."
  exit 1
fi
```


Runtime Error: Line 56 - gsdsgdsg

4 packages in queue, ●1 error



Oct 21st -15


GENIVI is a registered trademark of the GENIVI Alliance in the USA and other countries  
This work is licensed under a Creative Commons Attribution-Share Alike 4.0 (CC BY-SA 4.0)

25



Search by ID or name

←


## Zelda\_Test

112.314.134.04

● Device synchronized

**Packages**

Status All
Sort by A > Z

Click on the package you want to install and select its version to add it to the queue.
✕

A	
Automatic Multifunction Sports Suspension Steering Feedback...	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">v 3.561 installed</span>
Anti-Lock Breaking System	<span style="color: red; font-weight: bold;">● v 1.52 queued</span> <span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-left: 10px;">Uninstalled</span>
Aureum_LED_Headlights	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">v 3.561 installed</span>
<small>           Version name: 3.561            Release type: Stable (low risk of bugs)            Download: com.marz.snapprefs_v23_63dd74.apk (4.01 MB)            Number of downloads: 40,910 in total · 15 in the last 24 hours            MD5 checksum: 63dd74d230fe9f68b030b1ac2cf0d3f            Uploaded on: Sunday, December 6, 2015 - 00:58            Changes:           <ul style="list-style-type: none"> <li>- Updated for 9.20.4.0</li> <li>- Added Visual Filters - You can use Instagram like filters (17)</li> <li>- Added Visual Filter manager</li> <li>- Looping videos - You can watch videos forever</li> <li>- Added Blur tool</li> <li>- Fixed Vibration settings</li> <li>- Removed Auto-save for Stories temporarily</li> </ul> </small>	<small>v 3.45 v 3.261 v 2.231 v 2.229 v 1.561 v 1.48</small>
Alternate_Route_Calculation	<span style="color: red; font-weight: bold;">● v 3.579 queued</span> <span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-left: 10px;">v 3.561 installed</span>
Anti-Lock Breaking System (41.2213_Systems_Diagnostics.pdk...	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Uninstalled</span>

10 compatible, 4 installed, 0 broken, 4 queued

**Queue** Hide History

The installation of the queued packages will start automatically when you connect to your device.
✕

Bluetooth Package	v 3.560 installed successfully	<a href="#">log</a>
Alternate Rout Calculation	v 3.560 installed successfully	<a href="#">log</a>
Anti-Skidding Brake Microvariation	v 2.301 installed successfully	<a href="#">log</a>
Aureum_LED_Smart_Headlights	v 1.07 installed successfully	<a href="#">log</a>

Bluetooth Package	v 3.561	<a href="#">retry</a>	<a href="#">log</a>	<a href="#">cancel</a>	↑ ↓
Anti-Lock Breaking System	v 1.52	<a href="#">cancel</a>	↑ ↓		
Alternate Rout Calculation	v 3.579	<a href="#">cancel</a>	↑ ↓		
Anti-Theft Sensoric Suite	v 2.594	<a href="#">cancel</a>	↑ ↓		

4 packages in queue, ●1 error

