RATH™ by AVIRE

SmartView 2
Security Overview

SmartView 2 Comprehensive Security Overview

Ver. 10.0 November 2024

Thank you for purchasing the SmartView 2 Elevator Communication System.

Combining the brands of RATH™ Communications and JANUS Elevator Products, AVIRE Global is the largest Emergency Communication Manufacturer in North America and has been in business for over 35 years.

We take great pride in our products, service, and support. Our Emergency Products are of the highest quality and our experienced customer support teams are available to remotely assist with site preparation, installation, and maintenance. It is our sincere hope that your experience with us will continue to surpass your expectations.

Table of Contents

Product Overview . . . . . Page 3
About the Company . . . . . Page 3
Hardware and Software . . . . . Page 4
Hosted Application . . . . . Page 6
Access Control . . . . . Page 7
Network . . . . . Page 9
System Security . . . . . Page 10
Third Parties . . . . . Page 13
Customer Data . . . . . Page 14
Video Recordings . . . . . Page 17
Cryptography . . . . . Page 17
Application Physical Security . . . Page 18
Security Assurances . . . . . Page 19
Web Application Security Risk. . Page 19
Risk Analysis . . . . . Page 20
Work Station Requirements . . . . Page 20
Remote Access . . . . . Page 21
Contingency and Recovery . . . . Page 22
Operational Security . . . . . Page 23
Support . . . . . Page 24
Maintenance . . . . . Page 25
Quality Testing . . . . . Page 26
Security Overview . . . . . Page 26
Network Requirements . . . . . Page 29

Please note all information provided in the this document is only applicable to the SmartView 2 system. Any previous iterations or competitor products will not apply to this document.

Product Overview

The RATH SmartView 2 System is a two-way communication and visual elevator emergency system. When the “help” button is pressed in the elevator car, an auto-dial emergency phone will call out to an on-site or elevator monitoring service. When the call is answered by the monitoring service, a voice prompt will let them know there is a video feed available to view inside of the elevator car as well as the location of the call. If there is no response through the phone, monitoring can go to a secure link that leads to the viewing site for the SmartView system. From the viewing site, video will then be initiated by monitoring. If the elevator car is inhabited, a visual message can be sent to the display in the elevator car from the monitoring site. Dedicated response buttons in the elevator car are used to respond to visual messages.

About RATH™ by AVIRE

1. **When were we founded?**
   RATH Communications was founded in 1981 and JANUS Elevator Products was founded in 1988. They merged in 2022 and are now a combined brand under the AVIRE Global umbrella, a Halma Company.

2. **Approximately how many people does your organization employ?**
   RATH by AVIRE employs 84 out of their Sussex, Wisconsin USA office.

3. **How do you determine which employees have access to data?**
   Data access is limited to our tech support team as a troubleshooting tool, and our product development engineers.

4. **Are employees provided security awareness training and if so, how long are the logs of training maintained?**
   All employees are required to go through monthly security trainings through a third-party company called KnowBe4. Logs are maintained with KnowBe4 indefinitely.

5. **Are any information security functions outsourced to a third party?**
   We use Azure cloud compute provider as third party within good security practices. We use their infrastructure and their services for hosting the application. We also use Balena for fleet management for the operating system on the hardware. Communication with Balena is secure through their VPN. Access to Balena must always be given. There is no unauthorized access to a device.

6. **Does your organization adhere to information system security engineering principles in the specification, design, development, implementation, and modification of the product?**
   No, design is specifically catered towards application’s scope of work.

Hardware and Software Details

1. **What platform does the system use?**
   BalenaOS 2.115.18+rev2, Debian GNU/Linux 12 (bookworm)

2. **What is the host model of the software?**
   SmartView 2 is hosted within Azure Cloud. It is cloud-native architecture focused on scalability and reliability. It uses containerized applications to manage workloads, managed relational databases for reliable data storage, and storage solutions to accommodate growing data needs. This design ensures a robust, secure, and highly scalable application environment. We use Azure services in various hosting models but mostly uses are IaaS and PaaS.

3. **Does the system have the ability to archive, retrieve, and purge information?**
   The hardware stores settings and information relating to the local elevator. This is accessed via a secure login page. The information can be reset in software. The whole device can be reset via a hardware switch to purge all user information. The viewing site (smartviewhub.com) stores user data. Upon request, the RATH by AVIRE admin can delete the data.

4. **How does error logging and reporting work within the system?**
   On the hardware errors are self-identified and shown to the user via a status LED. Errors within the hardware are logged for debugging purposes. On the smartviewhub.com each request and response is logged along with the IP address and user agent by the application. Each important action (not database action) is logged by the application. Each error is logged by the application. Each change of any record (insert, delete, update) in the database is registered in the schema audit in database. On the development environment we also log request and response body, on the production body is not logged. We use Azure Monitor service for storing database server logs, application logs and any other infrastructure related logs. Log retention period varies from the few days to few years based on the service.

5. **Are there any third-party products as a part of the system?**
   BalenaOS is the operating system. A third-party WIFI dongle is also used for local programming only.

6. **What web browsers and mobile device operating systems will work with the system?**
   Microsoft Edge, Google Chrome, Mozilla Firefox, Apple Safari

7. **How do application administrators manage the application?**
   On the hardware the application administrator can access the set up website via a local network or WIFI hot spot from the device. This is accessed via secure login page. On the viewing site, smartviewhub.com, the user can access the camera feeds which are linked to their account via a secure login. Administrators can manage the application from the administration panel based on specific permissions in the database.

8. **Does an ActiveX control or other type of plugins or add-ons need to be installed to use this system? Java?**
   No

9. **Does software need to be installed on a computer / workstation?**
   Only a web browser needs to be installed. Updates and other Windows-pushed improvements can be performed.

10. **Are there any interfaces needed to or from this application/system? Example: live streams of data from other applications, data exports to other applications, data feeds.**
    No

11. **Who is responsible for Operating System patching?**
    RATH by AVIRE.

12. **Does the system have monitoring capabilities like a system log and are the logs stored securely?**
    Yes, logging is done and stored in Balena. All data including logs is encrypted through Balena. The viewing site smartviewhub.com) also has logging capabilities. All logs are encrypted in the Azure environment. Logs are available from RATH by AVIRE by request.

13. **Is the video session always recording?**
    No, the video session is never recorded.

14. **Can SmartView 2 be used in place of a security camera in the elevator car?**
    No, using the system for this purpose violates elevator code. RATH by AVIRE reserves the right to restrict access to devices being used outside the recommended application.

15. **What is the scope of customer records that the system will transmit, process, or store?**
    Information provided during registration and IP information for the hardware are the only customer records the system will store.

16. **Does the application have the capability to display a Standard Mandatory Consent Banner before granting access to the application?**
    No, the application doesn't have that capability. Standard Mandatory Consent Banner is usually used when authenticating with OAuth (for example Google).

17. **Does unit allow for any wireless access? If so, what is necessary for wireless access?**
    The device allows the user to plug in a WIFI USB dongle which allows temporary access to the set up login page during installation. The unit cannot run from an external WIFI it must be plugged into an Internet network during normal operation. WIFI dongle is only active for 20 minutes.

18. **Does unit support the use of anti-malware software?**
    There is no malware installed on SmartView 2. All firmware / software is static, and users cannot install any applications themselves. All firmware is controlled by RATH by AVIRE. All functionalities that go through the Internet connection is handled through Balena and Balena Cloudlink VPN. It was determined by our penetration testing partners there was no path for malware to be injected onto the devices.

19. **Can the hosted service provider provide an architecture document that includes elements such as network diagrams, data flows, and other security technologies that are in use?**
    An architecture diagram showing the public facing infrastructure can be made available. The vendor's internal network and system architecture is proprietary information and will not be released.

20. **Does this system or application store patient information or provide automation for medical devices?**
    The proposed application is an emergency communication system for elevators. It does not store patient information or provide automation for medical devices.

21. **What size is the text on the display in the elevator?**
    Text size compliance is determined by the height of the letter "I" per ASME 17.1 section 2.27.1.1.3 (l). On the SmartView 2 system, the letter "I" is 5.5mm tall.

Hosted Application

The hosted application refers to the SmartView viewing site (smartviewhub.com). The questions and corresponding answers in this section only applies to smartivewhub.com.

1. **What is the host model of the application?**
   SmartView 2 is hosted within Azure Cloud.

2. **How is communication between the instillation site and the hosted service provider secured?**
   Traffic between the on-site hardware, smartviewhub.com and accessing devices is encrypted in transit using TLS using an AES128-SHA256 cipher suite, which meets the requirements of FIPS-140-2. The onsite hardware and smartviewhub.com is configured to reject any attempt to negotiate lower grade cipher or unencrypted connections.

3. **Do you share networks, VPNs, firewalls and load balancers between your dedicated and any public cloud environments?**
   The public facing infrastructure for the SmartView system operates off the Azure cloud service. SmartView 2 infrastructure is not shared with any other application, however it utilizes shared services in hub and spoke topology in Avire's Azure tenant. Components such as Azure Firewall and Azure VPN Gateway. SmartView 2 virtual networks (virtual network per environment) are logically separated and isolated from each other.

4. **How are the hosted service provider's hosts that will serve the application hardened from malicious attacks and information leaks? Are servers hardened to a national standard (e.g. CIS Center Internet Security)?**
   The hosted environment complies with NIST SP 800-53 Rev 5

5. **Can the hosted service provider provide a listing of current patches if requested for hosts, including host OS patches, web servers, databases, and any other material application?**
   Yes

6. **How does the hosted service provider keep the environment current with security patches and updates? Is this a formal process?**
   The host environment is configured for automatic patching. LTS versions of software generally preferred within the host environment to ensure software remains secure for an extended lifetime, however, when software must be upgraded between major versions, there is a formal release procedure in place to ensure compatibility of major updates.

7. **What tools are used for staff to perform remote administration?**
   Remote administration of the hosted environment utilizes the Azure VPN Gateway, all incoming traffic is routed through Azure Firewall. For hardware devices remote administration is available through Balena cloud via web based shell.

8. **How does the hosted service provider monitor the integrity and availability of the server hosting environment?**
   Please refer to https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-integrity

9. **What is the password policy for the hosted service provider server infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed?**
   This information is confidential but password requirements exceed those in NIST SP 800-63B and two-factor authentication is required for access.

10. **What controls do you have in place to protect from the unauthorized introduction of software into your systems?**
    Access controls are applied to server infrastructure administration accounts and physical access to servers is controlled by Azure as previously described. The installed packages within cloud instances are checked against the required packages list to verify the two match. Remote access to the on-site hardware is only possible through Balena cloud, the access control for which has been previously described.

11. **Do developers receive training on security development and any potential threats and hazards?**
    Yes

12. **Does the data center which houses the hosted application environment meet TIA-942 Tier 3 standards or better?**
    Please refer to https://learn.microsoft.com/en-us/compliance/assurance/assurance-data center-architecture-infrastructure

Access Control

1. **What method(s) of access control does the SmartView 2 provide (Role Based, Mandatory, or Discretionary)?**
   Access control is mandatory, it allows only one user to access the system and they must use a unique email and password which they set after the first login.

2. **Can access control be controlled by Active Directory / LDAP / ADFS / SAML?**
   No

3. **Does the solution provide the capability and functionality to authenticate users with multi-factor authentication?**
   Yes, two-factor authentication through e-mail is available on smartviewhub.com.

4. **How are credentials created for the application?**
   Credentials are created initially by RATH by AVIRE through an online registration process on the viewing website (smartviewhub.com). Once initial credentials are created, the company appointed administrator has the ability to add/delete additional administrators and users. This does not currently integrate with Active Directory but it is part of the future development road map.

5. **How granular can the access control mechanism be to restrict functionality (including but not limited to role, user, screen, module, table, column, update, view only, field)?**
   There is only 1 single user on the hardware. On the viewing site, smartviewhub.com, the user can only access the camera feeds which are linked to their monitoring company. The access control mechanism only includes roles that are enforced from business logic (RATH by AVIRE administrator, company, company collaborator), it does not provide any form of granularity.

6. **Does the system automatically terminate privileged and non-privileged sessions after idle time?**
   Yes, the application uses the access and refresh token for the authentication process. An access token is created using the refresh token that gives access to the application. The expiration time of the access token is 5 minutes, and the expiry time of the refresh token is 24 hours. Additionally, a login blocking mechanism is implemented for 15 minutes after failed login attempts.

7. **Does the proposed application allow for the configuration of technical controls to enforce an organization's timeout policy?**
   By default, application will log a user out after 15 minutes of inactivity. This time can be modified in a user's account settings by the administrator of the account.

8. **Can the system be run in a user context without the need for privileged access on the local system?**
   No

9. **What capability and functionality does the unit provide and restrict access to mobile devices?**
   It does not restrict access to mobile devices. Local setup page and viewing site would still need login on mobile devices.

10. **Can the SmartView 2 enforce customer standards for identification and authentication? (Password complexity, length, reuse limits, etc.)**
    The the SmartView 2 has its own password complexity and length limits. The application has implemented validation of all sent data on the front-end side as well as on the back-end side. The user's password must be at least 8 characters long. 1 uppercase, 1 lowercase, 1 number, 1 special character. If customer standard requires AD, SAML, etc. that will not be compatible.

11. **Does RATH by AVIRE utilize any subcontractors with access to client data?**
    Yes, the external company performing the website development (Euvic) also has limited access to certain parts of the database.

12. **Will the system run in a virtual environment?**
    No

13. **Does the application provide a capability to limit the number of login sessions per user?**
    Yes, a user can only be logged in to one session at a time. If a user attempts to begin another session, they will be prompted to log out of their original before proceeding.

14. **Will system enforce a limit of consecutive invalid logon attempts by a user and will account be locked for a certain period of time after too many invalid attempts?**
    Yes, the hardware prevents the user from unlimited login attempts. It implements a timeout after 5 consecutive failed logins. A login blocking mechanism is implemented for 5 minutes after failed 5 login attempts. The login limit is one user at a time.

15. **Does unit allow for SSL/TLS implementation?**
    Yes

Network

1. **Does SmartView 2 work through proxy servers?**
   No

2. **What are the network requirements necessary to run the SmartView 2 system?**
   See installation manual for full list of requirements.

3. **What ports, protocols, and services are required for the system to function properly? What purpose does each port serve? Are ports inbound, outbound, or bi-directional?**
   See page 29 for full list.

4. **Does SmartView 2 run over a Virtual Private Network (VPN)?**
   Yes, Balena Cloudlink VPN (which runs on OpenVPN) is implemented for a secure network connection to the outside world.

5. **Has the proposed solution been tested and implemented using Citrix or Microsoft RDS? Citrix Secure Gateway or Microsoft RDS Gateway? A thin client environment?**
   No

6. **Will the solution work with a storage area network (SAN) CIFS/NFS? Has the solution been tested in this environment?**
   No

7. **What URLs are associated with system?**
   Smartviewhub.com and balena.com, smartviewhub.com is the user viewing site, balena.com is for tech support and device management. Users do not have access to Balena.

8. **Will unit work behind a firewall on site?**
   Yes, but the user must ensure that the ports and white listed networks from the manual and page 29 are allowed by the firewall protocols.

9. **Will viewing site have HTTPS implemented? Will it have HTTP Strict Transport Security (HSTS)?**
   Yes

System Security

1. **What process exist to remediate flaws in the system once they are discovered?**
   The device and website (smartviewhub.com) both allow for updates to be rolled out once the device is in the field.

2. **What mechanism is employed to detect and eradicate malicious code?**
   We use services like Web Application Firewall (WAF) to protect web application by monitoring and filtering traffic. It helps to detect SQLi, XSS, DOS, and more. The ORM, we use approaches like filtering body requests within JS to prevent Cross Site Scripting. We use good practices within HTTP headers and mechanisms like SOP/CORS and CSP that help to detect and mitigate certain types of attacks.

3. **Does the system perform input validation prior to accepting input to prevent injection type attacks?**
   The system has a mechanism that validates all forms both on the front end and back end.

4. **Can the system adequately detect and stop or limit data mining attempts?**
   We use Web Application Firewall to detect and stop data mining.

5. **How does the system prevent Denial of Service?**
   It is a part of a rule set defined in a Web Application Firewall. WAF counts the number of requests send to the application from IP addresses. If the number of requests is above the limit, it blocks the IP address of device for a set amount of time.

6. **In a multi-tenant environment, how does the system prevent unauthorized and unintended information transfer via shared resources?**
   We segregate the application, databases, and gateways into their own security groups with strict firewall policies that allow certain, approved ports to be in use for the required traffic flow.

7. **How does the system separate user functionality from information system management functionality physically or logically?**
   The application is divided into modules based on the concepts of the business domain. Each module has access to a specific group of stored data. Users are divided into appropriate roles and each role has access to specific resources and services. Authorization is checked at the login level by checking the user's role and at the database level by checking whether a given user has access to the requested resources.

8. **Are access agreement policies and procedures in place to ensure access to customer data is limited to only when consent is explicitly given?**
   Both websites (smartviewhub.com and smartviewconfig.com) have a user agreement. By using the site, you are consenting to the site using customer data. Please see smartviewhub.com for the full user agreement policy. RATH by AVIRE will only use your personal information in accordance the privacy policy

9. **What occurs to storage data at the end of life?**
   If a retired asset is evaluated and deemed to be non-accessible, it's cleared by an approved data eradication solution. Microsoft data centers use the NIST SP-800-88 clear guidelines. Depending on the on-site configuration and device availability, some devices are purged before destruction. Purge devices include NSA-approved degaussers for magnetic media and multi-pin punch devices for solid-state media. Microsoft data centers use the NIST SP-800-88 purge guidelines. If a retired asset is evaluated and deemed to be accessible, it's destroyed onsite using an approved standard operating procedure that meets NIST SP-800-88 guidelines. These DBDs are physically and logically tracked to maintain chain of custody through final disposition. Each Microsoft data center uses an on-site process to sanitize and dispose of failed and retired DBDs. During this process, Microsoft personnel ensure chain of custody is maintained throughout the disposal process. Please refer to https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction

10. **Is there any reuse of media involved with the application? If so, how is the media sanitized between uses to prevent inadvertent access to patient records? How will media be sanitized before being returned to the vendor for service?**
    In the event of a return of a unit, the vendor may re-use the hardware for other purposes including cannibalization for parts or re-use as reference hardware. In the event the vendor chooses to re-use such hardware, the hardware is fully formatted and set to factory defaults.

11. **Who will be responsible for the media disposal and re-use? Will it be the proposed application vendor or the organization?**
    Media disposal is the responsibility of Azure as they are hosting the application.

12. **What encryption algorithms are utilized to protect patient information from being intercepted or modified while in transit? Are they FIPS-140-2 compliant?**
    Traffic between the on-site hardware, smartviewhub.com and accessing devices is encrypted in transit using TLS using an AES128-SHA256 cipher suite, which meets the requirements of FIPS-140-2. The on-site hardware and smartviewhub.com is configured to reject any attempt to negotiate lower grade cipher or unencrypted connections.

13. **How will data be securely transmitted between the user and the application (both internal and external)?**
    HTTPS is implemented when the user is accessing the data. Data will be encrypted using HTTPS over TLS through Load Balancer. For internal we use SSL offloading.

14. **Is data encrypted in transit?**
    Yes, data is encrypted in transit using HTTPS over TLS – it is designed to provide encryption in transit. Since communication between a browser and website server via Load Balancer (with a secure certificate) is in an encrypted format, the data packets in transit cannot be tampered with or read even if they are intercepted.

15. **What protocol is used to transmit data?**
    Smartviewhub.com and device set up page use HTTPS. The site also uses TLS 1.2

16. **Are application vulnerability assessments performed by a qualified third party and are the results of those tests available for review?**
    The vendor contracts a third-party pen test company (Pen Test Partners) to perform vulnerability testing on the hardware as well as the website / cloud server. Yes, an overview / summary of testing is available for customer review.

17. **Does the application have the capability to time correlated audit events for the following actions:**
    - Account Creation
    - Account Modification
    - Account Disabling Actions
    - Account Enabling Actions
    - Account Deletion Actions
    - Group Membership Changes
    - Successful Logins
    - Failed Logins
    - Start and End Times of System Access

- Privileged Account Usage
- Privileged Account Changes
- Configuration Changes
- Application Events

The application supports the logging of all the above activities. The audit schema is implemented in the database, which has 2 tables. One automatically listens for changes in the records of the main schema and the other saves application logs.

18. **Are time stamps available for audit logs?**
Yes, logging on smartviewhub.com and on device through WAF, database, storage services, and the application. Audit logs are only available to users by request from RATH by AVIRE.

19. **Will error patching, updating, and upgrading hardware for out-of-date components be available for the life of the product?**
Error patching and updating will be available until the hardware is EOL or the hardware warranty period expires. Once the hardware is EOL or the warranty has expired and an alternative is available through RATH by AVIRE, patching and updating will no longer be available. Out of date hardware will be replaced with the applicable replacement at the customer's expense.

20. **Do you have staff dedicated\responsible for ensuring Data Security for your customers?**
The responsible owner for system data security is the Product Manager. The company data protection officer is the Head of AVIRE IT.

21. **Who is primarily responsible for cyber security within the hardware/software solution?**
The position responsible for the security of the vendor's solution is the Product Manager, who reports into the Director Product & Innovation who sits on the vendor's global board. The system owner is responsible for the security of the proposed solution, implementing controls identified during the assessment process, continuous monitoring of risk and reporting any exploitable deficiencies in the system.

22. **What security partners\vendors do you work with?**
Pen Test Partners LLP (UK Company No OC353362) provide penetration testing and threat mitigation consultancy services to the vendor. Pen Test Partners hold ISO27001 accreditation, are CREST approved and are an NSCS assured organization. Euvic Sp. Z o.o. (PL NIP 9691411637) provide software development and assurance services to the vendor. Euvic hold ISO 27001 accreditation.

23. **What actions do you take upon locating a security issue?**
Upon identification of a potential security issue, an analyst will review the described vulnerability and classify the threat level. A search of public information relevant to the vulnerability (e.g. NVD) will be conducted by the analyst and the analyst will assign a reference to the vulnerability. Based on the exploitability and impact of the vulnerability, the analyst will recommend a course of action. This will typically involve notifying impacted organizations and recommending any mitigation measures that may be applied in advance of a fix being published. Once the analyst has classified the exploitability and impact of the vulnerability the product development team will begin developing a fix to the vulnerability and this will be published as soon as it is available.

24. **Can users perform non-intrusive network audits of the provided service randomly, without prior notice?**
    Network audits of on-site hardware may be performed at any time without prior permission, however, audit of smartviewhub.com may trigger automatic threat protection measures that may result in a denial of service for otherwise legitimate users within the same IP address range and/or geolocation.

25. **What notice is required to do non-intrusive, intrusive scans, or other vulnerability assessments?**
    Such audits would need to be agreed on a case-by-case basis and may be chargeable.

26. **Please describe the process for performing quality assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.**
    The on-site hardware and smartviewhub.com are tested using a variety of techniques, including static and dynamic code analysis, manual code reviews, penetration testing through our security partner Pen Test Partners and web-scanning of smartviewhub.com. In addition all functions are manually tested before release into production.

27. **Describe the change control process for infrastructure, network, software.**
    A SecCM approach is applied following the guidance within NIST SP 800-128

28. **What protections are in place for the OWASP Top 10?**
    Developers are familiar with secure design techniques including mitigation of commonly exploited vulnerabilities. Penetration testing tests the application against a wide range of CWEs including those mapped to the OWASP Top 10.

29. **Has the hosted service provider done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities?**
    Yes

30. **Do developers receive training on security development and any potential threats and hazards?**
    Yes

Third-Parties

1. **Does the application use any third-parties?**
   Yes

2. **How do you monitor outsourced (third-party) operations?**
   The vendor uses providers accredited to ISO 27001 and conducts supplier audits to ensure compliance with our agreed contractual procedures. There is a segregation of development, staging and production environments to provide a separation of access control privileges between internal and customer-facing systems.

3. **What provisions are in place with third parties to provide for the security and protection of information and assets?**
   As mentioned above, there is a segregation of data between development, staging and production environments to prevent supplier access to customer information.

4. **Do you perform annual review of third parties? What does your annual review include? Will you provide copies?**
   The vendor conducts supplier performance reviews annually, which include but are not limited to security performance and monitoring of supplier accreditations. This information is confidential between RATH by AVIRE and its suppliers. However, for the hosted web environment (Azure) we refer you to the Azure compliance documentation: https://learn.microsoft.com/en-us/azure/compliance/

Customer Data

1. **What type of data is managed through his system?**
   Login credentials, system configuration (telephone numbers), audio data, and video data. Basic company information is always managed (name, address, phone number, contact e-mail address, installation site address, and elevator name).

2. **What is the scope of customer records that the system will transmit, process, or store?**
   Image stream and audio data are transmitted, all user configuration data is stored locally. Data stored locally on device is encrypted with a Fernet key.
   On Viewing Site:
   For Company Owner: Username, email address, company name, first name, last name, full address of business, phone number.
   For Company Collaborator: Username, email address, first name, last name

3. **How does RATH by AVIRE obtain data from the customer? Include file type(s) and the medium(s) utilized to transmit the data (e.g., SFTP, Encrypted email).**
   The user will login to the device by accessing the local-only website (smartviewconfig.com) during installation. The customer data is input via a secure HTTPS website. Encrypted email, camera unit - https/ws, https via application, database, encrypted storage. We can also obtain customer data via email and registration pages.

4. **Will the system have access to infrastructure that stores or transmits customer data?**
   Ethernet / WAN connections and PSTN / POTS connections.

5. **Is all client data encrypted at rest within the system? If so, what level of encryption?**
   Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, read replicas, and snapshots, encrypted DB instance, all logs. Also, there is implemented server-side encryption within the application server by AES-256 encryption algorithm. Database service uses a Key Management Service key to encrypt these resources. Storage service where client data is stored is also encrypted.

6. **Will the system have access to a database or application that stores or transmits customer data?**
   Application has access to database where customer data is stored. Application does not transmit.

7. **Will the system utilize workstation device(s) to access and/or transmit customer data?**
   Yes (Access only, no transit)

8. **Will the system utilize mobile device(s) to access and/or transmit customer data?**
   Yes

9. **Will the system utilize any other method to access and/or transmit customer data?**
   No

10. **Will data be stored in your organization's data center or a third-party data center for the system?**
    Data will be stored within Azure data centers which continuously innovate the design and systems of data centers to protect them from human-caused and natural risks. They implement controls, build automated systems, and undergo third-party audits to confirm security and compliance.

11. **Will data be stored in a client data center?**
    There is no data that will be stored in a client data center.

12. **Is there anywhere else data will be stored?**
    Yes, on the device.

13. **Will it be stored in workstation device(s)? Mobile Devices?**
    No

14. **Has RATH by AVIRE ever had a data breach or significant cyber security incident?**
    No

15. **What processes are in place to monitor or prevent the exfiltration of sensitive data?**
    Customer data is protected by encryption of user settings, login credentials. Physical access to the device and credentials are needed if any user settings to be altered. We have data encryption at rest and in transit. It is achieved through the use of encryption technologies like SSL/TLS and disk encryption. We use access control mechanisms to limit access to sensitive data like access / refresh tokens and role-based access control in the application level. We use firewall to restrict network communication and WAF (web application firewall) to detect malicious attempts. To detect/monitor data exfiltration we store network logs to look for traffic patterns, database logs about access and usage and application logs. It is good to provide regular training to employees on data security best practices including how to identify and prevent data exfiltration attempts. Two-factor authentication through email is also implemented.

16. **Does the system have any other methods to enforce minimum necessary rights? Are there reports available to allow the periodic auditing of user permissions?**
    The application has the ability to assign a user administrator access or collaborator access. Collaborator accounts are intended for employees that need to communicate with the trapped passenger but have no add /delete privileges for hardware or users. They also cannot edit any account information. Account creation and role assignment logs are available from RATH by AVIRE by request.

17. **Will the system have access to customer Employee Information?**
    No

18. **Will the system have access to customer Internal/Proprietary Information?**
    No

19. **Does system store any sort of patient data or information?**
    No

20. **Does the application store, process or transmit credit card data as defined by PCI-DSS?**
    The SmartView application does not store credit card data. A third-party processing platform (Stripe) does process credit cards on behalf of RATH by AVIRE.

21. **Will the system have access to customer PHI (Protected Health Information)? PII (Personally Identifiable Information)? PCI (Payment Card Industry)?**
    System can view passengers in elevator car. For some industries, viewing may be considered PII. Passengers are never recorded or stored and will only be viewable in the instance of an emergency call initiated by the monitoring party.

22. **How does the hosted service provider keep user data separate from other clients?**
    Account data (e.g. name, contact number and device location) and camera identification numbers are stored within a shared platform - smartviewhub.com

23. **Will the hosted service provider agree to allow the user to retain all rights and ownership of any data entered, stored or processed by the hosted service provider on behalf of the user?**
    Excepting to the extent that such records must be maintained to meet our own legal obligations and retention policy.

24. **How can we ensure that you do not use customer data for any other purposes?**
    Customer data is only stored and processed for the purposes of providing our services. Please refer to our privacy policy on smartviewhub.com.

25. **Will the hosted service provider agree to transfer all data that was created / processed/stored throughout the duration of the contract period in a pre-agreed upon format and media at the termination of the agreement?**
    The extent of data stored and maintained will be location information of the devices.

26. **Will the hosted service provider agree to expedite the transfer of all customer data upon request in the event of any dispute arising between the customer and the hosted service provider?**
    The extent of data stored and maintained will be location information of the devices.

27. **Will the hosted service provider agree to destroy or render unusable any information that was created and stored on behalf of the user during the lifetime of the contract?**
    Yes

Video Recordings

DUE TO SECURITY AND PRIVACY LAWS NO VIDEOS WILL BE RECORDED OR SAVED.

RATH by AVIRE takes personal privacy and facility privacy of the highest priority. For the security of our company, our users, and building occupants, the video feed taken during an emergency call will not be recorded or stored. At this time, RATH by AVIRE does not offer an API or the ability to use an in-house DVR for a user to record and store their sessions.

Cryptography

1. **Is all client data encrypted at rest within the system? If so, what level of encryption?**
   Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, read replicas, and snapshots, encrypted DB instance, all logs. Also, there is implemented server-side encryption within the application server by AES-256 encryption algorithm. Database service uses a Key Management Service key to encrypt these resources. Storage service where client data is stored is also encrypted.

2. **Who is your SSL CA provider?**
   Microsoft

3. **Can you provide assurances that their authentication practices are audited at least annually by a trusted third-party auditor?**
   We refer the customer to Microsoft's practice statement, which is designed to meet or exceed the requirements of generally accepted industry standards.
   https://www.microsoft.com/pkiops/Docs/Content/policy/Microsoft_PKI_Services_CPS_v3.2.4.pdf

4. **How are encryption keys for data managed? Please describe the process for both data at rest and in transit and in motion.**
   Encryption keys for data management are handled using robust processes to ensure the security of data both at rest and in transit.
   Database: For storage encryption (data at-rest), Database uses the FIPS 140-2 validated cryptographic module. Data is encrypted on disk, including backups and the temporary files created while queries are running. For in-transit data, database server encrypts it using TLS protocol v1.2/1.3, encryption is enforced by default. Encryption keys are rotated and managed by Microsoft.
   Storage: Data is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. All requests to storage service must be made over TLS to ensure that they are encrypted while traveling (data in-transit). Encryption keys are rotated and managed by Microsoft.
   Application instance: Data is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. All requests to the application must be made over TLS to ensure that they are encrypted while traveling (data in-transit). Moreover, all traffic utilizes end-to-end encryption. Encryption keys are rotated and managed by Microsoft.

5. **Does the hosted service provider utilize any encryption methods that were custom developed?**
   No

6. **Do encryption algorithms utilized by the host application service provider meet FIPS-140-2 standards?**
   Yes, we utilize encryption algorithms in our application that meet FIPS 140-2 standards. This means that all sensitive data handled by our application is protected using cryptographic methods that comply with these standards. Specifically, Azure, our cloud service provider, employs FIPS 140-2 validated encryption algorithms for data.

Application Physical Security

1. **Is the equipment hosting the application located in a physically secure facility?**
   Application is hosted within an Azure cloud instance. For full information about Azure security protocols, please visit the following site: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

2. **Does the facility require badge access at a minimum?**
   Please refer to https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security for a comprehensive answer.
   Microsoft designs, builds, and operates data centers in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data, and is committed to helping secure the data centers that contain your data. We have an entire division at Microsoft devoted to designing, building, and operating the physical facilities supporting Azure. This team is invested in maintaining state-of-the-art physical security.
   Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the data center resources. Data centers managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data center floor.

3. **Is the infrastructure (hosts, network equipment, etc.) hosting the application located in a locked cage-type environment?**
   Application is hosted within an Azure cloud instance. For full information about Azure security protocols, please visit the following site: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

4. **Can the hosted service provider disclose who amongst their personnel will have access to the environment hosting the application?**
   The vendor does not have physical access to the Azure data center in which the application is hosted. For information regarding the physical access control to Azure data centers, please refer to https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

5. **Does the hosted service provider perform criminal background check procedures for personnel that will have access to the physical environment?**
   All Azure and Azure Government employees in the United States are subject to Microsoft background checks.

Security Assurances

Does the product have any of the following certifications?

1. SSAE 16 / SOC 1 Type 1 and Type 2
2. SOC 2 Type 1 and Type 2
3. SOC 3
4. HITRUST
5. PCI
6. ISO 27001:2013
7. FedRAMP
8. HIPAA
9. NIST

As of November 2024, RATH by AVIRE has engaged CompliancePoint, Inc to assist in the scoping, evaluating of security controls, and writing documentation to obtain ISO 27001 and an AICPA SOC 2 report. Once obtained, ComplaincePoint will assist in obtaining HIPPA. A letter of intent is available for that work. For any questions about a certification, please contact our customer service team at 1-800-451-1460 or rath-janus@avire-global.com.

Web Application Security Risk

How does RATH by AVIRE address and mitigate the common risks described below?

- Broken Access Control
  - Access credentials can be reset by holding the reset button on 7100 (cannot be done remotely)
- Cryptographic Failures
  - All HTTP data transfers are restricted to internal servers
- Injection
  - SV2 data on the device is not accessible by injection based malicious attempts
- Insecure Design
  - Unit is routinely being evaluated by development team for insecure design related issues.
- Security Misconfiguration
  - Security updates can be deployed remotely, and during the product's life cycle these updates will be rolled out periodically
- Vulnerable and Outdated Components
  - Outdated components will be updated periodically during the product's life cycle
- Identification and Authentication Failures
  - We are preventing multiple types of automated attacks such as brute-forcing login, credentials sniffing, password encryption
- Security Logging and Monitoring Failures
  - All failures and access control related messages for the hardware are logged and stored on the device.
  - Logins, failed logins and high value transactions are logged locally. The website application has it's own logging data base to security and monitoring failures.
- Server-Side Request Forgery
  - Device will have (not yet implemented) restricted outbound access to the wider Internet. The internal server on the device is captive and limited to our single website.

Risk Analysis

1. **Does RATH by AVIRE perform security risk analysis of the system from a hardware, software, and network perspective?**
   The vendor conducts risk assessments in accordance with NIST SP 800-30. The solution is evaluated within the organizational risk frame to identify potential threat sources and events, identify vulnerabilities and pre-disposing conditions, determine the likelihood of occurrence, determine the magnitude of impact and determine the overall risk.

2. **Does RATH by AVIRE have a formal information security risk management program in place to address information security risk over the lift of the product?**
   RATH by AVIRE applied the NIST Risk Management Framework in accordance with NIST SO 800-53.

Workstation Requirements

Workstation refers to the PC or computer used to access the viewing website (smartviewhub.com).

1. **What are the minimum and recommended requirements for client workstations running Windows 10 or 11?**
   The installation workstation must have a web browser, this can also be done via a tablet or mobile phone.

2. **Will system work with virus scanners (for example CrowdStrike Falcon)?**
   The system has not been tested with virus scanners but future incompatibilities can be addressed by remotely updating the software. Anti-virus can be installed on any computer or device being utilized to access \smartviewhub.com

3. **Does the application support running in a limited environment to enforce organizational use policies? This would include running without workstation administrative privileges, or limited Internet access for example.**
   In order to access the system from a workstation, it must be possible to access smartviewhub.com (via the Internet) using an Internet browser. Provided this is possible, the solution should work in a limited environment, though clearly it is impossible to test all possible configurations and situations and so we would require precise information on the limitations of the environment, and potentially access to an exemplar workstation, to provide a full response.

4. **If the proposed application includes additional physical equipment as mentioned above, what security mechanisms are used to prevent theft or unauthorized physical access to the equipment?**
   Hardware provided by the vendor are installed in an elevator panel and elevator machine room which are already physically protected. Only an authorized elevator technician with the appropriate security key and tools can access the hardware. Hardware requires login credentials to access any of the configuration settings on the hardware.

5. **Does the proposed application require any changes to the physical environment in order to protect access to customer information? These could include locking doors, privacy screens and other types of hardware locks.**
   Elevator and elevator machine room should already have locks and access security in place due to elevator security protocols.

Remote Access

1. **Does the vendor utilize a remote access solution to support the application?**
   Vendor utilizes a third-party company named Balena for remote access. Balena is utilized for fleet management for the operating system on the hardware. Balena secures communication with the device through their own VPN.

2. **Does the remote access solution support individual employee vendor logins?**
   Yes, all staff with access to the Balena fleet have an individual (per user) account secured with 2FA.

3. **Can the vendor provide audit logs for remote access sessions if requested?**
   Audit logs of access through Balena can be produced for all devices in the fleet for the past 90 days. Individual devices can be configured to store audit logs for longer periods, but these logs must be retrieved on a per device basis.

4. **Does the remote access solution utilize dual factor authentication?**
   Yes, Balena utilizes two-factor authentication for its users.

5. **Can the remote access connection be disabled by default and manually enabled on an as-needed basis?**
   Remote access is utilized to perform OS updates, firmware updates, security updates, bug fixes, and application patches. At this time disabling remote access is not an option for users.

6. **Are the devices used for vendor remote access managed by the vendor's central security policy?**
   Yes, this is currently managed through policy, however, SSO integration between the vendor's Azure AD and Balena account management is planned and will provide additional robustness in the control of devices that can be used for remote access.

7. **What is required for remote access?**
   Network requirements listed on page 27 will allow for remote access through Balena. This access is limited to select members of the RATH by AVIRE tech support team and the development team.

8. **Will RATH by AVIRE products expect to access any application components on the network remotely?**
   Yes / access granting required.

9. **Describe any administrative remote access features in the solution?**
   On smartviewhub.com admins have access to add/remove camera and access recordings. On Balena (cloud platform) admins have access to device monitoring, remote firmware updates, and tech support actions (reboot, download firmware etc.)

Contingency Plan and Recovery

1. **What methods of backup and restore does the system support?**
   Database is backed-up each day through Azure backup, website data such as documents and other related files are replicated across three availability zones, one replica per zone. The on-site hardware (e.g. car and machine room units) does not have a backup and restoration method as the only data stored on the on-site hardware is configuration information.

2. **How long would it take to acquire replacement hardware in the event of a failure?**
   The hardware installed in the elevator is custom. If necessary, a replacement unit can be obtained from RATH by AVIRE overnight. The viewing website (smartviewhub.com) can be navigated to on any standard PC or web-enabled device. There is no custom software that needs to be installed or any complex hardware requirements.

3. **Are there any physical requirements for the proposed application that would need to be addressed if the primary site was available?**
   The software platform (smartviewhub.com) is hosted within the cloud and managed by RATH by AVIRE, and does not have special physical requirements. The need for the on-site hardware is inextricably linked with the primary site in which it is installed (i.e. the elevator) and thus if the primary site were unavailable there would be no need for the hardware.

   The need for the on-site hardware is inextricably linked with the primary site in which it is installed (i.e. the elevator) and thus if the primary site were unavailable there would be no need for the hardware.

4. **Will RATH by AVIRE support signing a Business Associate Agreement when required?**
   For SmartView 2 installations, vendor can support review and signing of a BAA.

5. **What type of cyberliability insurance do you have? Please describe the limits under the policy.**
   We carry a master cyberliability policy for £15M. We will not add any additional parties as insured under our policy.

6. **How is your data stored in the cloud? Is it a SAN or S3 or Glacier?**
   Data is stored in S3 buckets which are designed to sustain data in the event of the loss of an entire Availability Zone.

7. **How long are backups available? Do you perform test restores?**
   RDS full database backup are performed every 24 hours and are available for 14 days, transaction logs are copied to S3 every 5 minutes. There are no test restores performed.

8. **Explain any redundancy you have across multiple data centers or repositories and if those data repositories are within the US and controlled by your organization.**
   Our infrastructure is designed with redundancy across three Azure availability zones within the East US (Virginia) region to ensure high availability and data durability. One availability zone is composed of one or more data center. All data remains under the control of AVIRE, Azure organization, and approved thirdparty developers, ensuring compliance with data residency requirements and secure data management.

9. **Can the hosted service provider agree upon RPO and RTO time frames that are appropriate to the business function being provided to users?**
   RPO is typically 5 minutes as RDS database copies transaction logs in up to 5 minute intervals. RTO can vary depending on the size of the but RTO is typically under 30 minutes. In case of Availability Zone failure, manual action is required and RTO can be up to a few hours.

Operational Security

1. **What are your internal mobile device access capabilities and any security controls for protecting lost or stolen mobile devices containing data?**
   No customer information is stored on mobile devices. Endpoint access to camera feeds is controlled through two-factor authentication utilizing an authentication app on a mobile device as the second secret. Organizational policy requires employees to report any lost devices. Upon reporting, this triggers a process to retire the two-factor secret and assign a new one, eliminating any potential access through dual compromise (i.e. theft of a mobile phone as well as gaining access to an employee password).

2. **Explain your workforce hire, orientation and security training process and any data/customer confidentiality agreements you have in place. Are all employees under NDA and does this extend to customer data?**
   Employees with access to Balena or administrative access to SmartViewHub.com (i.e. those employees with potential access to camera feeds) receive training on IT and security operating procedures. Employees are required to complete monthly refresher training on cyber security, focusing on a different area of cyber security risk each month. Employees are explicitly instructed not to access camera feeds unless there is a live ticket for technical support. Accessing a customer camera feed without an open ticket for technical support is a disciplinary offense and would likely result in dismissal (subject to circumstance and without prejudice or commitment). Employees are contractually obliged to keep all information pertaining to their work confidential and this extends to customer data.

3. **Please describe your provisioning/deprovisioning process and role management structure for all accounts including standard access, administrative access, and service accounts.**
   Upon identifying a new requirement for administrative access to either smartviewhub.com or Balena, an employee's manager must raise a ticket through our IT helpdesk. IT will review the request, verify that the employee has undertaken the necessary training on the system and access procedures (including security and privacy) and provide login credentials directly to the employee.

   When an employee changes roles, this triggers an automatic review of access permissions and if permissions are no longer required, the accounts will be deleted, removing the employee's access. Similarly, when an employee leaves, their accounts are deleted as part of the deprovisioning of their IT access. Any other deprovisioning needs can be raised by an employee's manager.

   Access permissions and accounts are reviewed every month to ensure they are up to date and in-line with business requirements.

   Integration of account permissions with our Azure AD is planned and this will further simplify and ensure the robustness of the provisioning/deprovisioning process.

4. **Are all user accounts created with unique credentials?**
   Yes

5. **Do all users receive training on general security issues such as phishing, passwords, and malware?**
   All employees receive training as described in the above answers. The Customer is expected to provide similar raining to their own users, though we can provide this (for a cost) if required.

Support

1. **What maintenance and support services are provided with the product?**
   RATH by AVIRE will support any defects in hardware or manufacturing for 2 years. Any issues from installation or outside factors will be handled by the installing party with assistance from the RATH by AVIRE tech support team. Software updates and security patching is included until the hardware is end of life.

2. **What are the technical support procedures?**
   If there is any technical support required for the product the RATH by AVIRE technical support team is available by phone at 1-800-451-1460 ext. 3 or by email at techsupport.us@avire-global.com

3. **What hours are technical support available?**
   Monday-Thursday: 8:00am to 5:00pm CST, Friday: 8:00am to 2:30pm CST. Holidays may affect these hours.

4. **How are customer escalations handled?**
   Any issues that cannot be solved by the RATH by AVIRE technical support team will be escalated to tier 2 tech support. If the issue is still unable to be resolved, it will get escalated to product management who will facilitate corrective action with the engineering team.

5. **How is support tracked?**
   Support is tracked a ticketing system through FreshDesk

6. **Explain how the vendor monitors and reports upon notification of abuse or investigation. This might include regulatory violations, criminal or civil investigations and additional requests made by either an outside entity or internally.**
   Notifications of abuse or investigation are reviewed by the compliance officer and, where appropriate, outside counsel, and a response formulated on a case-by-case basis.

7. **What events are logged and shared with users?**
   Critical security breaches will be logged and shared with users.

8. **Does the hosted service provider have a plan for notifying users immediately of any breach or unauthorized access including hosted data, communications devices, servers or other infrastructure that directly or indirectly supports the hosted environment?**
   Data and security breaches are reported to impacted parties.

9. **Can the hosted service provider accommodate regular user account privilege access reviews involving user data?**
   User privileges for device access are exposed within smartviewhub.com to the customer administrator account. Review of these privileges is the responsibility of the customer.

10. **Will the hosted service provider agree to allow the SAHS Incident Response Team to interface and facilitate any incident with law enforcement, e-discovery, or subpoenas relating to user data?**
    The vendor will assist the customer in complying with any such requirement and will meet any legal obligations to comply with warrants, subpoenas, etc. The precise nature of such cooperation will clearly depend upon the nature of the investigation.

11. **Will the hosted service provider agree to provide all relevant logs and access to evidence in the case of a data breach to a customer Incident Response team?**
    Yes

12. **Can the hosted service provider supply general location information about the location of hosted customer data in order to comply with individual state information security legislation?**
    Yes

13. **In the event of a security incident, please provide vendor contact information. Is this contact available 24hrs/day x 7days/week?**
    Phone Line for issues: 800.451.1460, not available 24x7. This will be escalated to VP of Sales for issue resolution.

Maintenance

1. **How often is maintenance performed and is it performed on a routine predictable cycle?**
   Maintenance is performed by the elevator service company or building. Cycle will be determined by their policies.

2. **Will the equipment be vendor owned?**
   No

3. **What is warranty period?**
   2 Years

4. **What is covered under the warranty?**
   RATH by AVIRE products are warranted to be free of manufacturing defects in material and workmanship for two (2) years from the date of sale to the customer. RATH by AVIRE will, at its discretion, repair, replace or make appropriate fixes at its option, to any phone product found to be defective and is within the warranty period. See avire-global.com/en-us for a full warranty statement

5. **What does the upgrade cycle look for the unit?**
   At most once a month firmware updates and security improvements / patches when required.

6. **Will hardware and software upgrades be available for the life of the product?**
   Software updates will be pushed remotely to the units as they become available. If the product is discontinued or EOL, a comparable unit will be available at the customer's expense.

7. **What does remote update period look like?**
   Updates take anywhere from 1-15 minutes depending on the size of the change. Standard downtime is approximately 1 minute during device reboot. User is notified on LCD screen by Updating… message. If any interaction (call, video call) is initiated with the device, the device will hold the updates until the device is idle again.

8. **Does unit have the capability for service health monitoring?**
   Yes, Balena cloud platform offers service health monitoring which can be accessed by RATH by AVIRE tech support. User can access installation tests page on the local configuration website (smartviewconfig.com) which provides a simplified version of this.

Quality Testing

1. **Describe company's testing and quality assurance process?**
   In production, the product goes through a full QTP test procedure at time of build. After full build, the unit goes through an additional automated test procedure. Our production facility has quality assurance personnel to oversee the built and testing of the equipment is up to RATH by AVIRE standards. For whatever reason the product does not meet the testing or quality parameters the unit is scrapped to help alleviate further issues.

2. **Has the SmartView 2 undergone formal testing using a formal test plan? Are those plans available for review?**
   Yes, a test overview is available by request.

SmartView Security Details Overview

Device Safety and Security Details

Emergencies can occur at any time, and when they do, reliable communication becomes a lifeline. Our wide range of code-compliant solutions are certified, digitally connected, and reliable ensuring the safety of users and compliance with industry code and regulations.

The purpose of this document is to provide details on the structure of SV2 from a security standpoint, by listing and explaining the features.

Operating System

The SmartView 2 Operating System (OS) runs off a platform named Balena. Balena is an Internet of things (IoT) cloud platform that we use to create and manage devices. The Balena OS allows for easy portability to multiple device types and while allowing each device to have it's own OS.

Within Balena, RATH by AVIRE can go into a device and check it's OS version, SmartView 2 software version, device logs (up to the last 1000 lines), memory, temperature, and CPU usage. The RATH by AVIRE technical support team can view these parameters and download the last 1000 lines of logs to help triage any issues. A limited number of authorized, high-level users within RATH by AVIRE can also do this as well as reboot devices, change the software version, and access a secure terminal if more detailed logs need to be accessed. High-level users are restricted to members of the RATH by AVIRE engineering team.

The hardware configuration settings and account passwords are encrypted so RATH by AVIRE cannot obtain this information from the terminal. We will not make any changes within this terminal without permission from an on-site representative. Source code is not accessible through the terminal and cannot be modified by any member of the RATH by AVIRE team.

Balena is a secure platform in which only RATH by AVIRE authorized employees have an account. Access is granted to those employees on an as-needed basis and limited to support roles only (engineering and technical support). Only the head of RATH by AVIRE engineering acting as the administrator on Balena can accept members into the group, and set their access role (member, observer etc). Access will never be granted to any individual outside of a support role. For more information about platform access please see the SmartView 2 Terms of Use available on https://www.smartviewhub.com.

Configuration Page

For security reasons, the SmartView 2 hardware can only be configured when physically connected to the device. This can be done either through the provided Wi-Fi dongle's simulated Wi-Fi network or plugging an Ethernet enabled device directly in to the ETH OUT port on the Machine Room unit. The provided Wi-Fi dongle is plugged into the USB2 port on the Machine Room unit.

Both of these methods require physical access to the machine room or the alternate location the Machine Room unit is installed in. It is recommended that the Machine Room unit be installed in a secure location so there is no other way the hardware settings can be accessed. If an individual tries to go to smartviewconfig.com while not locally connected to the Machine Room unit, the configuration page will not appear and instead show an invalid web address landing page. This is because of the IP rules built into the hardware for security purposes. If you use the Wi-Fi dongle and leave it plugged in, the dongle will automatically time out after 20 minutes making the configuration page inaccessible to any potential infiltrators.

When an individual is locally connected to the Machine Room unit and navigates to smartviewconfig.com, they will be asked to log in with a unique username and password. The username is password is set when logging into the hardware for the first time. If someone tries to log in with incorrect credentials, after 5 incorrect attempts the device is locked for 5 minutes. The hardware will not accept any login attempts during that time, even if the device has a hard reset performed on it via the reset button on the Machine Room unit. When logging in, the password field is hidden visually on the screen (which can be viewed by clicking the 'eye' icon). When logged to the hardware, the first thing you will see on the home screen is the status of the Machine Room unit, whether it is online or not. The home screen will also have the option to pair the Elevator unit to the Machine room unit, a function required for security purposes. Once paired, the home page will also display the status of the Elevator Unit.

In the system menu of smartviewconfig.com there is the settings page, where you set outbound phone numbers, the installation address, and other hardware settings. The installation tests page checks certain functionalities on boot up and displays the results. The elevator camera page is to preview the camera feed and adjust the camera angle if necessary. Note, the elevator camera page cannot be used to activate the screen to send messages. The static IP page allows to assign a static IP to the hardware instead of using a DHCP address. The login section can be used to update the username and password of the hardware. After 5 minutes of inactivity, the configuration page will automatically log out.

Software Versions and Updates

The SmartView 2 system can have its software changed through over the air updates to reduce bugs, add new features, and keep security up to date. Over the air updates can only be initiated by RATH by AVIRE engineering. The device's software version can be viewed either in the home page of smartviewconfig.com or displayed on the Elevator unit screen after you hold the yes/no (or equivalent) buttons for 10 seconds.

As long as the SmartView 2 hardware has an Internet connection, it will download the update automatically once released by RATH by AVIRE without on-site initiation. If Internet has been removed from the device, the download will begin when it is restored.

In instances such as the device placing an emergency call, the timing of this update might be inconvenient, The SmartView 2 system will prioritize other functionalities ahead of the update meaning there is no interruption or clash in operation. The update will download in the background while the device can continue to run normally, with the exception that the Elevator unit screen will display a ‘updating’ image. When the download is complete, it will not be installed if there is an active voice and / or video call. It is only after the voice / video call has ended that the download is completed, ensuring there is no interruption in the event of an emergency. If a voice / video call is initiated during a download, the update image on the Elevator unit is removed and the voice / video call, will function as normal.

Any update released to SmartView 2 devices will not change or modify any of the hardware settings or the username and password.

IP Rules

The SmartView 2 hardware has built-in IP rules is to limit the connections to the outside world to significantly reduce device entry points to potentially exploit. It’s because of these rules that the configuration page is only accessible when locally connected to the hardware. However, IPs and protocols need to available for certain functionalities. The current outbound traffic table can be found on page 28 of this document.

SmartView Hub

For the video streaming element, the hardware utilizes a proprietary viewing website, smartviewhub.com. This is a HTTPS site which is an extension from HTTP but with additional encryption for a secure communication over the network.

Like the configuration page, the password field is hidden visually on the screen (which can be viewed by clicking the ‘eye’ icon) on the login page. If necessary, the password can be modified within the user’s profile setting on the website or via a secure link send to the user’s e-mail address. By default, if a user is inactive on the SmartView Hub for 15 minutes (which can be changed in the profile account settings), they are logged out and will have to log in again. Hardware updates will not impact login credentials for the SmartView Hub.

For additional security, accounts can have two-factor authentication enabled via e-mail. This will require a 6-digit access code to be entered before accessing the site and it’s connected devices.

Detailed Network Usage and Requirements

Before installing a SmartView 2 system on-site, the following ports will need to be open for outbound traffic for the system's basic functionalities. Failure to set up the network properly will result in registration issues and delays in installation time.

These IP rules are meant to limit the connections to the outside world to significantly reduce device entry points to reduce exploitation. Because of these rules, the hardware configuration page is only accessible by a local connection to the Machine Room unit (7100). However, IPs and protocols need to be available for certain functionalities. The current outbound traffic for the system is as follows:

Destination	On Port	Usage	Expiration Date
smartviewhub.com	TCP - 443	SmartView 2 monitoring/video streaming/ message transfer	N / A
api.balena-cloud.com		Balena API	
logs.balena-cloud.com		System logs on Balena cloud	
registry-data.balena-cloud.com		Balena connection, updates and reports	
registry2.balena-cloud.com			
cloudlink.balena-cloud.com			
delta.balena-cloud.com			
google.com		Used by elevator unit to check connection to the network	
DNS	UDP - 53	Standard port for DNS name resolution, used by Balena services	N / A
NTP	UDP - 123	Standard port for the Network Time Protocol, used by Balena	N / A

Minimum Network Speed:

- Download: 5 MB/s
- Upload: 5 MB/s

RATH™
by AVIRE

N56 W24720 N. Corporate Circle • Sussex, WI 53089 | 800-451-1460
avire-global.com/en-us