Verso Vision System Description and IT Requirements

System Description

Verso Vision solution uses artificial intelligence and video analysis to detect activity and risky situations in a room and notify personnel via mobile devices. Notifications are sent to personnel via nurse call system or via a mobile device, letting them know when a patient gets out of bed or falls in their room, for example. The system uses camera sensors installed in rooms, and the image stream is processed in real time on a local server. The image stream is not recorded, and personnel do not have access to it – Verso Vision solution is therefore not a camera surveillance system. The data diagram below shows the process flow of the Verso Vision system.

Process flow

1. The nurse evaluates a patient's fall risk and sets the alarm levels using NurseUI in a web browser (e.g. Chrome, Edge, Firefox, IE)

2. The system updates the monitoring configuration for the patient place

3. The system monitors the patient's room and activities

4. If the patient falls in the room, the system detects the fall and sends an alarm to the nurse's Mobile Device via the nurse call system

5. The nurse decides on the next action (e.g., visiting the room, calling for additional help) based on the alarm. Optionally, the nurse can open an anonymized live video stream of the patient's room to support this decision

6. The system collects data related to the event and generates a report. The details of data recording and reporting are agreed upon with the Customer
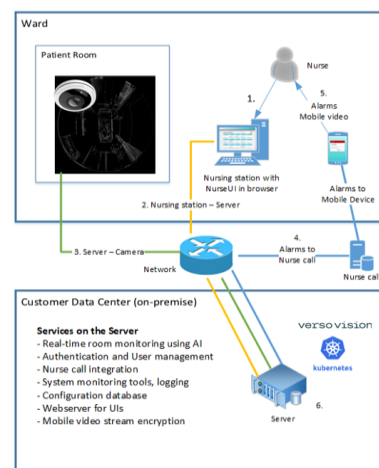
Servers and Nurse call Solutions

Servers

On behalf of Verso, the server can be placed in a data center or at the site where the system is in use, the final decision on the server location is made by the customer's IT experts.

The server hardware is installed at the designated location by either Verso or a specialist at the site. The operating systems of the servers will be Linux, as specified separately. The server's capacity must support agreed number of patient places, in accordance with Verso Vision's guidelines.

Scalability and accessibility

The system architecture is based on containers, which achieves good maintainability through orchestration technologies (Kubernetes). Orchestration technologies ensure scalability and

Verso Vision Oy   VAT number: FI31288246
Kympinkatu 3C   info@versovision.com
40320 Jyväskylä   www.versovision.com
FINLAND

accessibility of the system. In addition, the system data will be backed up regularly on a schedule and method agreed with the Customer. Availability may be improved by adding redundant server capacity, and the system can be configured as a high-availability (HA) system. The specific availability and monitoring arrangements will be agreed upon separately with the Customer.

Nurse Call System and Mobile Video

Alarms from the Verso system are delivered to personnel either via the customer's nurse call system or through Verso's mobile application. Verso provides integrations with common nurse call systems. The Verso mobile app runs on Android devices (support for iOS is planned for a later release).

The Verso Vision mobile application runs on a device connected to the on-premises wireless network and communicates with Verso Vision server through specified network connections. The mobile application does not require access to the public internet.

Mobile video

When an alarm is triggered, it is possible to open an encrypted, anonymous mobile video connection to the room using the nurse's mobile device. The customer can choose whether mobile video is enabled.

The technical requirement is that mobile devices must have access to the Verso server, meaning they must be connected to the internal wireless network.

User Interfaces and Access rights

User Interface for Nurses' Workstations

After the software is installed, a browser-based user interface for managing Verso alerts will be made available on nurses' workstations. Supported browsers include Chrome, Firefox, and Edge, and no browser plug-ins are required. Browsers must support the certificate selected by the customer.

A Verso Vision shortcut will be created or distributed to the nurses' workstations, linking directly to the user interface.

User authentication can be handled using either shared user IDs or the customer's Active Directory (AD)-based authentication solution. If shared user IDs are used, login details can be embedded into the shortcut to enable direct access. The user interface only displays alarm settings relevant to each patient room and location.
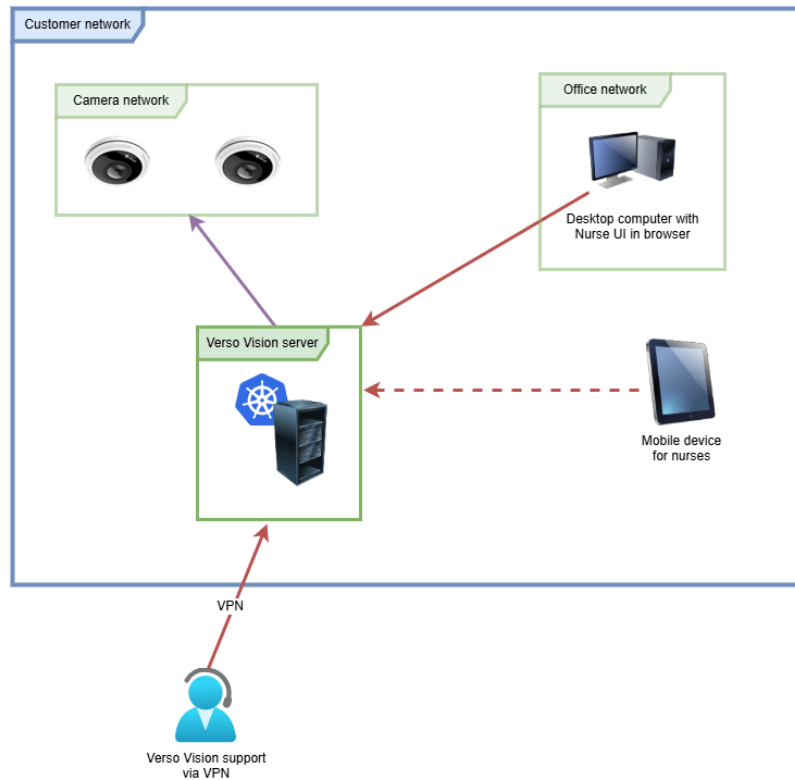
Network requirements

Network connections

The Verso Vision server provides necessary services over the customer's internal network. Maintenance requires access to specific public internet services. All required network traffic is outbound only; no inbound network connections are needed.

Additionally, certain internal network connections are required, for example, server access to cameras and access from nurses' workstations to the browser-based user interface hosted on the server.

Verso Vision will provide a list of required network connections.

Verso Vision Oy   VAT number: FI31288246
Kympinkatu 3C   info@versovision.com
40320 Jyväskylä   www.versovision.com
FINLAND

Domain name and Certificate for the Verso User Interface

Verso Vision recommends using secure network connections for system services, which requires a domain name and certificate. The domain name is typically in the format *versovision.customerdomain.com*.

If mobile video is used through a nurse call system, a commercial certificate is recommended due to compatibility issues with Android devices and customer-signed certificates.

IP Addresses to Verso Vision Solution

Verso delivers the server pre-installed. Ideally, the customer's IT department provides IP addresses in advance to facilitate server preparation. Verso will send a list of required IP addresses for the server and connected devices, such as cameras.

Remote connections

The Verso Vision system requires remote access for installation and customer support. Remote connections can be established via the customer's VPN or via other agreed method.

Detailed Network Openings

From Verso Vision server to public internet

For Verso Vision support, the following network openings are required:

Port	Protocol	Source	Destination	Purpose
123/UDP	NTP	Verso Vision server	ntp.vv-intra.xyz	Time synchronization Local NTP server can be used as well
443/TCP	HTTPS	Verso Vision server	harbor.vv-intra.xyz	Verso Vision software repository for system updates
443/TCP	HTTPS	Verso Vision server	versovision.atlassian.net	Automated monitoring
443/TCP	HTTPS	Verso Vision server	*.archive.ubuntu.com *.security.ubuntu.com	Operating system updates

Connections from the server to cameras

To be able to control and monitor cameras and to read their video streams, the Verso Vision server need to be able to access the following ports in every camera in the camera network.

Port	Protocol	Source	Destination	Purpose
554/TCP	RTSP	Verso Vision server	Camera	Video streaming
80/TCP 8080/TCP	HTTP	Verso Vision server	Camera	Camera management UI
443/TCP	ONVIF	Verso Vision server	Camera	Camera configuration

Verso Vision Oy   VAT number: FI31288246
Kympinkatu 3C   info@versovision.com
40320 Jyväskylä   www.versovision.com
FINLAND

Connections to Verso Vision server

To be able to access the Verso Vision system locally, the following ports in the network interface of the host operating system need to be made available in the local network.

Port	Protocol	Source	Destination	Purpose
443/TCP	HTTPS	Nursing station	Verso Vision server	Nurse UI
443/TCP	HTTPS	Mobile device	Verso Vision server	Video stream (optional)
80, 30000 – 32000 TCP	HTTP	Remote support via VPN	Verso Vision server	Management UIs
443/TCP	HTTPS	Remote support via VPN	Verso Vision server	Maintenance
22/TCP	SSH	Remote support via VPN	Verso Vision server	Maintenance

Connections from the mobile device to the server

For the mobile devices, the following network openings are required:

Port	Protocol	Source	Destination	Purpose
443/TCP	HTTPS	Mobile device on wireless network	Verso Vision server	Alarm messaging