OMRON
MICROSCAN

Appendix F: LVS® 95XX Data Sharing

P/N 84-9310051-02 Rev D

GS1 Solution Partner

Disclaimer

The information and specifications described in this manual are subject to change without notice.

Latest Manual Version or Technical Support

For the latest version of this manual, or for technical support, see your local Omron website. Your local Omron website can be located by visiting **https://www.ia.omron.com** and selecting your region from the Global Network panel on the right side of the screen.

Security Measures

Anti-Virus Protection
Install the latest commercial-quality antivirus software on the computer connected to the control system and maintain to keep the software up to date.

Security Measures to Prevent Unauthorized Access
Take the following measures to prevent unauthorized access to our products:

- Install physical controls so that only authorized personnel can access control systems and equipment.
- Reduce connections to control systems and equipment via networks to prevent access from untrusted devices.
- Install firewalls to shut down unused communications ports and limit communications hosts and isolate control systems and equipment from the IT network.
- Use a virtual private network (VPN) for remote access to control systems and equipment.
- Adopt multifactor authentication to devices with remote access to control systems and equipment.
- Set strong passwords and change them frequently.
- Scan for viruses to ensure safety of USB drives or other external storage devices before connecting them to control systems and equipment.

Data Input and Output Protection
Validate backups and ranges to cope with unintentional modification of input/output data to control systems and equipment.

- Check the scope of data.
- Check validity of backups and prepare data for restore in case of falsification or abnormalities.
- Safety design, such as emergency shutdown and fail-soft operation in case of data tampering or abnormalities.

Data Recovery
Back up and update data periodically to prepare for data loss.
When using an intranet environment through a global address, connecting to an unauthorized terminal such as a SCADA, HMI or to an unauthorized server may result in network security issues such as spoofing and tampering.
You must take sufficient measures such as restricting access to the terminal, using a terminal equipped with a secure function, and locking the installation area by yourself.
When constructing an intranet, communication failure may occur due to cable disconnection or the influence of unauthorized network equipment. Take adequate measures, such as restricting physical access to network devices, by such means as locking the installation area.
When using a device equipped with the SD Memory Card function, there is a security risk that a third party may acquire, alter, or replace the files and data in the removable media by removing or unmounting the removable media. Please take sufficient measures, such as restricting physical access to the controller or taking appropriate management measures for removable media, by means of locking the installation area, entrance management, etc.

Software
To prevent computer viruses, install antivirus software on the computer where you use this software. Make sure to keep the antivirus software updated.
Keep your computer's OS updated to avoid security risks caused by a vulnerability in the OS.
Always use the latest version of this software to add new features, increase operability, and enhance security. Manage usernames and passwords for this software carefully to protect them from unauthorized uses.
Set up a firewall (e.g., disabling unused communication ports, limiting communication hosts, etc.) on a network for a control system and devices to separate them from other IT networks.
Make sure to connect to the control system inside the firewall.
Use a virtual private network (VPN) for remote access to a control system and devices from this software.

Data Sharing

Numerous methods are available to share data with the LVS-95XX; listed below are three examples:

1. Reports and ReportData Tables
2. Retrieving Results by Reference
3. Listening to the Serial Port (COM1)

All verification results are stored in a Microsoft Jet 4.0 database. The database is compatible with Microsoft Access 2000 or newer. Default location of the database:

- Windows 10: C:\Users\Public\LVS-95XX\LVS-95XX.mdb

Reports and ReportData Tables

Two tables store the results: Reports and ReportData. Each table is described below.

Reports

The Reports table contains one record per verification. The fields are listed below:

Field	Description
ReportID	System-generated unique number.
SectorID	Usually 1 but could be > 1 if there is more than one sector.
LclTime	Local time that the report was generated.
GmtTime	GMT (Greenwich Mean Time) that the report was generated.
X1	X start coordinate for drawing the box on the thumbnail.
Y1	Y start coordinate for drawing the box on the thumbnail.
SizeX	Size of box starting from X.
SizeY	Size of box starting from Y.
Reference	Reference as set up on the **Setup** tab.
OverallGrade	Overall grade.
DecodedText	Decoded text.
Thumbnail	The thumbnail of the barcode (Binary Large Object).

ReportData

The ReportData table contains more than one record per verification; this is a one-to-many relationship with the Reports table.

Field	Description
ReportID	Links to **ReportID** in the Reports table.
Category	Indicates where to place the data on the report.
Sequence	Indicates where to place the data on the report.
ParameterName	Parameter name for the printed report.
ParameterValue	Value for each parameter.

Retrieving Results by Reference

If **Reference** is selected on the **Setup** screen, results can be viewed and exported from the **Archive** screen. The files are exported as text files and are delimited with the vertical bar character "|" (ASCII Decimal 124). The files have a file extension of VBD (Vertical Bar Delimited). Commas are not used, as commas are decimal separators in some regional settings. The files can be imported into most spreadsheets or databases. To import into Microsoft Excel, follow the steps below:

1. Open a new spreadsheet.
2. Click **Data** > **Import External Data** > **Import Data**.
3. Locate and open the saved .VBD file.
4. Choose **Delimited** and then click **Next**.
5. Switch off all other delimiters and check **Other**.
6. Type the vertical bar character in the box.
7. Click **Finish**.
8. Click **OK**.

Listening to the Serial Port (COM1)

To make the LVS-95XX as flexible as possible, all results are published to Com 1. To test this feature and assist you in development, connect another computer to the verifier using a serial crossover cable and run an ASCII terminal application. The port settings on both the terminal and the LVS-95XX must be set as follows:

Baud	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Each time you verify a barcode, the results appear on the terminal window. An application can be developed to take advantage of this feature to automate and integrate the LVS-95XX with your database or other application.

Important: To change CommPort settings, refer to the **Change CommPort Settings** section in **Appendix G: Special Features**.