Operating Manual

Secure Operating Manual Fluent

Title:	Secure Operating Manual Fluent			Part number:	n.a.
ID:	403097, en, V1.0			Translated from:	n.a.
Version:	Revision:	Issue:	Document History:		
1	0	2024-12-12	First edition		

Table of Contents

1 About This Manual

1.1 Scope of This Manual

This manual provides cybersecurity information to customers for the Fluent software system according to IEC-81001-5-1.

1.2 Definitions, Acronyms and Abbreviations

Abbreviations / Terms	Description
ASM	Application Software Manual
FAS	Field Application Scientist
FSE	Field Service Engineer
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
IoT	Internet of Things
LTSC	Long-Term Servicing Channel (Microsoft)
Maintained Software	Maintained software are software components for which Tecan will notify customers regarding known risks related to security and provide updates.
MQTT	Message Queuing Telemetry Transport
OS	Operating System
Supported Software	Supported software are software components from 3rd parties for which Tecan will notify customers regarding known risks related to security and the availability of compatible updates.

2 General Information

Description	Information
Product Name	Fluent (all models)
Software System Name	Fluent Software System
Software Application Name	FluentControl
Reference to SBOM	Provided by Tecan upon request

2.1 Supported Software

Tecan will monitor the availability of security updates for supported SW. Tecan will provide information about compatible updates on its website.
https://www.tecan.com/knowledge-portal.
Customers are responsible for checking the platform regularly for updates.
Customers are responsible for downloading updates provided by 3rd party and applying them to their systems.
In case available security updates are not compatible with the system, Tecan informs customers about other mitigations that can be used instead of applying the updates.
The following list contains all software items categorized as supported software.

- SAP Crystal Reports
- Microsoft .NET Framework/Runtime
- Microsoft Visual C++
- Microsoft Windows 10 LTSC
- Microsoft SQL Server
- Microsoft Edge WebView2 Runtime

2.2 Maintained Software

Tecan will monitor the availability of security updates for maintained SW. Tecan will provide information about compatible updates on its website
https://www.tecan.com/knowledge-portal.
Customers are responsible for checking the platform regularly for updates.
Updates will either be provided for download on the website or installed by Tecan personnel.

Tecan will provide regular Windows security updates to customers with Tecan embedded PC. The updates are cumulative which means that customers can always install the most recent update which contains all previous updates.

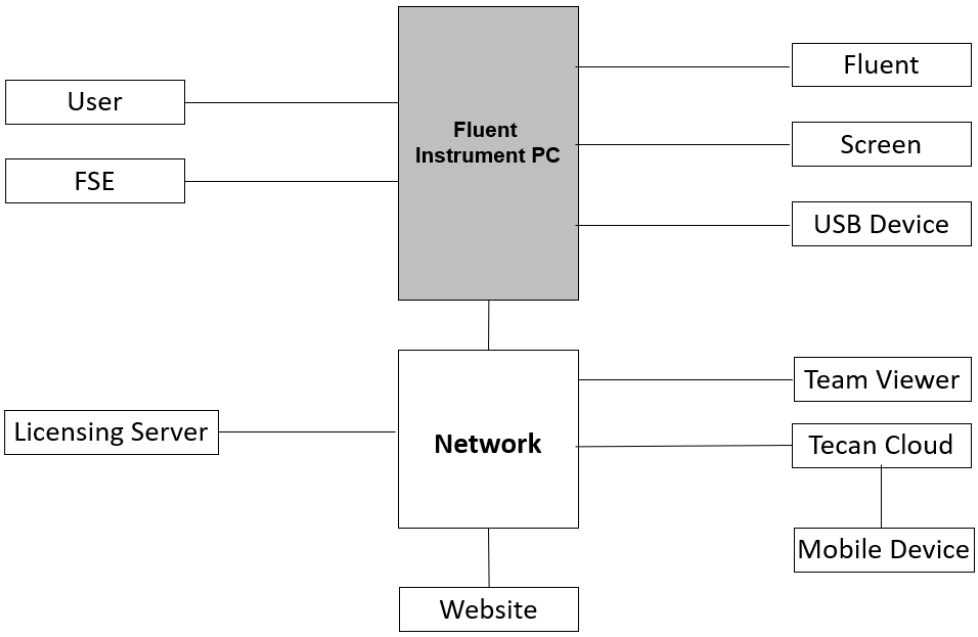
The following list contains all software items categorized as maintained software.

- Tecan FluentSetup
- Tecan FluentControl
- Tecan Licensing Client
- Tecan IoT Client

- Tecan G (OLEG)
- Tecan Sample Tracking
- Tecan MAP IAM
- Tecan Magellan
- Tecan Hydrowasher Driver
- SiLA1 client
- SiLA2 client
- UMS
- Inheco MTC driver
- IDS uEye
- Arena SDK (Arena Library only)
- Tecan 3D Simulator

3 System Overview

In this chapter and in the system diagram, all external systems or applications that are connected to the system are described to provide an overview of the integration and dependencies that the system requires.



3.1 Description of External Interfaces

Name	Protocol	Purpose
IoT Client (Tecan Cloud)	HTTPS, MQTT	Sending data from the instrument to cloud (MQTT). Remote update of IoT Client and instrument registration (HTTPS). Please refer to document 403014 IT Considerations for Introspect software.
FluentControl API	COM	Option to control FluentControl from external applications.
Generic USB Device	USB	Communication with external storage and modules like keyboard and mouse.
Tecan Licensing Server	HTTPS	The device gets license from Tecan server via the internet.

Name	Protocol	Purpose
Team Viewer	HTTPS	The device establishes communication with the Team Viewer server for remote support via the internet. Requires download of Team Viewer exe via link provided by Local Helpdesk. Team Viewer exe is not part of the delivered SW system. Please refer to document 401994 Tecan Remote User Guide for security information related to this process.
User	-	PC login with user password. FluentControl login with user password.
FSE	-	PC login with Windows password (provided by customer). FluentSetup login using FSE authenticator.
Customer PC	USB Ethernet	The customer PC is connected via a USB cable to the USB- port on the Fluent. The customer PC is connected via an Ethernet cable to the RJ45 port on the outlet panel to stream the Deckcheck camera signal.
Customer screen	DP	The external screen is connected to the Fluent Instrument PC.
Network	Ethernet	The customer PC is connected to the network of the customer for local data exchange and optionally to the internet.
Mobile device	HTTPS	Tecan Cloud data can be displayed on the smart phone of the user or other mobile device. This is currently based on a web browser, in the future possibly via an app.
Websites	HTTPS	The user/FSE can access websites to download or upload data via internet: - Team Viewer software can be downloaded for remote support from the Team Viewer website*. - Manuals can be downloaded from the Tecan website*. - Snapshot files can be uploaded to the Tecan storage location using a link from the Local Helpdesk. - Software updates can be downloaded from the Tecan website*.

***Websites for Download:**

https://get.teamviewer.com/tecanqs

https://www.tecan.com/knowledge-portal

4 User Access and Authentication

This chapter describes what user types and roles are existing and what needs to be considered during operation.

Physical access control shall be in place as defined by local laboratory and facility regulations or GLP / GMP.

The administrator of the operating system of the Fluent Instrument PC (OS admin) receives full Windows admin rights. The customer assumes full responsibility once the installation of the instrument has been completed. From this point on, Tecan personnel no longer has access. In the event of a service call, the customer must provide Tecan personnel with Windows access.

The customer OS admin shall create personalized user accounts for all operators of the device. FluentControl admin shall create personalized accounts for FluentControl operators.

Summary of different roles and privileges are shown in the table below:

No.	User Group	User Sub-Group	Windows Account and Privileges	FluentControl Account and Privileges	Setup / Service SW Access
1	End user (customer)	Operator	“User” Read & execute	“User” Execution of defined processes (no rights to modify processes)	No
2	End user (customer)	Key operator	“User” Read & execute	“Admin” Setup, modification, validation and execution of processes	No
3	End user (customer)	OS admin	“Admin” Full admin rights	Optional	No
4	Tecan personnel	FSE, FAS	Windows access rights to be provided by customer OS admin to Tecan personnel	Windows access rights to be provided by customer FluentControl admin to Tecan personnel	FluentSetup (certificate/FSE authenticator) Xflex Service SW (on FSE laptop) XInfiniTe-F50 Service SW (on FSE laptop)

5 System Setup and Configuration

5.1 Network Configuration

To allow additional Tecan Digital Services, the following configurations are required:

- IoT Client: For more information please refer to
  Document: 403014 IT Considerations for Introspect Software.
- Team Viewer: Outbound connections on TCP port 443 need to be enabled to accommodate https requests.
- License server: Outbound connections on TCP port 443 need to be enabled to accommodate https requests.
- Tecan and Team Viewer websites need to be reachable (https).

For instruments with internal PC the required settings have been pre-configured by Tecan. However, it is the customer's responsibility to integrate the system into the local network and to adapt the required configurations.

5.2 Decommissioning of the System

It is in the responsibility of the system user to properly decommission the system. Tecan recommends the following actions in case the complete product is decommissioned:

- Revert network configuration described in 5.1 for additional Tecan services.
- Deactivation of the user accounts.
- Inform Tecan to deactivate the cloud services linked to the decommissioned system.
- Inform Tecan to deactivate licences linked to the decommissioned system.
- Wiping of the system hard drive.
- Destroy any relevant BitLocker Recovery Key.

Tecan recommends following in case only the system’s PC is decommissioned:

- Wiping of the system hard drive.
- Destroy any relevant BitLocker Recovery Key.

6 System Operation and Maintenance

Please refer to the following checklist during system operation and maintenance:

- Customers shall regularly check the availability of software security updates on the Tecan web portal **https://www.tecan.com/knowledge-portal/**.
- Customers shall perform regular backups of their system (please refer to Document 399935, FluentControl™ Application Software Manual, Chapter 13 Data Handling).
- Users shall always shut down the system and the running software properly.
- Disconnecting the power cord while the system is powered or closing the application software by shutting down the operating system, may result in the system ending in an undefined state.
- Tecan recommends shutting down and restarting the system periodically to avoid performance problems.

7 Security Controls

The following security controls shall be implemented by the customer to mitigate the risk for cyberattacks:

Risk	Mitigation
An attacker could edit data files used by FluentControl rendering Fluent system unusable.	- Set up windows access control and ensure system operators have the lowest suitable access rights. - Enable bitlocker
Tecan FSE has Admin Access to Fluent Software system, and can change user access.	Change UMS admin password to a strong password at system handover part of IQ/OQ).
An attacker could try one password after another to gain access to system.	- Implement a password policy that include password strength, complexity rules, and update rules, and not to share passwords between different systems. - Enable email to Admin when account locks because of too many incorrect password entries.
A password re-used in a different system is compromised allowing an attacker to gain access to the Fluent Software system.	- Implement a password policy that include password strength, complexity rules, and update rules, and not to share passwords between different systems. - Enable email to Admin when accound locks because of too many incorrect password entries.
Attack through open Internet connection.	Implement firewall and end point protection to allow only connections needed by the Fluent Software System. Please refer to Section “5.1” [▶ 12] for details on the necessary ports.