8.4.1 OT Field Device to PLC

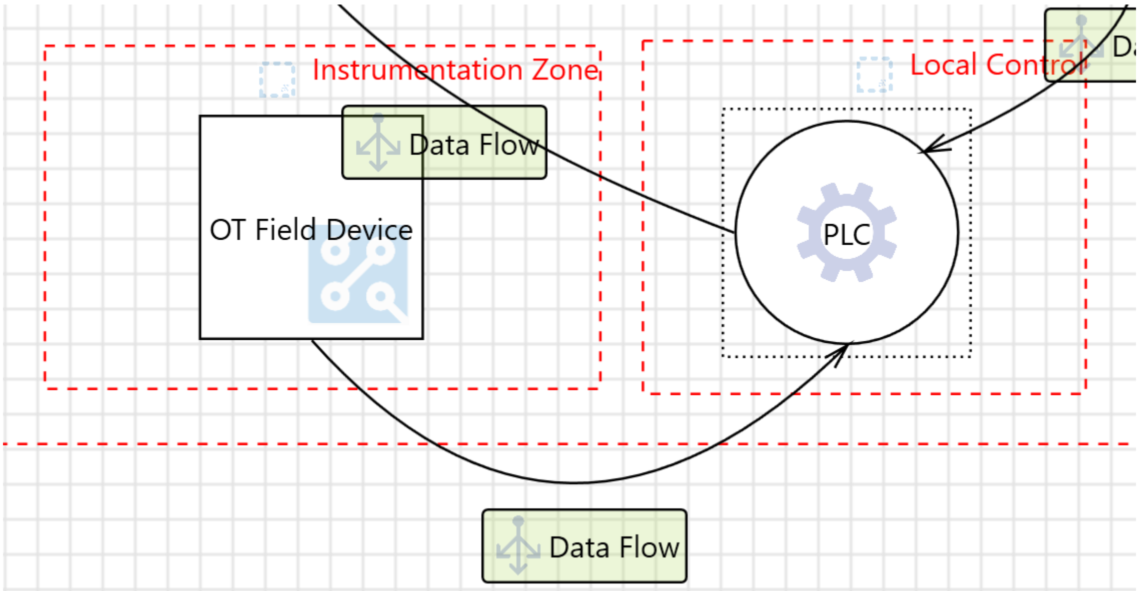

Figure 15: OT Field Device to PLC

Figure 15 depicts a data flow between an OT field device and a Programmable Logic Control (PLC). The field device is placed in Level 0 of the Purdue Model (Instrumentation Zone) and PLC in Level 1 (Local Control).

An adversary may spoof OT Field Device with a fake one.

Category:	Spoofing
Description:	An adversary may replace the OT Field Device or part of the OT Field Device with some other OT Field Device
Mitigation:	Ensure that devices connecting to Field or Cloud gateway are authenticated.

An adversary may exploit known vulnerabilities in unpatched devices.

Category:	Tampering
Description:	An adversary may leverage known vulnerabilities and exploit a device if the firmware of the device is not updated
Mitigation:	Ensure that the gateway implements a process to keep the connected devices firmware up to date

An adversary may execute unknown code on PLC.

Category:	Tampering
Description:	An adversary may launch malicious code into PLC and execute it
Mitigation:	Ensure that unknown code cannot execute on devices. UEFI Secure Boot restricts the system to allow the execution of binaries signed by a specified authority.

An adversary may eavesdrop on the communication between the device and the field gateway

Category:	Information Disclosure
Description:	An adversary may eavesdrop and interfere with the communication between the device and the field gateway and possibly tamper with the data that is transmitted
Mitigation:	Secure Device to Field Gateway communication. For IP-based devices, the communication protocol could typically be encapsulated in an SSL/TLS channel to protect data in transit. For other protocols that do not support SSL/TLS investigate if there are secure versions of the protocol that provide security at the transport or message layer.

An adversary may gain unauthorised access to privileged features on OT Field Device

Category:	Elevation Of Privilege
Description:	An adversary may get access to the admin interface or privileged services like Wi-Fi, SSH, File shares, FTP etc., on a device
Mitigation:	Any administrative interfaces the device or field gateway exposes should be secured using strong credentials. Also, any other exposed interfaces like Wi-Fi, SSH, File shares, FTP should be secured with strong credentials. Default weak passwords should not be used.