8.4.2 Engineering Workstation to PLC

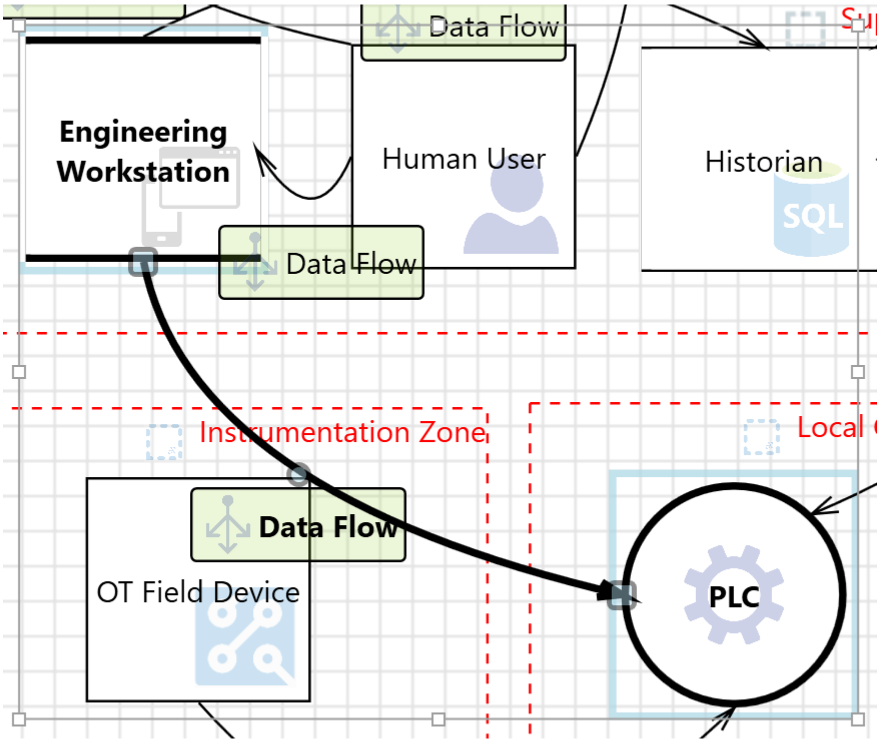

Figure 16: OT Field Device to PLC

Figure 16 depicts a data flow between an Engineering Workstation and a Programmable Logic Control (PLC). The engineering workstation is placed in Level 2 of the Purdue Model (Supervisory Zone) and PLC in Level 1 (Local Control).

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 only to allow execution of binaries signed by a specified authority. This feature prevents unknown code from being executed on the platform and potentially weakening the security posture of it. Enable UEFI Secure Boot and restrict the list of certificate authorities that are trusted for signing code. Sign all code deployed on the device using one of the trusted authorities.

An adversary can deny actions on Field Gateway due to a lack of auditing.

Category:	Repudiation
Description:	An adversary may perform actions such as spoofing attempts, unauthorised access etc., on the Field gateway. It is important to monitor these attempts so that adversaries cannot deny these actions
Mitigation:	When multiple devices connect to a Field Gateway, ensure that connection attempts and authentication status (success or failure) for individual devices are logged and maintained on the Field Gateway. Also, in cases where Field Gateway maintains the OT Hub credentials for individual devices, ensure that auditing is performed when these credentials are retrieved. Develop a process to periodically upload the logs to storage for long term retention.