8.4.3 Historian to PLC

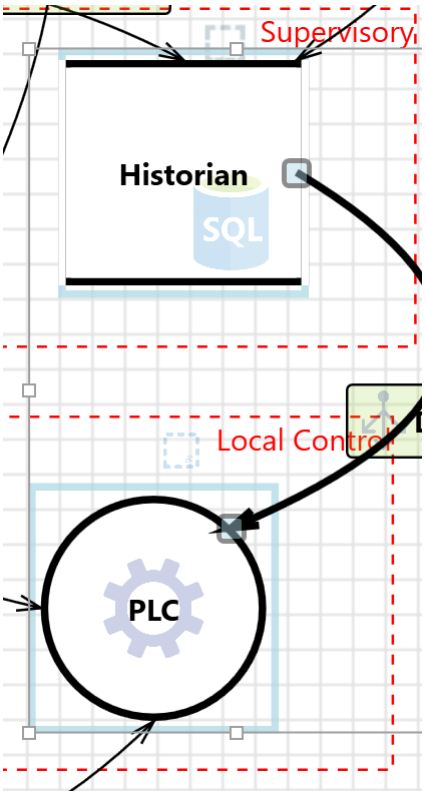

Figure 17: Historian to PLC

Figure 17 depicts a data flow between a Historian 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). The historian's primary function is to capture and retain large volumes of real-time data from various sources, such as sensors, meters, controllers, and other devices deployed in the industrial environment. This data includes measurements, events, alarms, and other relevant information. The historian organises and indexes the data in a structured manner, allowing for efficient retrieval and analysis.

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 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.