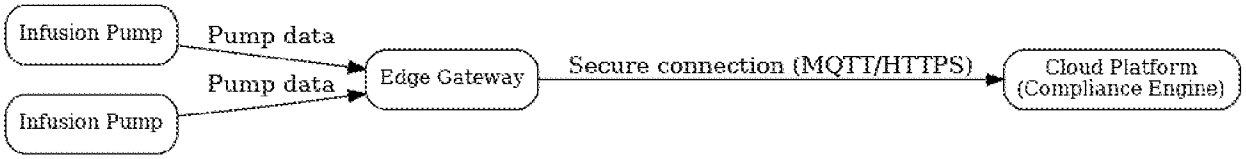
Figures


Infusion Pump
Pump data
Infusion Pump
Pump data
Edge Gateway
Secure connection (MQTT/HTTPS)
Cloud Platform
(Compliance Engine)

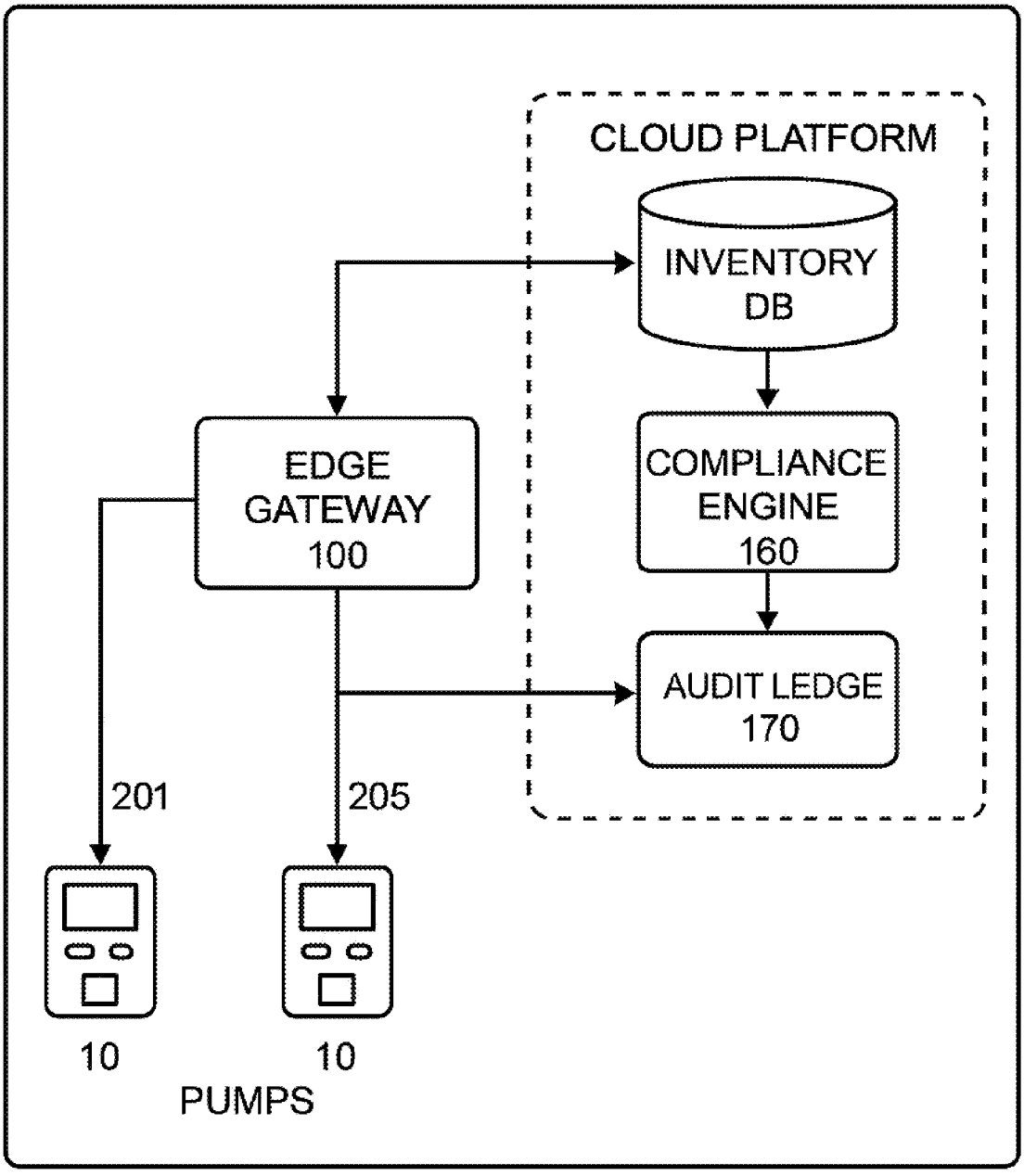
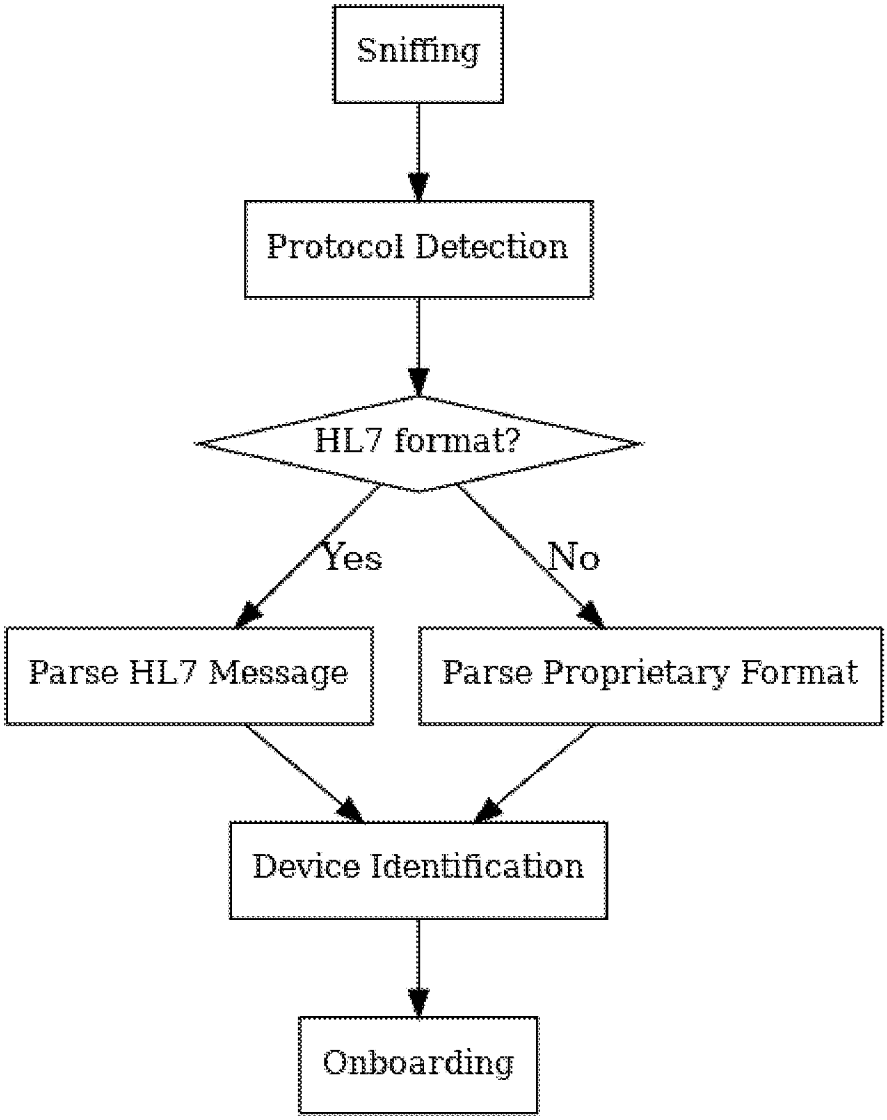


FIG. 1 – System Architecture

Figure 1: Schematic architecture of the plug-and-play infusion pump monitoring system. An **Edge Gateway** is connected to multiple **Infusion Pumps** and relays data to a **Cloud Platform** that hosts the compliance engine. The gateway passively "sniffs" each pump's data (e.g. HL7 messages or proprietary packets) without disrupting normal operation, then forwards the normalized pump data over a secure MQTT/HTTPS connection to the cloud for centralized inventory and compliance management. This design enables plug-and-play integration of diverse pumps and maintains a live inventory in the cloud for compliance tracking.


Sniffing
Protocol Detection
HL7 format?
Yes
No
Parse HL7 Message
Parse Proprietary Format
Device Identification
Onboarding

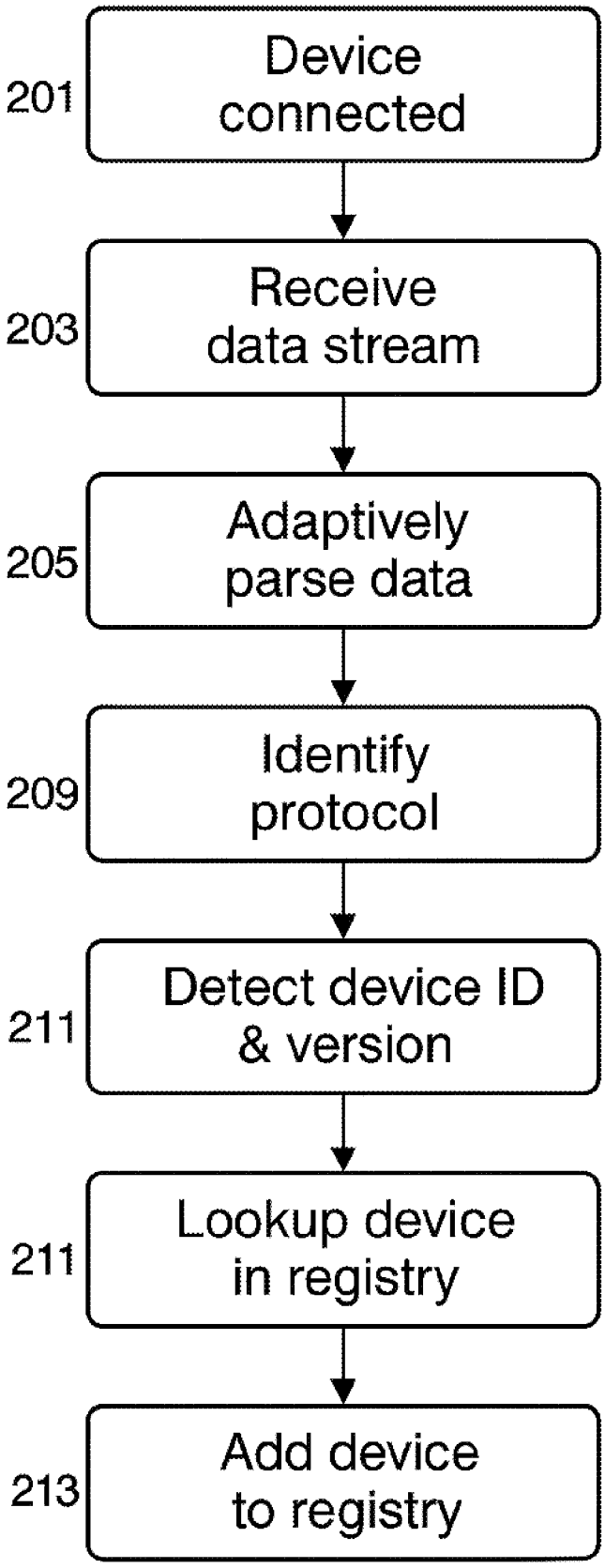
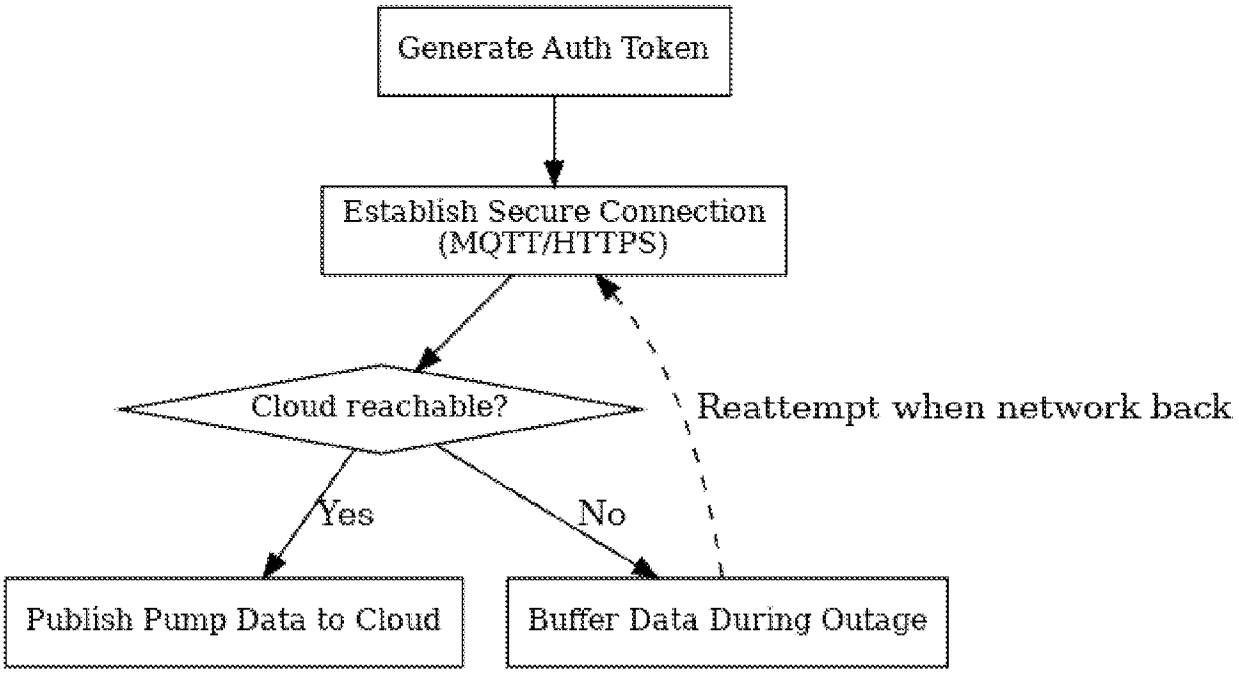


FIG. 2A – Flowchart–automatic pump-

Figure 2A: Flowchart of the automatic pump detection process in the edge gateway. When a new infusion pump is connected, the gateway **sniffs** the incoming data stream and runs **protocol detection** logic. A decision step checks if the data matches an **HL7 format** (Yes path); if so, the gateway parses the HL7 message. If not (No path), the system tries a **proprietary format** parser for the pump's data. Once the communication protocol is recognized and the message parsed, the gateway extracts the pump's identity and configuration (**device identification**), determining the model and firmware version. The pump is then **onboarded** into the system – the gateway creates a device record and announces the new pump to the cloud inventory, all without manual intervention.



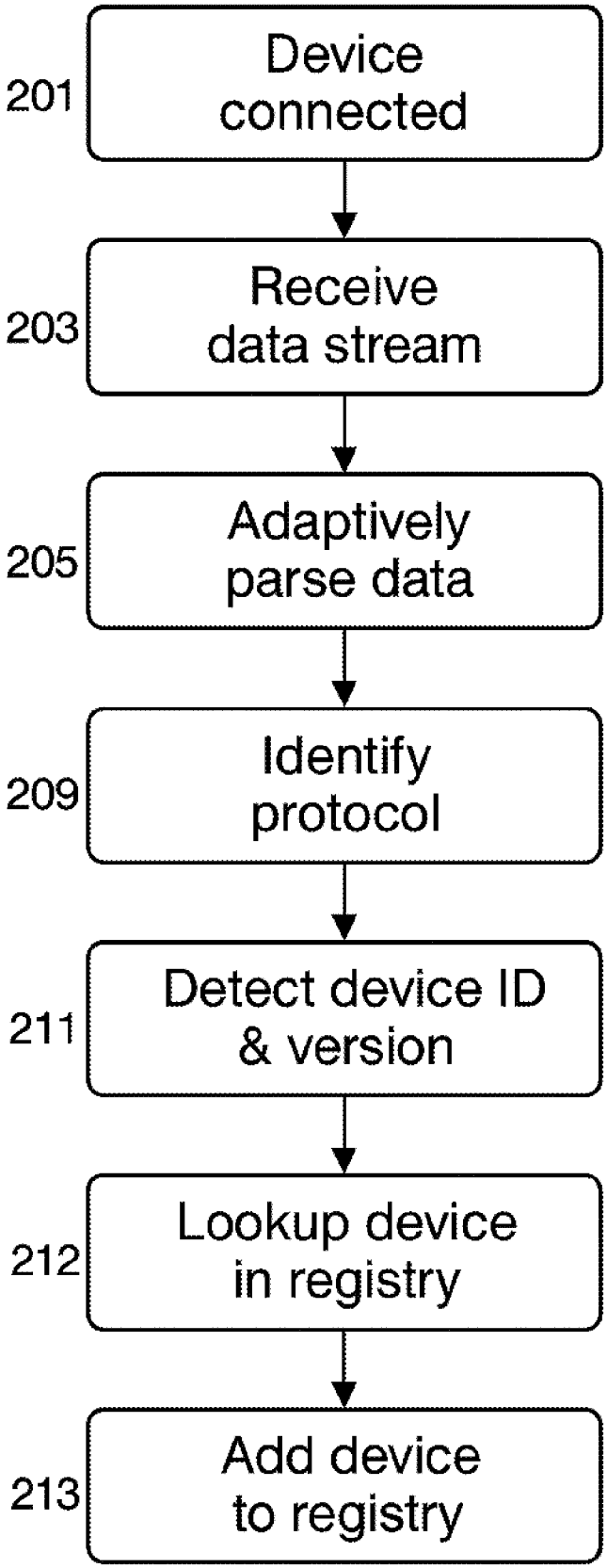


FIG. 2A Flowchart—automatic pump-detection and onboarding in the gateway

Figure 2B: Continuation of the flowchart for initiating secure communication (after device identification in Fig. 2A). The gateway **generates an authentication token** (e.g. a JWT) to securely identify itself, then **establishes an encrypted MQTT/HTTP session** with the cloud. Next, it begins streaming the pump's data upstream (**publish pump data**). A network check ensures the cloud is reachable: if **Yes**, data flows to the cloud in real time; if **No**, the gateway will **buffer data during the outage** and automatically reattempt the connection when network is restored. This fail-safe design guarantees no data is lost during connectivity drops – buffered events are sent once the secure link is re-established, and the gateway's passive tap does not interfere with the pump's operation.

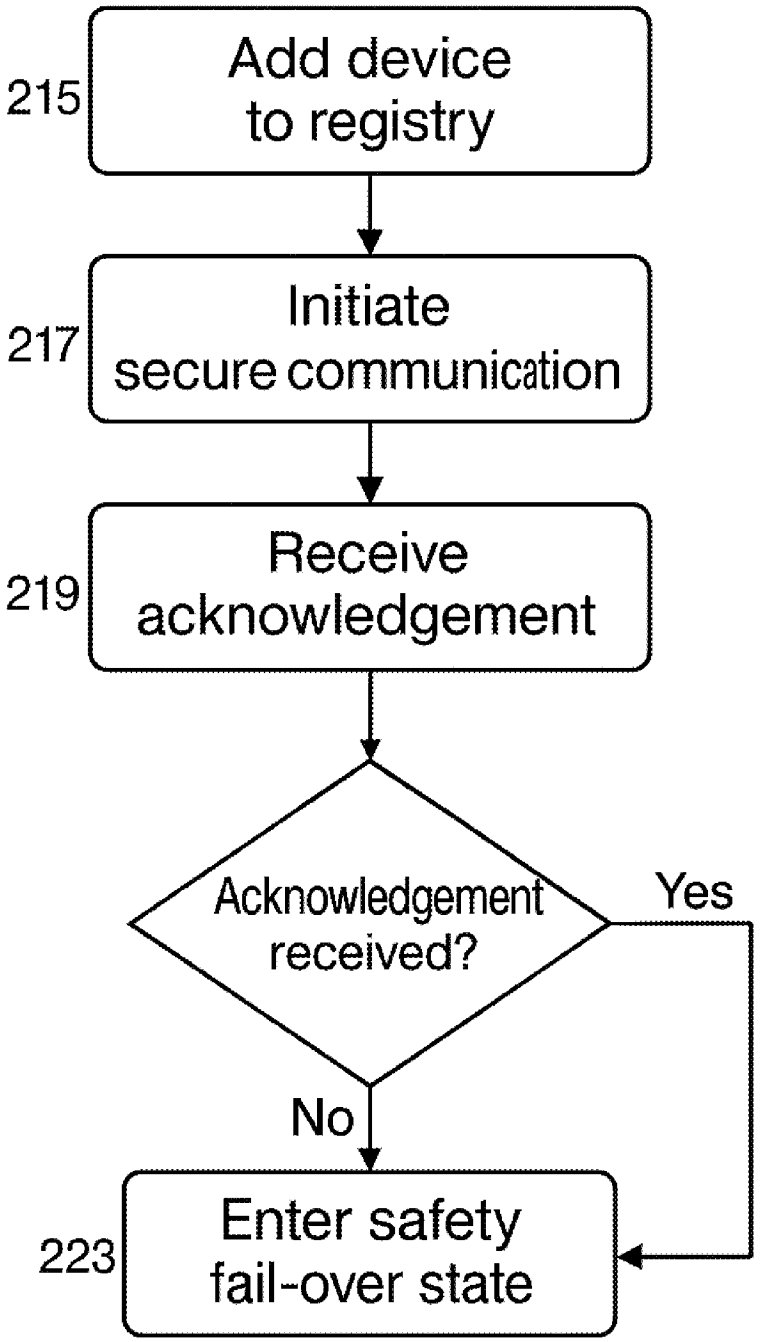


FIG. 2B Continuation of FIG. 2A, detailing secure-communication initiation and safety fail-over steps

Figure 3A: Example cloud-maintained inventory dashboard for all detected pumps. Each row represents a discovered infusion pump with fields for **Pump ID**, **Model**, **Firmware Version**, **Library Checksum** (drug library version identifier), **Last Seen** timestamp, and **Compliance Status**. In this schematic table, pumps are listed along with their key configuration data – for instance, Pump 1234 is an Alaris GX on firmware v1.2.3 with a specific library file checksum. The system updates this inventory in real time as pumps connect or change state, and flags any compliance issues (e.g. an outdated drug library or firmware) in the status column. This live inventory replaces manual audits, giving administrators an up-to-date view of device configurations across the fleet.

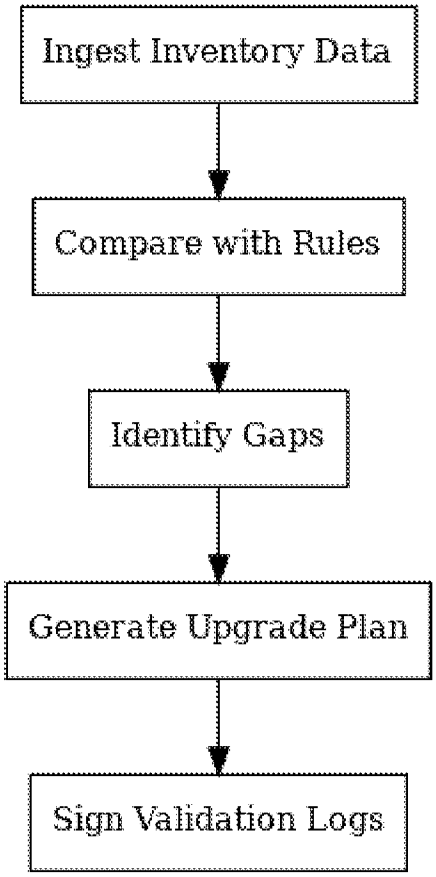
Pump ID	Model	Firmware Version	Library Checksum	Last Seen	Compliance Status
1234	Alaris GX	v1.2.3	XYZ123	Dec 10 2025 17:00	Library Outdated
5678	Alaris GX	v1.2.3	XYZ123	Dec 10 2025 16:55	Compliant
9012	Pump-ModelY	v2.1.0	ABC987	Dec 10 2025 16:30	Firmware Outdated

DEVICE-ID	MODEL	FIRMWARE	PROTOCOL	DRUG-LIBRARY CHECKSUM	COMPLIANCE FLAG
12345678	PumpX-1000	1.2.3	HL7	A6B2	Yes
23456789	PumpX 2000	1.4.0	SOAP	D4E3	No
34567890	PumpY-500	3.1.7	HL7	D4E3	Yes
45678901	PumpZ 300	2.0.5	SOAP	2024-01-01 14:35	Yes
45678901		2.0.5	SOAP	2024-01-02 08:59	Yes

FIG. 3A Example cloud inventory dashboard/ DB schema for every detected pump

Figure 3A: Example cloud-maintained inventory dashboard for all detected pumps. Each row represents a discovered infusion pump with fields for **Pump ID**, **Model**, **Firmware Version**, **Library Checksum** (drug library version identifier), **Last Seen** timestamp, and **Compliance Status**. In this schematic table, pumps are listed along with their key configuration data – for instance, Pump 1234 is an Alaris GX on firmware v1.2.3 with a

specific library file checksum. The system updates this inventory in real time as pumps connect or change state, and flags any compliance issues (e.g. an outdated drug library or firmware) in the status column. This live inventory replaces manual audits, giving administrators an up-to-date view of device configurations across the fleet.



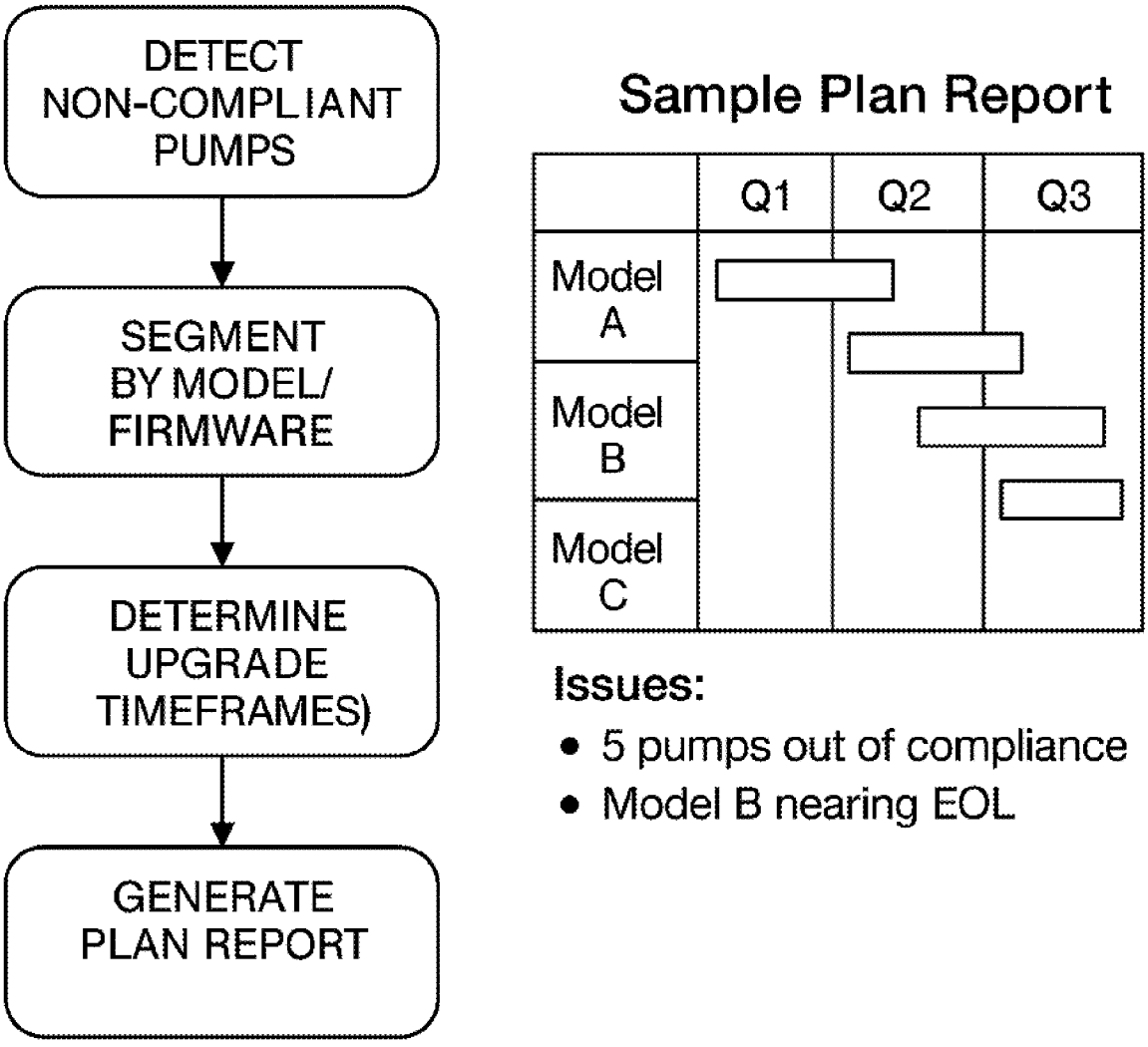


FIG. 3B Compliance-analysis & staged-upgrade planning workflow

Figure 3B: Workflow for compliance analysis and upgrade planning. The cloud's compliance engine **ingests the inventory data** of all pumps (step 301) and **compares** each entry **with defined rules** and reference standards (step 303). It **identifies gaps** or non-compliance issues, such as pumps with outdated firmware or library (step 305), and then **generates an upgrade plan** (step 307) with prioritized remedial actions. For example, it may schedule firmware updates for high-risk units first or group updates by care area. After execution of upgrades, the system produces **signed validation logs**, cryptographically verifying that each pump was updated and compliant. This end-to-end

process ensures the entire pump fleet is kept in line with the latest safety requirements, with an auditable trail of all changes.