Federated Learning als Optimierer für Embedded-KI

Damit Embedded-KI lange Freude macht

Embedded-KI setzt sich in der Industrie zunehmend durch. Dafür sorgt nicht zuletzt die Möglichkeit, kleinere KI-Modelle lokal zu etablieren und so Lösungen mit günstigem Preis-Leistungs-Verhältnis und hoher Datensicherheit zu schaffen. Doch um auf Dauer optimal zu funktionieren, brauchen diese Modelle »Nachhilfe« – und Federated Learning kann sie geben. Was dabei zu beachten ist. Von Oliver Roth

Im Fertigungsprozess zählt Tempo: Wenn an Maschinen Veränderungen bei Klängen und Geräuschen, Schwingungen oder Temperatur detektiert werden – genügend Sensoren vorausgesetzt –, dann ist schnelle Reaktion gefragt. Daten an Server im Ausland zu schicken und Empfehlungen oder Entscheidungen großer zentraler KI-Modelle abzuwarten, ist dann nicht die beste Option – und zwar unabhängig von der Kostenseite und möglichen Sicherheitsbedenken. Erstrebenswert ist stattdessen eine lokale KI-Instanz, die Empfehlungen oder Entscheidungen in Echtzeit liefert.

Aktuelle Embedded-Controller sollten nicht nur KI-Modelle zur Anomalieerkennung beherrschen, sondern auch weitergehende Aufgaben auf der Edge-Ebene bewältigen, etwa eine KI-basierte prädiktive/reglerische Optimierung (z.B. optimierte Setpoints, geringerer Verschleiß oder stabilere Toleranzen). Diesen Anforderungen werden heutige ARM-Plattformen meist problemlos gerecht, speziell wenn es sich wie beim »Universal Controller« von Grossenbacher Systeme um Carrierboard/SoM-Designs handelt. Problematischer sind Geräte auf Basis von Mikrocontrollern. Sie können zwar ausreichen, kommen durch einen anderen Aspekt aber schnell an ihre Grenzen.

Lokales Lernen fordert die Hardware

Denn der unvermeidliche Modelldrift oder Umgebungsdrift samt Verschlechterung der KI-Ergebnisse verlangt nach einem Instrument, das die Optimierung der KI-Modelle in den Controllern im Feld ermöglicht. Genau das leistet Federated Learning (FL), ein Verfahren, bei dem mehrere Geräte oder Standorte ein gemeinsames KI-Modell trainieren, ohne ihre Rohdaten zu teilen.

Um FL mit in die Controller integrieren zu können, ist neben zusätzlichem Speicher eine gewisse Performance-Reserve erforderlich, damit die FL-Software funktioniert. Dabei handelt es sich um Client-Server-Lösungen wie das KI-Framework »Flower«, dessen clientseitige Komponenten aus Sicherheitsgründen auf dem Controller in einem eigenen Container laufen sollten. Diese Komponenten managen das lokale Training und die Kommunikation mit einem (Remote-)Server und bieten diverse Funktionen, darunter lokales Data Handling für strikte »Privacy by Design«, »Computation« (Lernen) des Modells mit optimierten Algorithmen, lokale Modell-Updates, sichere Kommunikation mittels kryptografischer Verfahren (z.B. TLS/SSL) sowie ein Monitoring und die Erfassung von Metriken zur globalen Qualitätssicherung.

Zwar sind Lösungen möglich, die dedizierte Edge-Gateways – üblicherweise selbst auf ARM-Basis – als Ebene oberhalb der Geräte auf Basis von Mikrocontrollern (MCU) einziehen und die Funktionen des FL-Clients dort ansiedeln, aber deren Wirtschaftlichkeit und Zukunftssicherheit erscheinen zumindest diskutabel.

Lokal trainieren, global profitieren

Doch zurück zum Federated Learning: Statt Rohdaten in die Cloud zu schicken, lernt das Modell dabei direkt im – dazu befähigten – Controller und optimiert dabei Parameter, etwa Weights und Setpoints. Das bringt drei Vorteile im Kontext industrieller Anwendungen:

➔ **Reaktionsgeschwindigkeit:** Feedbackschleifen innerhalb von Sekunden.

➔ **Datensouveränität:** Rohdaten bleiben beim Betreiber.

➔ **Betriebssicherheit:** Netzstörungen gefährden den Betrieb nicht, weil Updates nachgeholt werden können.
Um dies zu erreichen, erfolgt das Training der KI-Modelle lokal in kleinen, robusten Lernzyklen, sogenannten Epochen. Dabei werden nur die nötigen Parameter zwischengespeichert, um Speicher- und Rechenressourcen zu schonen. Eine regelmäßige Validierung gegen definierte Referenzdatensätze (»Slices«) stellt sicher, dass die Modelle trotz dezentralem Lernen konsistent und verlässlich bleiben. Im Fehlerfall lässt sich der Trainingszustand dank integrierter Rollback-Funktion gezielt zurücksetzen.
Beim Federated Learning senden die einzelnen Controller, wie beschrieben, in regelmäßigen Abständen lediglich die daraus abgeleiteten, optimierten Modellparameter an einen zentralen Aggregationsserver. Der Server fasst die dezentralen Lernschritte anschließend zu einem verbesserten Globalmodell zusammen, das wiederum an alle beteiligten Systeme zurückgespielt wird. Auf diese Weise entsteht ein kontinuierlicher, geschlossener Lernkreislauf über die gesamte Flotte hinweg. Das reduziert Übertragungskosten, wahrt Betriebs- und Prozessgeheimnisse und stabilisiert zugleich die Modellqualität.
Dieser Lernkreislauf bedingt eine dauerhaft stabile Infrastruktur für Remote-Updates zur »Modellpflege«, die Grundlage für neue Geschäftsmodelle bildet – für OEM ebenso wie für deren Entwicklungspartner. Dazu trägt auch bei, dass Updates und Telemetrie nach den Vorgaben des Cyber Resilience Act (CRA) und der Norm IEC 62443 ausgestaltet werden müssen – vom Signieren und Versionieren der Modelle bis hin zum dokumentierten Nachweis der Update-Historie.

Fazit: Mit FL zu lernfähigen Industrieprodukten

Mit der Entwicklung eines KI-Modells ist es in der industriellen Praxis längst nicht getan. Erst die kontinuierliche Pflege und Weiterentwicklung der Modelle im Feld macht KI dauerhaft nutzbar – und genau hier setzt Federated Learning an. Dieser Ansatz ermöglicht es, lernende Systeme direkt an der Maschine weiterzuentwickeln, ohne dass sensible Rohdaten das geschützte Fertigungsumfeld verlassen müssen. Für Betreiber entsteht so ein klarer Mehrwert: höhere Prozessstabilität und Qualität sowie ein Plus an Datensouveränität.
Dabei verändert FL den Blick auf die technische Basis. Es betrifft nicht nur Software, sondern ebenso die Embedded-Hardware-Architektur, die Toolchain und die gesamte Lifecycle-Pflege – von sicheren Updates über Monitoring bis hin zu Compliance-Nachweisen nach CRA und IEC 62443. In aktuellen ARM- oder Yocto-basierten Steuerungen ist FL schon heute realisierbar, sofern Rechenleistung, Speicher und die Schnittstellen zur Kommunikation entsprechend ausgelegt sind.
Darüber hinaus erfordern Embedded-KI und FL neue Projektdimensionen. KI-Modelle werden zu betreuten Systemen, und diese für dauerhaften Erfolg unentbehrliche kontinuierliche Betreuung ist die Grundlage für innovative Geschäftsmodelle weit jenseits klassischer Serviceverträge oder Update-Abonnements. Damit wird FL zu weit mehr als einer Softwaretechnologie – es entwickelt sich in der Industrie zum Inkubator für eine neue Generation lernfähiger, vernetzter Produkte und Lösungen mit klarem Endkundennutzen.
OEM, die sich frühzeitig als Anbieter solcher Produkte und Lösungen positionieren wollen, sind gut beraten, sich Partner mit Erfahrung und ganzheitlichem Ansatz zu suchen. Dieser Ansatz kann vielfältig sein – bei Grossenbacher Systeme umfasst er einen Baukasten aus Hardware, Software und Services: skalierbare Controller- und SoM-Plattformen, OS/Apps »out of the box«, sichere Updatepfade, Telemetrie – und nicht zuletzt Begleitung bei der Modellentwicklung und Pflege. Denn die ist weder eine Zusatzleistung noch ein zweiter Schritt, sondern ein »lebenslanger« integraler Bestandteil von Embedded-KI-Lösungen. ak

Ablauf von Federated Learning …

➔ Initialmodell vom Server: Ein zentrales, vortrainiertes Modell wird an alle Controller im Feld (Clients) verteilt.
➔ Lokales Training: Jedes Gerät trainiert das Modell lokal mit seinen eigenen Betriebsdaten und in kurzen Trainingszyklen.
➔ Upload der Updates: Statt Rohdaten überträgt die Maschine nur die Modell-Updates, ggf. in komprimierter oder quantisierter Form.
➔ Aggregation: Der Server fasst alle Updates zu einem verbesserten Globalmodell zusammen – meist mit der Methode FedAvg (Federated Averaging).
➔ Rückverteilung des Globalmodells: Das optimierte Modell wird versions- und signaturgesichert wieder an alle Geräte verteilt.
➔ Monitoring: Ein Monitoring-System prüft das Modell fortlaufend auf Datenabweichungen (Drift), Ausreißer (Outlier) oder vordefinierte Kennzahlen (KPIs). Bei Qualitätsrückgang erfolgt ein Rollback zur vorherigen Modellversion.

… und Vorteile von Federated Learning

➔ Robustheit – dank gesicherter Funktion selbst bei Ausfall einzelner Clients.
➔ Sicherheit – durch digitale Signatur, verschlüsselte Kommunikation und klar geregelte Zugriffsrechte (u.a.).
➔ Heterogenität – mit flexiblen Verfahren für unterschiedliche Hardware im Feld (ggf. »Personalization Layers« zur Abbildung lokaler Besonderheiten).
➔ Compliance – in Form nachverfolgbarer Dokumentation jeder Änderung am Modell (Audit-Trail) und sicherer Updates gemäß IEC 62443.
➔ Metriken – ermöglichen praxisnahe Kunden-KPIs wie Energieverbrauch, Ausschussrate oder MTBF (Mean Time Between Failures). Sie steuern, wann ein neues Modell implementiert wird.

Oliver Roth

ist CEO der Grossenbacher Systeme. (Bild: Grossenbacher Systeme)