FROM BLIND SPOTS TO RESILIENCE

SECURING CONNECTED TRANSIT OPERATIONS



MEET THE PANEL

FROM BLIND SPOTS TO RESILIENCE

Securing Connected Transit Operations

MODERATOR



Benjamin Scott

Director, Operational Technology & Critical Infrastructure

FORTINET



Jorge A. Ovando Zalapa — 01

Director of Information Technology

SANTA CRUZ METROPOLITAN TRANSIT DISTRICT



Dr. Manjit K. Sooch — 02

Director of Innovation and Technology

ALAMEDA-CONTRA COSTA TRANSIT DISTRICT



Sabah Lone — 03

Technical Solutions Consultant

VONTAS



Dr. Pretty George — 04

Executive Director and Vice President, Information Technology

LONG BEACH TRANSIT

SESSION AGENDA

FROM BLIND SPOTS TO RESILIENCE

Securing Connected Transit Operations

10:45–10:50	**WELCOME + OPENING CONTEXT** Ben Scott / Moderator	05 MIN
10:50–11:01	**SANTA CRUZ METRO** Jorge Zalapa	10+1 MIN
11:01–11:12	**AC TRANSIT** Dr. Manjit Sooch	10+1 MIN
11:12–11:23	**VONTAS** Sabah Lone	10+1 MIN
11:23–11:34	**LONG BEACH TRANSIT** Pretty George	10+1 MIN
11:34–11:49	**MODERATED PANEL DISCUSSION** Operational resilience / Cross-agency lessons	15 MIN
11:49–11:58	**AUDIENCE Q&A** Questions from the room	09 MIN
11:58–12:00	**KEY TAKEAWAYS + CLOSE** Actions to take back to your agency	02 MIN

FRIDAY / OCT 30

10:45 AM — 12:00 PM

75

MINUTES

WHAT WE'RE HERE TO PROTECT

- SERVICE CONTINUITY
- PASSENGER SAFETY
- PUBLIC TRUST

BLIND SPOTS
LIVE AT THE SEAMS.

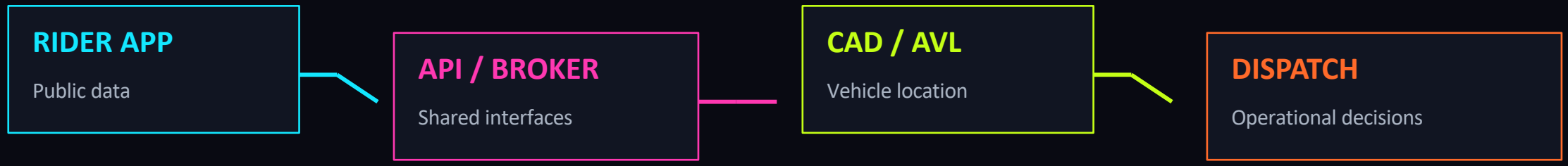
01 **DEPENDENCIES** — Passenger systems / APIs / dispatch

02 **UNMANAGED OT** — Controllers / legacy networks / edge devices

03 **VENDOR TRUST** — Remote access / cloud scheduling / managed platforms

THE INVISIBLE DEPENDENCY CHAIN

CONNECTED DOES NOT MEAN SEGMENTED



01 / DIRECT

Connect rider tools to shared transit data and services.

02 / SECOND ORDER

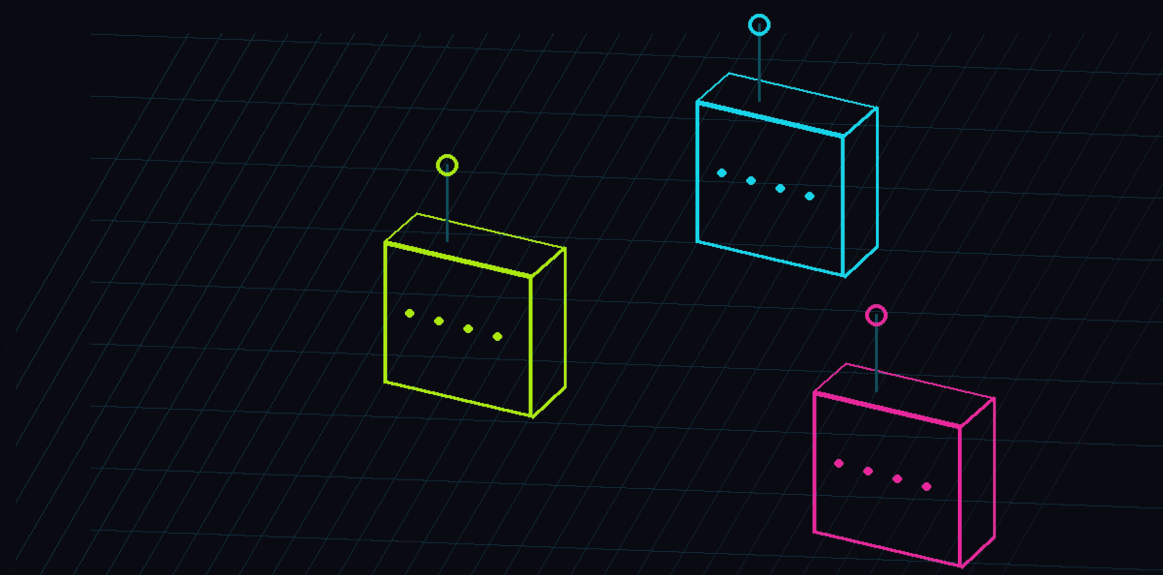
If trust boundaries fail, compromised interfaces could reach more sensitive workflows.

03 / SYSTEMIC

Operational decisions may rely on untrusted data, or isolation may remove essential rider services.

Illustrative technical cascade. Actual cases: SEPTA October 2026, LA Metro March 2026. No confirmed app-to-dispatch intrusion.

THE PATH NO ONE INVENTORIED



PLCs / MODEMS / DEPOT GATEWAYS

Every new field connection can create an access path beyond the approved architecture.

01 / DIRECT

Add remote-connected controllers and maintenance interfaces.

02 / SECOND ORDER

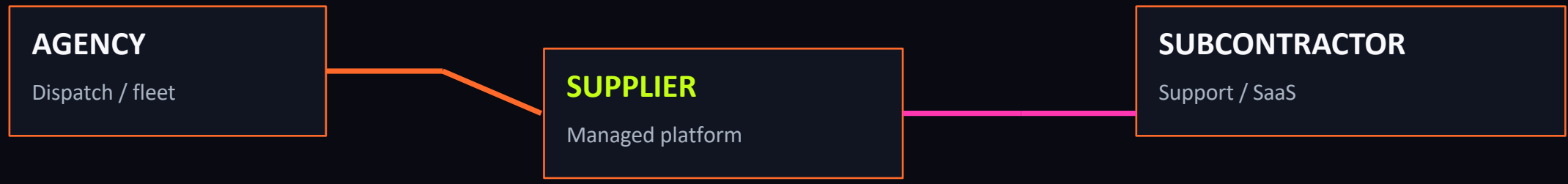
Untracked access or flat networks can bypass intended IT/OT segmentation.

03 / SYSTEMIC

Configuration loss or isolation could degrade facilities, charging throughput, and service availability.

FTA Safety Bulletin 26-02 (July 2026) and CISA OT Zero Trust guidance (Apr 2026).

THE VENDOR IS PART OF OPERATIONS



WHO CAN CONNECT? WHO CAN REVOKE ACCESS? WHO CAN RECOVER?

01 / DIRECT

Contract out scheduling, maintenance, charging, or passenger services.

02 / SECOND ORDER

Shared platforms or standing support access create dependencies beyond agency control.

03 / SYSTEMIC

A supplier incident can affect multiple agencies and stop a function even when agency IT stays clean.

May 2026 Allegany County vendor-related paratransit disruption, public reporting.

DO NOT AUTOMATE
WHAT YOU CANNOT VERIFY.

01

TRUSTED DATA

Integrity, lineage, completeness

02

TRUSTED IDENTITY

Human, service, device + agent permissions

03

SUPPLY CHAIN

Vendor, model + data dependencies

04

TRUSTED TESTING

Digital twins, adverse inputs, rollback

05

TRUSTED OPERATIONS

Monitor drift; human override; recovery

AI recommends. Authorized people remain accountable. Fail-safe paths must be designed and exercised.

NSA/CISA AI-in-OT guidance (Dec 2025).

SEVEN QUESTIONS TO ASK YOUR TEAM.

01 Which three systems would stop essential trips if unavailable for 24 hours?

02 Where can cloud, supplier, or AI services write into operational workflows?

03 Who can see and disable every vendor access path within minutes?

04 What trusted data is required to dispatch, charge, or board safely?

05 Can riders still book, pay, and receive accessible updates offline?

06 Who can override automated decisions, and where is the audit trail?

07 Have we exercised recovery of the complete rider journey?

90 DAYS TO MAKE TRUST TESTABLE.

DAYS 01–30

MAP

Name three essential services. Map AI use, suppliers, data, IT/OT paths, accessible fallback, and owners.

DAYS 31–60

CONSTRAIN

Validate read/write paths. Expire standing vendor access. Approve AI decision boundaries. Establish manual service.

DAYS 61–90

PROVE

Run a cross-modal exercise. Test rider notice, safe fallback, and return-to-service acceptance.

DELIVERABLES / DEPENDENCY MAP • ACCESS REGISTER • AI DECISION RULES • EXERCISE EVIDENCE

CLOSING THOUGHT

RESILIENCE IS MEASURED BY THE SERVICE WE CAN STILL DELIVER.



KNOW
Critical dependencies

PRACTICE
Degraded operations

VERIFY
Safe service recovery