



AI & Digital Transformation – Automating Physical Security Operations with AI

Gerry Pittman | Senior Product Manager



“If you had a security team that never got tired, never missed an alert, and responded in milliseconds.....

How would that change your security operations?”



AI & Digital Transformation

Automating Physical SOC Operations using AI

Presenter:



Gerry Pittman
Senior Product Manager
AI Solutions

Agenda

Context & Background

- Rising complexity of security

Automation in Action

- AI-Driven solutions & SOC Lifecycle

Market Requirements

- Use Cases Real-World examples

Future SOC

- Generative AI & Next-Level Automation

Key Takeaways

- Implementation & ROI Benefits





Context & Background

What is Autonomous Security Operations?

Automating manual tasks with infinite variations across

- Observation
- Interpretation
- Reaction

Performed by a system without direct human control

- Edge devices/sensors
- Systems and applications
- Operating process



Estimate of over 20 Million security personnel in physical security operation business. What could automation accomplish?

Key Problem: Manual Workload



- **Overwhelming alarms & footage**
- **Operator fatigue & missed threats**
- **Inconsistent compliance documentation**
- **Need to reduce human error & free up time**



Automation in Action

Key Opportunity: Automation & AI-Driven Efficiency

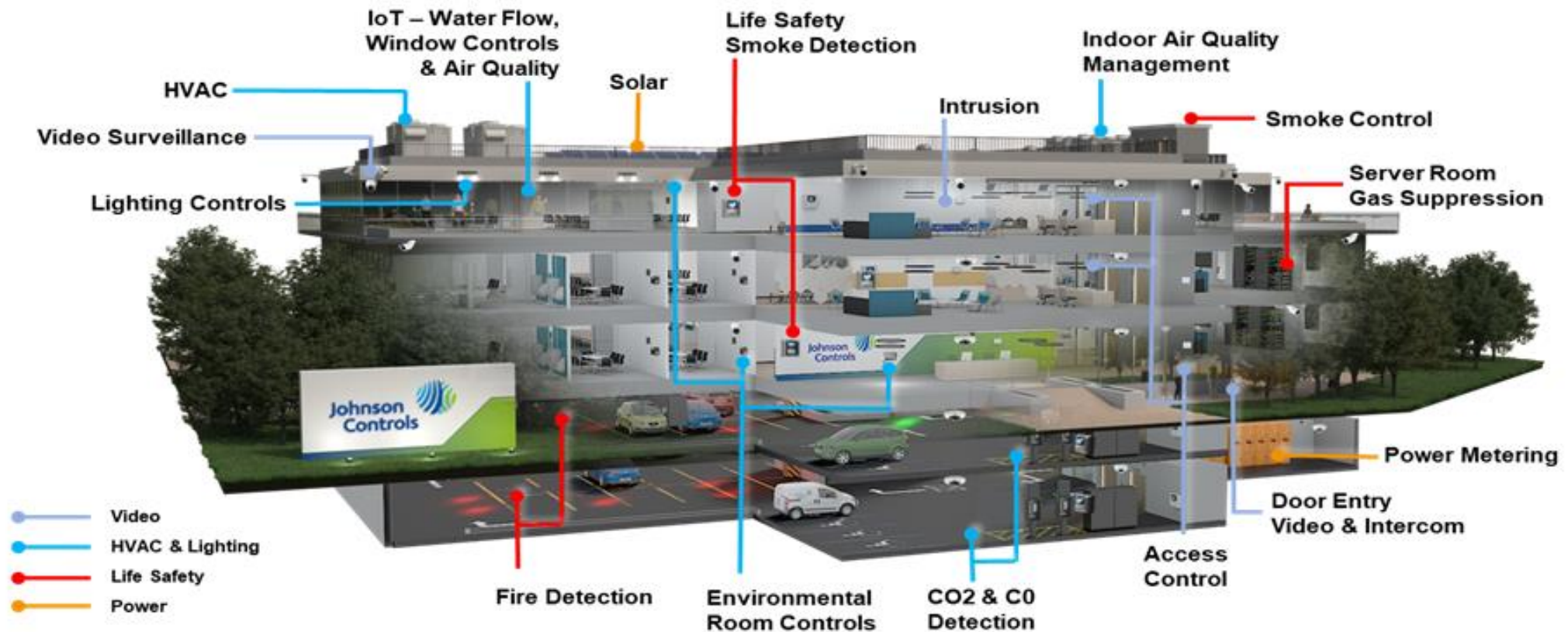
AI Strengthens the Capabilities of SOC

1. Increased situational awareness
2. Prevent before issues happen
3. Reduce False positives
4. System of Systems reducing alarm noise
5. Monitor Video Streams **even if not displayed**
6. Drives faster decisions during live/forensic search
7. Reduce operational cost and losses

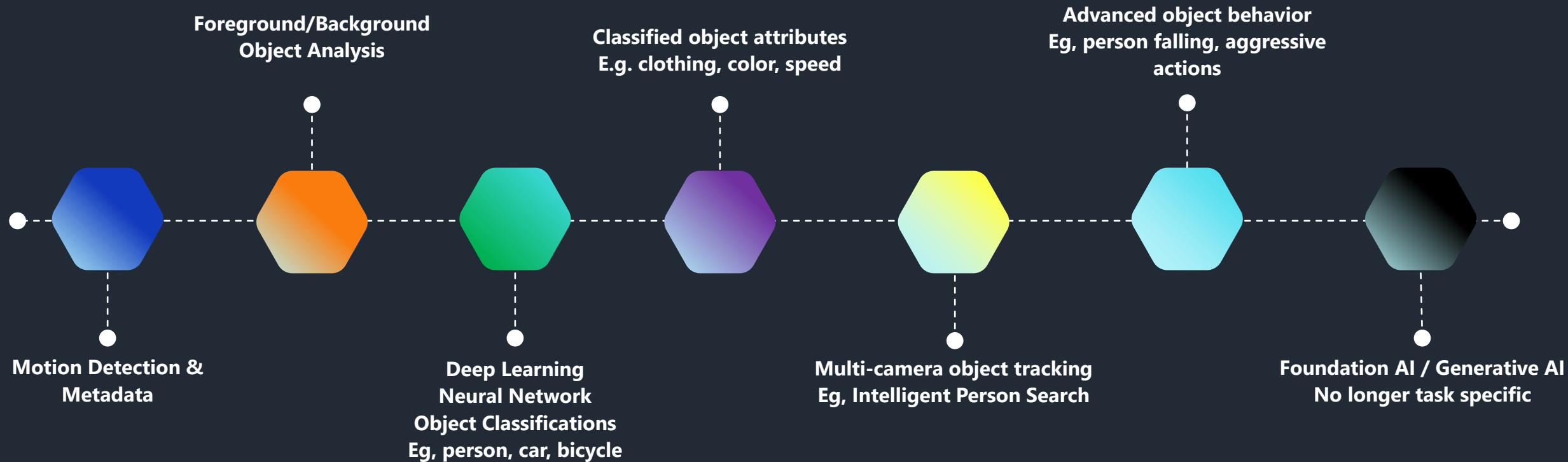


Power of AI: Protecting People & Assets at Scale

Addressing Automation with AI – Starts with Smart Edge

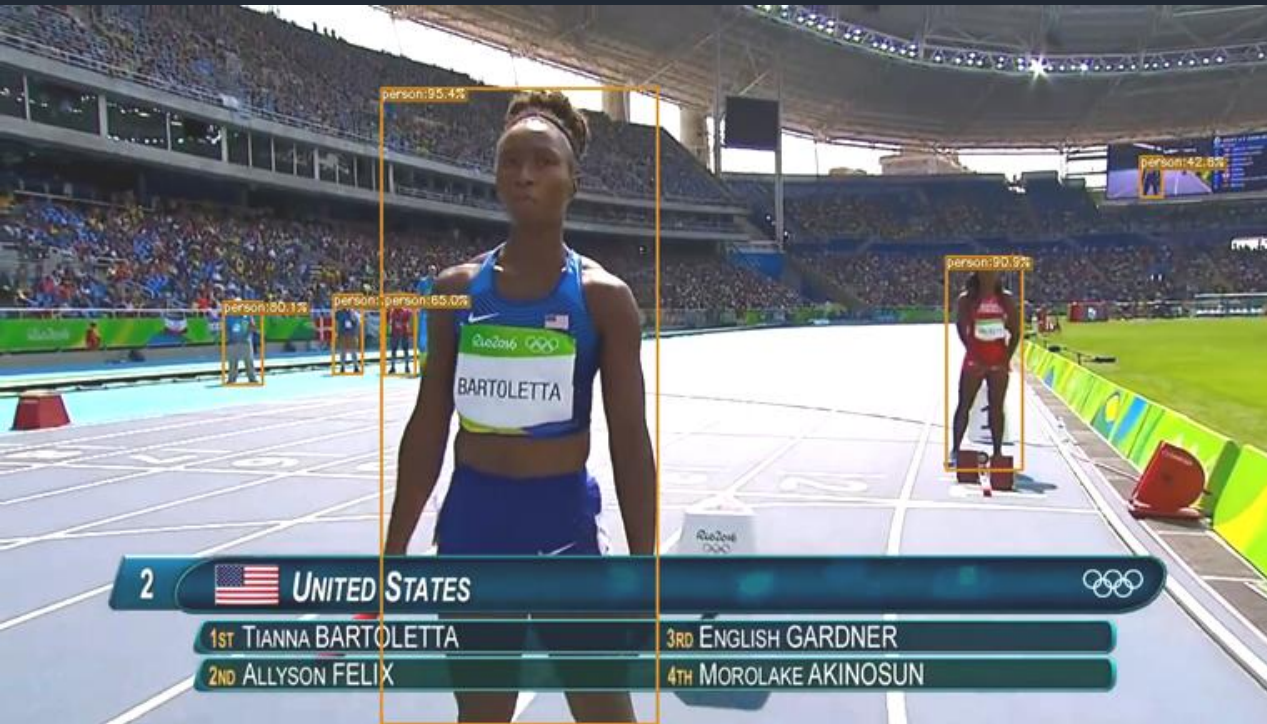


Evolution of Video Analytics



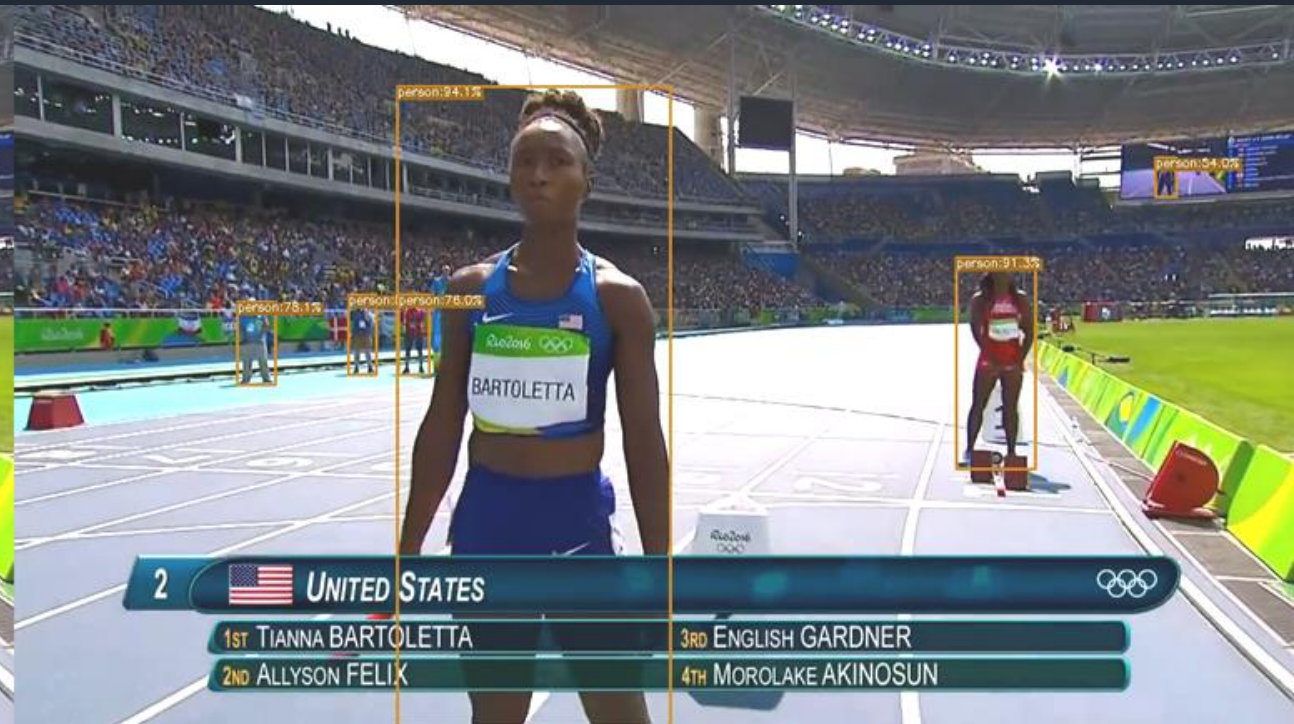
Object Detection Continues to Evolve

Object Detection Model 2023 (6%)



30% increased object
detection distance

Object Detection Model 2024 (5%)



20% more
accurate

250% more
objects in a scene

The background is a dark blue gradient with a complex network of glowing teal lines and dots, resembling a global communication or data network. A faint, wireframe-style globe is centered in the background. A horizontal teal bar spans the width of the image, serving as a backdrop for the title.

SOC Lifecycle

From Devices to Full SOC Integration

Technology / Analytics / Metadata

Value / Outcome / Experience

Building Systems & People



Access | Video | Intrusion | BMS |
Elevator | Parking | Fire Alarm |

External Data



Social Media | Weather Data |
External Threats

Sensors



Occupancy | Lighting | Acoustic |
Motion | Other

Connected Partner Program



Shooter Detection | Drones | PIAM |
Visitor Management | Other

Open API

Bi-directional building and
sensor data ingestion via
OT/IT Universal Gateways

AI-Driven Security Solutions



Detection->Analysis->Investigation->Collaboration->Response

End-to-End Workflow: Data In -> Event Resolution

AI correlates & Orchestrates, not just detects

AI automates OR assists at each phase



Data Cleansing &
Aggregation



KPIs & Analytics



Visualization &
Reporting



Policies and
Procedures

Five Phases of the SOC Lifecycle



Detection & Analysis

- AI classifies & prioritizes alerts
- Considers time, location, badge data
- Reduces false positives & highlights real threats
- Operators focus on critical events first



Investigation & Collaboration



- System compiles relevant video clips & logs
- Real-time sharing with managers, roving guards
- Speeds up evidence gathering
- Fosters consistent SOPs across large facilities

Response & Automation

- Automated doors, alerts, or escalations
- Operator oversight for final decisions
- Fast resolution times & consistent outcomes
- AI “learns” from each resolved incident



Visualizing End-to-End Automation





Understanding Market Requirements

Markets have Diverse Needs



Government

- Regulatory and Cyber Compliance
- High Assurance Visitor Management
- Complex access restrictions
- Centralized Management



Transportation

- Perimeter Security
- Complex Access Restrictions
- Public Safety & Protection
- Investment to maintain and expand



Education

- Diversity of Facilities
- Real-Time Awareness
- Need for Mass Communication
- Campus Safety & Protection



Healthcare

- Real-Time Awareness
- Patient & Staff Protection
- Service Continuity
- Asset and Privacy Protection



Critical Infrastructure

- Perimeter Security
- Remote Monitoring
- Cyber & Regulatory Compliance
- Business Continuity

Use Case: Retail Automation

- AI flags suspicious scanning & correlates POS data
- 30% reduction in internal theft
- Real-time triage of alarms & suspicious transactions
- Operations & layout optimized with analytics



Use Case: Healthcare Environment



- Patient safety: fall detection & restricted zones
- Compliance with HIPAA/regulations
- 40% faster incident response
- Automated logs & thorough incident records

How many hours a week do your security operators spend manually reviewing video clips or investigating false alarms?



Data Fusion Use Case: Multi-Building Campus



- . Fence breach + Tailgating → correlated
- . Real-time threat escalation
- . Automatic lockdown of relevant doors
- . Illustrates synergy of edge analytics + SOC platform



The Future SOC – AI Driven, Not Just AI Assisted

Future SOC's will be AI-Driven

Today

Operators assess live video systems

Monitor

Manually look for a reported incident

Review

Determine patterns and the incident

Identify

Refine the views, events, and timing

Filter

Save and Encrypt the Evidence for review

Export

Future

Autonomous Edge AI Monitoring

Automatically Assess Anomalies

Prevention, Live and Automated SOP

Security Intelligence: Rules Engine

AI Augmented Operator Experience: RPA

Future Security Platforms will be AI-Driven

- Web & mobile UX for anytime, anywhere access
- Unified security with access control, video, and intrusion
- Embedded security intelligence
- Workload automation and operator assist
- Out of the box integrations
- Cloud based deployment for scale and efficiency

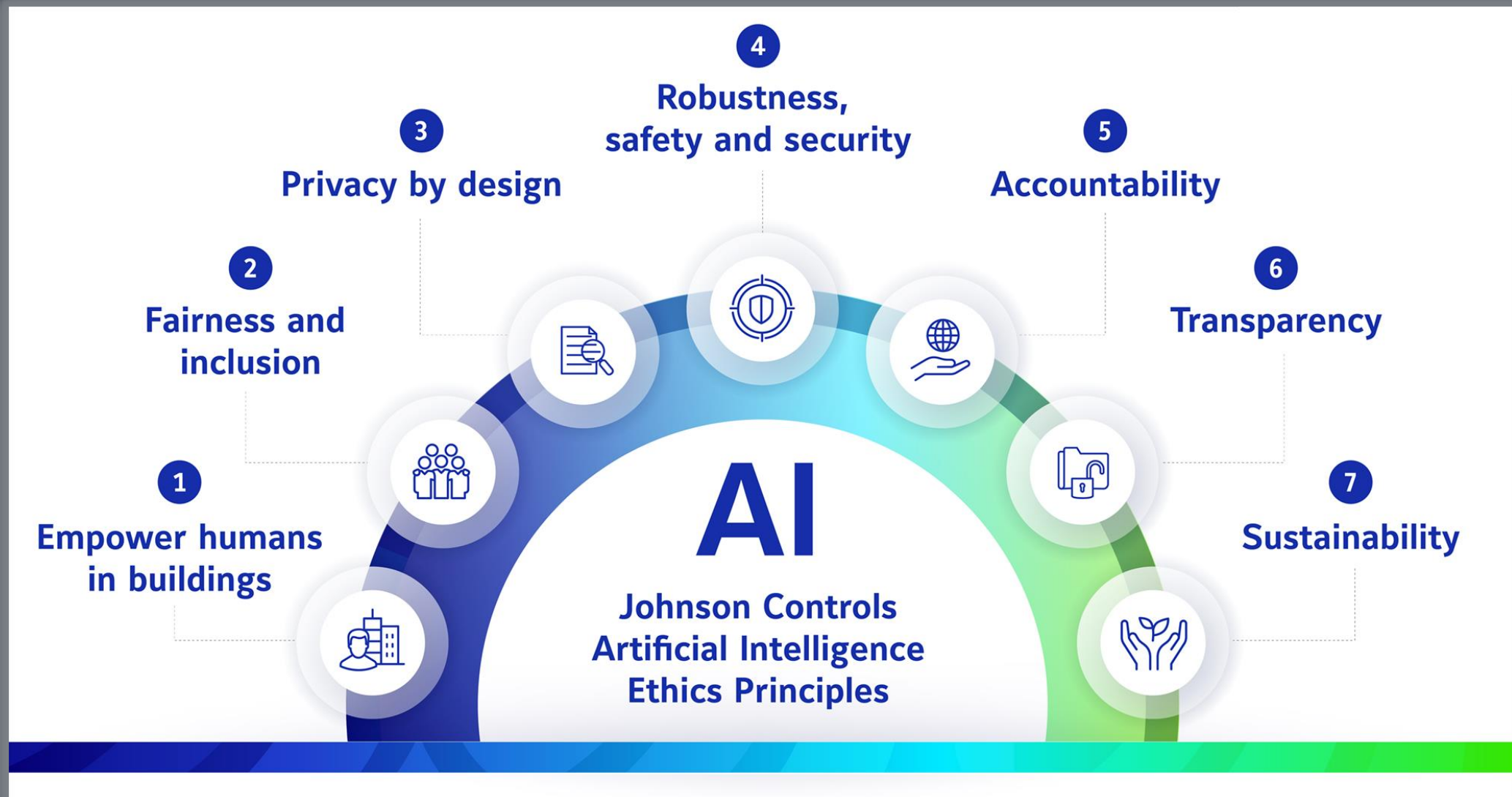


Future Technology | Foundation AI / Generative AI

- Move from Task Specific AI to supporting Multiple Domains
- Popular Foundation AI Models
 - **ChatGPT** – chatbot
 - **Microsoft Copilot** – personal assistant chatbot
 - **DALL-E** – image generation
 - **CLIP** – understanding images
- Combine vision and language AI to provide real understanding to video surveillance and more...
 - Enhance forensic searches
 - Revolutionize the types of alerts that can be generated



Ethics & Compliance



Key Takeaways

1. Edge AI for real-time, on-device processing
2. SOC Lifecycle Automation fosters efficiency
3. Generative AI can transform searches & SOPs
4. Real-World ROI: Fewer false alarms, better compliance
5. Ethics & Testing are mandatory for trust
6. Shift from Reactive to Proactive Security



Envisioning the AI-Driven Future

- Curated dashboards of priority alerts
- Natural-language video searches
- Adaptive policies for new threat patterns
- Cutting response times to seconds



Call to Action – How do I get started?

1. Assess SOC maturity & pain points
2. Explore edge device upgrades
3. Integrate core systems
4. Pilot generative AI
5. Address ethics & compliance thoroughly





Thank you!

Have thoughts about SIA Education@ISC?

Scan the QR Code on the left to provide your feedback
on SIA Education@ISC Sessions at ISC West

In partnership with
 **SIA**
EDUCATION at ISC

Built by
 **PX** In the business of
building businesses