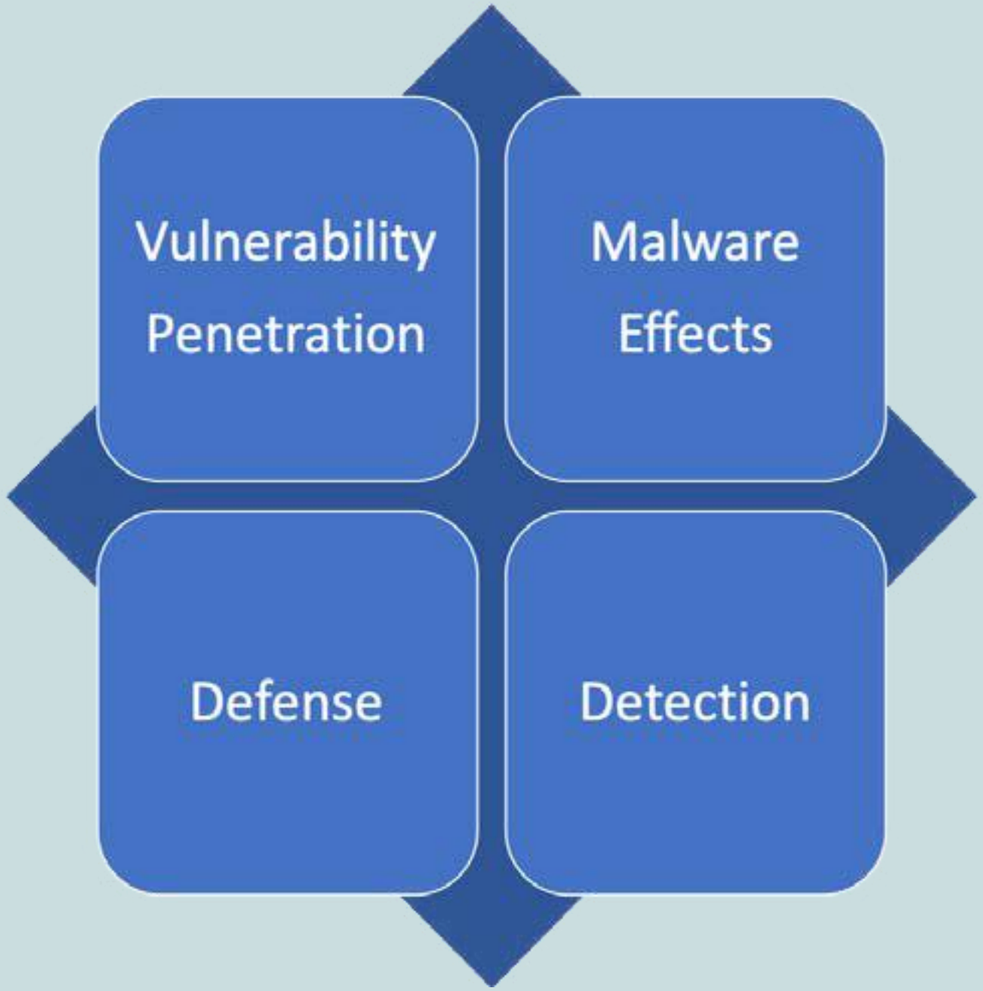
Eavesdropping, Packet Inspection & Other Wireless Sensor Cybersecurity Matters

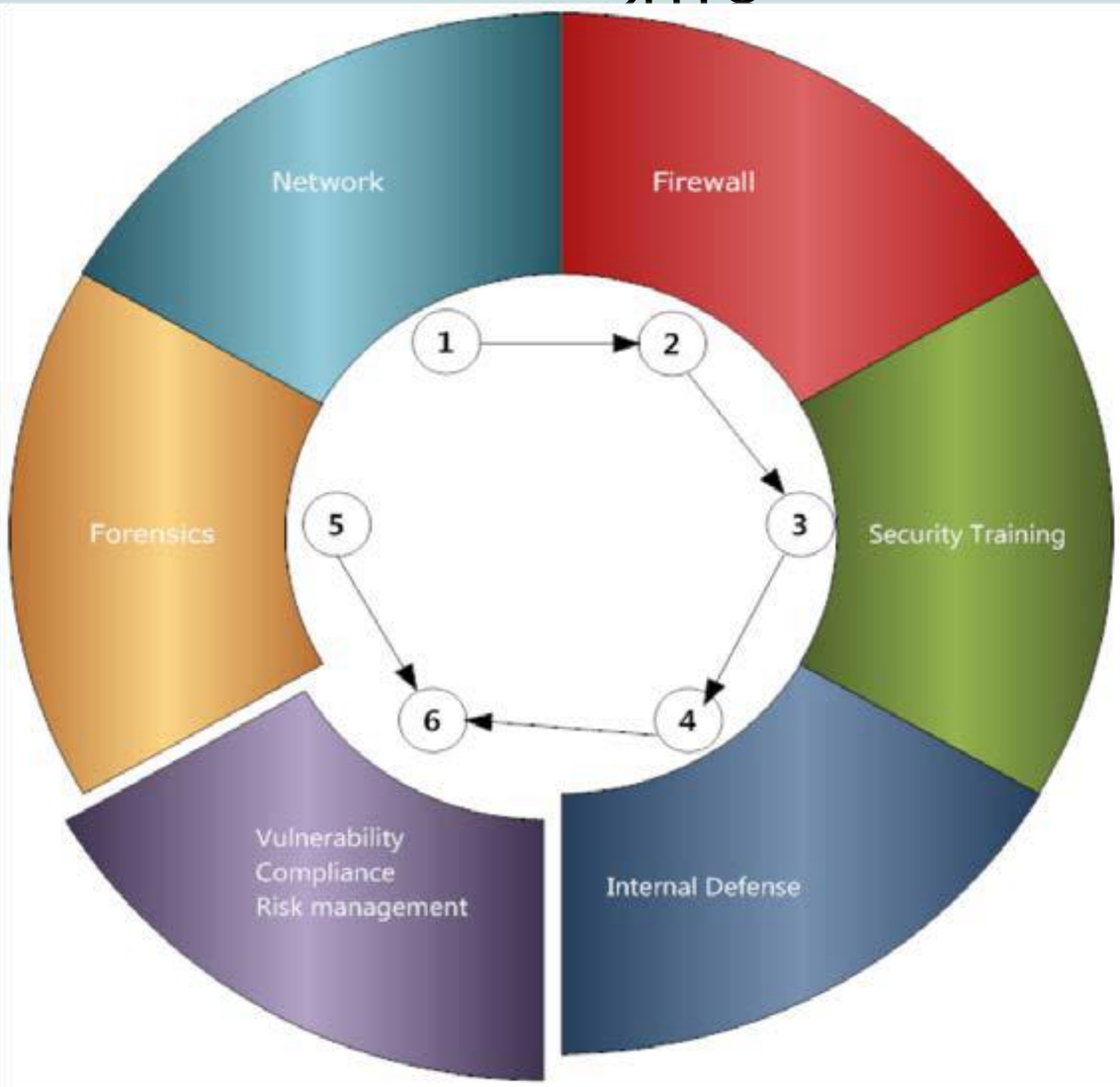
Ken Morris
KnectIQ
12 December
2018

FOUR MAJOR ASPECTS OF CYBERSECURITY

knectIQ



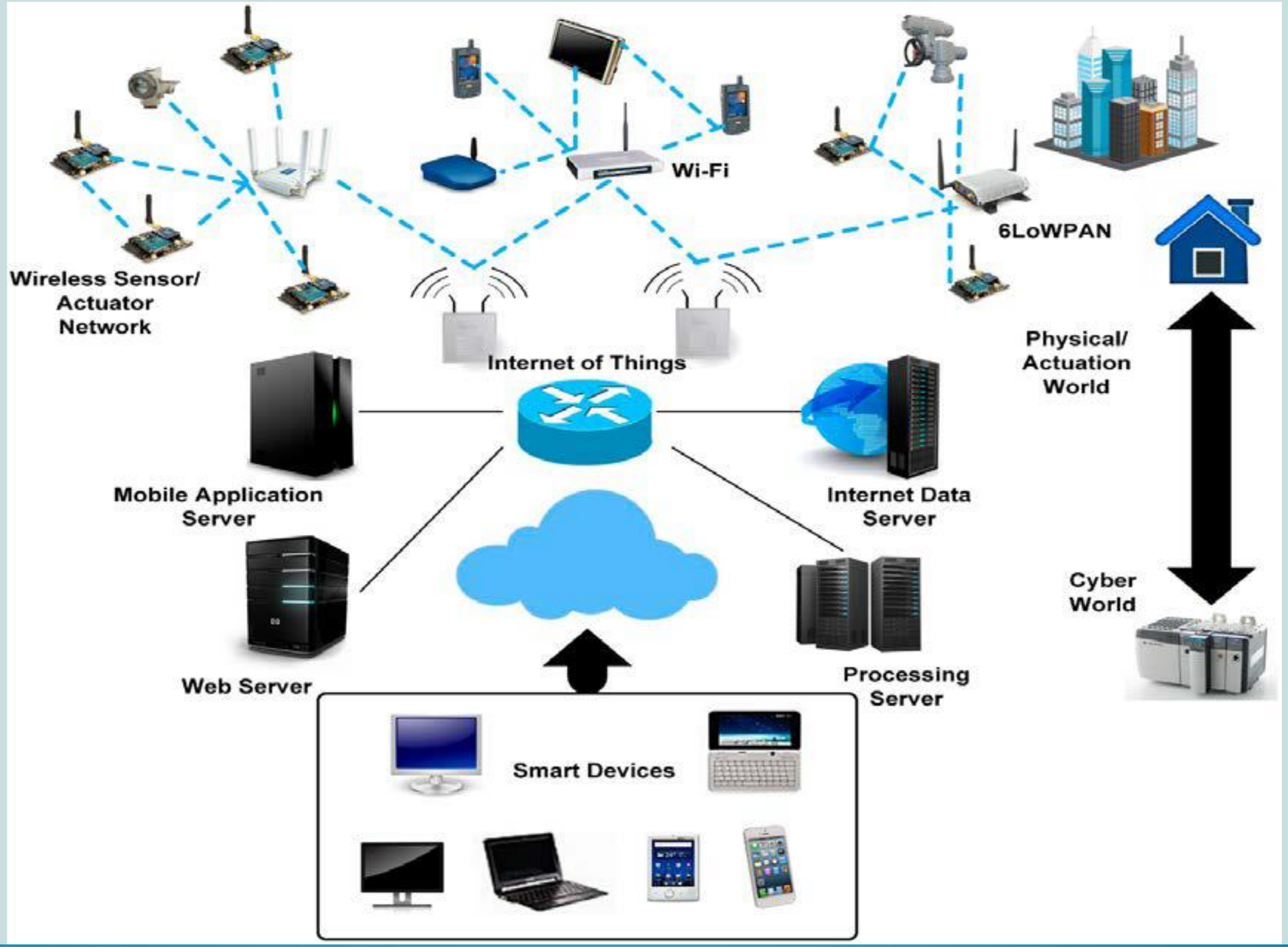
Conventional Cybersecurity - 2018



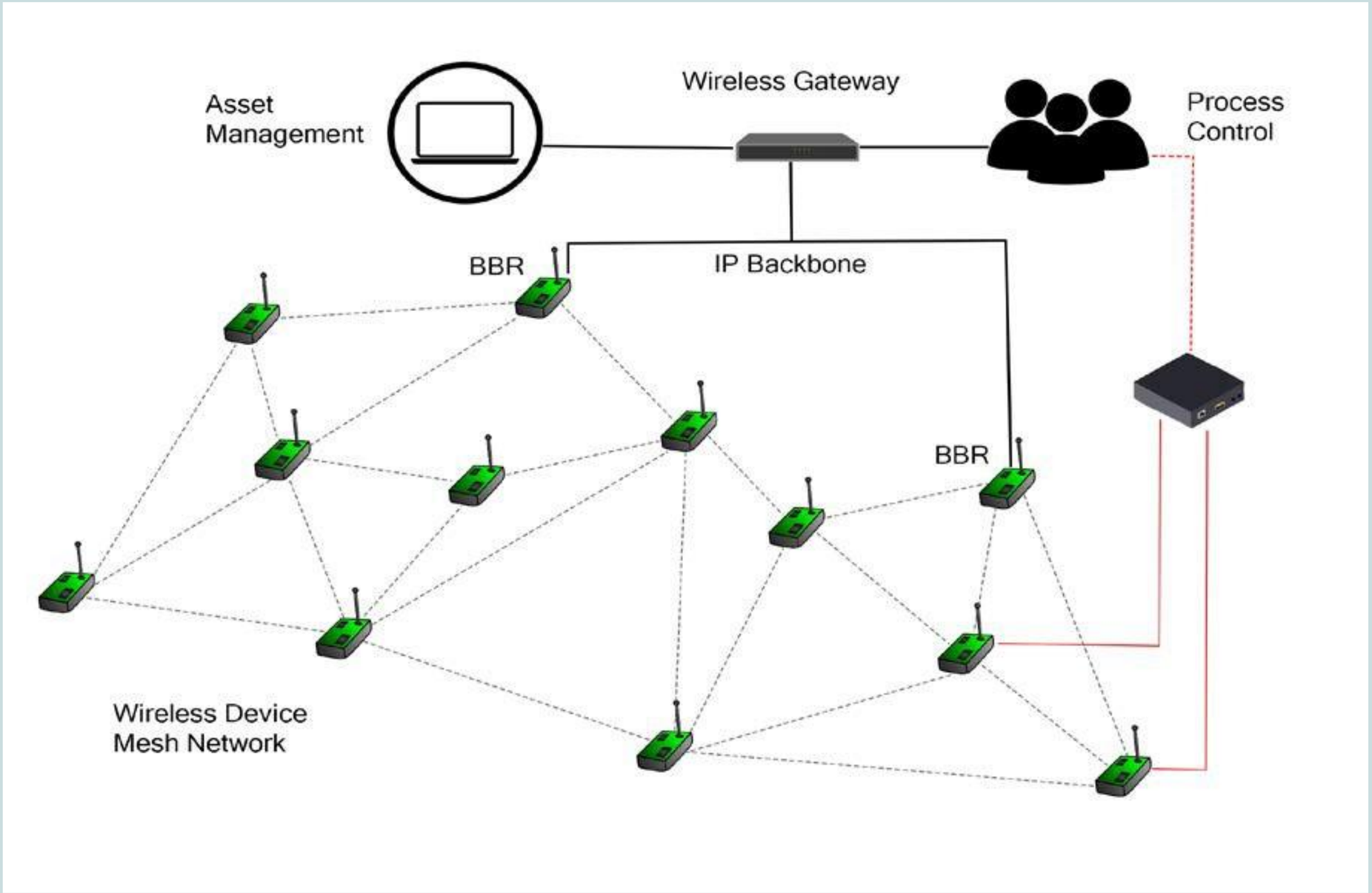
Threat Surfaces – Trust Fundamentals

- Root of Trust
- Stored Keys/Credentials

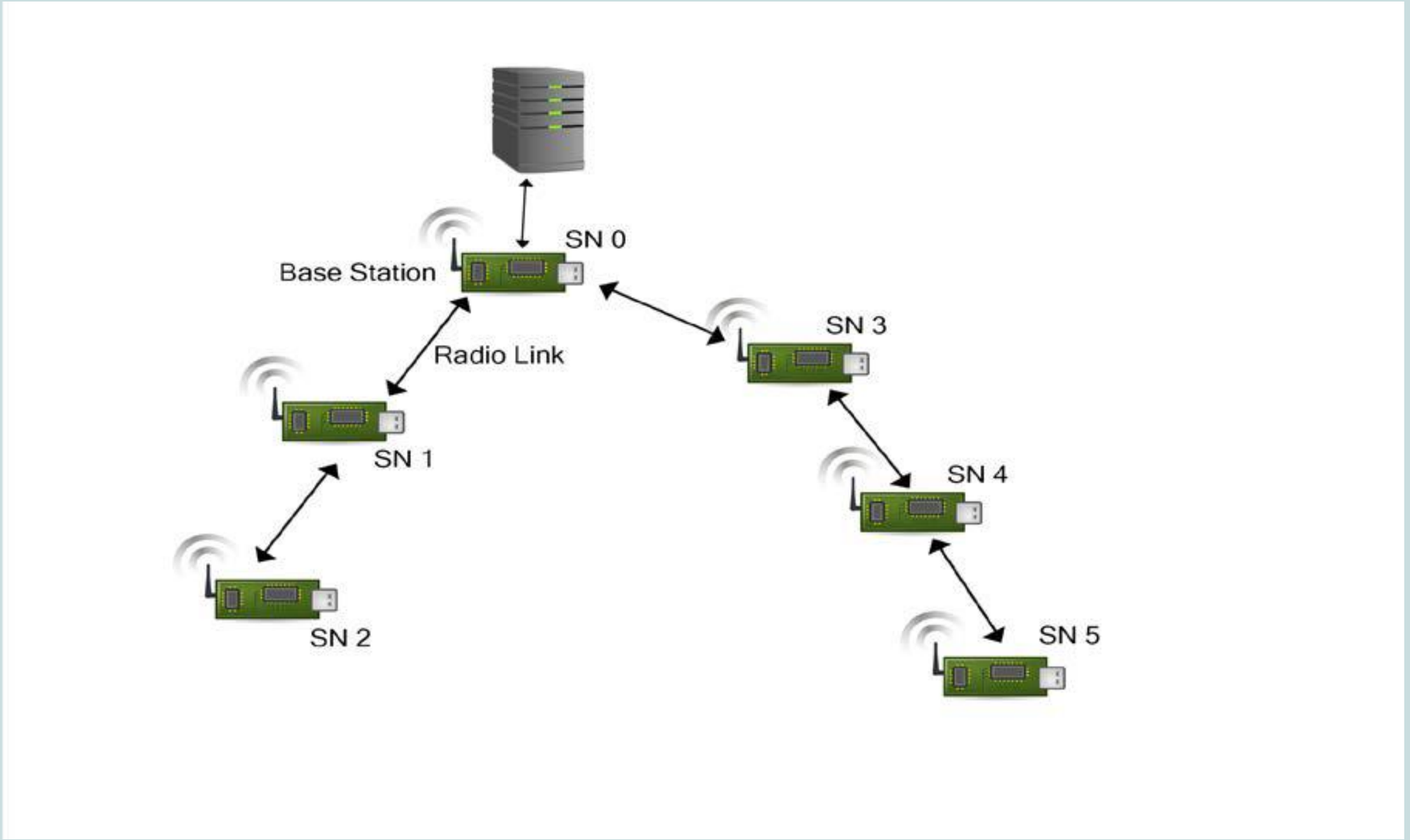
knectIQ

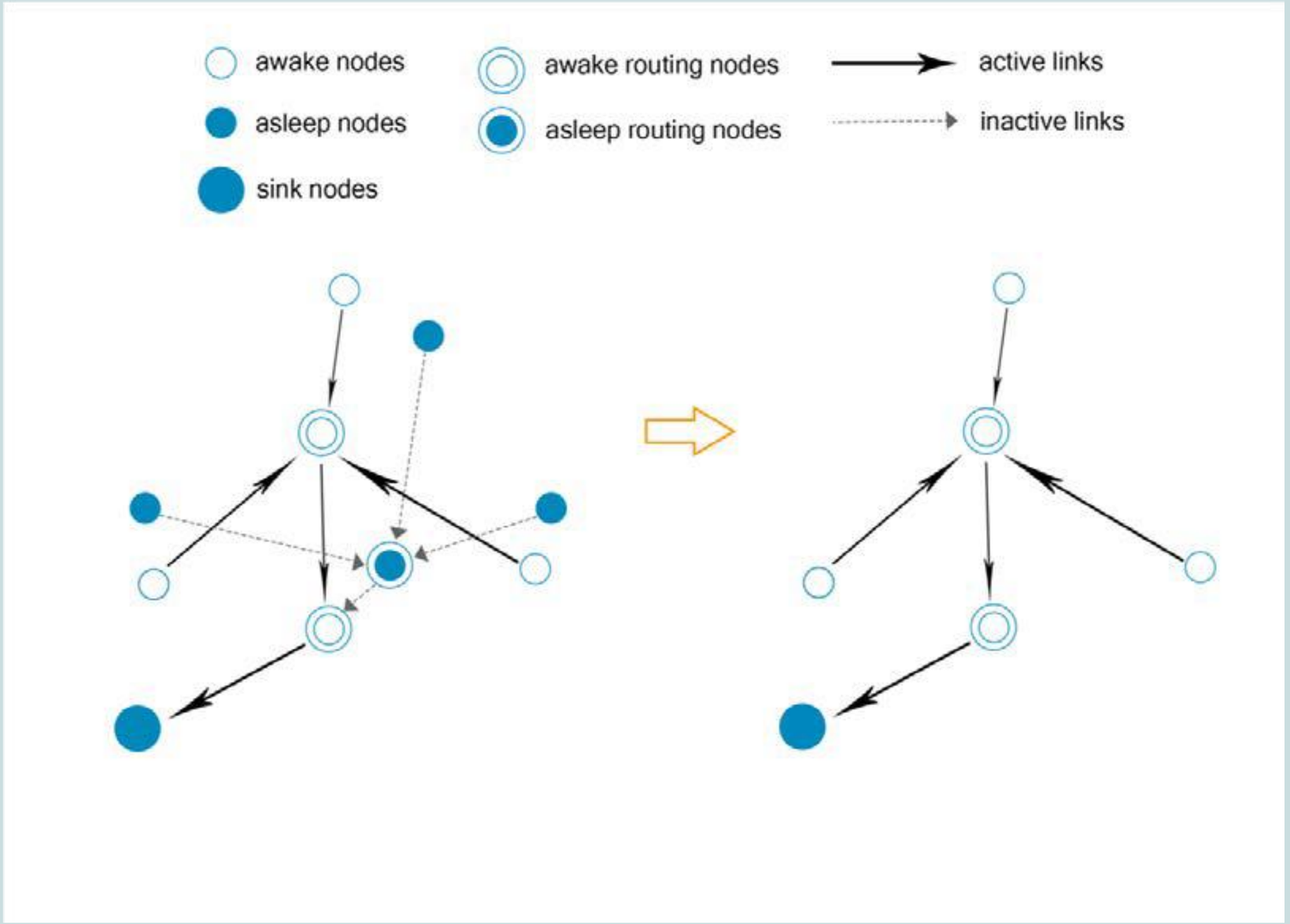

Wireless Sensor/
Actuator
Network
Wi-Fi
6LoWPAN
Physical/
Actuation
World
Internet of Things
Mobile Application
Server
Internet Data
Server
Cyber
World
Web Server
Processing
Server
Smart Devices

knectIQ

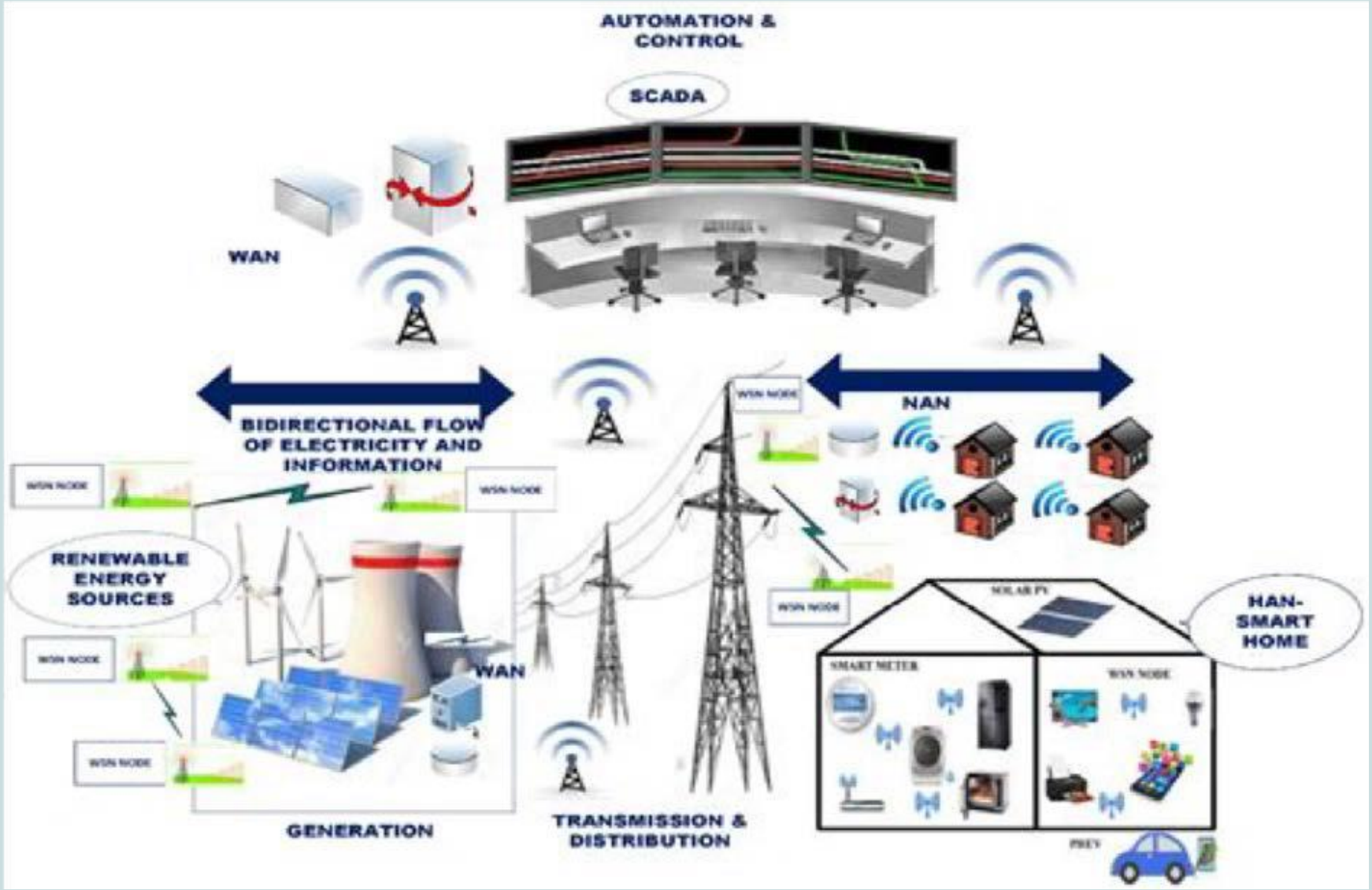

Asset
Management
Wireless Gateway
Process
Control
BBR
IP Backbone
BBR
Wireless Device
Mesh Network

knectIQ

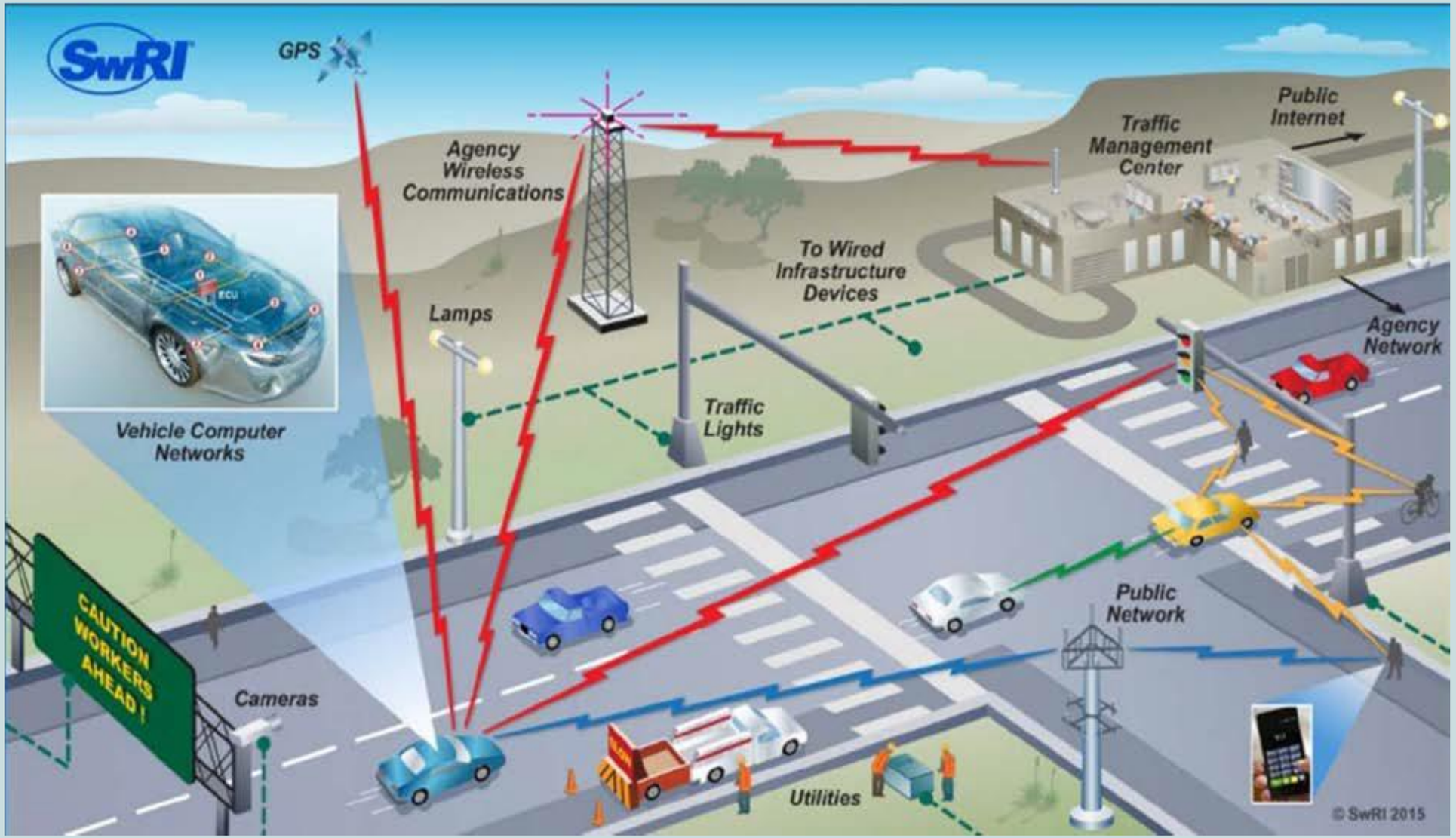



awake nodes
asleep nodes
sink nodes
awake routing nodes
asleep routing nodes
active links
inactive links

knectIQ


AUTOMATION &
CONTROL
SCADA
WAN
BIDIRECTIONAL FLOW
OF ELECTRICITY AND
INFORMATION
NAN
RENEWABLE
ENERGY
SOURCES
WAN
HAN-
SMART
HOME
GENERATION
TRANSMISSION &
DISTRIBUTION

knectIQ


SwRI
GPS
Agency
Wireless
Communications
Traffic
Management
Center
Public
Internet
To Wired
Infrastructure
Devices
Lamps
Agency
Network
Traffic
Lights
Vehicle Computer
Networks
CAUTION
WORKERS
AHEAD !
Public
Network
Cameras
Utilities
© SwRI 2015

knectIQ


IOT SECURITY RISKS
01 INDUSTRY
02 CARS
Two cybersecurity experts caused a ruckus in 2015 when they took control over a Jeep as it was cruising down the freeway.
03 VIDEO CAMERAS
The wireless networks used for transferring video signals can be insecure.
04 CYBER-WARFARE
It is likely that Stuxnet represents the first example of an entirely new class of cyberweapons.
05 POWER GRIDS
Cybersecurity experts have been warning of the risk of hackers breaching the power grid and natural gas pipelines.
06 BUILDINGS
07 CITIES
Few cities engage in regular cybersecurity testing, and many have weak security controls in place.
08 MEDICAL DEVICES
The security used in many medical devices and hospitals lags behind that used in many other industries.
09 AIR TRAVEL
Last year, Chris Roberts, a security researcher at One World Labs, hacked into a United Airlines jet while onboard and modified its software.
10 RETAIL
In 2014, hackers managed to break into Target's financial systems not by way of an HVAC unit.
CAMERAS CAN BE EXPLOITED
Even video cameras, which are intended to improve security, can be hacked.
CONNECTIVITY OFFERS NEW RISKS
As cars and industrial facilities become increasingly connected to the cloud, security risks increase.
ATTACKS LIKELY UNDER-REPORTED
It is difficult to gauge the true risk of software breaches in the industrial and retail sectors, which tend to downplay their risk of being compromised.
AIRPLANES CAN BE HACKED
Software vulnerabilities have been identified in several commercial aircraft.
Science fiction–esque cyber-war is now possible and Iran now has one of the largest cyber-armies in the world.
MALWARE DESIGNED FOR WARFARE
POWER GRIDS ARE VULNERABLE
The utility and building industries are increasingly vulnerable to software attacks and software bugs that can cripple infrastructure.
NEW RISKS FOR CITIES AND BUILDINGS
HOSPITALS ARE ALREADY TARGETS
There are already examples of hospitals that have been shut down by ransomeware attacks. Many medical devices are also insecure.

SECURITY GAPS IN ICS NETWORKS

knectIQ

- Understanding what you have in your network
- No visibility into critical control-layer activity
- Blind-spots of physical access to devices

knectIQ

- Physical cyber attacks can occur
- Controller logic is the most critical part of an ICS network
- Standard network monitoring is not enough – institute control-layer aware deep packet inspection
- Sensor reading is not reliable for finding malicious activity

Attack Scenario

knectIQ

- Nodes periodically send data
- Packets encrypted with AES and ECC
- Establish shared secret keys between pairs of nodes

- Differential Power Analysis (DPA) on AES
- Simple Power Analysis (SPA) on ECC
- Side Channel Attacks

knectIQ

ROOT OF THE PROBLEM

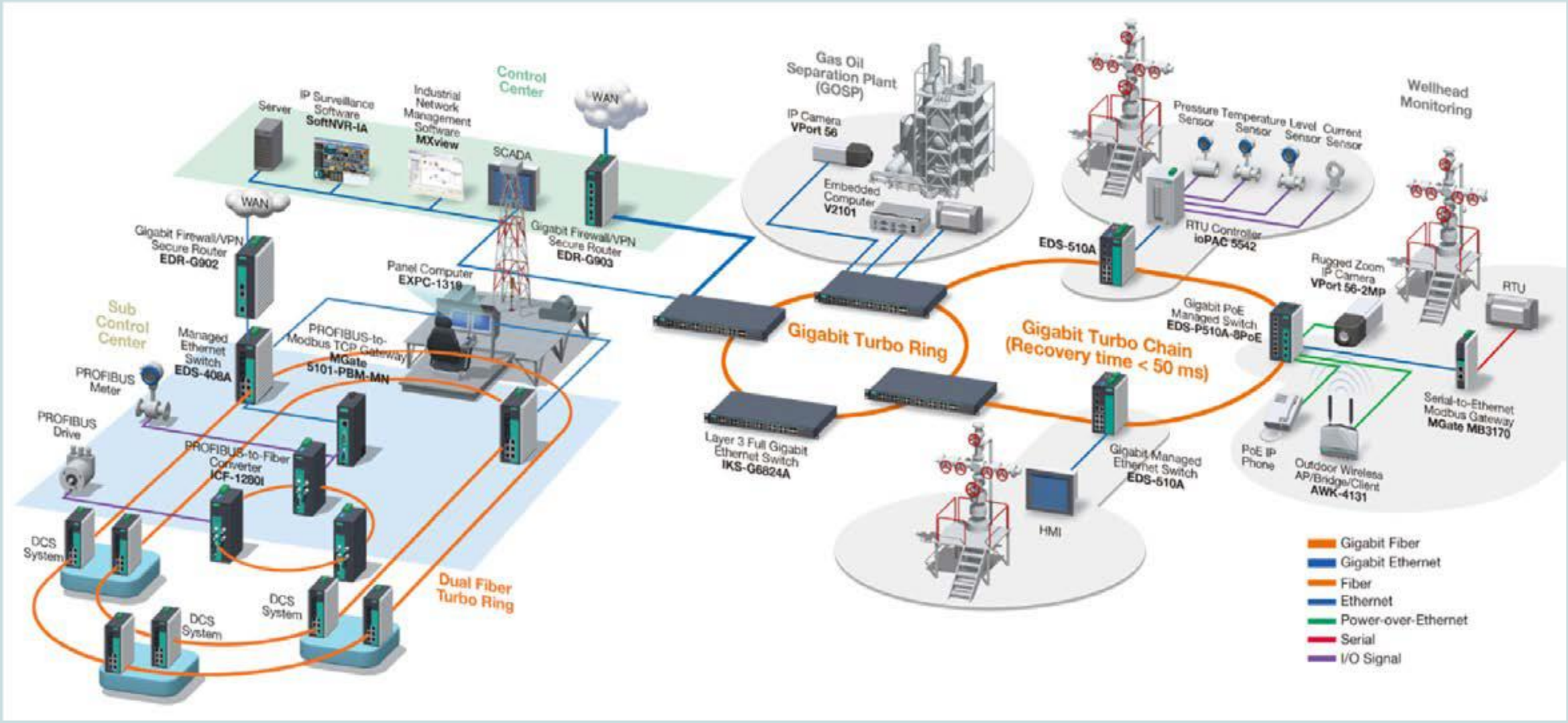
Stored Keys or Secrets

knectIQ

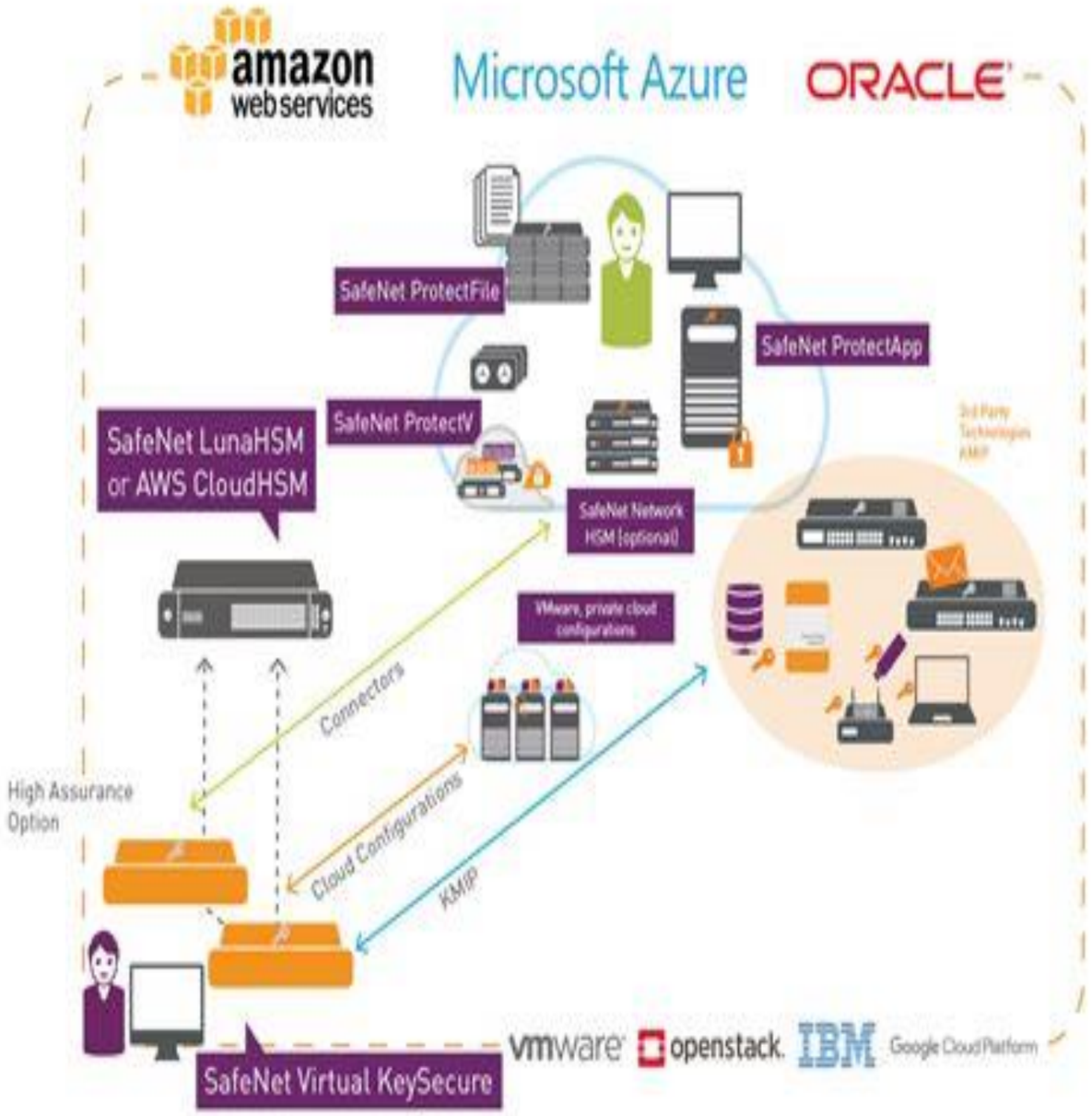
SOLUTION

- Dynamic White Listing
- Eliminate Stored Keys and Secrets

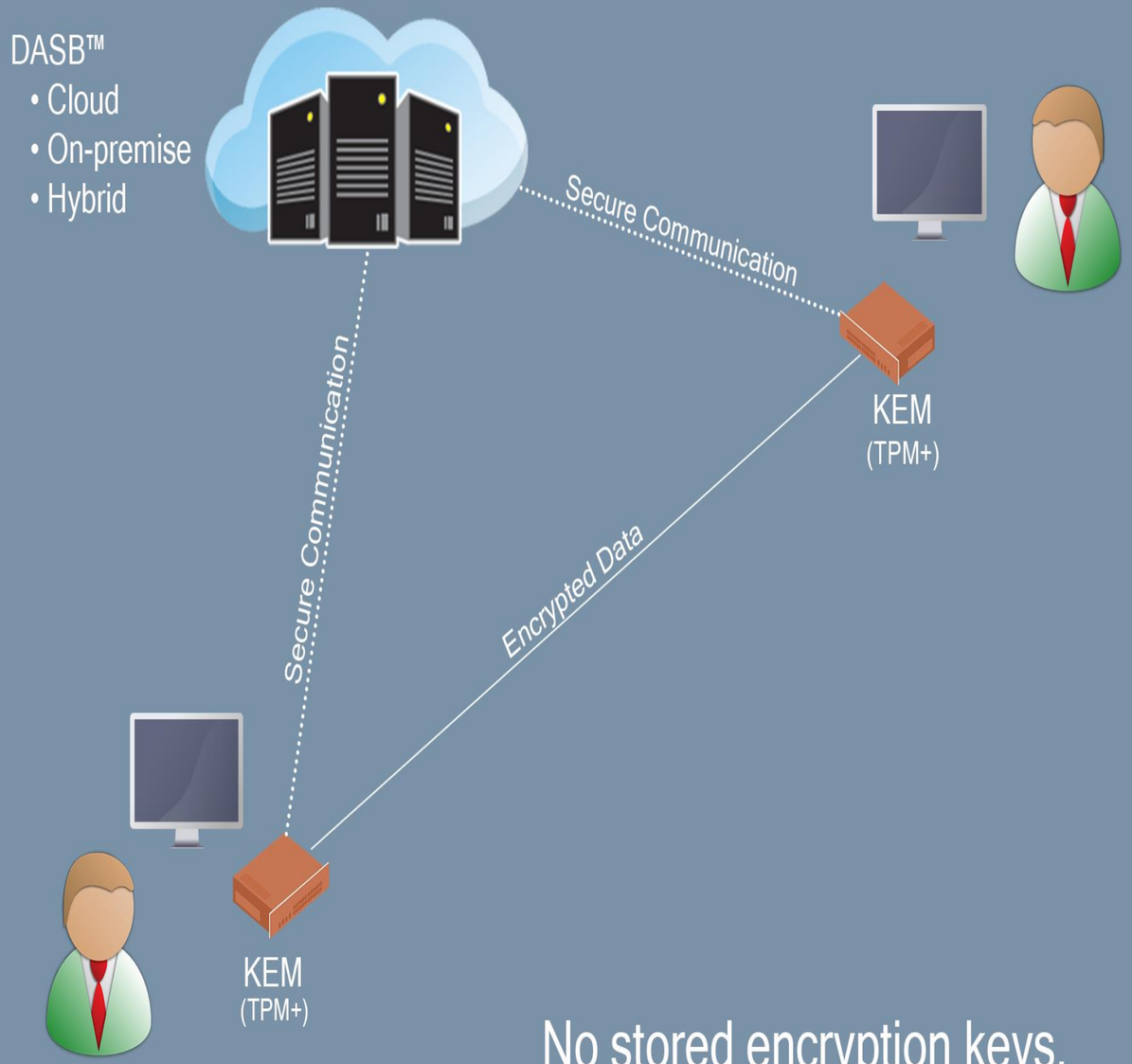
knectIQ


Control Center
Server
IP Surveillance Software
SoftNVR-IA
Industrial Network Management Software
MXview
SCADA
WAN
WAN
Gigabit Firewall/VPN Secure Router
EDR-G902
Gigabit Firewall/VPN Secure Router
EDR-G903
Panel Computer
EXPC-1319
Sub Control Center
Managed Ethernet Switch
EDS-408A
PROFIBUS-to-Modbus TCP Gateway
MGate 5101-PBM-MN
PROFIBUS Meter
PROFIBUS Drive
PROFIBUS-to-Fiber Converter
ICF-1290I
DCS System
DCS System
DCS System
Dual Fiber Turbo Ring
Gas Oil Separation Plant (GOSP)
IP Camera
VPort 56
Embedded Computer
V2101
Layer 3 Full Gigabit Ethernet Switch
IKS-G6824A
Gigabit Turbo Ring
Gigabit Turbo Chain
(Recovery time < 50 ms)
EDS-510A
Pressure Sensor
Temperature Sensor
Level Sensor
Current Sensor
RTU Controller
ioPAC 5542
Wellhead Monitoring
Rugged Zoom IP Camera
VPort 56-2MP
RTU
Gigabit PoE Managed Switch
EDS-P510A-8PoE
Serial-to-Ethernet Modbus Gateway
MGate MB3170
PoE IP Phone
Outdoor Wireless AP/Bridge/Client
AWK-4131
Gigabit Managed Ethernet Switch
EDS-510A
HMI
Gigabit Fiber
Gigabit Ethernet
Fiber
Ethernet
Power-over-Ethernet
Serial
I/O Signal

From This….



To This….



No stored encryption keys.
Authenticated and authorized endpoints.

knectIQ

Q&A

knectIQ

Contacts

Ken Morris

kmorris@knectiq.co
m 651.343.3117

1915 Highway 36 W
Suite 100
Roseville, MN 55113