Check Point
SOFTWARE TECHNOLOGIES LTD

ICS MONITORING FIELD EQUIPMENT METHODS

Check Point security solution

Shlomi Feldman | SCADA Solution Expert

WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

Shop floor connectivity scenarios

Check Point
SOFTWARE TECHNOLOGIES LTD

In this short guide we will introduce few typical connectivity scenarios of PLC's and machines/sensors on a production shop floor and how we can monitor the traffic in each case.

We will cover the following options, including IoT devices using MQTT protocol:

- I/O Connectivity Monitoring
- Communication Connectivity Monitoring
- IoT Connectivity Monitoring

PLC to Field devices - I/O Connectivity

- I/O connectivity refers to the most popular option where field equipment and sensors are connected directly to the PLC I/O modules (no visible protocol exist)
- The status of the field equipment is presented by the **PLC registers addresses**

Challenge

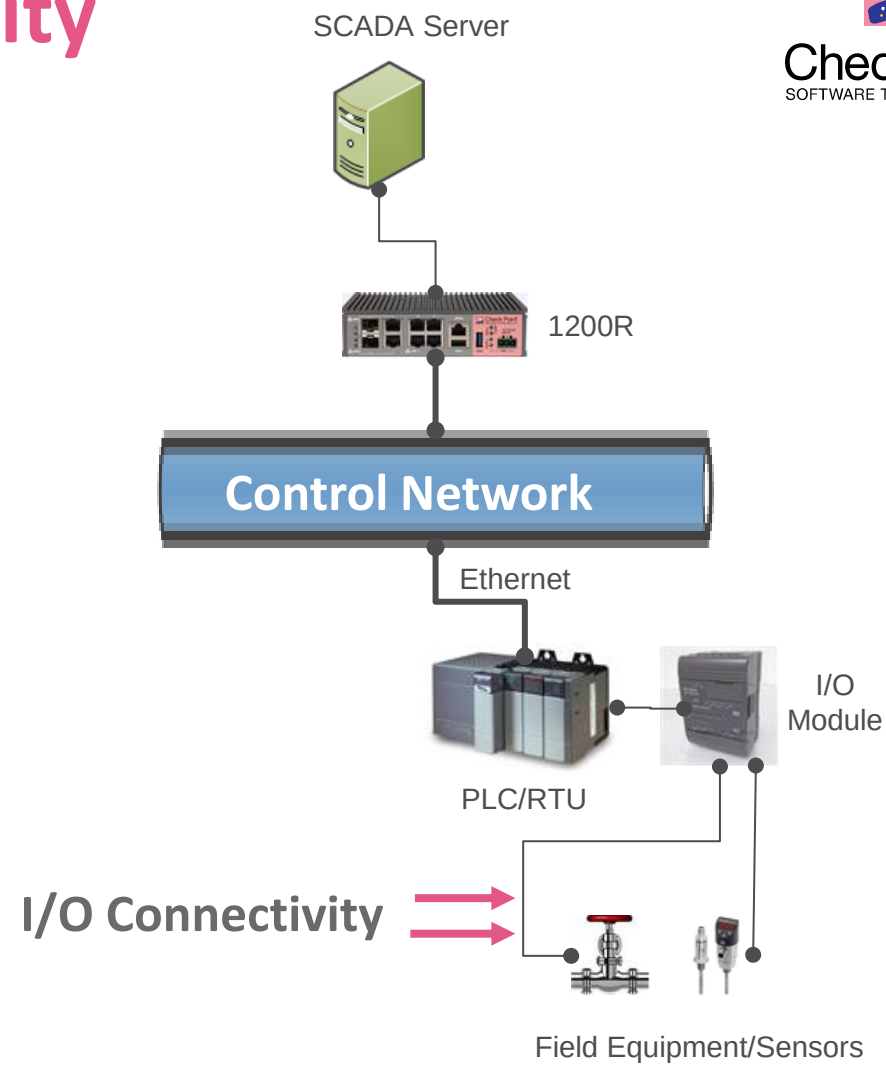
In case there are multiple field devices or sensors connected to the same PLC, how can we monitor and secure any specific device/sensor?

How we can protect this environment?

- Installing 1200R (or other gateway) between the PLC and the SCADA server (Inline or in Tap mode)
- Monitoring the protocol commands traffic between the PLC and the SCADA server

Solution

- Using Protocol DPI capabilities to monitor specific device/sensor addresses and values, and set policies per address or value
  - Currently we have DPI support for **Modbus, CIP, IEC-104 and DNP3**

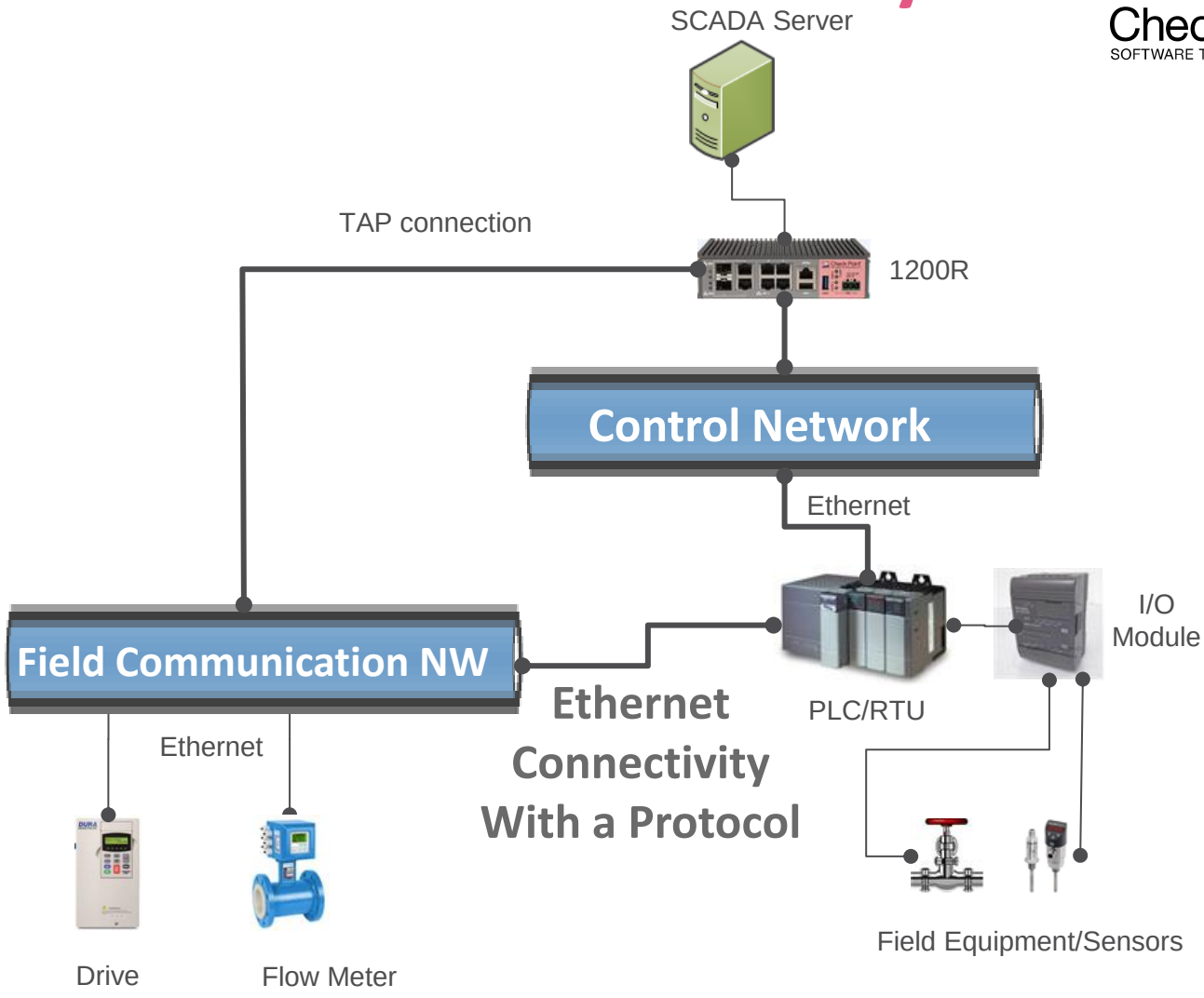


PLC to Field devices - Communication Connectivity

- This working mode is based on Ethernet connectivity between the PLC and the field equipment/sensors, using visible protocols such Ethernet/IP, Profinet and CIP

How we can protect this environment?

- (Assuming 1200R is installed between the PLC and the SCADA server), adding a Tap connection to a span port of the Field Communication Network switch to get the necessary visibility to the traffic at this layer
- Using Application control blade monitoring communication protocol commands traffic in the network, alerting concerning irregular activity

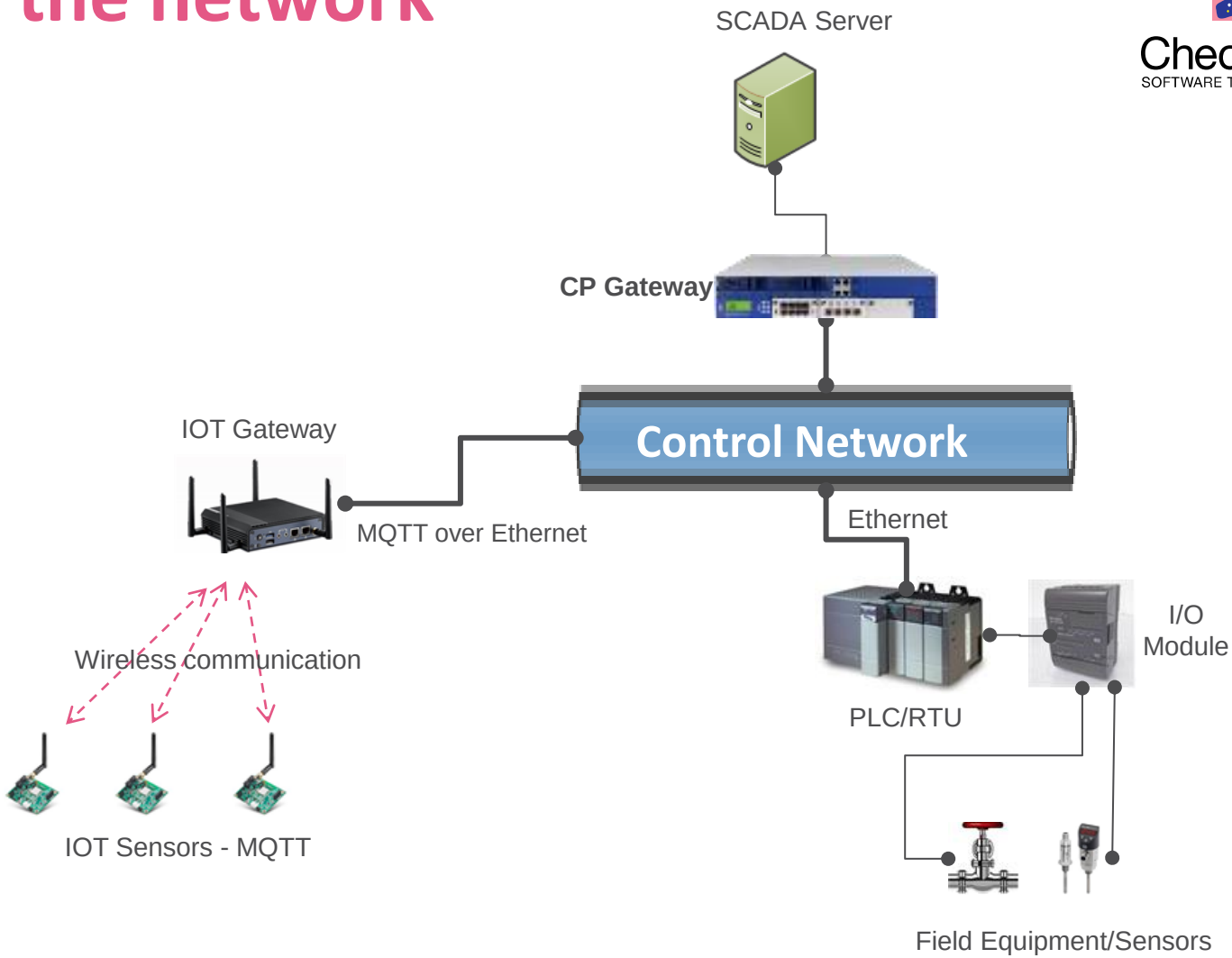


Adding IoT Sensors to the network

- Lately we start seeing convergence of IoT sensors to the ICS environment.
- There are many possible topologies of connectivity. We will relate to sensors obtain communication capabilities, with specific focus on those using MQTT.
- The sensors communicate with an IoT gateway, which can be connected to the ICS network

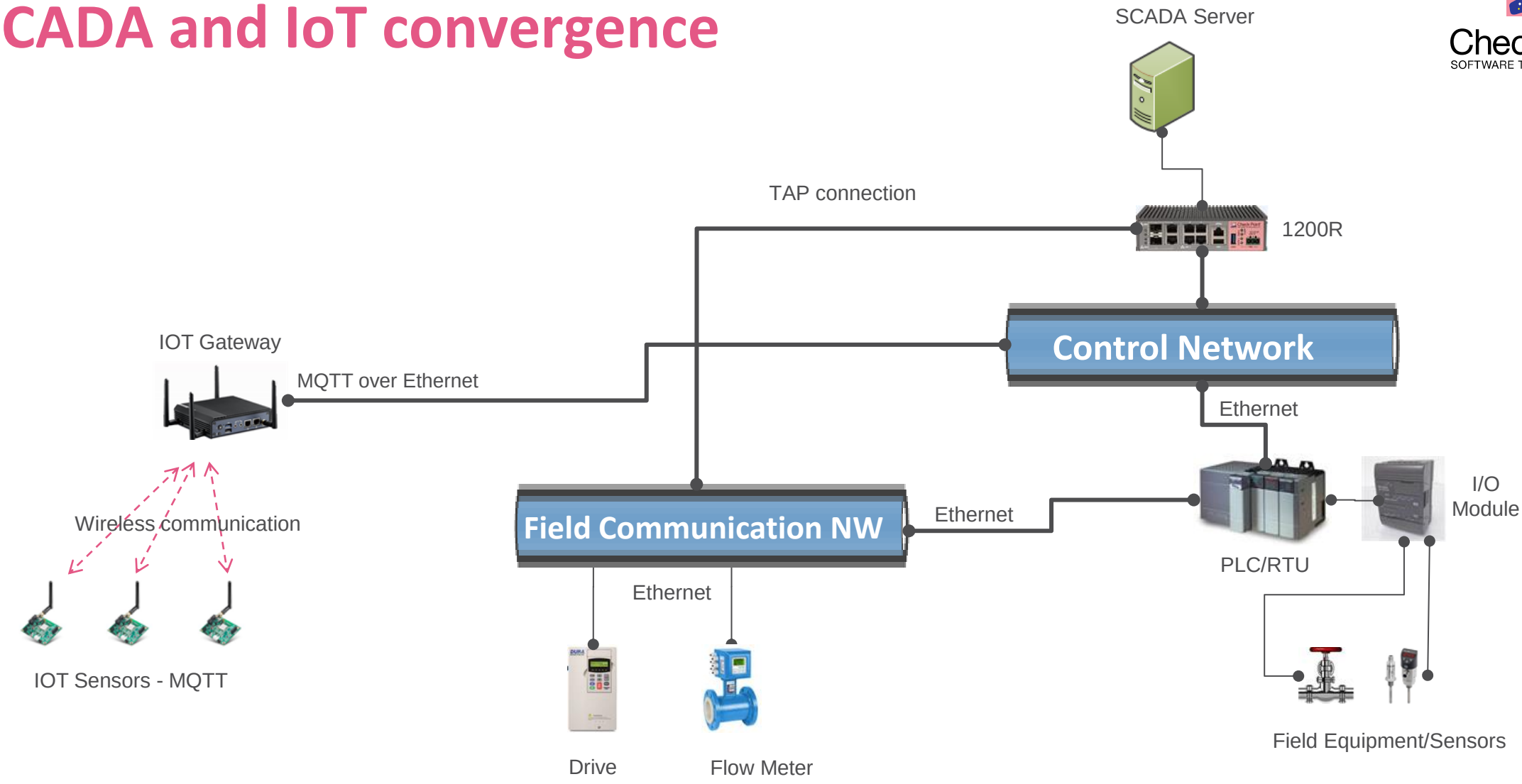
How we can protect this environment?

- With **GAIA based appliances** (only) we can monitor MQTT commands and values between the IoT gateway and the IoT cloud, and set policies



Please note that MQTT support is available but not in GA. Please contact HQ for any question on the status of this new solution

SCADA and IoT convergence



Summary

- Check Point offers complete solution set for the 3 connectivity methods
- Check Point offers support for large variety of SCADA protocols and MQTT to be used in new converged SCADA + IoT Industrial environment

Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION