

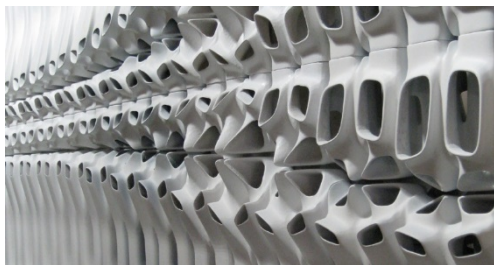


Safety and Security in Cyber Physical Production Systems

Azfar Khalid, PhD, CEng, MIMechE



Senior Lecturer
School of Science & Technology
Nottingham Trent University
Nottingham, UK

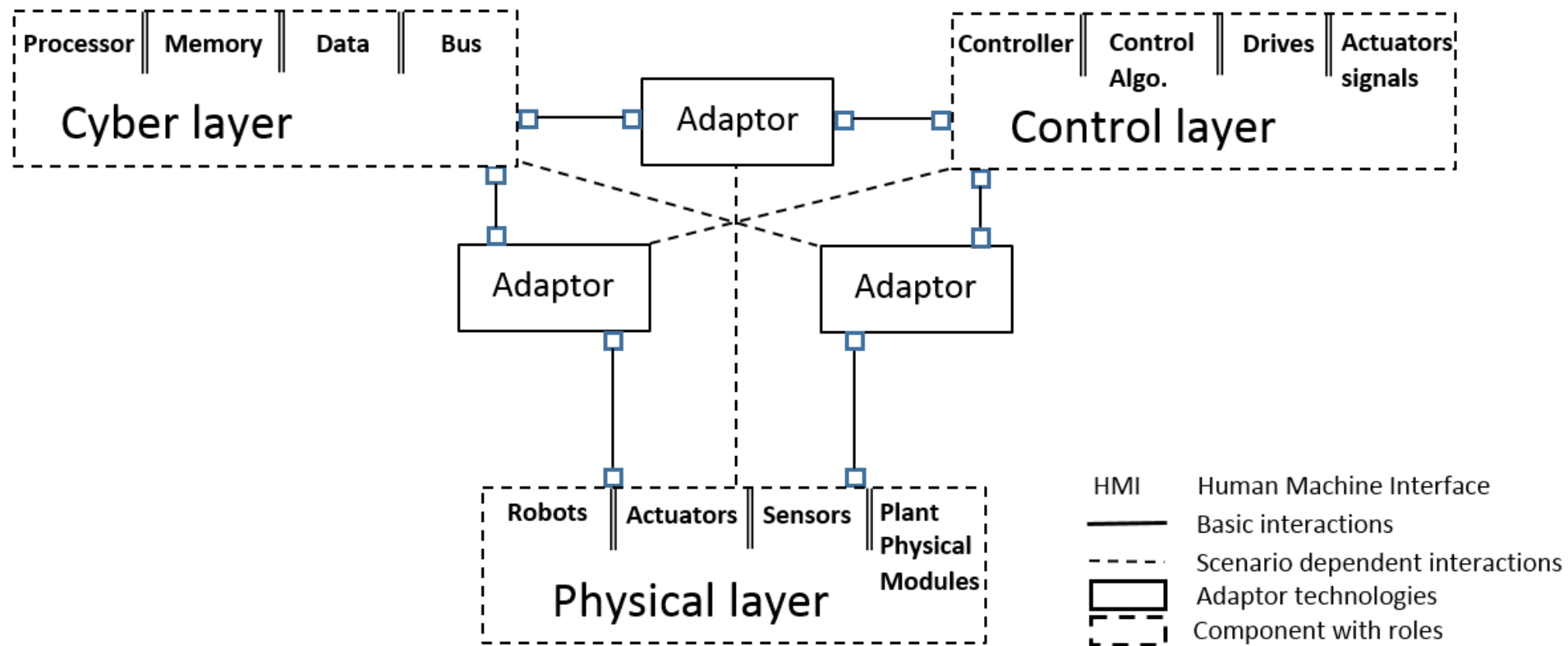


Road map

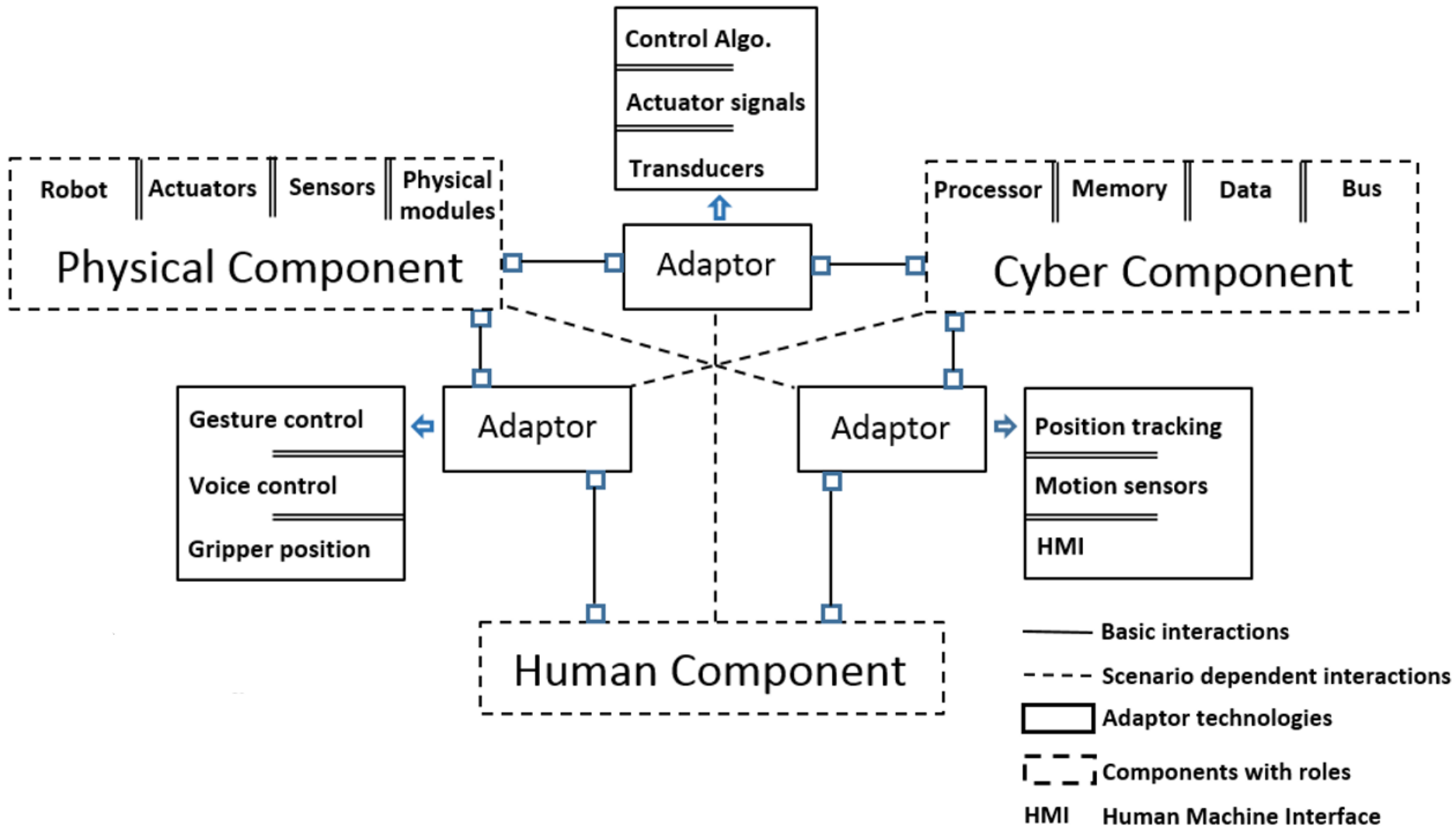
- Cyber Physical Production Systems
- Human Robot Collaboration
- Safety & Security
- Use cases
 - Cobot in Production Line
 - Cobot in Logistics



Cyber Physical System



Cyber Physical Production System Model



Human Robot interaction in industrial environment

Absolute separation of working areas with passive safety mechanisms without PLC



Common working areas with safety PLC



Seamless merging of the working areas (human-robot-collaboration)



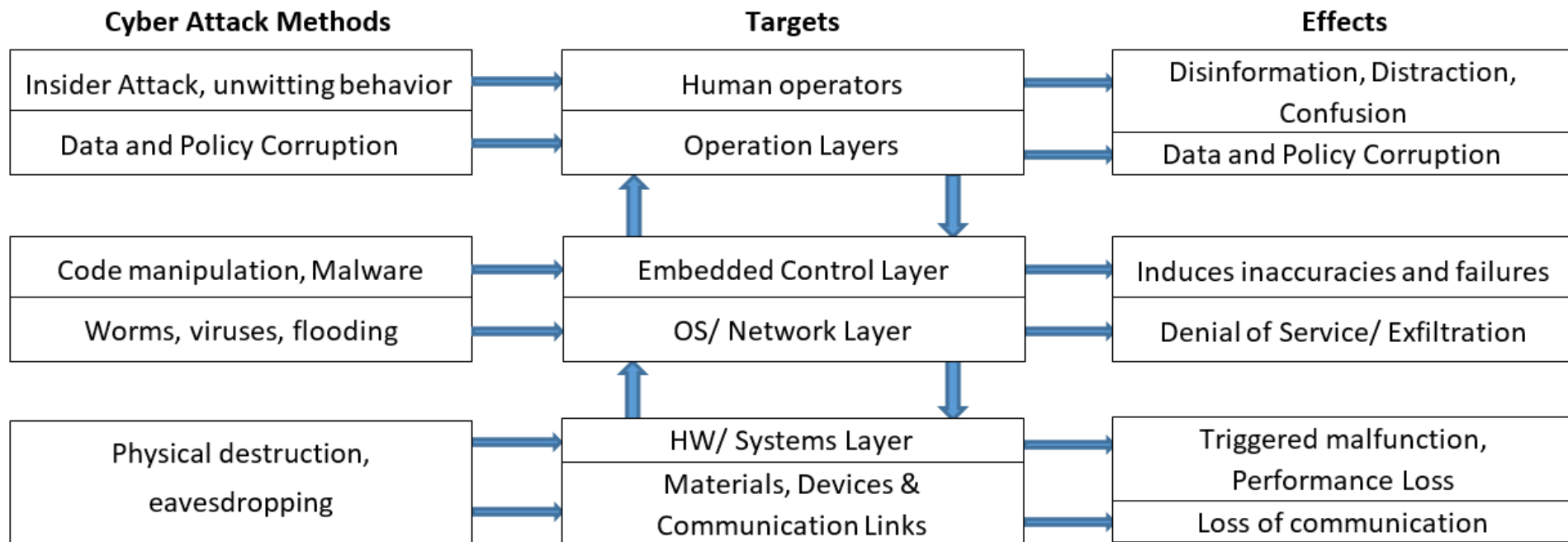
State of the Art in Collaborative Robotics

Robot / Manuf.	Application area	Specs.	Sensors	Capabilities
ABB Switzerland, Yumi – IRB 14000	Electronics and small parts assembly	Payload- 0.5 kg Reach- 559 mm	Camera, force sensors	Collision detection
Rethink Robotics, Boston, USA, Sawyer	Material handling, packaging, kitting	Payload- 4 kg Reach- 1260 mm	Cameras in head & wrist, force sensors	Force limited compliant arm
Universal Robots, Denmark, U10	Packaging, palletizing, pick and place etc.	Payload- 10 kg Reach- 1300 mm	Force sensors	Collision detection
KUKA, Germany, LBR iiwa 14 R820	Handling, fastening, measuring	Payload- 14 kg Reach- 820 mm	Torque sensors	Speed and force reduction upon collision
NASA, USA, Robonaut 2	Space robotics	Payload- 9 kg Reach- 2438 mm	3D and IR cameras, load cells, force sensors	Elastic joints

Hazards Identification Sources

From Robot	From the Industrial Process	From Control System Malfunction
Speed, force, torque, acceleration, momentum, power etc.	Ergonomic design deficiency	Reasonably foreseeable misuse by the operator
Operator location under heavy payload robot	Transition time from collaborative to other operations	Control layer malfunction under a cyber-attack
Robot end-effector protrusions	Time duration	Obstruction in front of active sensors
Mental stress to operator	Process complexity	Multiple workers involvement
Fast worker approach speed	Physical obstacles	Vantage point of operator
Tight safety distance limit	Process parameters, e.g., temperature, loose parts	wrong perception of process completion by the robot

Risk Identification - CPPS Security issues



[Reference] R. Elder, "Defending and operating in a contested cyber domain," *Air Force Scientific Advisory Board, Winter Plenary*, 2008.

Risk Identification - CPPS Security issues

		Reconnaissance	Weaponize	Delivery	Execution	Objective
Anthropocentric	Cyber	Blue	Blue	Blue	Blue	Blue
	Physical	Blue	Blue	White	Blue	Blue
	Control	Blue	White	White	White	Red
	Cyber	Blue	White	Blue	White	Red
	Human	Blue	White	Blue	White	Red
Cyber Physical System	Cyber	Blue	Blue	Blue	Blue	Blue
	Physical	Blue	Blue	White	Blue	Blue
	Control	Blue	White	White	White	Red
	Cyber	Blue	White	Blue	White	Red
IT System	Cyber	Blue	Blue	Blue	Blue	Red

Risk Identification - CPPS Security issues

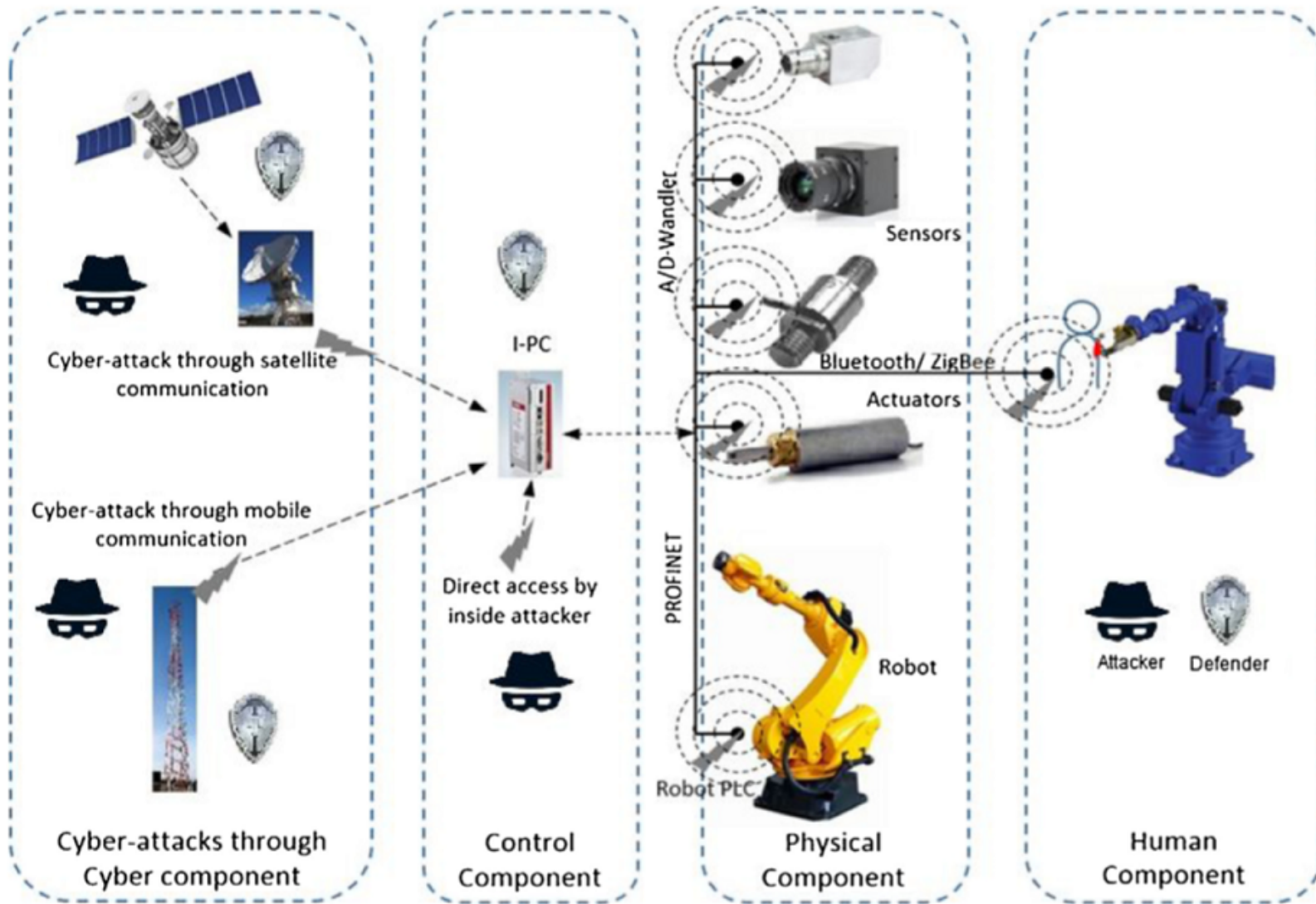



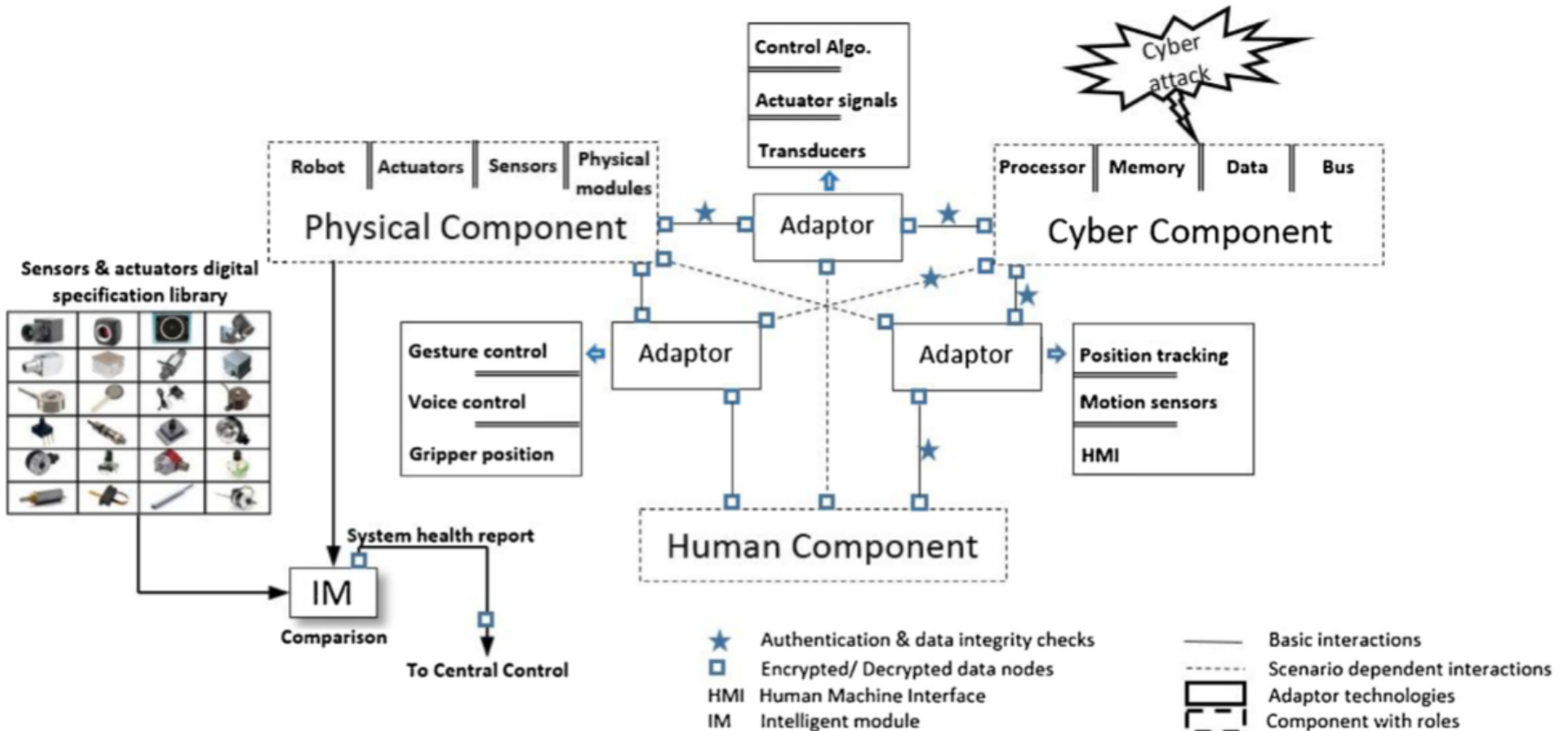
Fig. 3. Cyber-attack routes in CRCPS and logical causal effect diagram for HRC.

Risk Identification - CPPS Security issues

Assessment & categorization of cyber-attacks on CRCPS.

Attack intensity on CRCPS	Authentication	Availability	Confidentiality	Extent of attack on controllability	Possible effects
Low	<ul style="list-style-type: none"> - GPS spoofing/ Movement tracking/ position faking - Tunnelling - Message tempering - Message suppression - Non-repudiation 	<ul style="list-style-type: none"> - Jamming - Greedy behaviour - Grey hole - Sink hole - Broad cast tempering - Spamming 	<ul style="list-style-type: none"> - Non-repudiation 		Short period control loss
Medium	<ul style="list-style-type: none"> - Sybill - Node impersonation - Key/Certificate replication - Masquerading - Unauthorized pre-emption 	<ul style="list-style-type: none"> - DOS - Jamming - Black hole - Worm hole - DDoS - Malware 			Effect on sensor node efficiency
Serious or high risk	<ul style="list-style-type: none"> - Replay 		<ul style="list-style-type: none"> - Eavesdropping 		Full

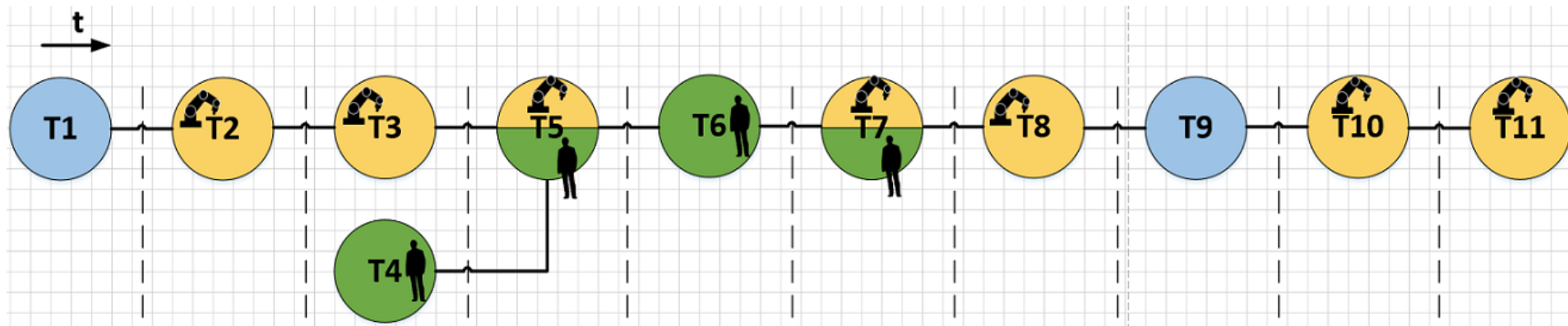
Risk Identification - CPPS Security issues



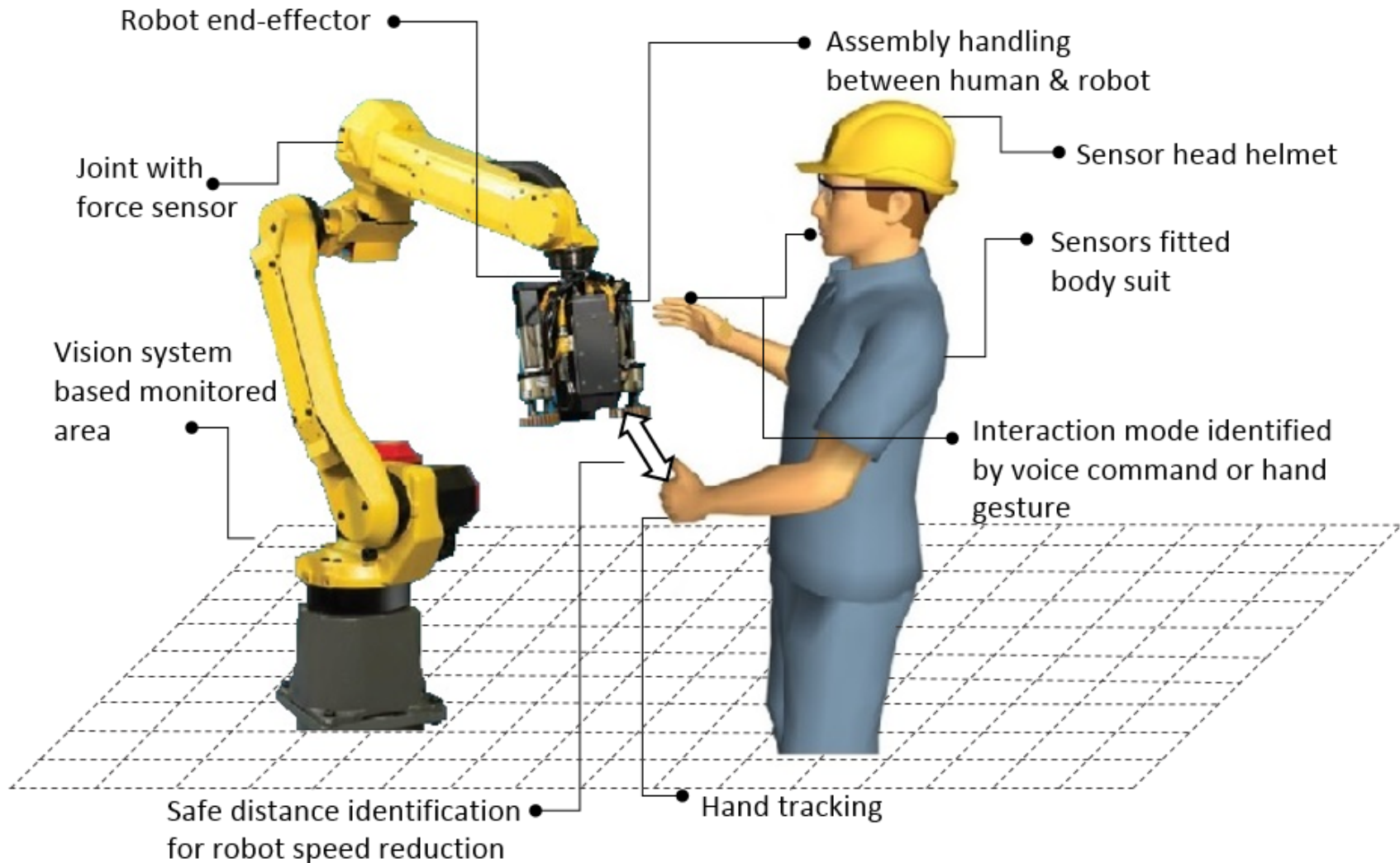
Collaborative Human-Robot CPS under Cyber-attack and the two-pronged strategy as a mitigation plan.

Use Case

- Cobot in production Line
- Semi-Automatic assembly



CPPS Technologies – Working with Robots



Demonstrator



Cyberphysical Safety Components

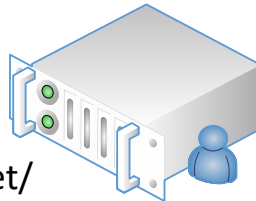


Industrial heavy payload robot with control unit

(FANUC R-2000iB 165F with R30iA controller)

- Safety laser scanners (SICK S3000): 01
- HD cameras : 02
- Wearable 3D Motion capturing system: 01

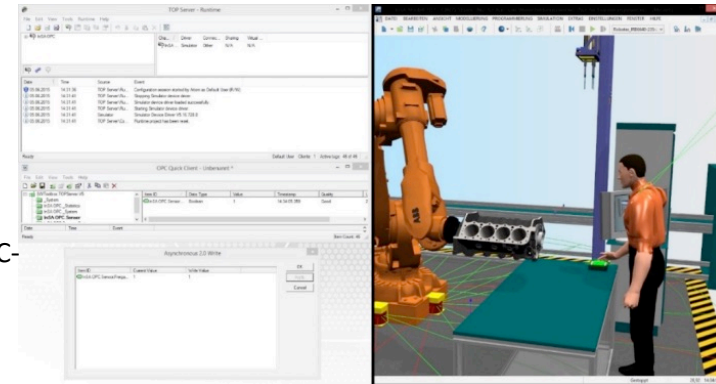
Industrial-PC/Soft PLC



ProfiNet/
ProfiSafe
Interface

Coupling
through OPC-
Server

Simulation of the assembly scenario in
CIROS Studio



Risk Identification

For example, Safety distance computation

$$SD = (K \cdot T) + C$$

Indices	Security laser scanner (16 Hz)	ToF camera (20 Hz)	Motion tracking IMU (60 Hz)	Quality assist ultrasonic sensor (50 Hz)
Data delay rate (D_i) (ms)	62.5	50	16.6	20
Sensor detection capability (d) (mm)	70	145	38	40
Number of sensors (S)	1	2	4	2
Additional distance based on sensor resolution (C) (mm)	448	1048	192	208
Safety distance (SD) ^a (mm)	1120	1720	864	880
RT (ms)	62.5	100	66.64	40
PLI ^b	0.5	0.5	0.5	0.5
SDI	0.48	0.25	0.63	0.62
RI ^b	0.6	0.6	0.6	0.6
RTI	0.6	0.375	0.58	0.75
Total	2.18	1.725	2.31	2.47

^a $K = 1600$ mm/s, $T = 0.42$ s, $C = 8(d - 14)$

^b Assumed values

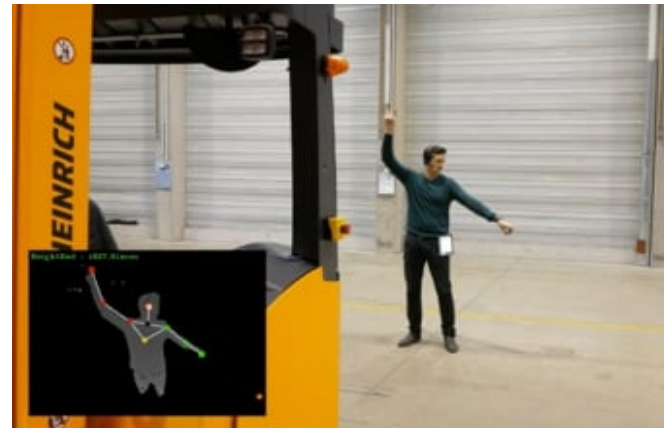
Virtual Commissioning visualization

- Intelligent multiple worker identification tracker.
- Human avoidance algorithm.
- Real-time safety distance computation.
- Worker position estimation in case of obstacles.
- Gripper path optimization in presence of multiple workers.



Use Case

- Cobot in Logistics
 - Smart warehouse
 - Drive by wireless
 - Autonomous vehicles
 - Stereo vision
 - Teleoperation robots
 - Gesture & speech Control

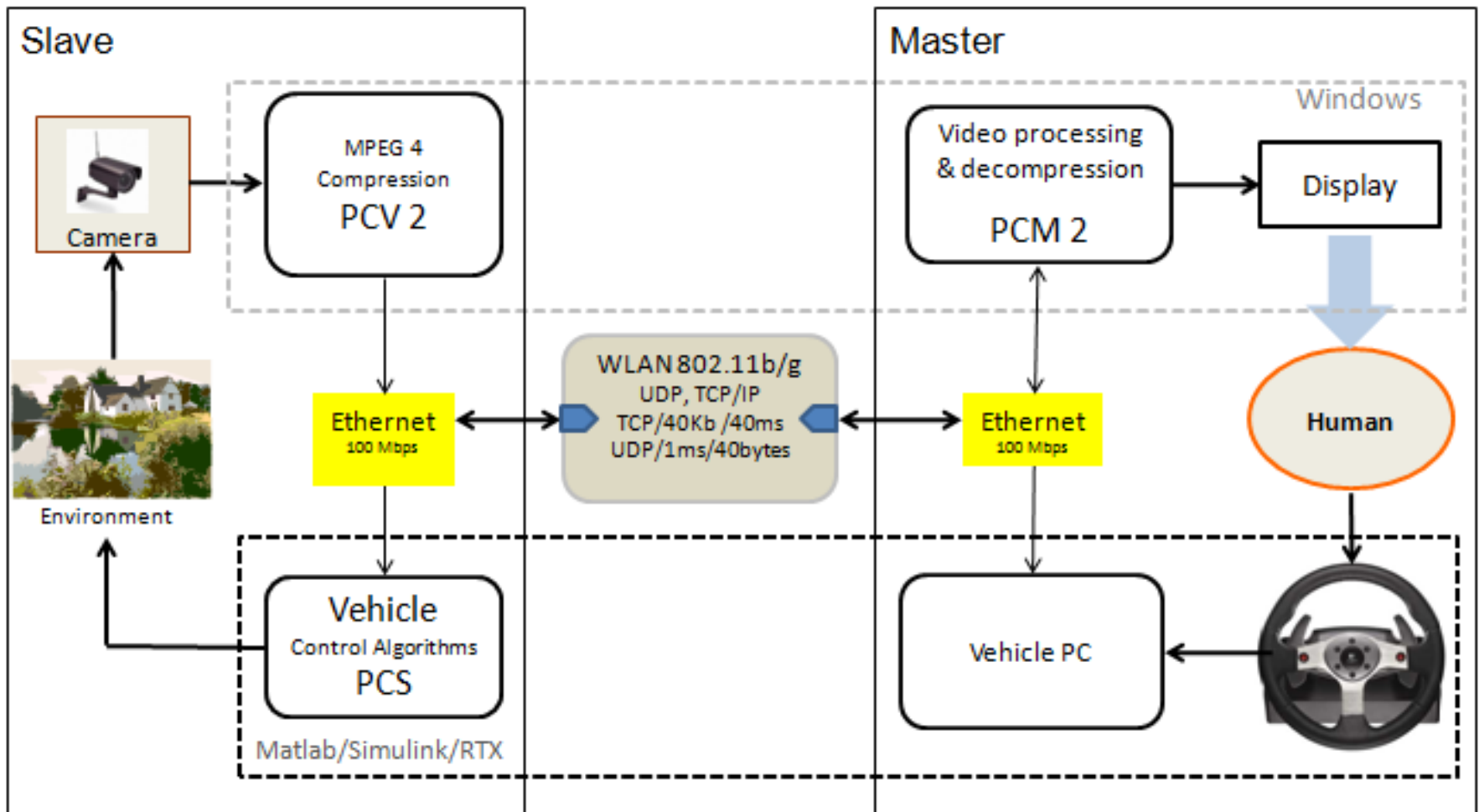


Teleoperation Robot Vehicle



- Monitoring/Supervision
- Control/Diagnosis
- Network/Communication + Control
- Master/Slave

Teleoperation Robot Vehicle



Co-design Framework

Performance Monitoring (QoC) of the mobile vehicle

Error bounds (ISE, ITAE, IAE etc.)

Communicate QoC to Operator

Same network or another for reliability (Diagnosis)

Network QoS (e2e)

Delay, Packet Loss rate, Jitter, Reliability

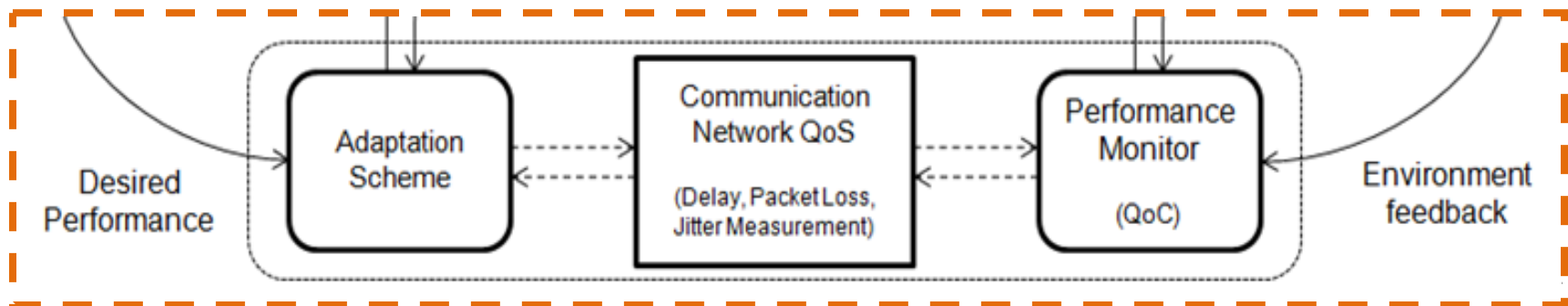
Bounded for QoS oriented e2e architecture

Adaptation Scheme

Robust control/estimation

Controller reconfiguration

QoS adjustments for QoC

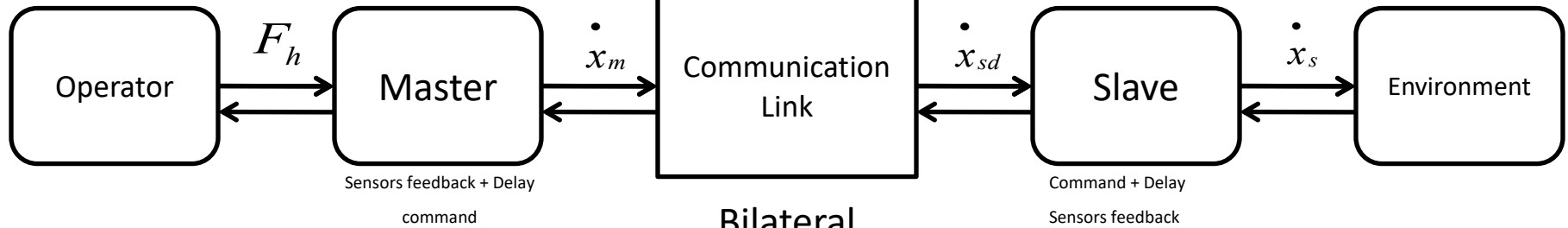


Teleoperation types



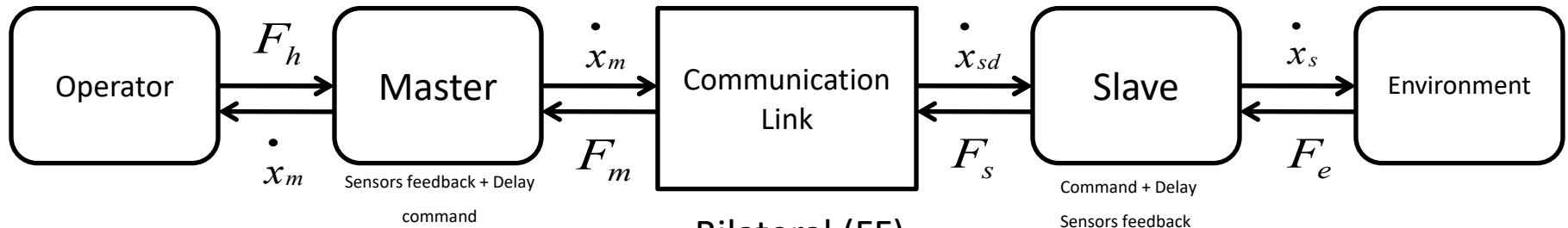
Unilateral

No Feedback !!



Bilateral

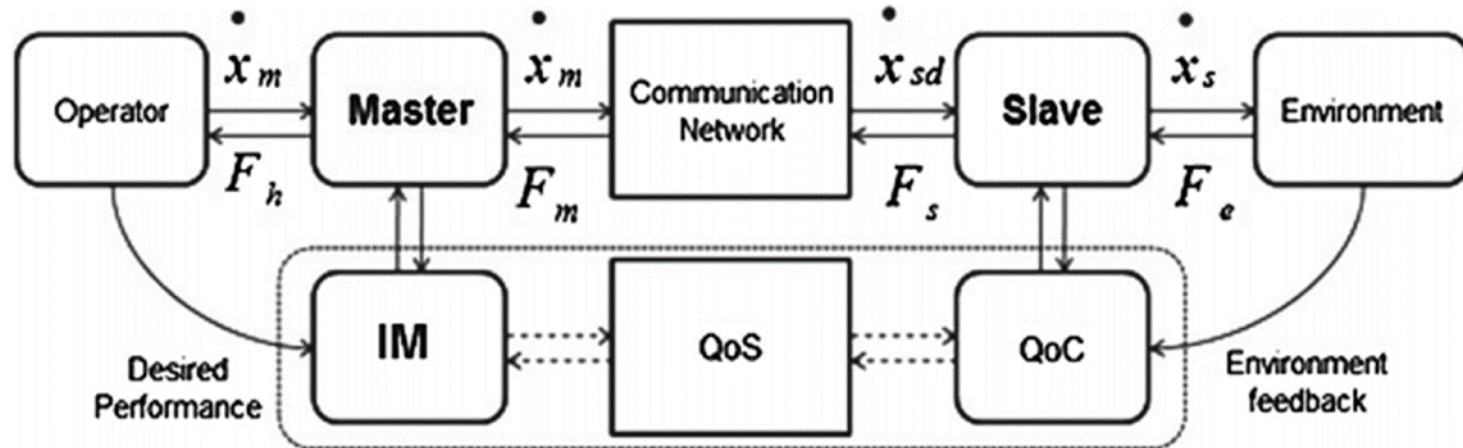
Camera Feedback !!



Bilateral (FF)

Camera + Force Feedback !!

Teleoperation Robot Vehicle



$$M_m \ddot{x}_m + B_m \dot{x}_m = F_h + F_m$$

Where

$$M_s \ddot{x}_s + B_{s1} \dot{x}_s = F_s - F_e$$

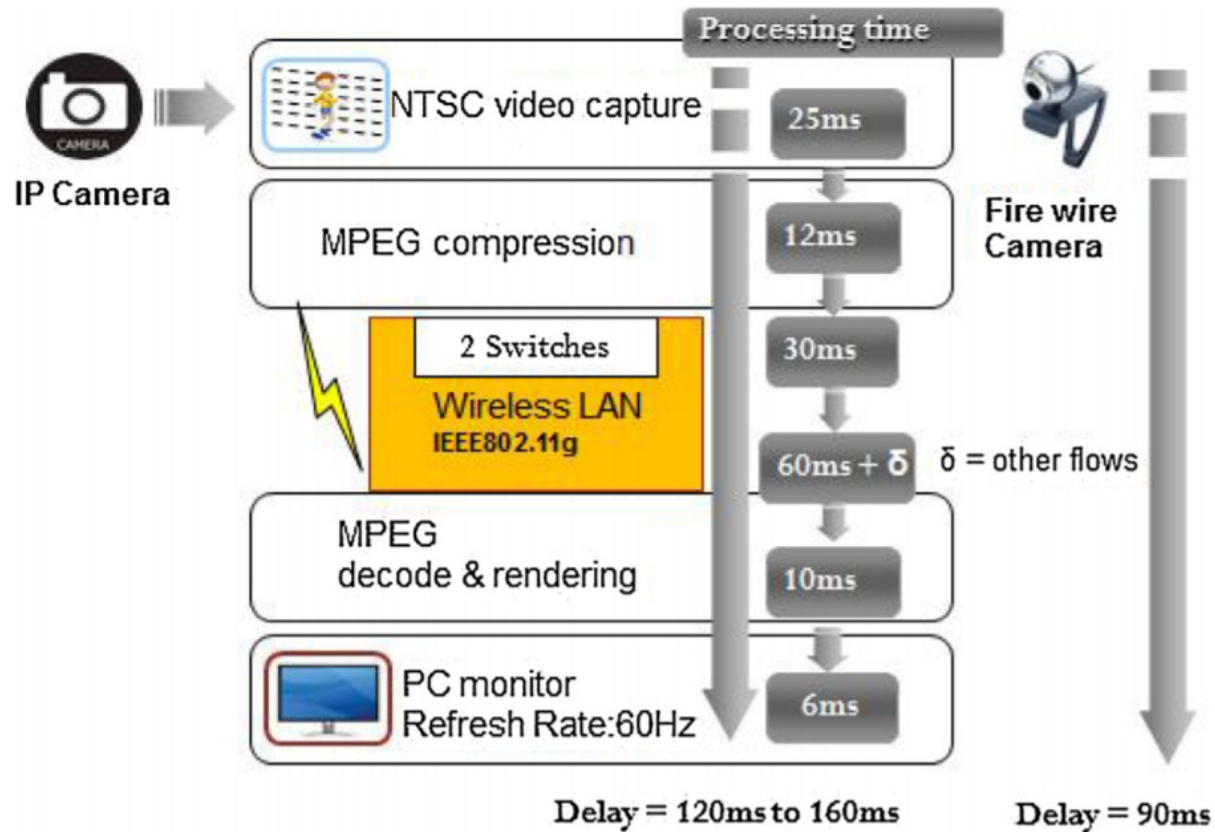
F_m and F_s - Force pair applied to the motors at the master/slave

F_h and F_e - Reaction couple from the operator and the environment

$$e = x_m(t-\tau) - x_s(t)$$

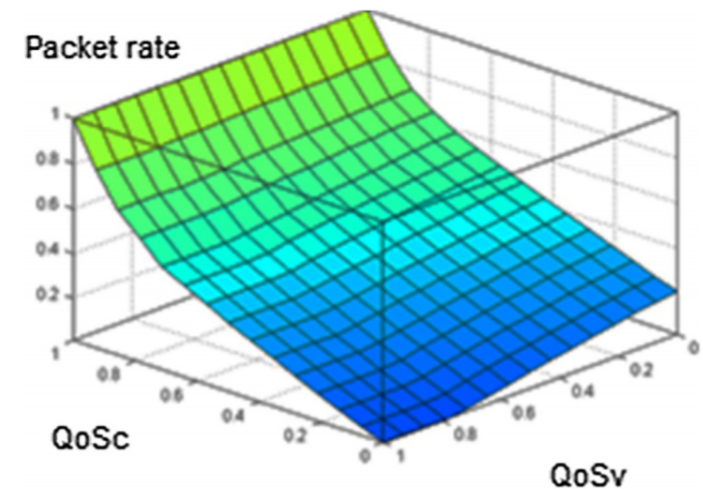
e - Position tracking error

Teleoperation Robot Vehicle – System Delay

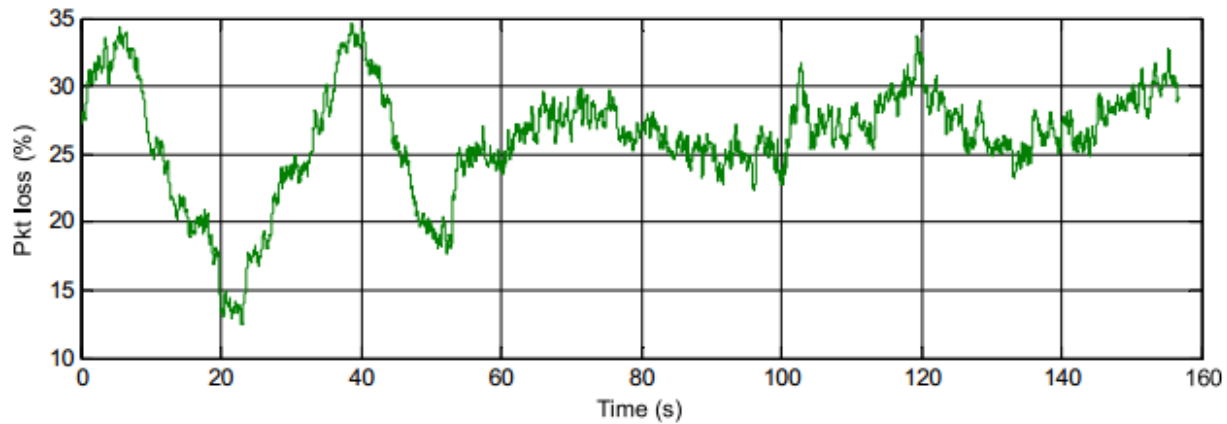
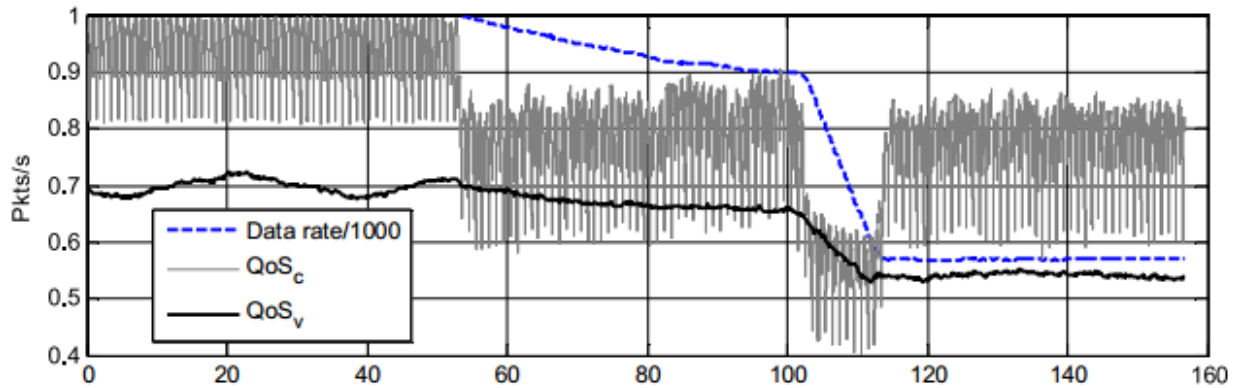


Teleoperation Robot Vehicle – Fuzzy Controller

- A fuzzy controller is designed for ensuring the quality of service of video flow (QoS_v) as well as the control flow (QoS_c)
- The variation in packet rate of the video as a controlling parameter in the teleoperation application.



Teleoperation Robot Vehicle – Fuzzy Controller



Summary

- Integration of Safety and Security in CPPS
- Safeguarding of Costly Physical Components
- Extent of cyber attack on Controllability
- Passive attacks are lethal as valuable system level and control information can be leaked.