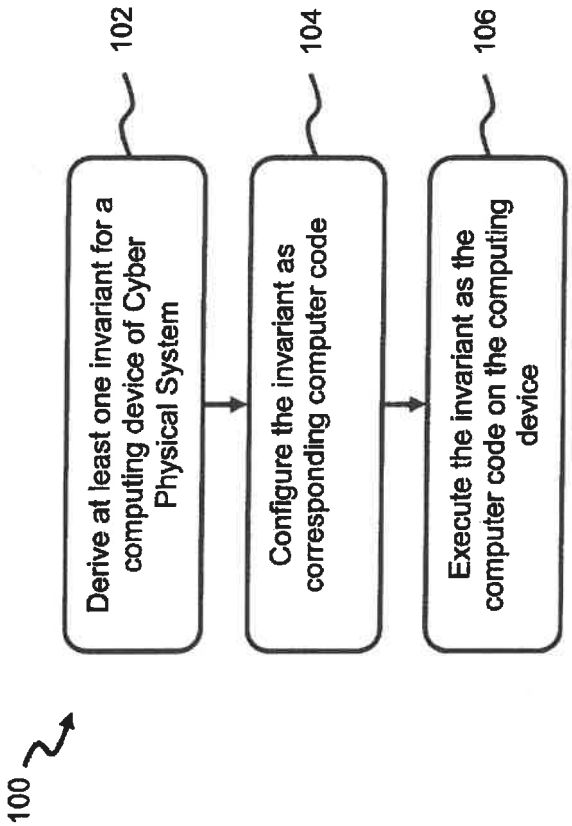
100
Derive at least one invariant for a computing device of Cyber Physical System
102
Configure the invariant as corresponding computer code
104
Execute the invariant as the computer code on the computing device
106

FIG. 1

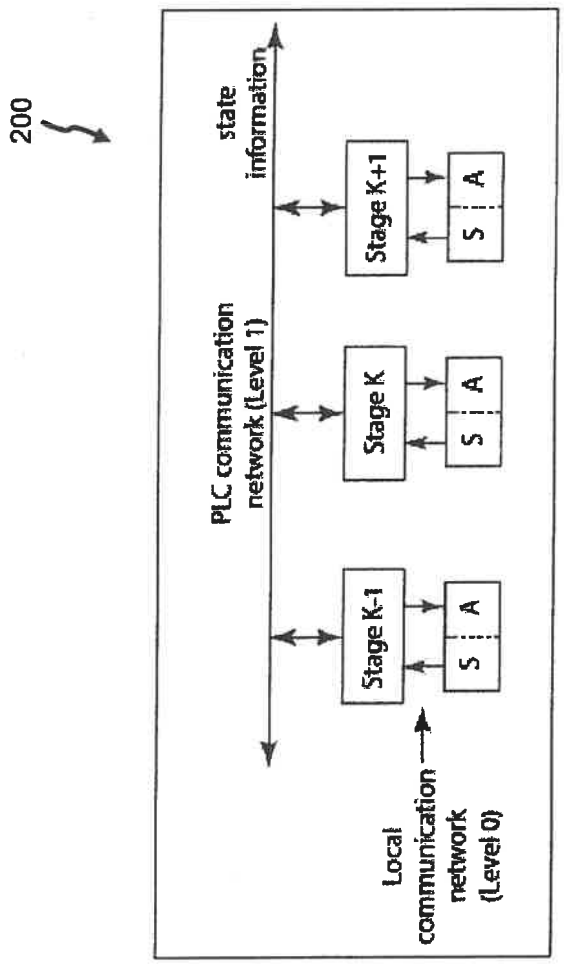
200
PLC communication network (Level 1)
state information
Stage K-1
Stage K
Stage K+1
S
A
Local communication network (Level 0)

FIG. 2

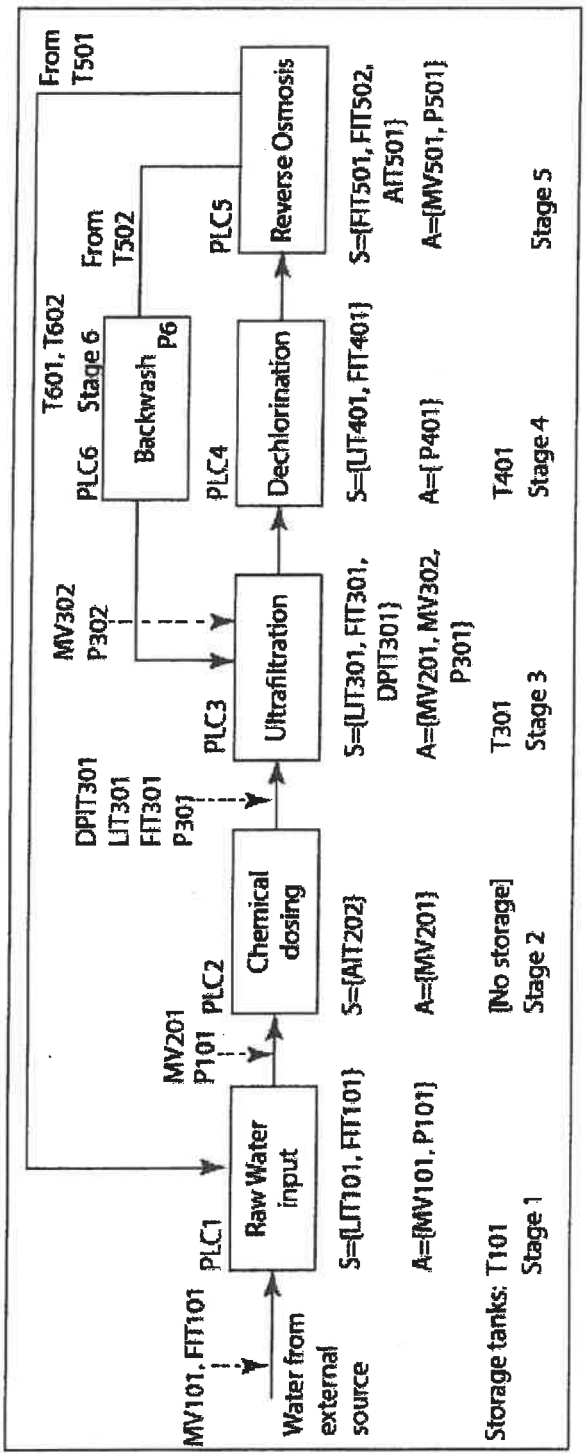
300
Water from external source
MV101, FIT101
PLC1
Raw Water input
MV201
P101
PLC2
Chemical dosing
DPIT301
LIT301
FIT301
P301
PLC3
Ultrafiltration
MV302
P302
PLC6
Backwash
P6
T601, T602
Stage 6
From T502
PLC4
Dechlorination
PLC5
Reverse Osmosis
From T501
Storage tanks: T101
Stage 1
S={LIT101, FIT101}
A={MV101, P101}
[No storage]
Stage 2
S={AIT202}
A={MV201}
T301
Stage 3
S={LIT301, FIT301, DPIT301}
A={MV201, MV302, P301}
T401
Stage 4
S={LIT401, FIT401}
A={P401}
Stage 5
S={FIT501, FIT502, AIT501}
A={MV501, P501}

FIG. 3

400

PLC	Sensor/ Actuator*	State variable	States	Purpose
1	si: FIT101	v_1	No flow: $v_1 \leq \delta$ Flow: $v_1 > \delta$	Measures flow rate of water entering tank T101.
	sio: LIT101	v_2	$v_2 \in \{LL, L, H, HH\}$	Indicates water level in tank T101.
	ai: MV101	v_3	Closed: $v_3 = 0$ Open: $v_3 = 1$	Motorized valve; water flows into tank T101 only when MV101 is open.
	ao: P101	v_4	OFF: $v_4 = 0$ ON: $v_4 = 1$	Pump to move water from stage 1 to stage 3 via stage 2.
	so: FIT201	v_{14}	No flow: $v_{14} \leq \delta$ Flow: $v_{14} > \delta$	Measure flow rate of water from T101 to T301.
2	sio: FIT201	v_{14}	$v_5 \in \{LL, L, H, HH\}$	Measures flow rate of water entering tank T301.
	ai: P101	v_4	OFF: $v_4 = 0$ ON: $v_4 = 1$	
	ao: MV201	v_5	Closed: $v_5 = 0$ Open: $v_5 = 1$	Motorized valve must be open when P101 is ON for water to flow into tank T301.
3	sio: LIT 301	v_6	$v_6 \in \{LL, L, H, HH\}$	
	so: FIT301	v_8	No flow: $v_6 \leq \delta$ Flow: $v_6 > \delta$	
	so: DPIT301	v_7	No backwash: $v_7 \leq \sigma$ Backwash: $v_7 > \sigma$	
	ai: P101	v_4	OFF: $v_4 = 0$ ON: $v_4 = 1$	
	ao: MV302	v_9	Closed: $v_9 = 0$ Open: $v_9 = 1$	Motorized valve must be open when P101 is ON for water to flow into tank T301.
	ao: P301	v_{10}	OFF: $v_{10} = 0$ ON: $v_{10} = 1$	Pump to move water from tank T301 to tank T401.
4	sio: LIT401	v_{11}	$v_{11} \in \{LL, L, H, HH\}$	Indicates water level in tank T401 that holds the output of the UF unit.
	so: FIT401	v_{12}	No flow: $v_{12} \leq \delta$ Flow: $v_{12} > \delta$	Measures flow rate of water exiting tank T302 and flowing to the dechlorination stage.
	ao: MV302	v_9	Closed: $v_9 = 0$ Open: $v_9 = 1$	
	ai: P301	v_{10}	OFF: $v_{10} = 0$ ON: $v_{10} = 1$	
	ao: P401	v_{13}	OFF: $v_{13} = 0$ ON: $v_{14} = 1$	Pump to move water from tank T401 to RO unit.

* Sensor/actuator nomenclature: s: sensor, a: actuator, i: input, o: output.

FIG. 4

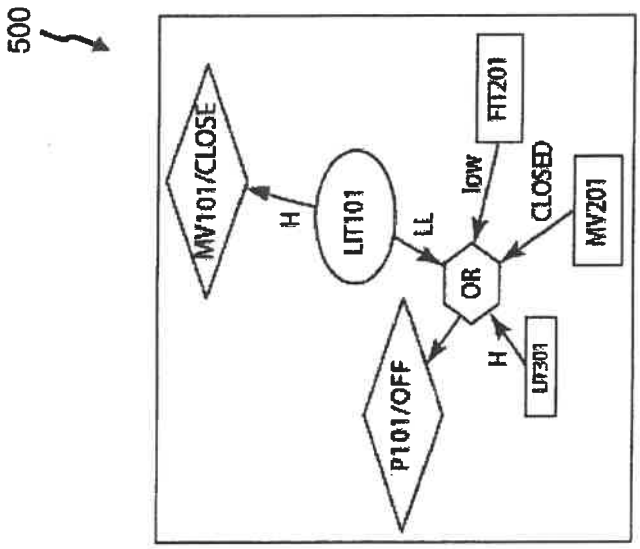
500
MV101/CLOSE
H
LIT101
LL
low
FIT201
CLOSED
MV201
OR
H
LIT301
P101/OFF

FIG. 5

600

PLC	Invariants*	
	Backward check	**Forward check**
1	P1BC1: $v_2 = \text{L} \rightarrow (v_3 = 1 \text{ AND } v_1 > \delta)$ P1BC2: $v_2 = \text{H} \rightarrow (v_3 = 0 \text{ AND } v_1 \leq \delta)$	P1FC1: $v_2 = \text{"LL"} \rightarrow v_4 = 0$ P1FC2: $v_5 = \text{"H"} \rightarrow v_4 = 0$
2	P2BC1: $v_4 = 1 \rightarrow v_8 = 1$ P2BC2: $v_4 = 0 \rightarrow v_8 = 0$	P2FC1: $v_5 = \text{"HH"} \rightarrow v_8 = 0$ P2FC2: $v_5 = \text{"H"} \rightarrow v_8 = 1$
3	P3BC1: $v_5 = \text{"H"} \rightarrow v_8 = 1 \text{ AND } v_4 = 1$ P3BC2: $v_5 = \text{"HH"} \rightarrow v_8 = 0 \text{ AND } v_4 = 0$	P3FC1: $v_5 = \text{"LL"} \rightarrow v_{10} = 1$ P3FC2: $v_{10} = 0 \rightarrow v_6 < \delta$ P3FC3: $v_8 > \sigma \rightarrow v_{10} = 0$ P3FC4: $v_{11} = \text{"L"} \rightarrow v_{10} = 1 \text{ OR } v_9 = 1$ P3FC5: $v_{11} = \text{"H"} \rightarrow v_{10} = 0$
4	P4BC1: $v_{11} = \text{"L"} \rightarrow v_{10} = 1 \text{ OR } v_9 = 1$	Forward check in PLC4 presently not implemented.

*Each invariant is assigned a code for ease of reference in the implementation.

FIG. 6

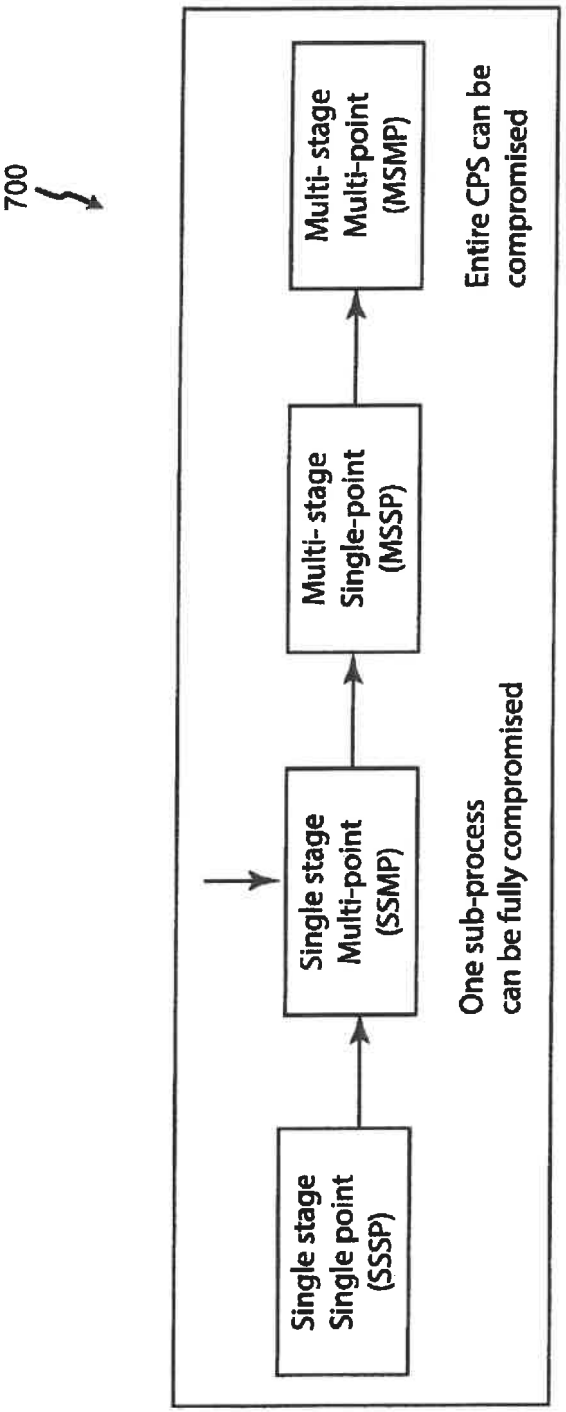
700
Single stage
Single point
(SSSP)
Single stage
Multi-point
(SSMP)
Multi- stage
Single-point
(MSSP)
Multi- stage
Multi-point
(MSMP)
One sub-process
can be fully compromised
Entire CPS can be
compromised

FIG. 7

800

Scenario[1]	Sensor[2]	Attack
A1 (2:1:2:1)	1: LIT101, {FIT101}	(0 → 1) (1 → 0)
	3: LIT301	Only Level sensor values are altered.
A2 (12:12:4:4)	1: LIT101, {FIT101, FIT201}	(00 → 11) (01 → 10) (10 → 01) (11 → 00)
	3: LIT301, {FIT301, DPIT301}	(00 → 11) (01 → 10) (10 → 01) (11 → 00)
A3 (2:12:2:4)	1: MV101	(0 → 1) (1 → 0); only one sensor attacked.
	3: P101, MV201	(00 → 11) (01 → 10) (10 → 01) (11 → 00)
A4 (12:176:4:16)	1: MV101, P101	(00 → 11) (01 → 10) (10 → 01) (11 → 00)
	3: P101, MV201, P301, MV302	(00 → 11) (01 → 10) (10 → 01) (11 → 00)
A5 (176:704:16:64)	1: FIT101, FIT201, MV101, P101	(0000 → 1111) (0001 → 1110) (0010 → 1101) (0011 → 1100)(0100 → 1011) (0101 → 1010) (0110 → 1001) (0111 → 1000)(1000 → 0111) (1001 → 0110) (1010 → 0101) (1011 → 0100)(1100 → 0011) (1101 → 0010) (1110 → 0001) (1111 → 0000)
	3: FIT301, DPIT301, P101, MV201, P301, MV302	Only 10 experiments were conducted in this case.
A6 (56:176:8:16)	1: LIT101, {MV101, FIT101, FIT201}	(001 → 011)(001 → 110)(010 → 101)(011 → 100)(100 → 011)(101 → 011)(110 → 001)(111 → 000)
	3: LIT301, {FIT301, DPIT301, P101, MV302}	Only 10 experiments were conducted in this and the above case.

[1]a:b:c:d: a: attack combinations in PLC1, b: attack combinations in PLC3, c: attacks implemented in PLC1, d: attacks implemented in PLC3. Two or more sensors/actuators compromised in addition to LIT where mentioned excepting A3:1.

[2]n: X– n denotes the PLC and X the sensors affected by the attack. Level sensors (LIT) are continuously manipulated by the attacker to ensure that the water level indicated to the corresponding PLC corresponds to the altered states of the actuators and sensors. Items in brackets are explained in Example 4.

FIG. 8

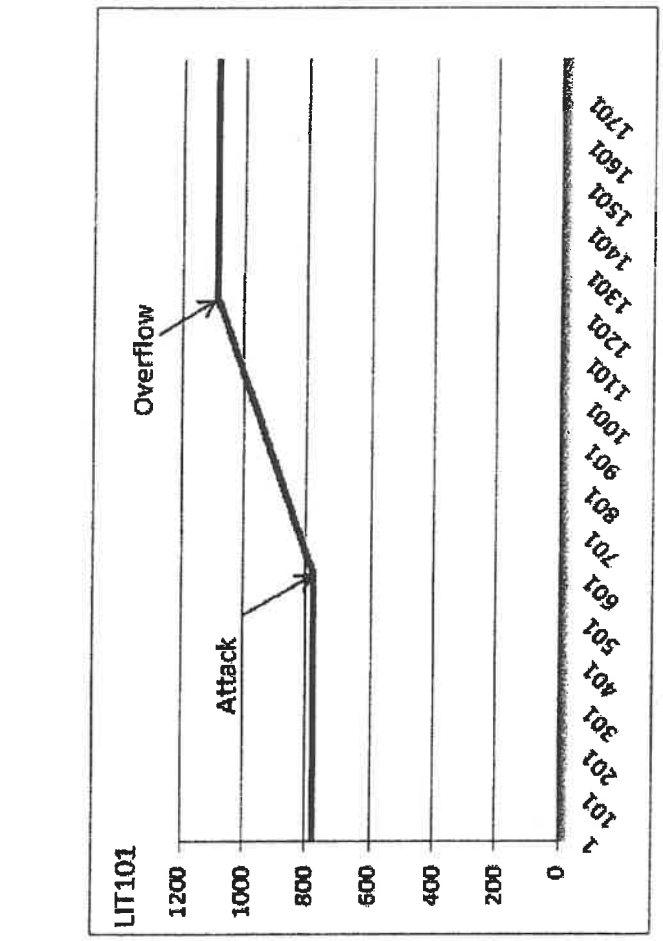
900
LIT101
1200
1000
800
600
400
200
0
Overflow
Attack
1
101
201
301
401
501
601
701
801
901
1001
1101
1201
1301
1401
1501
1601
1701

FIG. 9