

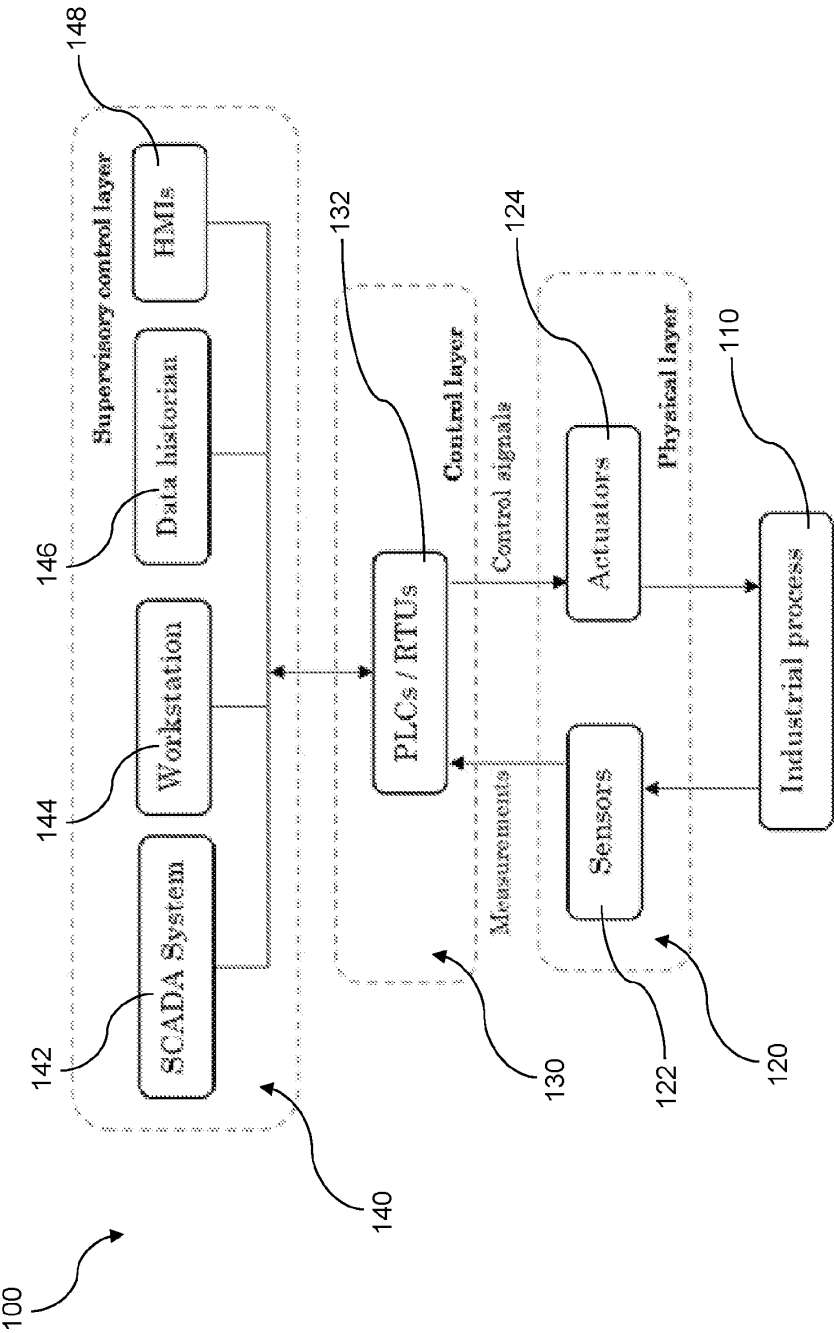


Figure 1

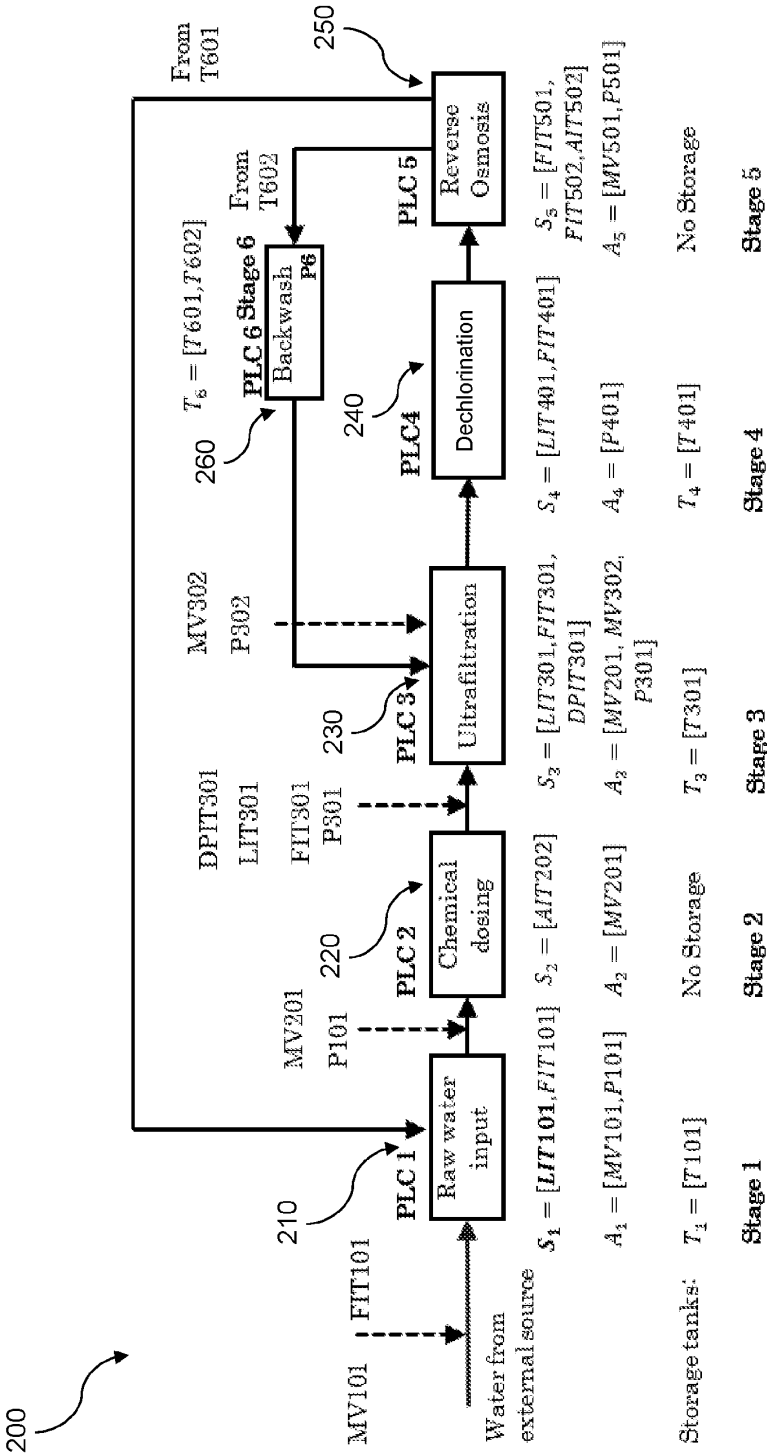


Figure 2A

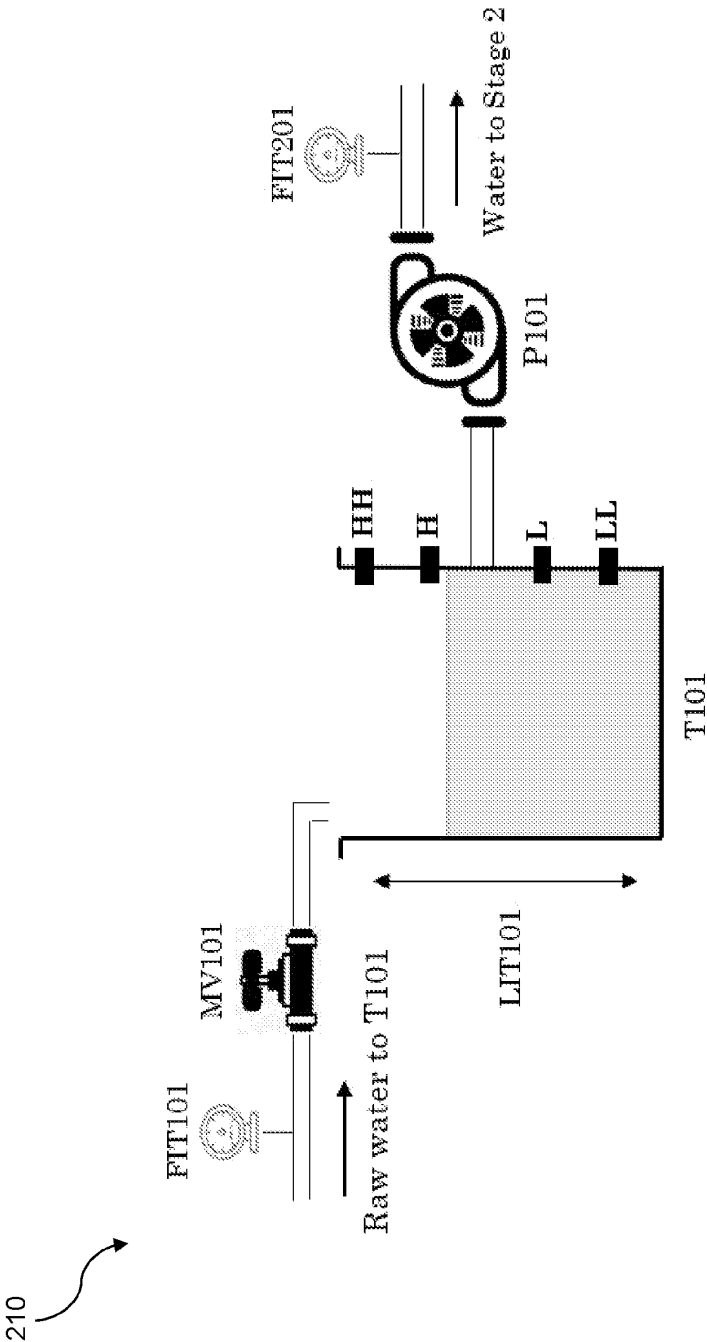


Figure 2B

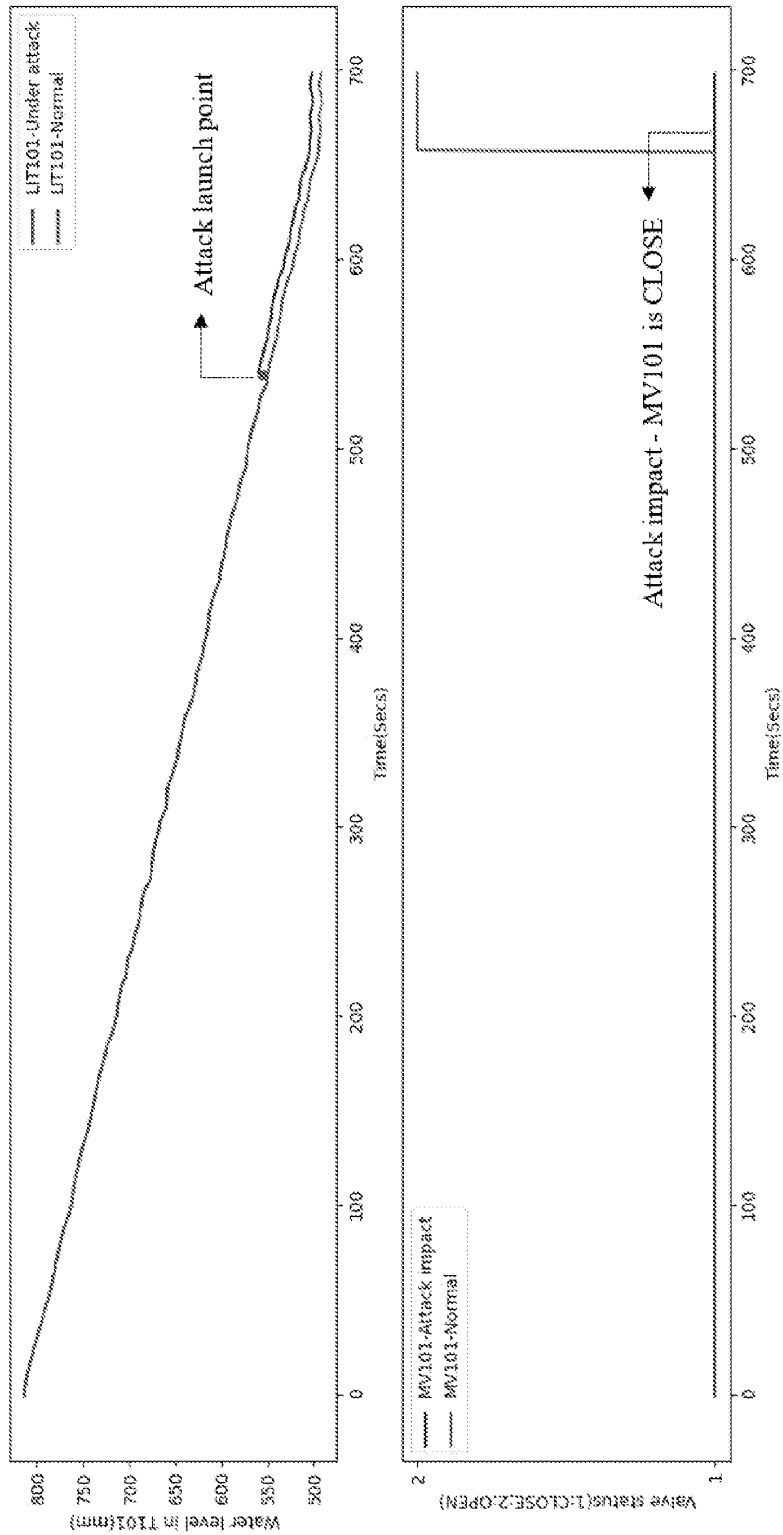


Figure 3

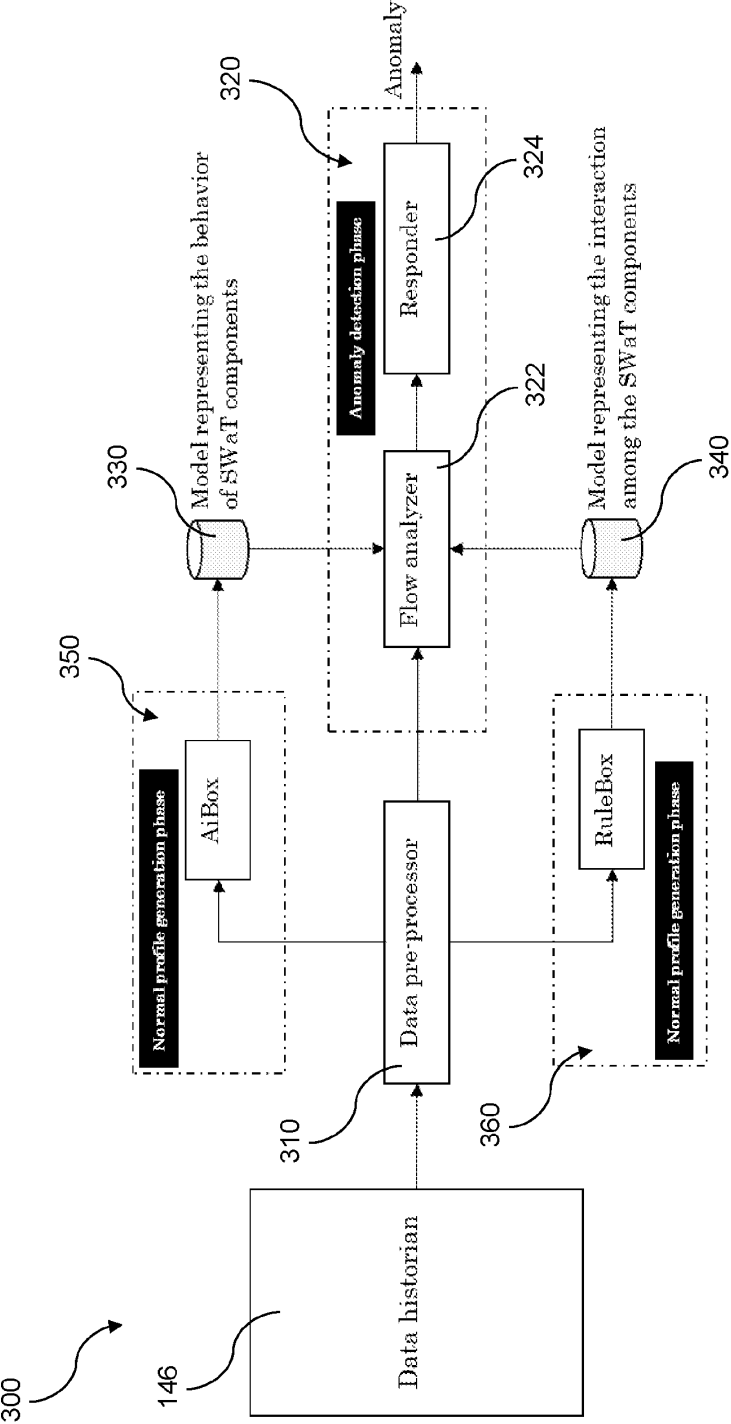


Figure 4A

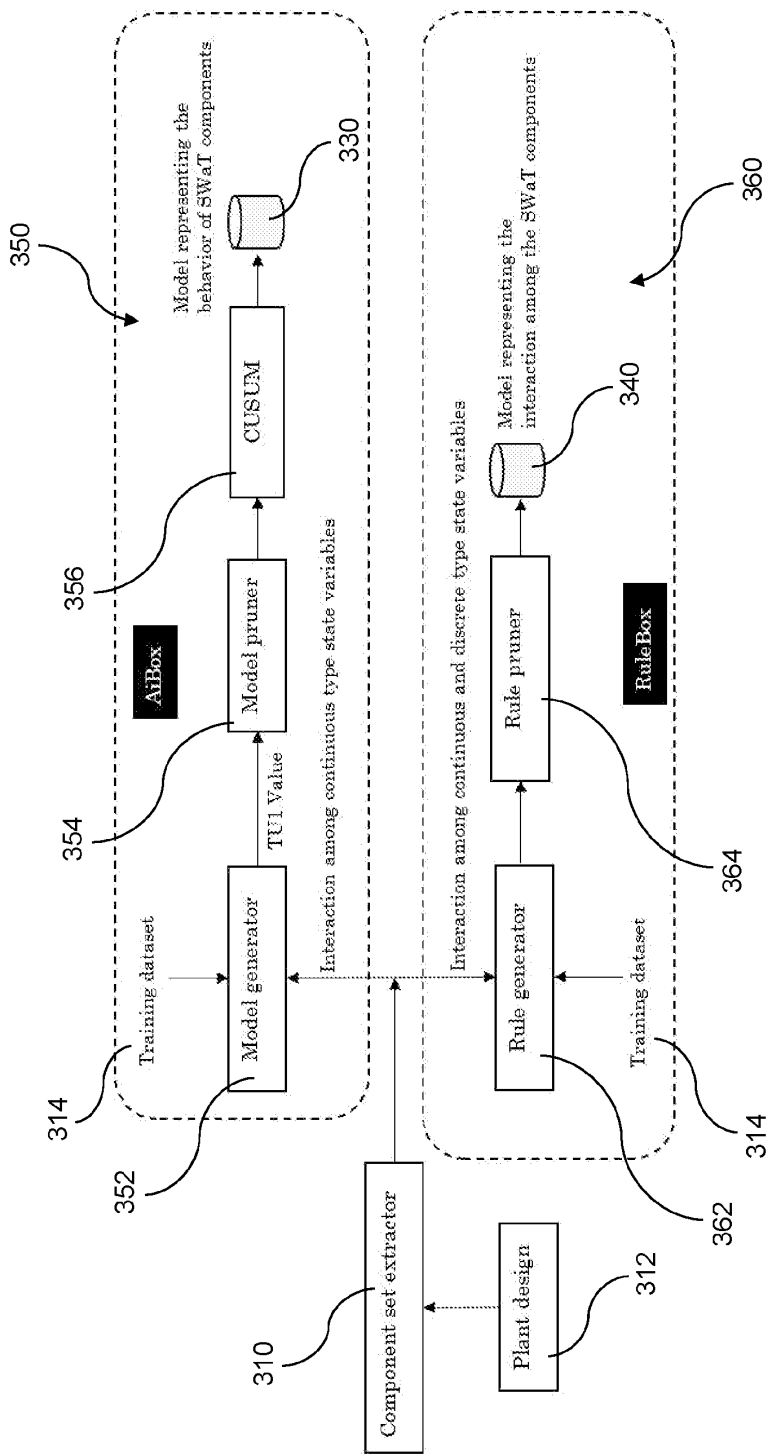


Figure 4B

Invariant No.	State Variable	Invariant Description
INV 1.1	LIT101	If $LIT101(t) > H$, then $MV101 = OFF$
INV 1.2		If $LIT101(t) < L$, then $MV101 = ON$ and $P101 = OFF$
INV 1.3		$LIT101(t) = LIT101(t-1) + \eta(FIT201(t)-FIT101(t))$
INV 1.4		$LL < LIT101 < HH$
INV 1.5		If $LIT101$ increases, then $MV101 = ON$
INV 1.6		If $LIT101$ decreases, then $MV101 = OFF$ and $P101 = ON$
INV 2	FIT101	$FIT101(t) = FIT101(t-1) + \gamma MV101(t)$
INV 3	FIT201	$FIT201(t) = FIT201(t-1) + \gamma P101(t)$
INV 4	MV101	If $MV101(t) = OFF$, then $FIT101 = 0$
INV 5	P101	If $P101(t) = OFF$, then $FIT201 = 0$
<i>η and γ are constants of unit conversion</i>		

Figure 5

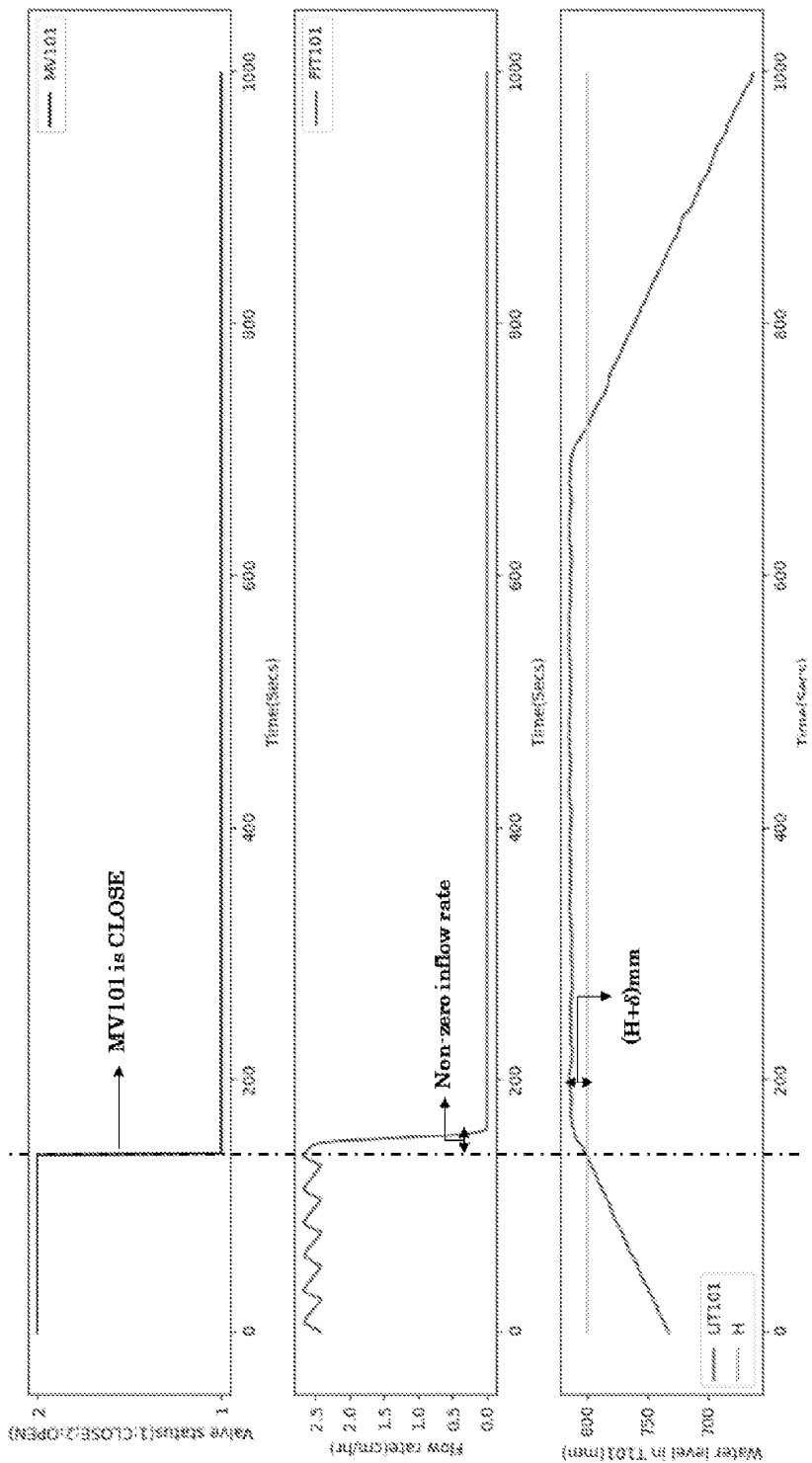


Figure 6

No.	Independent State Variable	Dependent State Variable	Sample Rule
1	FIT101	MV101	If MV101 is OPEN, then after 5 seconds, FIT101 should be > 0.81 m ³ /h
2			If MV101 is CLOSED, then after 7 seconds, FIT101 should be < 3.5 m ³ /h
3	If MV101 is OPEN, then LIT101 should be < (H+50) mm		
4	LIT101		If MV101 is CLOSED, then LIT101 should be > (L-20) mm
5			If P101 or P102 is ON, then LIT101 should not be < (L-10) mm
6	FIT101	P101 or P102	If P101 or P102 is ON, then after 10 seconds, FIT201 should be > 0.5 m ³ /h

Figure 7

No.	Attack Scenario	Attack Intention
1	1	Open MV101
2	2	Turn on P102
3	3	Increase LIT101 by 1 mm/s
4	6	Set value of AIT202 to 6
5	7	Increase water level in tank T101 to above H
6	8	Set value of DPIT to >40 kPa
7	10	Set value of FIT401 to < 0.7 m ³ /h
8	11	Set value of FIT401 to 0
9	16	Decrease water level in tank T401 by 1 mm/s
10	17	Do not let MV303 open
11	21	Keep MV101 open continuously and set value of LIT101 to 700 mm
12	22	Stop UV401, set value of AIT502 to 150, and force P501 to remain on
13	23	Set value of DPIT301 to >0.4 bar, keep MV302 open, and keep P602 closed
14	24	Turn off P203 and P205
15	25	Set value of LIT401 to 1000 mm and keep P402 on
16	26	Keep P101 on continuously and set value of LIT301 to 801 mm
17	27	Keep P302 on continuously and set value of LIT401 to 600mm until time 1:26:01
18	30	Keep P101 on continuously, keep MV101 open continuously, and set value of LIT101 to 700 mm
		P102 started itself because LIT301 level became low
19	31	Set LIT401 to < L
20	32	Set LIT301 to > HH
21	33	Set LIT101 to > H
22	34	Turn P101 off
23	35	Turn P101 off and keep P102 off
24	36	Set LIT101 to < LL
25	40	Set value of FIT401 to 0
26	41	Decrease LIT301 by 0.5 mm/s

Figure 8A

No.	Attack Scenario	Attack Mode	Attack Target State Variable	Attack Intention
1	A1.1*	NA	LIT101	Read the value of LIT101
2	A1.2*	Gradual-bias		Continuous attack on LIT101
3	A2*	Constant		Access SCADA through Remote Desktop Protocol (RDP) to change the H value of LIT101
4	A3.1*	Fixed-bias	DPIT301	Spoofing DPIT301
5	A3.2*	Constant		
6	A4*	Constant	FIT401	Set FIT401 to a constant to affect UV process
7	A5**	NA	MV101 and FIT101	Attack MV101 and FIT101 to flood T101 with more water
8	A6.1*	NA	P101	Log into SCADA to change P101 state
9	A6.2*	Chatter		Launch chatter attack on P101 for 5 seconds
10	A7*	Constant	LIT401	Set LIT401 to a constant 725 mm
11	A8*	NA	P602	Turn on P602 to refill the backwash tank T602
12	A9*		MV303	Open MV303 to water during filtration process
13	A10*	Constant	LIT401	Set LIT401 to H to turn off P301
*: Single-point attack; **: Multi-point attack				

Figure 8B

No.	Attack Scenario	Attack Detection Rate						
		DNN	SVM	1D-CNN records	1D-CNN attacks	TABOR	LAD-ADS	Anomaly Detection System 300 (AICrit)
1	1	0	0	0.99	1	0.04	0.98	0.99
2	2	0	0	1	1	0.93	0.792	1
3	3	0	0	0.22	0.9	0	0.68	0.37*
4	6	0.71	0.72	0.9	1	0.99	0.005	0.001
5	7	0	0.88	1	1	0	0.05	0.99
6	8	0.92	0.91	1	1	0.61	0.98	0.98
7	10	1	0.43	1	1	0.99	0.8	0.75
8	11	0.97	1	1	1	0.99	0.98	0.93
9	16	0	0	0.23	1	0	0.55	0.22*
10	17	0	0	0.63	1	0.59	0.2	0.71
11	21	0	0.01	0.9	1	0.08	0.97	0.98
12	22	0.99	1	1	1	0.99	0.98	0.98
13	23	0.86	0.87	1	1	0	0.94	0.96
14	24	0	0	0.169	1	0	0.01	0
15	25	0	0.01	0.019	0.2	0	0.97	0.98
16	26	0	0	1	1	0.99	0.79	0.86
17	27	0	0	0.06	1	0.19	0.46	0.87
18	30	0	0	1	1	0.99	0.94	0.98
19	31	0	0	0.303	0.2	0	0.86	0.93
20	32	0	0.9	0.93	1	0	0.93	0.98
21	33	0	0	0.88	1	0.89	0.84	0.92
22	34	0	0	0.6	1	0.99	0	0
23	35	0	0	0	0	0.25	0.36	0.3
24	36	0	0.11	0.87	1	0.88	0.87	0.83
25	40	0.99	0.92	1	1	0.99	0.86	0.9
26	41	0	0.35	0.638	1	0	0.845	0.87
<i>*Detected after the attack was removed.</i>								

Figure 9A

No.	Anomaly Detectors	False Positive Rate (%)	
		Automated Mode	Manual Mode
1	MLP	0	0.87
2	DAD	0	0
3	Anomaly Detection System 300 (AiCrit)	0	0

Figure 9B

Attack Scenario	Detection Time (seconds)		
	MLP	DAD	Anomaly Detection System 300 (AiCrit)
A1.2	18	10	16
A2	5	2	2
A3.1	Not detected	Not detected	3
A3.2			4
A4			19
A5	24		32
A6.2	Not detected		23
A7	15		10
A8	Not detected		19
A9	detected	2	3
A10	9	2	5

Figure 9E

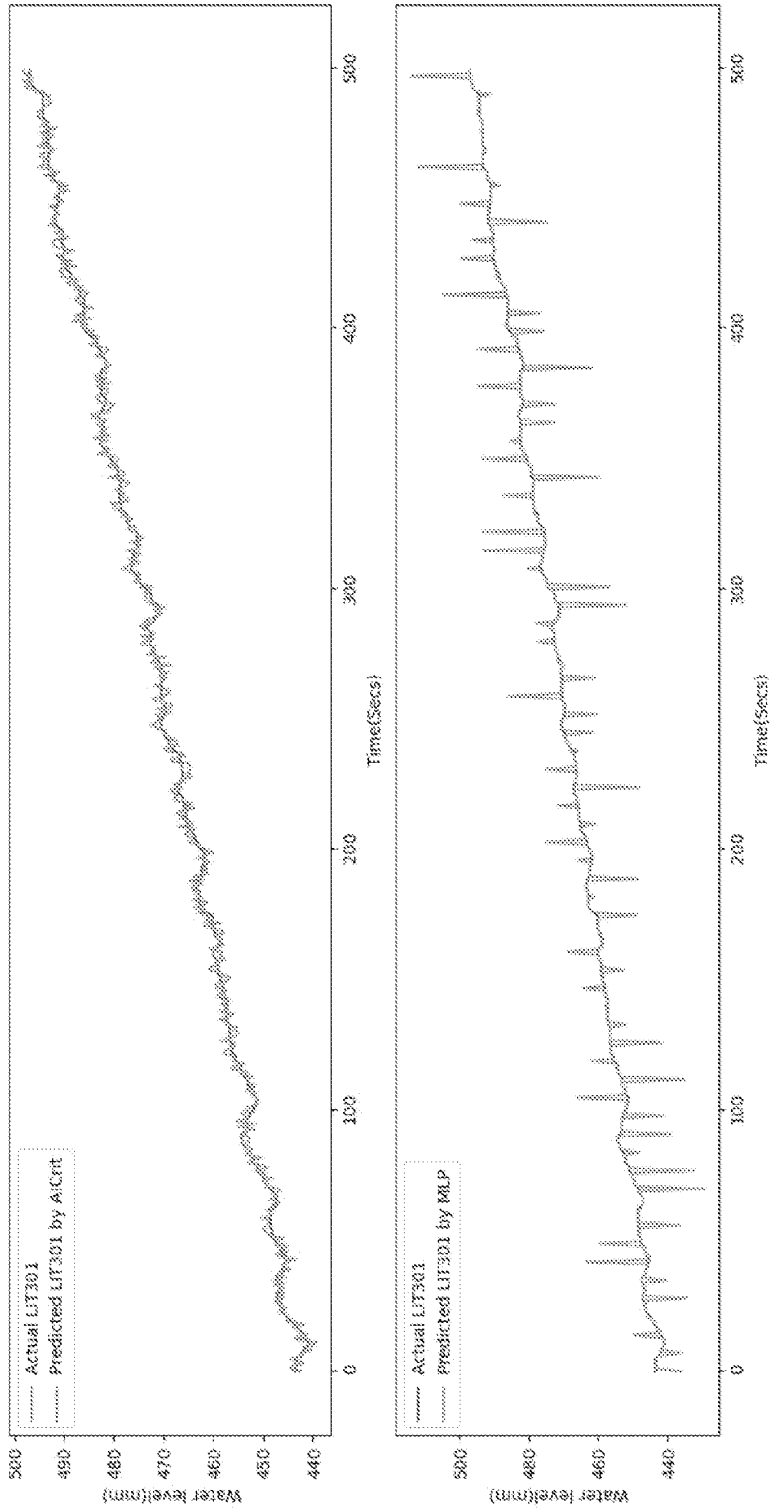


Figure 9C

No.	Attack Scenario	Attack Target State Variable	Attack Launch Time	Attack Detection Time	Detection Time (seconds)	Tag Raised Alert
1	A1.1	LIT101	10:34:05	-	-	-
2	A1.2		10:55:28	10:56:44	16	LIT101 _R ,
3	A2		11:02:36	11:02:38	2	LIT101 _A
4	A3.1	DPIT301	11:18:22	11:18:25	3	MV301 _R , MV303 _R
5	A3.2		11:18:19	11:18:23	4	MV303 _R
6	A4	FIT401	11:24:17	11:24:35	19	P401 _R
7	A5	MV101, FIT101	11:31:26	11:31:58	32	MV101 _R
8	A6.1	P101	11:35:07	-	-	-
9	A6.2		11:35:07	11:35:30	23	P101 _R
10	A7	LIT401	11:39:40	11:39:50	10	MV302 _R , LIT401 _A
11	A8	P602	12:18:20	12:18:39	19	P602 _R
12	A9	MV303	12:25:20	12:25:23	3	MV303 _R
13	A10	LIT401	12:39:21	12:39:26	5	LIT401 _R , LIT401 _A
<i>Subscript A means alert was raised by the first behavioural models 330; Subscript R means alert was raised by the second behavioural models 340</i>						

Figure 9D