

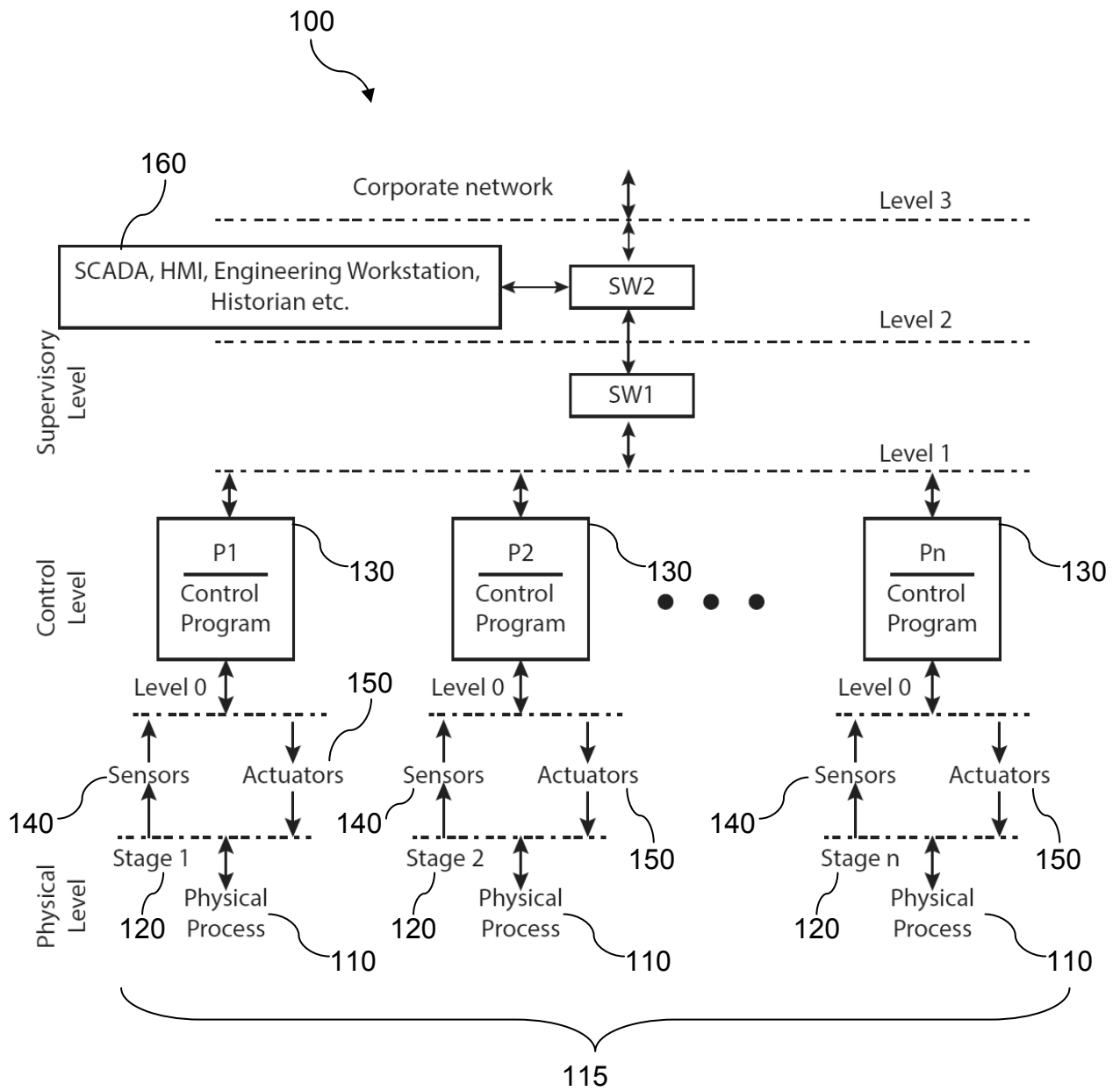


Figure 1

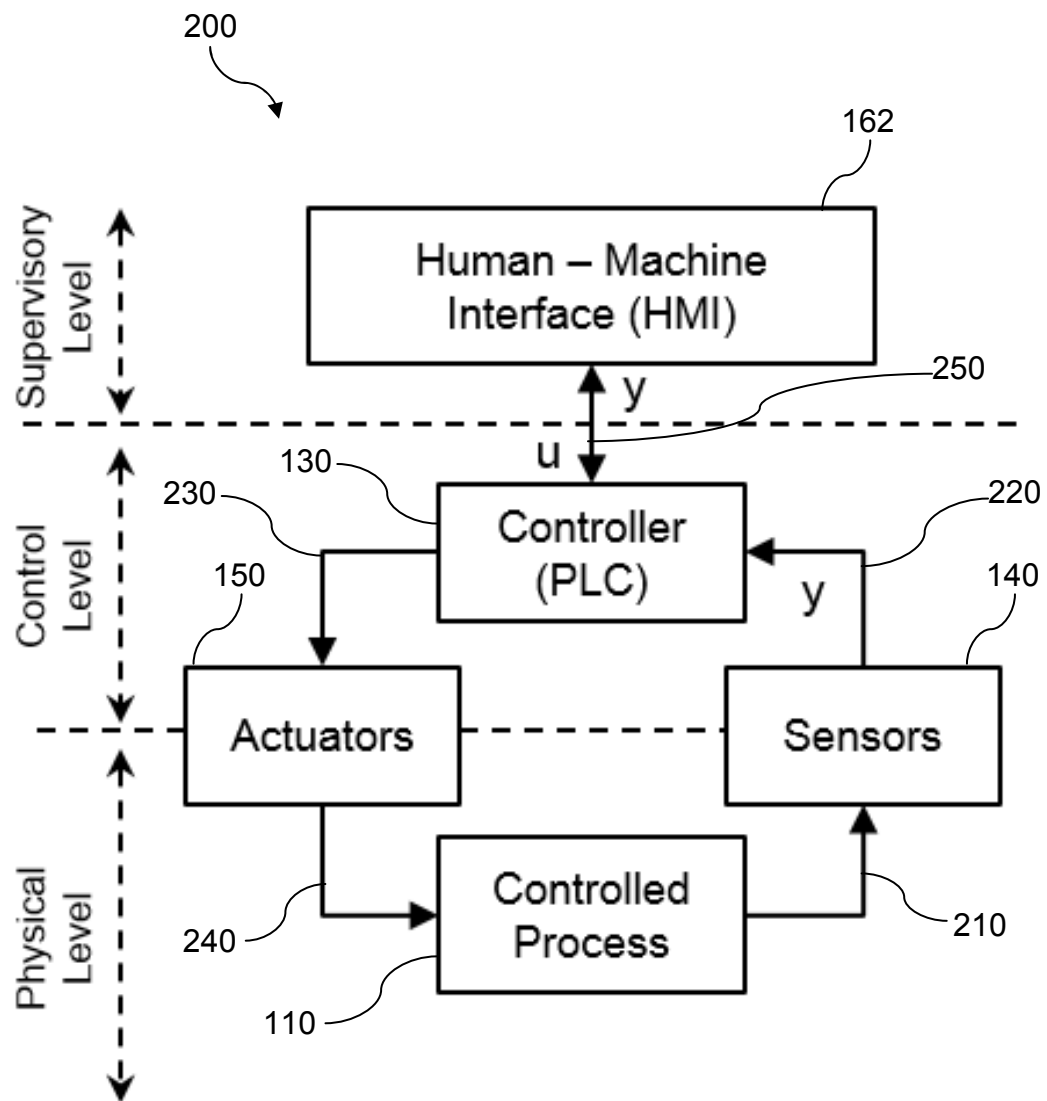


Figure 2

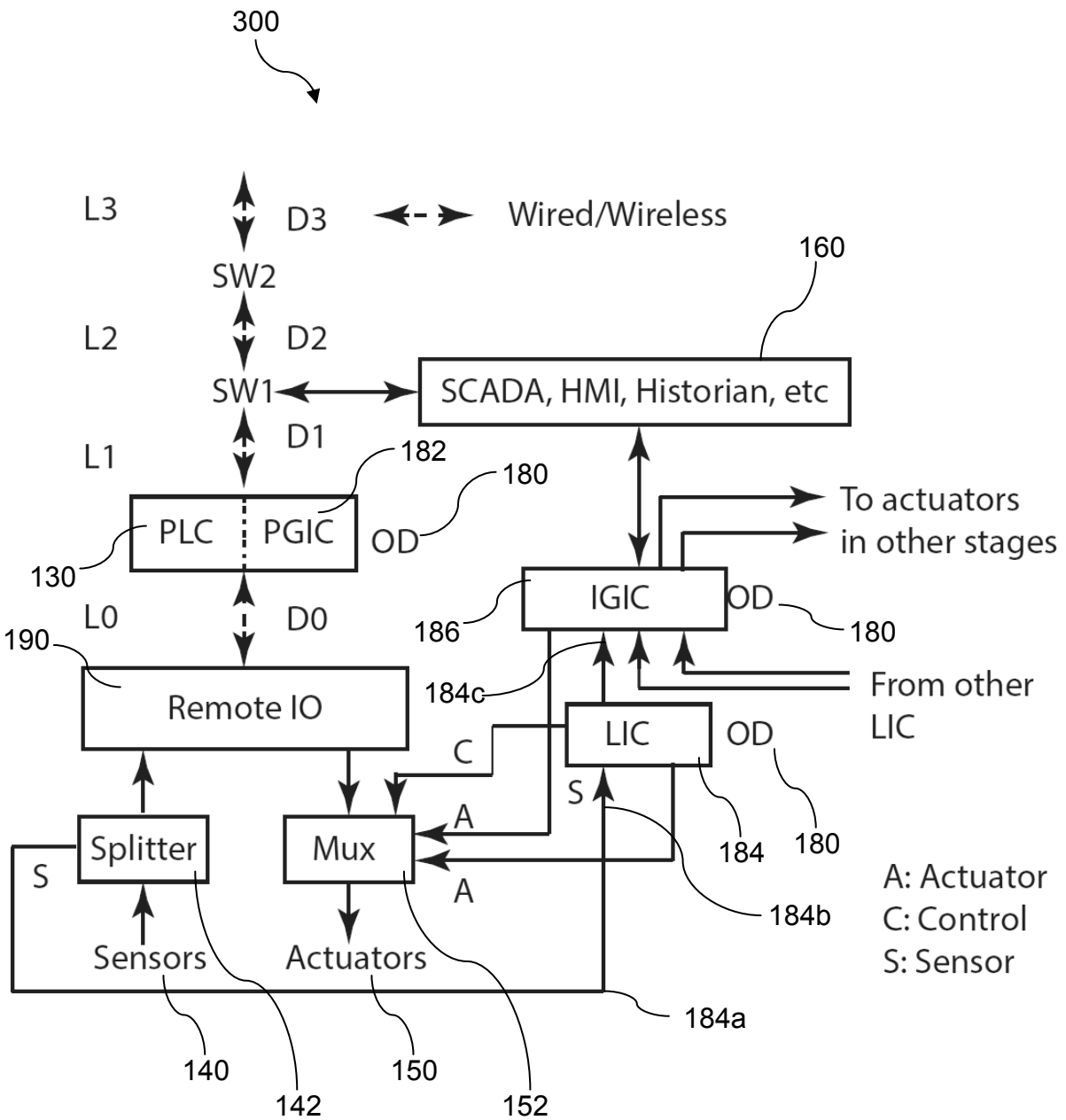


Figure 3

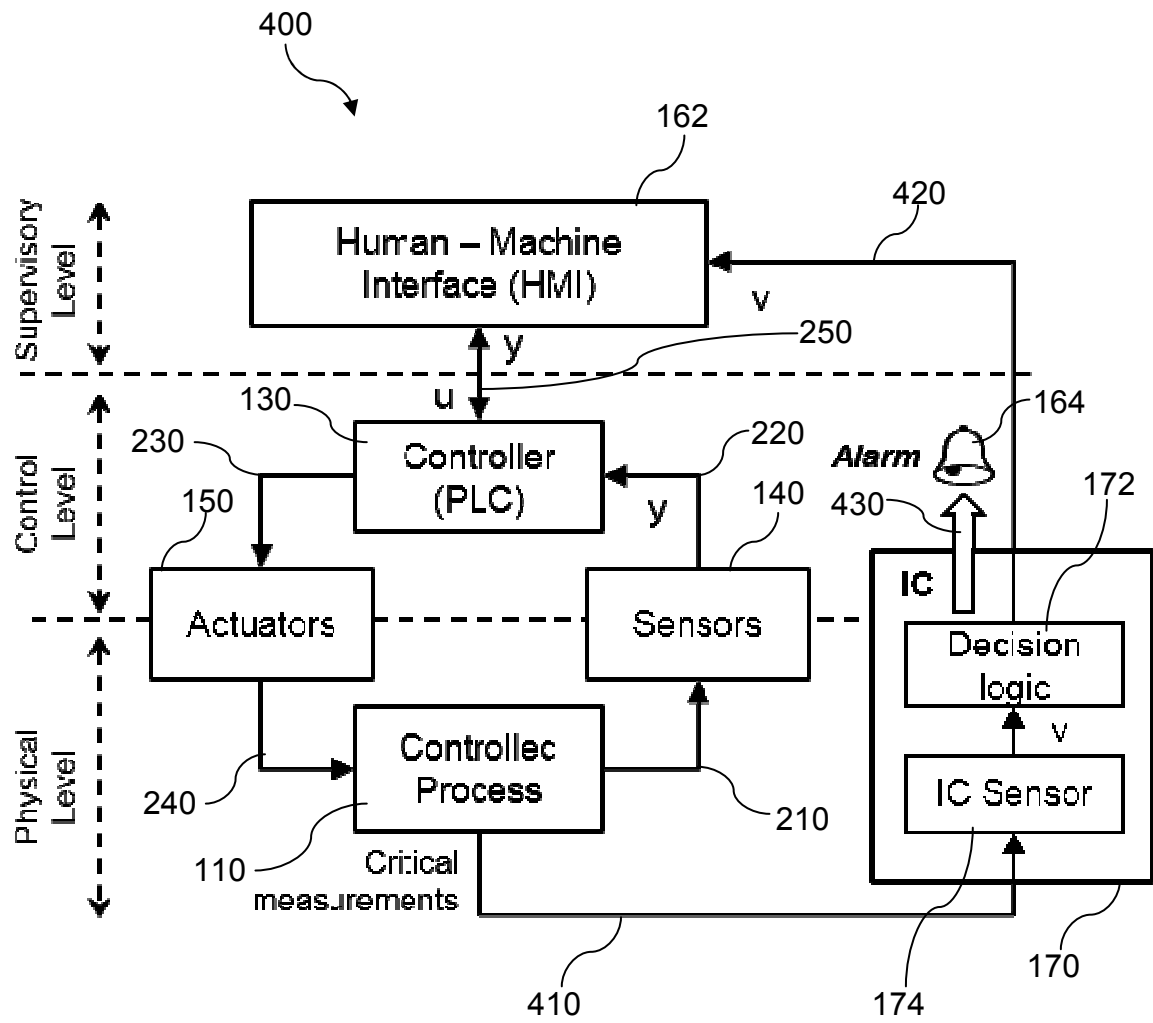


Figure 4

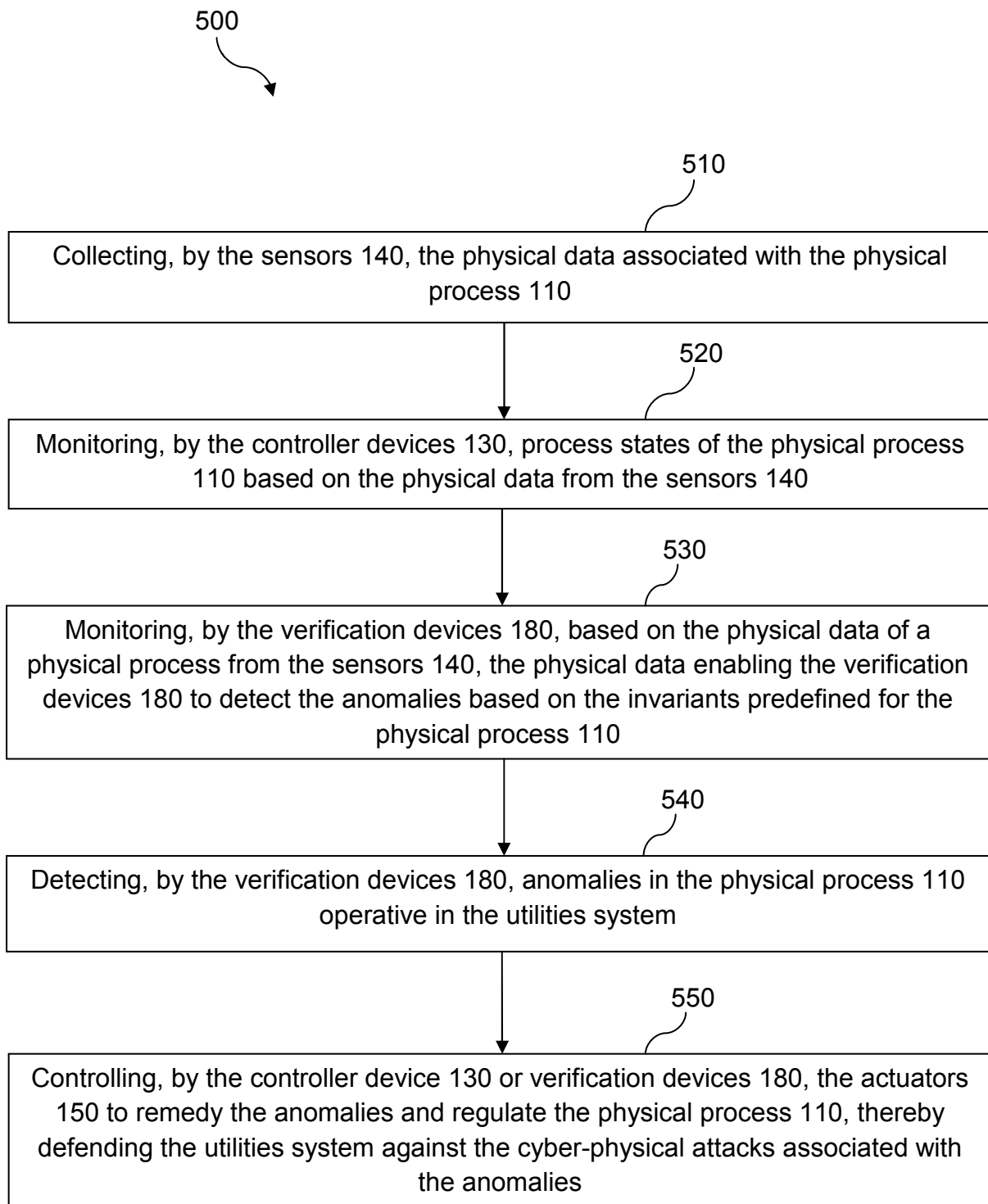


Figure 5

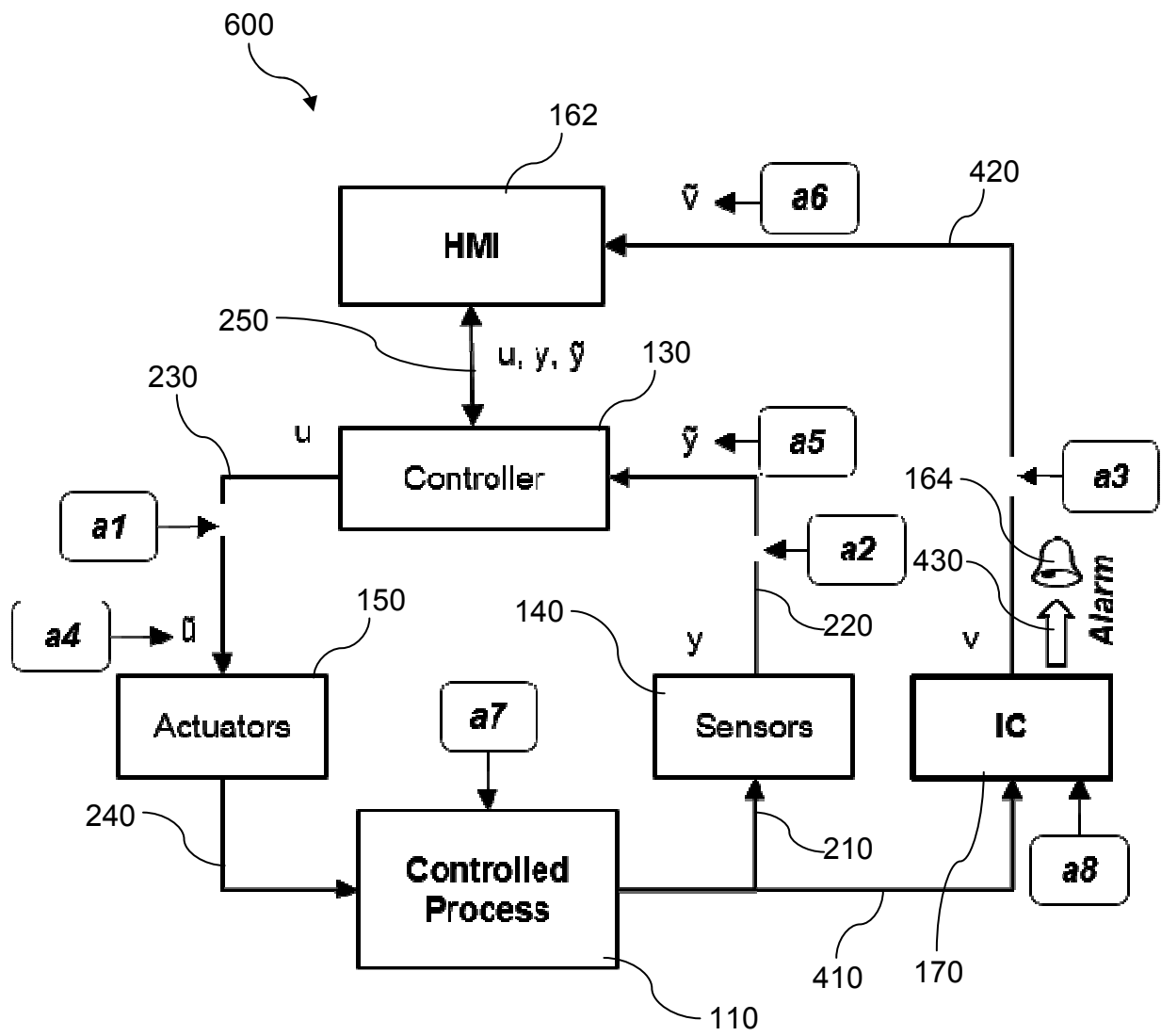


Figure 6

700

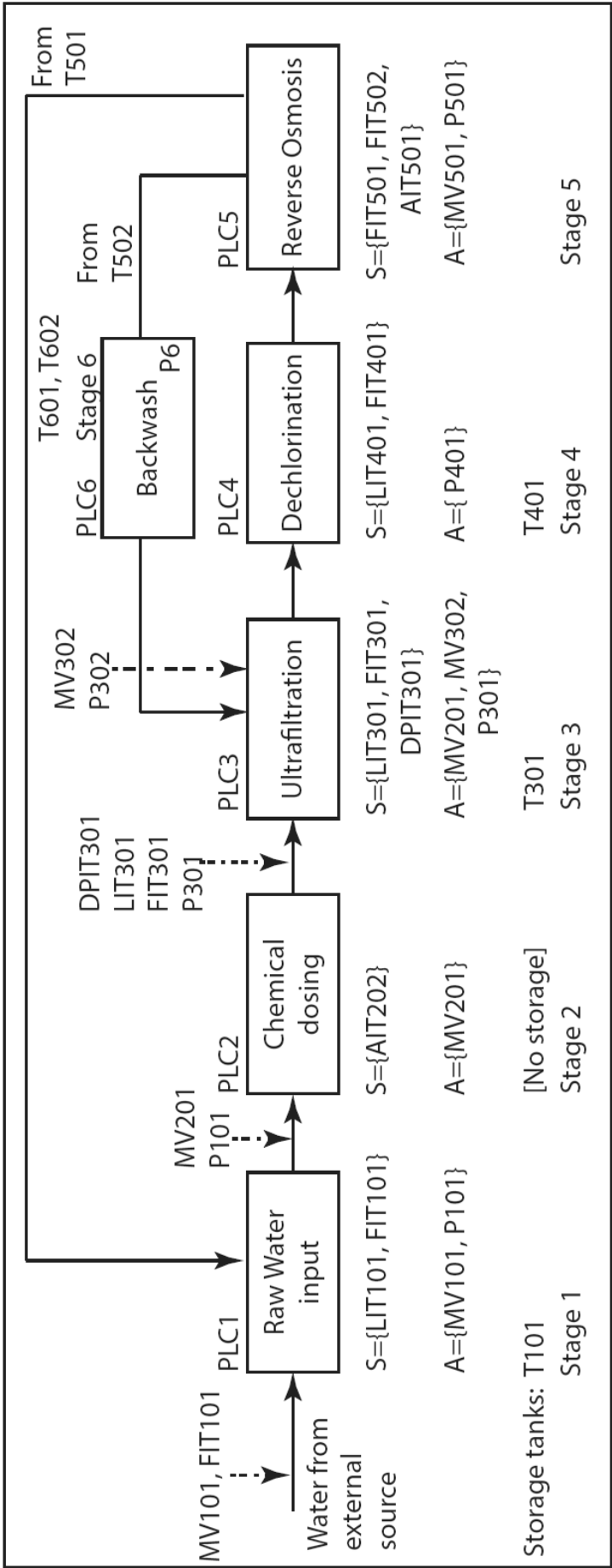


Figure 7



Model element	Description
$x_{k+1} = Ax_k + Bu_k$	x_k and u_k , respectively, denote the state and input vectors in SWaT at time step k . A and B are matrices of constants.
$y_{k+1} = Cx_k + D\eta_k$	y_{k+1} is a vector of sensor readings at step $k+1$ received by a PLC; C and D are constant matrices; η denotes sensor noise vector under normal system operation. $y_{k+1} = y'_k$ when the system is under attack; y'_k is the data sent by an attacker to the PLC and depends on the type of attack. ³
$L_{k+1}^i = a_i L_k^i + b_i(f_k^{i,in} - f_k^{i,out})$	Water level in tank i at step $k+1$. $f_k^{i,in}$ and $f_k^{i,out}$ denote, respectively, flow of water into and out of tank i , $1 \leq i \leq 5$. a_i and b_i are proportionality constants.
$\hat{x}(k+1) = y(k) + \alpha(f_k^{i,in} - f_k^{i,out})$	Estimating the system state $\hat{x}$. α is the flow rate to water level conversion factor.
$\frac{\sum_{i=1}^n (\hat{x}(i) - y(i))}{n} > \epsilon$	When true, this condition (an invariant) implies an attack, or a component failure. ϵ and n are attack detection parameters determined experimentally. In the experiments reported here, $n = 10$ and $\epsilon = 0.55$.

Figure 8



Region 1		
Element type	Label	Function
Logical: Data	LIT101	Senses water level in tank T101 in stage 1.
Logical: Data	P101	Pump to move water from tank T101 to tank T301 via a chemical dosing station.
Logical: Code	PLC 1	Code in PLC 1 to control stage.
Physical	MV101	Motorized valve that when opened allows the flow of water from an external source into tank T101.
Region 2		
Logical: Data	DPIT301	Differential pressure sensor across the Ultrafiltration unit.
Logical: Data	LIT301	Senses water level in tank T301 in stage 3.
Physical	Ultrafiltration unit	Membrane based unit to remove small particles from incoming water.

Figure 9