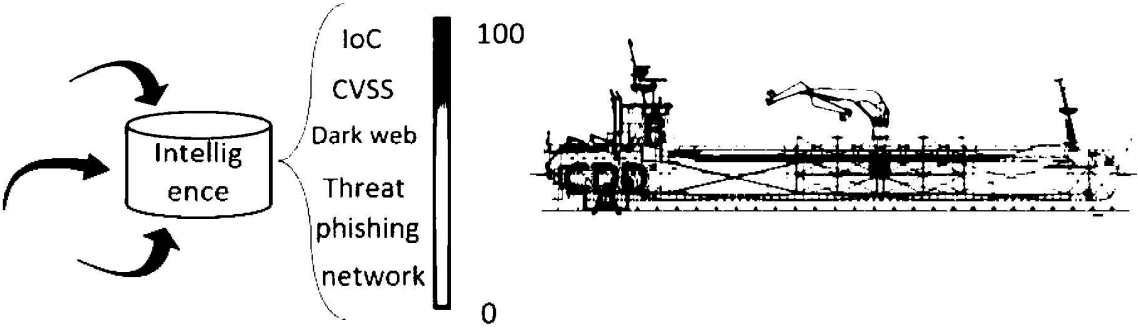
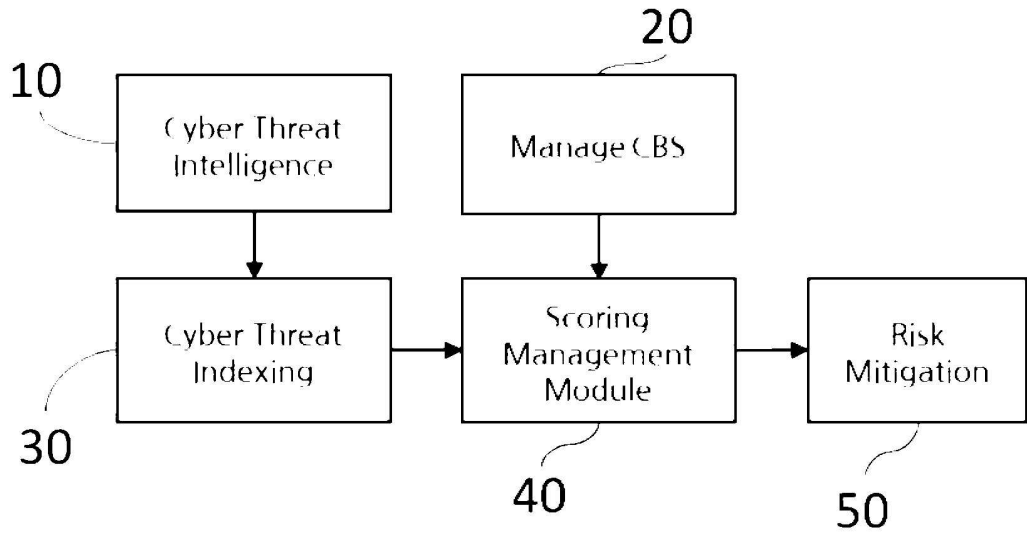


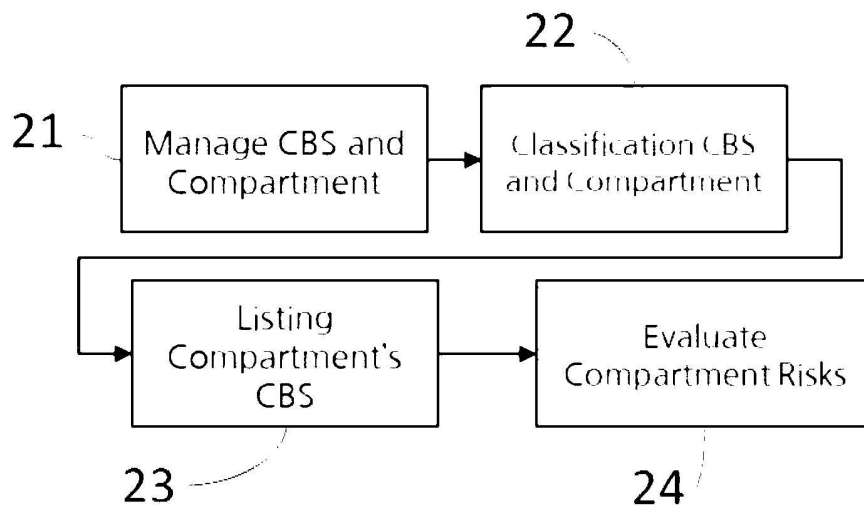
【FIG. 1】



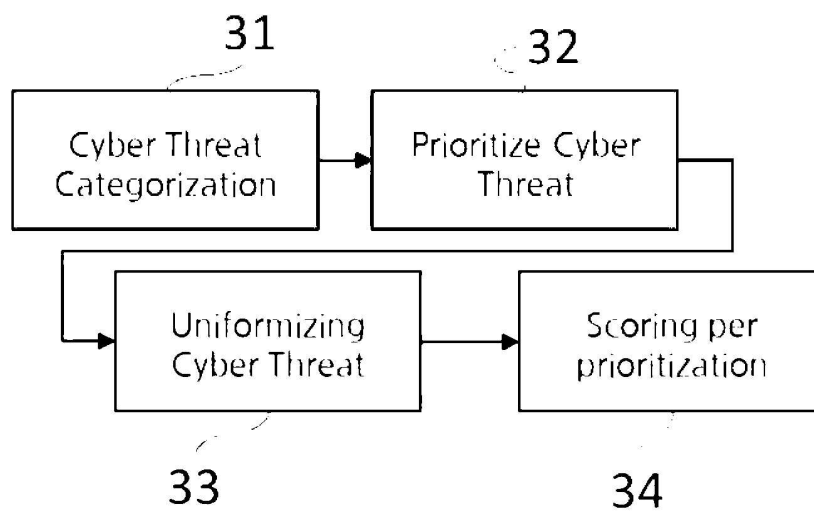
【FIG. 2】



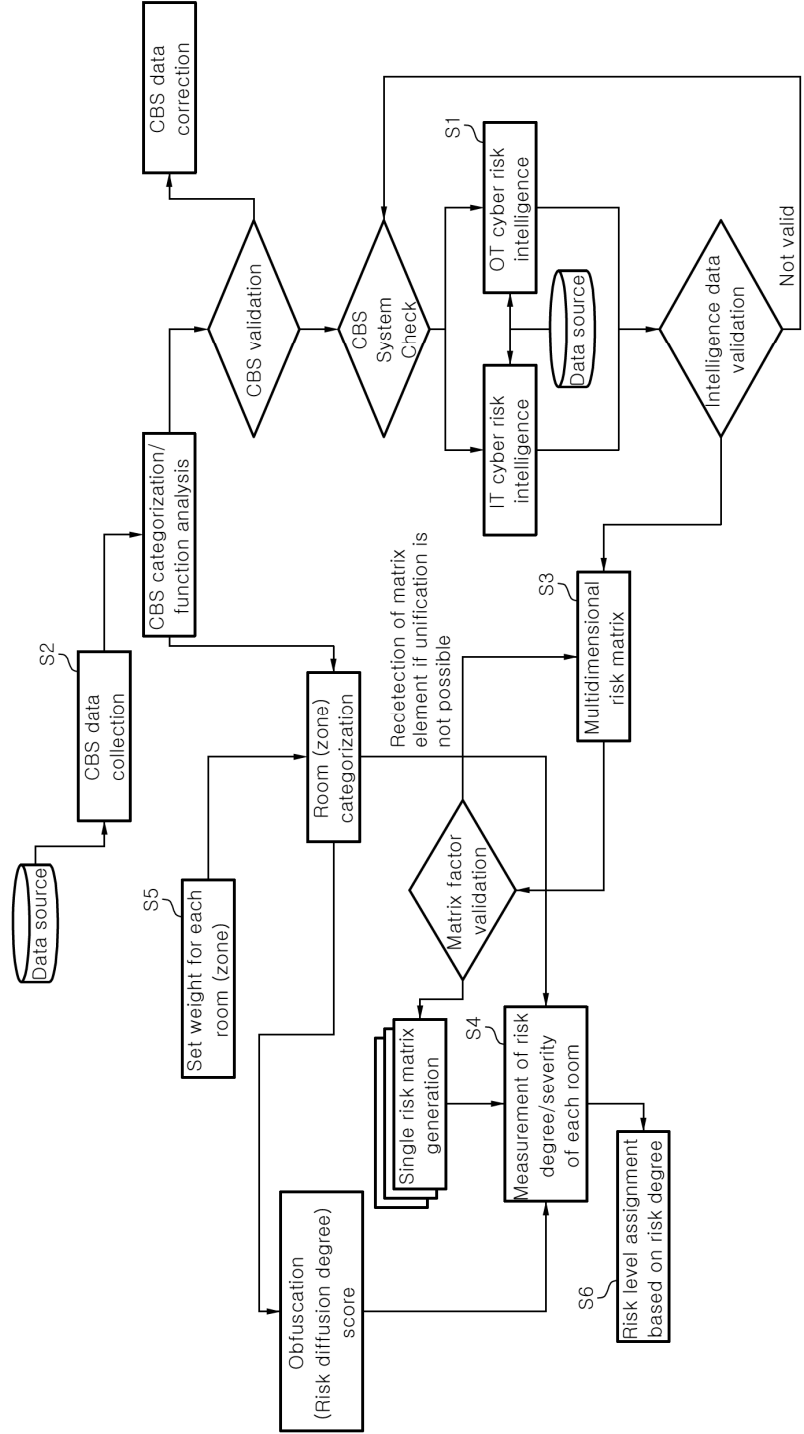
【FIG. 3】



【FIG. 4】



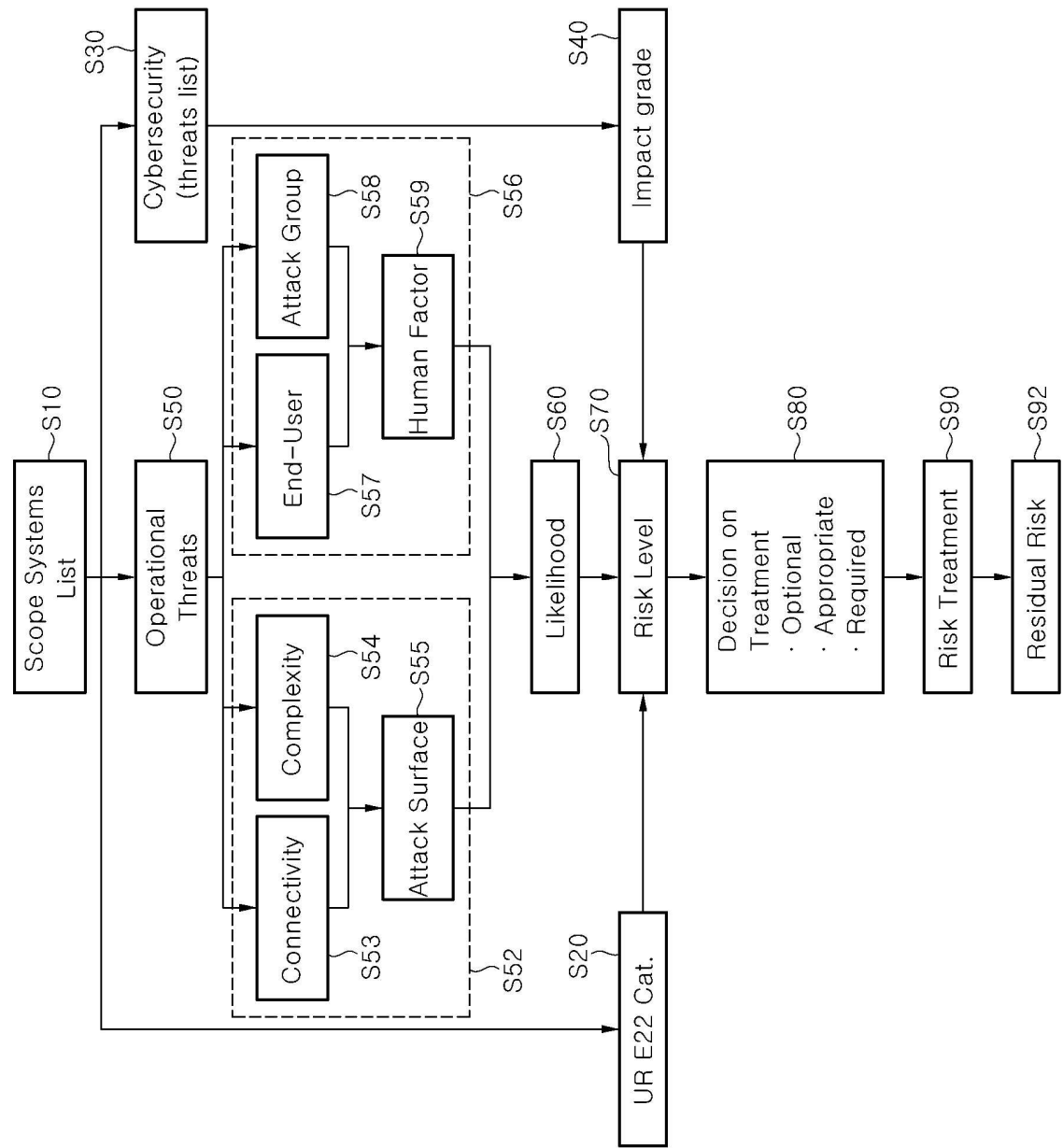
【FIG. 5】



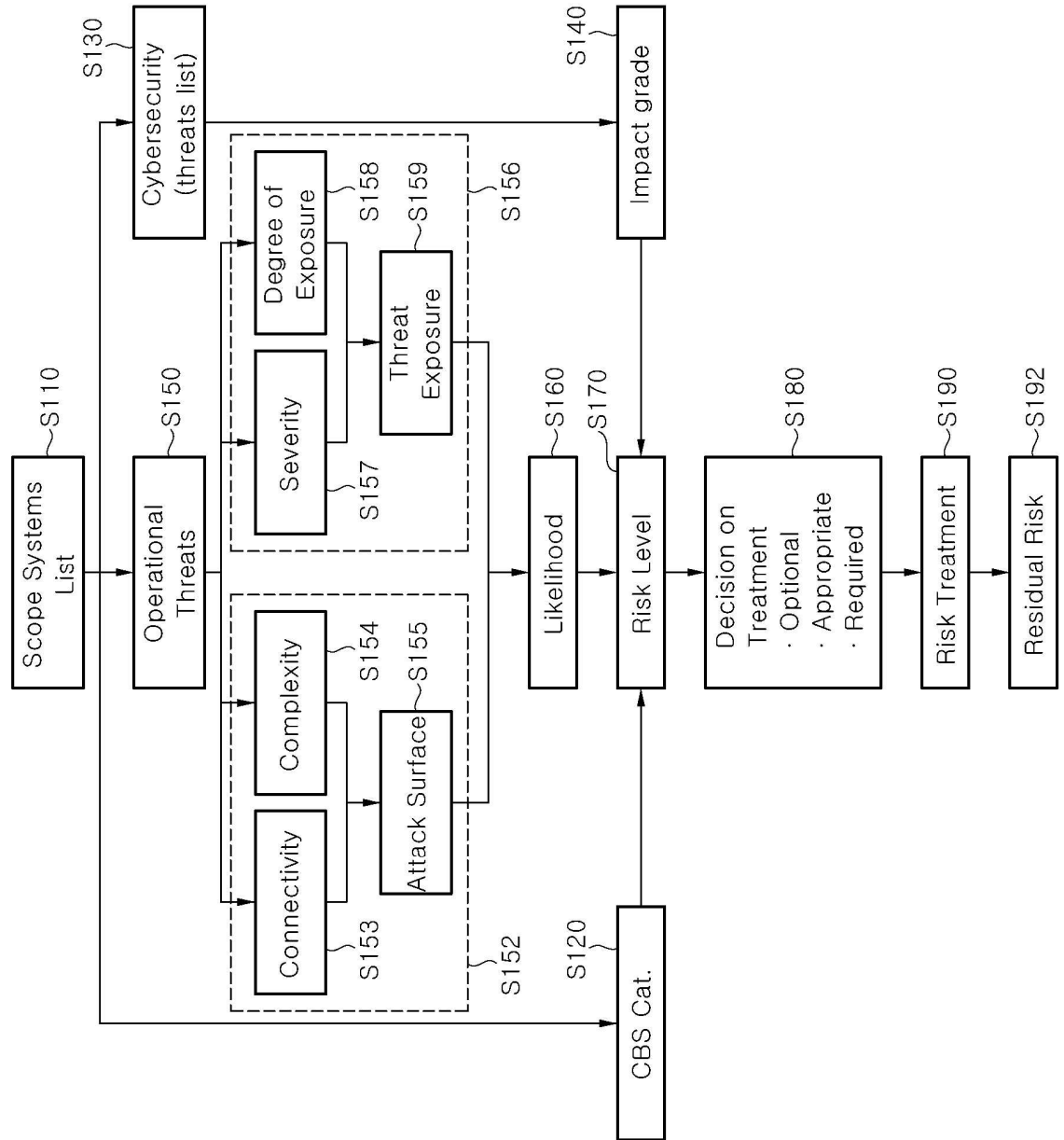
【FIG. 6】

ISO 27001	Phase	IACS Rec 171
Scope	1	Scope Systems List
Normative references	2	UR E22 Cat.
Terms and definitions	3	Cybersecurity (threats list)
Context of the organization	4	Impact grade
Leadership	5	Operational Threats
Planning	6	Likelihood
Support	7	Risk Level
Operation	8	Decision on Treatment
Performance evaluation	9	Risk Treatment
Improvement	10	Residual Risk

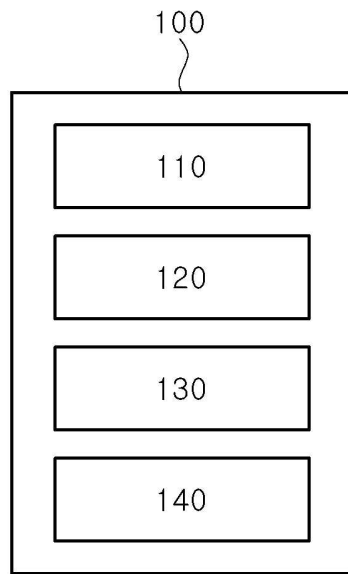
【FIG. 7】



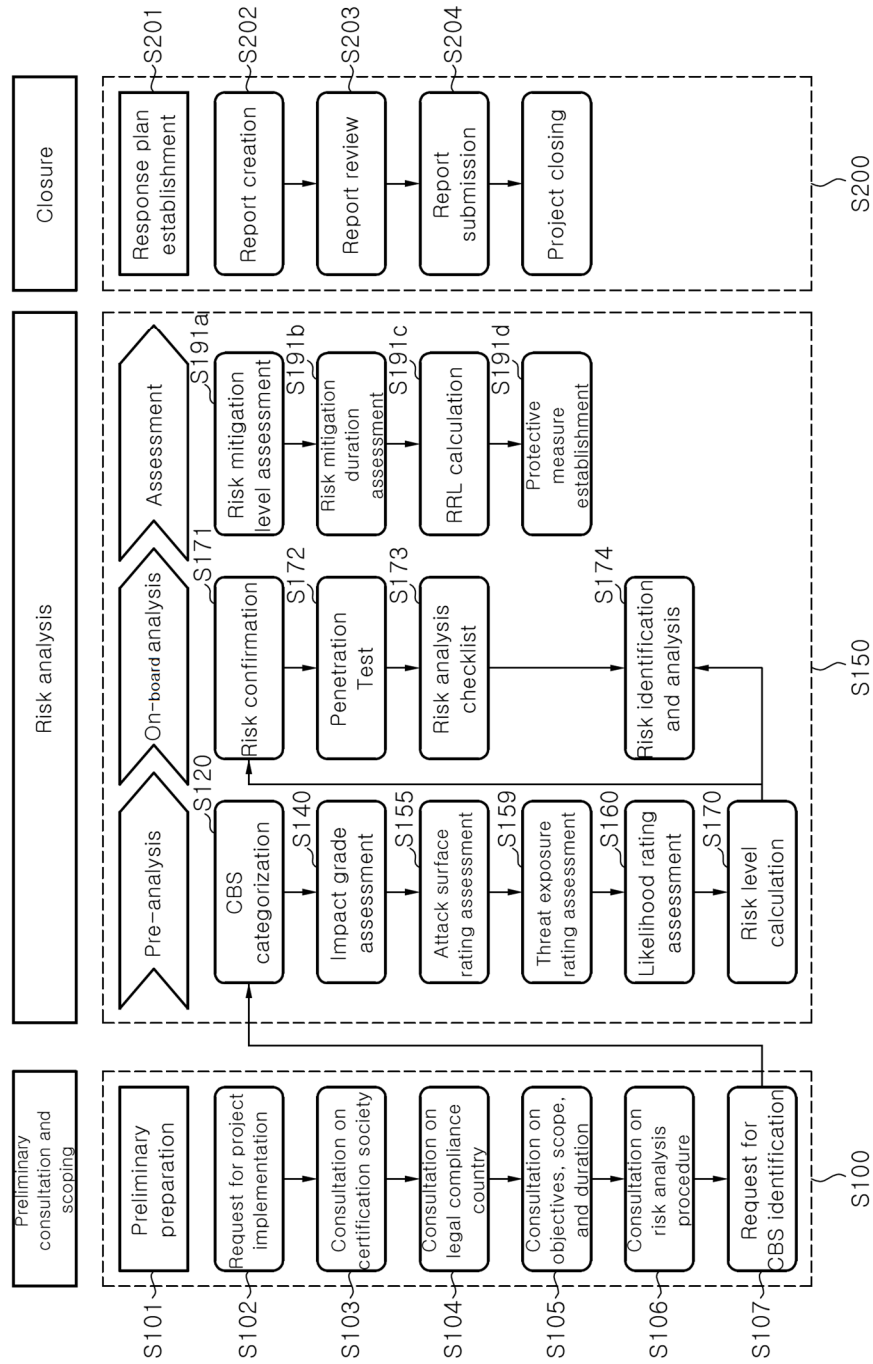
【FIG. 8】



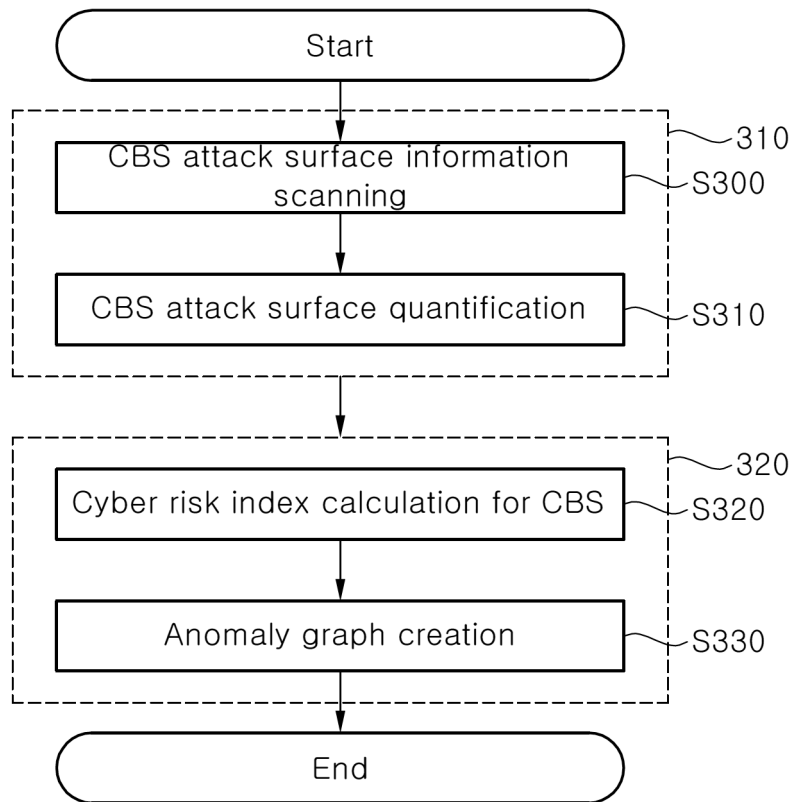
【FIG. 9】



【FIG. 10】



【FIG. 11】



【FIG. 12】

TYPE	Attack Surface Score															Threat Score		
	CVE score		Network					System										
								Secure control										
	O/S	Installed program	Open Port	Using weak Protocol	Running Daemon	Identification and authentication	Use control	System integrity	Data confidentiality	Restricted data flow	Timely response to events	Resource availability	Source IP	Destination IP	Detection Rule			
CBS n	c1	c1	n1	n2	n4	s1	s2	s3	s4	s5	s6	s7	t1	t2	t3			

【FIG. 13】

