A Method to Choose Between Automation and Human Operators for Recovery Actions During a Cyber Attack

Douglas L. Van Bossuyt

Naval Postgraduate School

NAVAL
POSTGRADUATE
SCHOOL

NAVAL POSTGRADUATE SCHOOL

A Method to Choose Between Automation and Human Operators for Recovery Actions During a Cyber Attack

Douglas L. Van Bossuyt, PhD
Bryan M. O'Halloran, PhD
4 April 2019
Presented at 17th Annual Conference on Systems Engineering Research

The need: Recovery from cyber attacks

- Modern complex systems are vulnerable to cyber attacks
- Cyber attacks are going to happen no matter what we do
- Systems have to be recoverable from cyber attacks
- Either automated systems or human operators can be used to perform recovery actions during a cyber attack
- Goal of recovery actions can be either a safe shutdown state, a return to nominal operations, or a degraded operating state

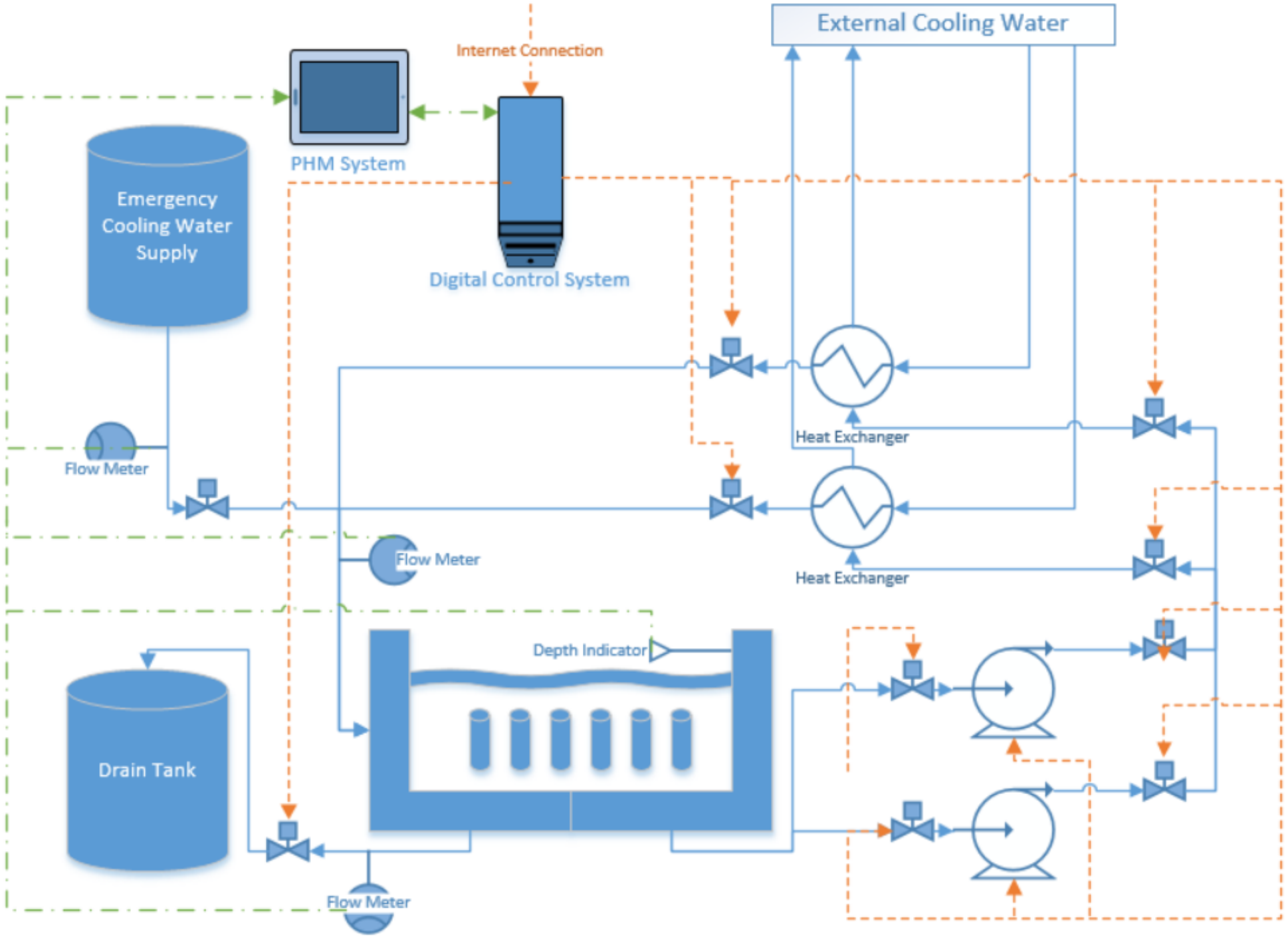
Methodology

- Preparatory step: Setup the analysis
- Step 1: Hazard/threat analysis
- Step 2: Analyze recovery actions
- Step 3: Trade-off study between automated and human recovery actions
- Step 4: Recovery decision-making

Preparatory step: Setup the analysis

- Develop a functional model of the system
- Develop a database of function-to-component mappings with PHM information
- Conduct analysis of system for prognostics and health management sensor inclusion per L'Her et. al.'s method and Function Failure Identification and Propagation method
- Result is a list of cut sets showing the failure cases ranked by probability and a PHM subsystem plan to detect incipient failures

One line diagram of spent fuel pool case study with PHM system



Failure Scenario Chain of Events	Probability of Occurrence (Per Year)
Heat Exchanger Motor Valve #1 Fails Closed, Heat Exchanger Motor Valve #2 Fails to Open, Water Boils Off From Cooling Pool	2.7E-4/yr
Pump #1 Fails to Operate, Pump Valve #3 Fails Closed, Water Boils Off From Cooling Pool	5.3E-5/yr
Pump #2 Fails to Operate, Pump Valve #1 Fails Closed, Water Boils Off From Cooling Pool	5.3E-5/yr
Heat Exchanger #1 Clogs, Heat Exchanger #2 Clogs, Emergency Cooling Water Supply Exhausted, Water Boils Off From Cooling Pool	1.8E-6/yr
Drain Valve Fails Open, Emergency Cooling Water Valve Fails to Open, Water Boils Off From Cooling Pool	2.7E-7/yr

Table 1. Top five most likely failure scenarios determined Using L'Her et. al.'s method and the FFIP method of functional risk analysis

Step 1: Hazard/threat analysis

- Use O'Halloran et. al.'s method to assess threat of cyber attacks on a system
  - Results in identifying worst case scenario cyber attacks
- Down-select to most probable or most concerning cyber attack scenarios
- Result is a list of cyber attack scenarios – NO probabilities attached intentionally

Scenario Label	Hazard Scenario
Scenario 1	Cyber Attack Disables Pumps #1 and #2, Emergency Cooling Water Tank Depleted, Water Boils Off From Cooling Pool
Scenario 2	Cyber Attack Opens Drain Valve, Emergency Cooling Water Tank Depleted, Water Boils Off From Cooling Pool
Scenario 3	Cyber Attack Closes Pump Valves #1 and #3, Emergency Cooling Water Tank Depleted, Water Boils Off From Cooling Pool
Scenario 4	Cyber Attack Opens Drain Valve, Cyber Attack Prevents Emergency Cooling Water Valve From Opening
Scenario 5	Cyber Attack Closes Heat Exchanger Valves #1 and #3, Emergency Cooling Water Tank Depleted, Water Boils Off From Cooling Pool
~~Scenario 6~~	~~Cyber Attack Disables Pumps #1 and #2, Cyber Attack Opens Drain Valve, Cyber Attack Prevents Emergency Cooling Water Valve From Opening~~
~~Scenario 7~~	~~Cyber Attack Closes All Valves, Water Boils Off From Cooling Pool~~

Table 2. Spent fuel cooling pool hazard list as identified by O'Halloran et. al.'s method. A horizontal line through a hazard indicates that the hazard has been removed from further consideration due to being ruled as invalid for further analysis.

Step 2: Analyze recovery actions

- L'Her et. al.'s method provides some recovery actions
- Additional recovery actions may need to be developed based on cyber attack scenarios identified in Step 1
- Develop recovery action probabilities of success and cost information for both human operator and automated recovery actions
  - Human reliability assessment techniques are useful to determine probability of operator success

Recovery Action	Hazard Scenario	Recovery Action Description
Recovery 1	Scenario 1	Pump Control Override to Restart Pumps
Recovery 2	Scenario 2	Install and Turn On Pump Between Drain Tank and Cooling Pool to Recycle Water
Recovery 3	Scenario 3	Install and Open Backup Pump Valves #1 and #3
Recovery 4	Scenario 4	Install and Turn On Pump Between External Water Source and Emergency Cooling Water Tank
Recovery 5	Scenario 5	Install and Turn On Fire Water Source to Replenish Cooling Pool

Table 4. Specific recovery actions that can be taken to stop incipient failures caused by cyber attacks. Recovery actions in italics font indicate that they were not previously identified by L'her et. al.'s method.

Step 3: Trade-off study between automated and human recovery actions

- Conduct a trade-off study to determine if it is better to use a human operator or an automated system to attempt to perform a recovery action
- Calculate following values:
  - Probability of successful recovery
  - Recovery action cost
  - Successful attack cost

Formula details

- Probability of successful recovery $P_{RS} = P_{DMA} * P_{IRA} * P_{RAS}$
- Recovery action cos $COST_{Recovery} = COST_{Humans} + COST_{Equip} + COST_{Maint} + COST_{Res} + COST_{Other}$
- Successful attack cos $COST_{SuccAtt} = COST_{Repair} + COST_{Downtime} + COST_{Remediation} + COST_{OtherSucc}$

Recovery Action	Human / Automation	Probability of Recovery Success	Recovery Action Cost	Successful Attack Cost
Recovery 1	Human Operator	0.85	$0.5M/yr	$10M
	Automated System	0.78	$1.2M/yr	$10M
Recovery 2	Human Operator	0.52	$2.1M/yr	$12M
	Automated System	0.85	$2.7M/yr	$12M
Recovery 3	Human Operator	0.92	$0.75M/yr	$15M
	Automated System	0.95	$0.5M/yr	$15M
Recovery 4	Human Operator	0.7	$1.2M	$9M
	Automated System	0.82	$1.4M	$9M
Recovery 5	Human Operator	0.87	$0.6M	$17M
	Automated System	0.75	$0.3M	$17M

Table 3. Results of analysis of recovery actions performed by either human operators or automated systems. Costs are on a yearly basis.

Step 4: Recovery decision-making

- Using a cost basis to make decisions on either human operators or automated recovery systems
- Note that we are not assigning a probability to cyber attacks – only to outcomes
  - We believe we cannot adequately predict future probabilities of cyber attacks
  - Any cyber security we have today will be broken tomorrow
- We develop Risk Numbers similar to Risk Priority Numbers
  - Rn = Cost * Probability of Occurrence

Formula details

- Successful Recovery: $R_{N-Success} = COST_{Recovery} * P_{RS}$
- Failed Recovery $R_{N-Failure} = (COST_{Recovery} + COST_{SuccAtt}) * (1 - P_{RS})$
- Risks associated with both outcomes $R_{N-Rec-Outs} = R_{N-Success} + R_{N-Failure}$
- Summed Risk Numbers for Humans and Automatio $\sum R_{N-Rec-Outs_{Human}} = R_{N-Human}$

$$\sum R_{N-Rec-Outs_{Automation}} = R_{N-Automation}$$

Results

Recovery Action	$R_{N-Rec-Outs_{Human}}$	$R_{N-Rec-Outs_{Automation}}$	Decision
Recovery 1	2	3.4	Human
Recovery 2	7.86	4.5	Automation
Recovery 3	1.95	1.25	Automation
Recovery 4	3.9	3.02	Automation
Recovery 5	2.81	4.55	Human
			Summation
		$R_{N-Automation}$	16.72
		$R_{N-Human}$	18.52

Table 5. Summary table of risk numbers. Units are *probability* $*$ *Cost*(\$)/1*E*6.

Discussion

- This method is specifically useful in determining if a human operator or an automated system is better for recovering from a cyber attack
- Uncertainty in the data was not presented in the case study but it may be used in the formulas if desired
- Focusing on recovery actions rather than cyber security is an acknowledgement of our inability to provide perfect security

Future work

- Expand method to examine how staffing levels can impact the analysis
  - How many operators do we need for many potential recovery actions?
- Examine how mixed human operator and automated system recoveries can be analyzed
- Examine how recovery actions may be vulnerable to sophisticated cyber attacks

Conclusion

- We presented a method to decide if using a human operator or an automated system is better to perform a recovery action during a cyber attack
- Performing this analysis on recovery actions acknowledges our inability to make 100% secure systems

Questions?