Teaching undergraduates to analyze major incidents as failures in risk management systems

Case Study: Rogers 2022 Outage

Dr. Lianne Lefsrud, P.Eng., Professor and Risk, Innovation & Sustainability Chair (RISC)

CSChE Process Safety Management Division (PSMD)

26 May 2026

David and Joan Lynch School
of Engineering Safety and
Risk Management

GKN Aerospace in Garden Grove with 7,000 gallons of methyl methacrylate

50,000 residents evacuated

California Chemical Leak LIVE Updates | Aerial View of California Plant With Failing Chemical Tank

Watch ›

Uploaded: May 23, 2026 · 40 Likes

Officials ordered tens of thousands of people to evacuate their homes in… More

"We Sincerely apologize for the significant disruption... We are working tirelessly with all relevant experts to resolve this situation as safely as possible and in a timely manner."

GKN Aerospace

CLASS ACTION LAWSUIT FILED OVER CHEMICAL TANK DANGER

FOR MORE INFORMATION CALL 714-741-5444 CREWS BATTLE FIRE AT PALLET YARD IN POMON 7:06 57°

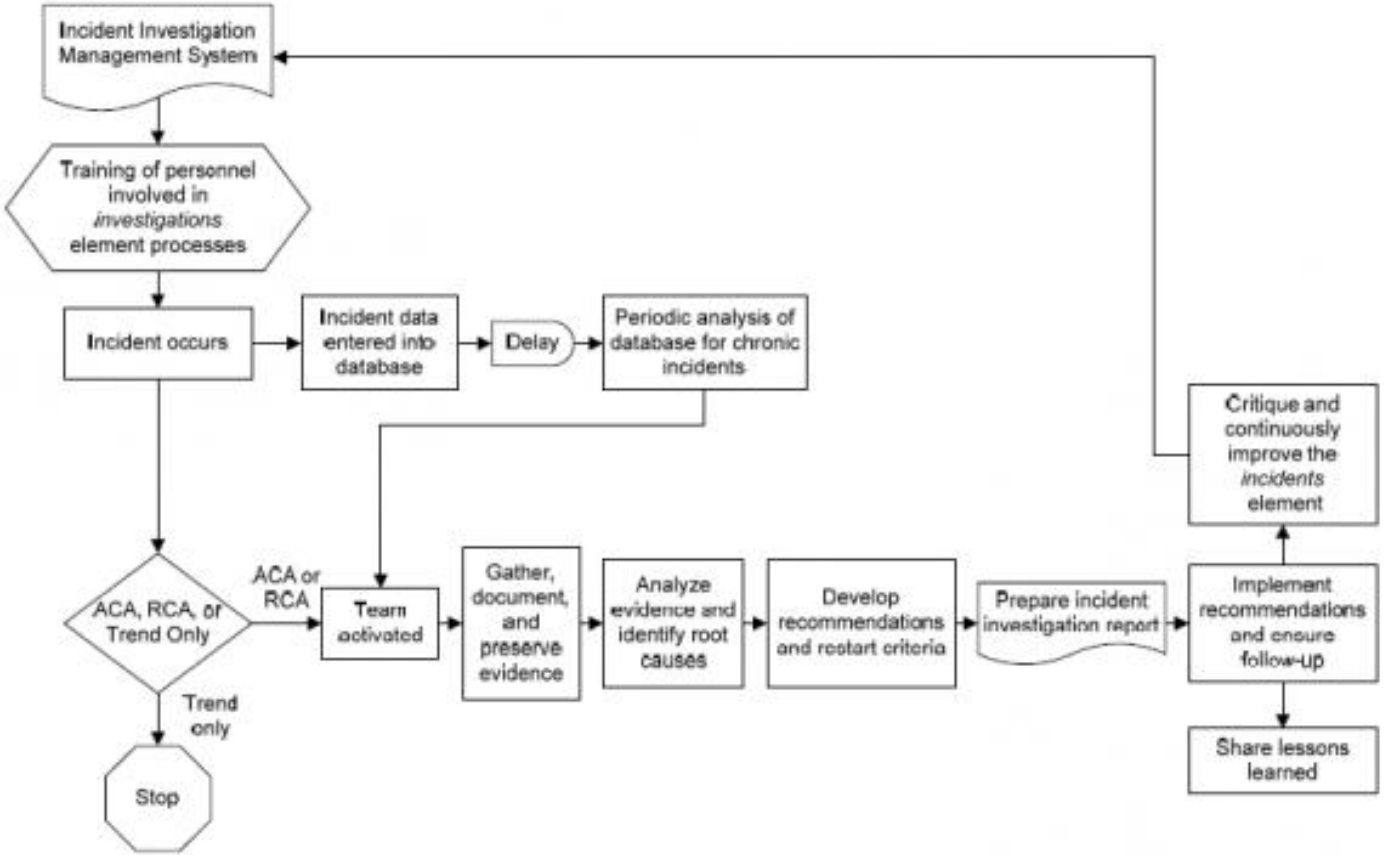


FIGURE 19.1. Incident Investigation Flowchart

https://www.aiche.org/ccps/introduction-incident-investigation

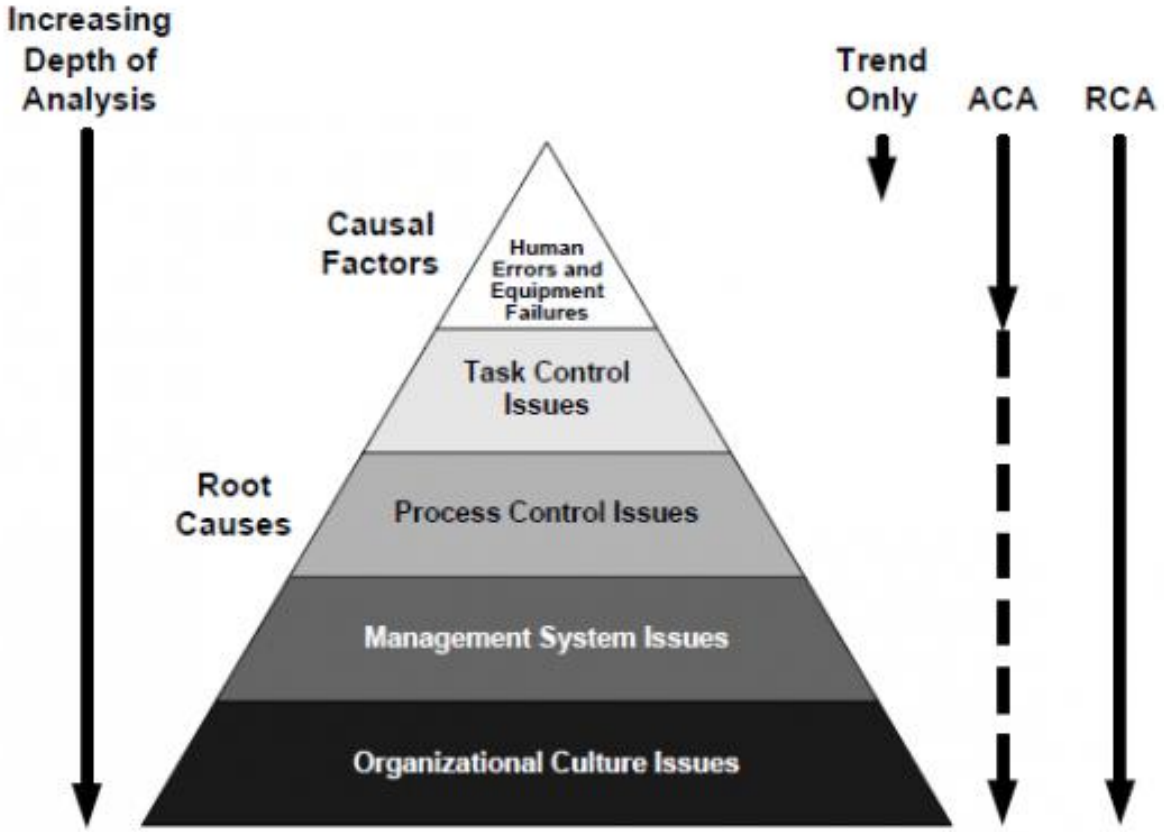
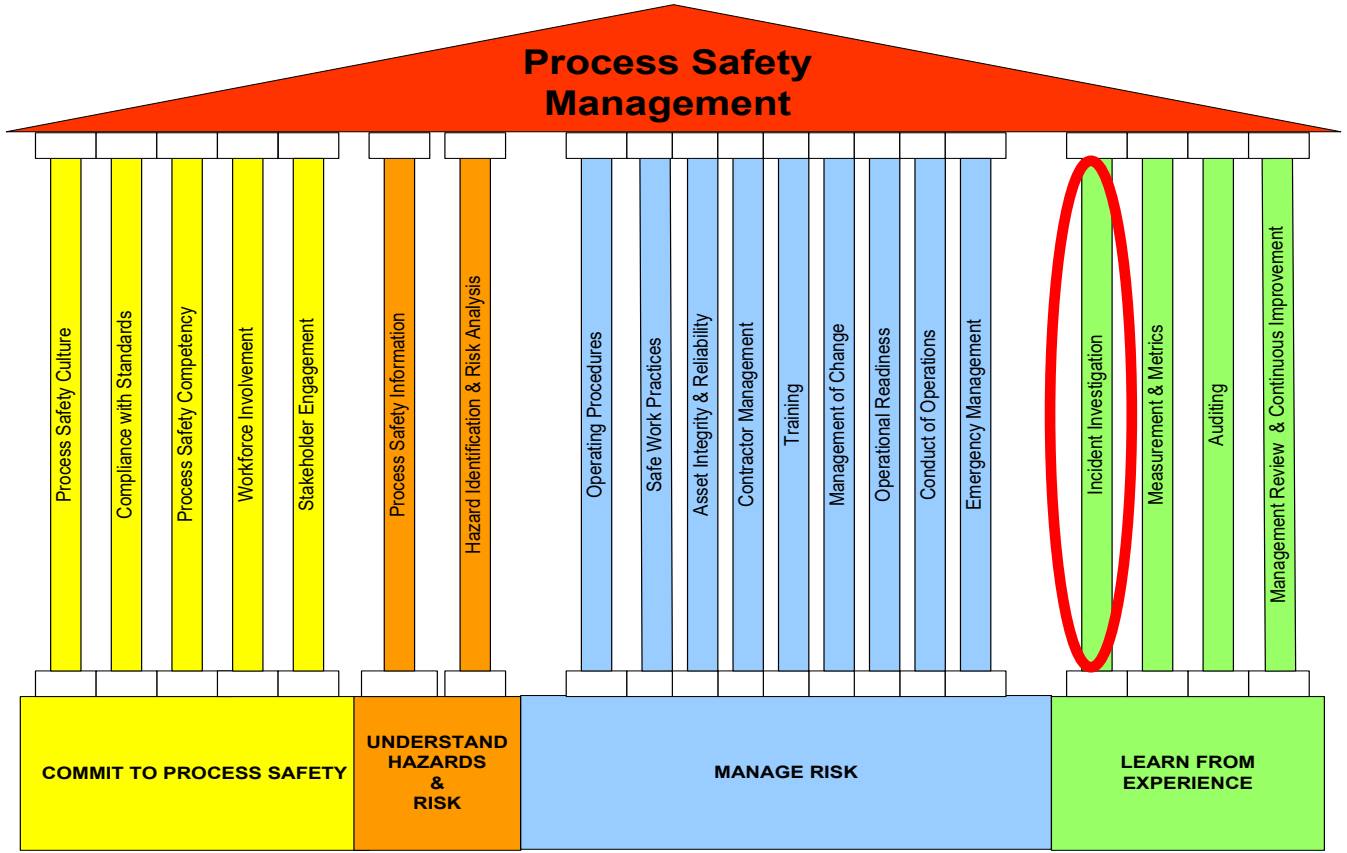


FIGURE 19.2. Incident Investigation Levels of Analysis

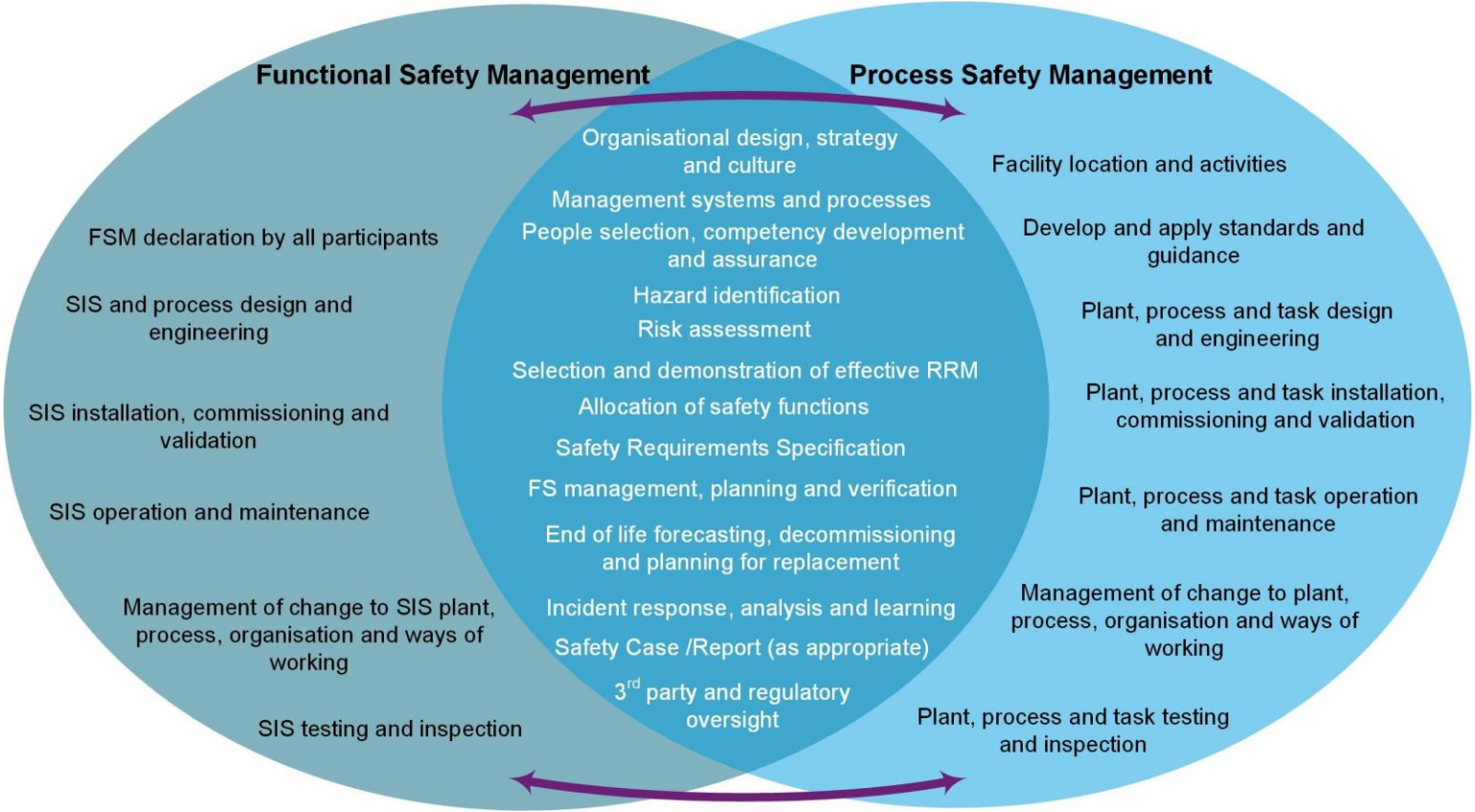
https://www.aiche.org/ccps/introduction-incident-investigation

CCPS's SAFETY MANAGEMENT SYSTEM



20 Safety Management System Elements

IChemE FUNCTIONAL AND PROCESS SAFETY MANAGEMENT SYSTEM



Major Process Safety Incident vs Root Cause Map

(Quick Reference Guide)

IChemE

Safety & Loss Prevention Special Interest Group

Sector		Date	Event	Country	Type	Fatalities	Injuries	Abnormal Operations	Escalation Potential	Earthquake	Tsunami	Flood	Cyclone/Hurricane	Extreme Cold/Ice	Hazard Identification	Process Design	Equipment/Piping Design	Matterials of Construction	Instrumentation	Safety Instrumented Systems	Protective Systems	Plant Layout	Occupied Buildings	Process Monitoring	Process Control	Cyber Security Breach	Alarm Management	Creeping Change	Hazard Awareness	Operations Risk Assessment
								Context		"Natech" Triggers – Natural Hazards					Root Causes – Design Factors									Operations Factors						
Oil & Gas	Upstream	06-Jul-88	Piper Alpha	UK	Explosion	167	?										X				X	X								
Oil & Gas	Upstream	27-Jul-05	Mumbai High North	India	Explosion	22	?									X						X							X	X
Oil & Gas	Upstream	20-Apr-10	Macondo	USA	Explosion	11	17	X							X	X	X		X	X				X						X
Oil & Gas	Upstream	11-Feb-15	Camarupim	Brazil	Explosion	9	26	X							X	X			X			X							X	X
Oil & Gas	LNG	19-Jan-04	Skikda	Algeria	Explosion	27	74		X							X		?	X	?		**X**	X							
Oil & Gas	GPP	25-Sep-98	Longford	Australia	Fire	2	8	X							**X**					X				X			X		X	
Oil & Gas	Ship	24-Mar-89	Valdez	USA	Pollution	0	0		X					X			X		X					X						
Oil & Gas	Rail	06-Jul-13	Lac Mégantic	Canada	Fire	47	?								X		X				X							X		X
Oil & Gas	Downstream	04-Jan-66	Feyzin	France	BLEVE	18	84									X	X				X								X	
Oil & Gas	Downstream	23-Jul-84	Romeoville	USA	Explosion	17	22								X			X											X	
Oil & Gas	Downstream	22-Mar-87	Grangemouth	UK	Explosion	1	0	X	X						X		X		X	**X**	X								X	
Oil & Gas	Downstream	24-Jul-94	Milford Haven	UK	Explosion	0	26	X	X								X		X					X			X			X
Oil & Gas	Downstream	23-Feb-99	Avon	USA	Fire	4	1	X							X													X		X
Oil & Gas	Downstream	17-Aug-99	Izmit	Turkey	Fire	0	0		X	X						X	X	X			X	X								X
Oil & Gas	Downstream	16-Apr-01	Humber	UK	Explosion	0	5		X						X		X													
Oil & Gas	Downstream	23-Mar-05	Texas City	USA	Explosion	15	180	X							X	X			X				X	X				X		X
Oil & Gas	Downstream	05-Nov-05	Delaware City	USA	Asphyxiation	2	0																						X	
Oil & Gas	Downstream	16-Feb-07	McKee	USA	Fire	0	4		X					X	X	X				X	X	X								
Oil & Gas	Downstream	02-Apr-10	Anacortes	USA	Explosion	7	0	X							X		X	**X**	X					X				X		X
Oil & Gas	Downstream	11-Mar-11	Chiba	Japan	BLEVE	0	6		X	X							**X**				X	X						X		X
Oil & Gas	Downstream	06-Aug-12	Richmond	USA	Fire	0	26											**X**												X
Oil & Gas	Downstream	18-Feb-15	Torrance	USA	Explosion	0	4	X	X						**X**				X	X				X						
Oil & Gas	Terminal	19-Nov-84	San Juan Ixhuatepec	Mexico	BLEVE	542	4,248										X		X	X	X	X						X		X
Oil & Gas	Terminal	11-Dec-05	Buncefield	UK	Explosion	0	43		X						**X**	X			X	X		X		X	X			X		
Oil & Gas	Terminal	23-Oct-09	Bayamón	Puerto Rico	Explosion	0	3		X						**X**	X			X	X		X		X	X				X	X
Power Gen	Nuclear	28-Mar-79	Three Mile Island	USA	Near Miss	0	0		X						X	X			X			X					**X**			X
Power Gen	Nuclear	26-Apr-86	Chernobyl	Russia	Explosion	> 30	~ 7,000	X	X						X	X	X			X									X	X
Power Gen	Nuclear	11-Mar-11	Fukushima Daiichi	Japan	Explosion	0	13		X	X	X				X				X			X								**X**
Power Gen	Coal	08-Apr-99	Gannon	USA	Explosion	3	48																							X
Power Gen	Coal	10-Nov-07	Dallman	USA	Explosion	0	0	X	X								X	X	X	X	X		X							X
Petrohemical	Manufacture	01-Jun-74	Flixborough	UK	Explosion	28	104	X	X													X	X						X	X
Petrohemical	Manufacture	23-Oct-89	Pasadena	USA	Explosion	23	314	X									X		X		X	X								
Petrohemical	Manufacture	21-Sep-92	Castleford	UK	Fire	5	201	X														X	X						X	
Petrohemical	Manufacture	01-Feb-94	Ellesmere Port	UK	Fire	0	18		X						X		X		X										X	
Petrohemical	Manufacture	27-Mar-98	Hahnville	USA	Asphyxiation	1	1								X														X	X
Petrohemical	Manufacture	13-Jun-13	Geismar	USA	BLEVE	2	167	X							X														X	X
Petrohemical	Manufacture	03-Jun-14	Moerdijk	Netherlands	Explosion	0	2	X							X				X	X					X				X	
Petrohemical	Manufacture	31-Aug-17	Crosby	USA	Decomposition	0	21					X	X		**X**						X	X						X	X	X
Agrochemical	Manuf.	10-Jul-76	Seveso	Italy	Toxic Release	0	~ 500	X	X						X	X			X	X					X				X	X
Agrochemical	Manuf.	03-Dec-84	Bhopal	India	Toxic Release	2153	>200,000	X							X	**X**		X											X	X
Agrochemical	Manuf.	21-Sep-01	Toulouse	France	Explosion	31	2442		X						X			X				X							X	X
Agrochemical	Manuf.	15-Nov-14	La Porte	USA	Toxic Release	4	0	X							X		X				X		X				X		X	X
Agrochemical	Store	17-Apr-13	West	USA	Explosion	15	> 160		X						X			**X**				X							X	
Pharma	Manuf.	04-Jan-92	Grimsby	UK	Runaway	0	0	X	X						X	**X**			X						X			X		X
Pharma	Manuf.	29-Jan-03	Kinston	USA	Explosion	6	38								**X**		X				X		X						X	X
Pharma	Manuf.	28-Apr-08	Cork	Ireland	Runaway	1	1								**X**	X	X													X
Water	Dist	23-May-84	Abbeystead	UK	Explosion	16	28	X							**X**	X			X										X	
Water	Treat	06-Jul-88	Camelford	UK	Pollution	1	~ 400								X							X								X
Water	Treat	05-Apr-93	Milwaukee	USA	Disease	69	>403,000								X	**X**								X	X					
Food		03-Sep-91	Hamlet	USA	Fire	25	54								X			X	X	X	X	X	X							
Food		11-Apr-03	Louisville	USA	Explosion	1	0		X						**X**		X		X		X			X	X				X	
Food		07-Feb-08	Port Wentworth	USA	Explosion	14	36								X	X					X								**X**	X

Event	Preventative Maintenance	Inspection	Material Degradation	Work Planning	Maintenance Risk Assessment	Energy Isolation	Control of Work	Housekeeping	Human Factors	Role Clarity	Personal Protective Equipment	Communication	Procedures	Training	Supervision/Leadership	Contractor Selection	Production over Safety	Normalisation of Deviance	Quality Assurance/Control	Management of Change	Failure to Learn	Emergency Preparedness	Process Safety Management	Design Standards	Land Use Planning	Regulatory Compliance Audits	Investigation Reports
	Root Causes – Maintenance Factors								Personal			Competency					Culture							Regulator			Links
Piper Alpha					X	X	**X**		X			X	X	X	X					X		X	X				Click
Mumbai High North									**X**	X		X	X	X												X	
Macondo	X								X	X		X	X	**X**	X							X	X	X		X	Click
Camarupim							X		X	X		X	X	X	X		X			**X**		X	X			X	Click
Skikda	X	X	X						X					X								X	X	X	X		
Longford			X						X			X	X	X	X			X				X	X			X	Click
Valdez									**X**			X	X	X	X							X	X			X	
Lac Mégantic			X						X				**X**	X	X		X			X		X	X			X	
Feyzin													**X**	X								X		X			Click
Romeoville		X	**X**										X											X			
Grangemouth							X						X	X			X			X	X		X				Click
Milford Haven	X	**X**	X				X		X			X		X						X		X	X				Click
Avon	X	X	X	X		X	**X**						X	X	X		X			X			X				Click
Izmit			X						X			X		X								**X**	X			X	Click
Humber	X	X	X									X								**X**			X				Click
Texas City	X		X				X		X	X		X	**X**	X			X	X		X	X		X			X	Click
Delaware City					X		**X**		X				X	X													Click
McKee		X			X															**X**				X			Click
Anacortes			X										X					X					X	X		X	Click
Chiba		X		X										X								X	X		X		Click
Richmond		X	X														X					X	X	X	X		Click
Torrance	X	X	X			X	X						X		X					X	X		X				Click
San Juan Ixhuatepec	X													X			X			**X**		X	X	X	X		
Buncefield	X				X				X			X	X	X			X			X		X	X		X		Click
Bayamón	X								X				X	X			X				X	X	X	X			Click
Three Mile Island									X			X	X	X								X				X	
Chernobyl									X			X	X	X			X			**X**	X	X	X			X	
Fukushima Daiichi													X	X								X	X			X	
Gannon					X	X	**X**		X			X	X		X								X			X	
Dallman	**X**		X										X	X				X									
Flixborough		X	X		X				X			X	X	X	X		X		X	**X**		X	X		X		Click
Pasadena	X				X	X	**X**					X	X	X				X		X	X	X	X				
Castleford					X		**X**		X					X	X					X	X	X	X				Click
Ellesmere Port	**X**	X	X									X	X	X								X	X	X			Click
Hahnville							**X**						X														Click
Geismar												X	X							**X**	X		X				Click
Moerdijk									X			**X**	X	X						X	X	X	X			X	Click
Crosby									X			X										X	X	X	X		Click
Seveso									X			X	**X**					X				X	X	X			
Bhopal	X								X				X	X	X		X			X		X	X		X		
Toulouse					**X**			X					X	X							X	X	X		X	X	Click
La Porte	X						X		X		X	X	X	X				X		X	X	X	**X**	X		X	Click
West					X									X							X	X			X	X	Click
Grimsby													X					X		X							
Kinston								X				X	X	X									X	X			Click
Cork									X				X	X								X		X			Click
Abbeystead													X	X						X				X			Click
Camelford									**X**			X	X	X								X	X				
Milwaukee														X			X					X					
Hamlet		X			X				X			X		X			X	X		X	X	X	X	X		**X**	Click
Louisville	X	X										X	X	X							X					X	Click
Port Wentworth								X	X			X	X	X	X			X		X	X	X	X			X	Click

IChemE (2022) Learning from Major Incidents

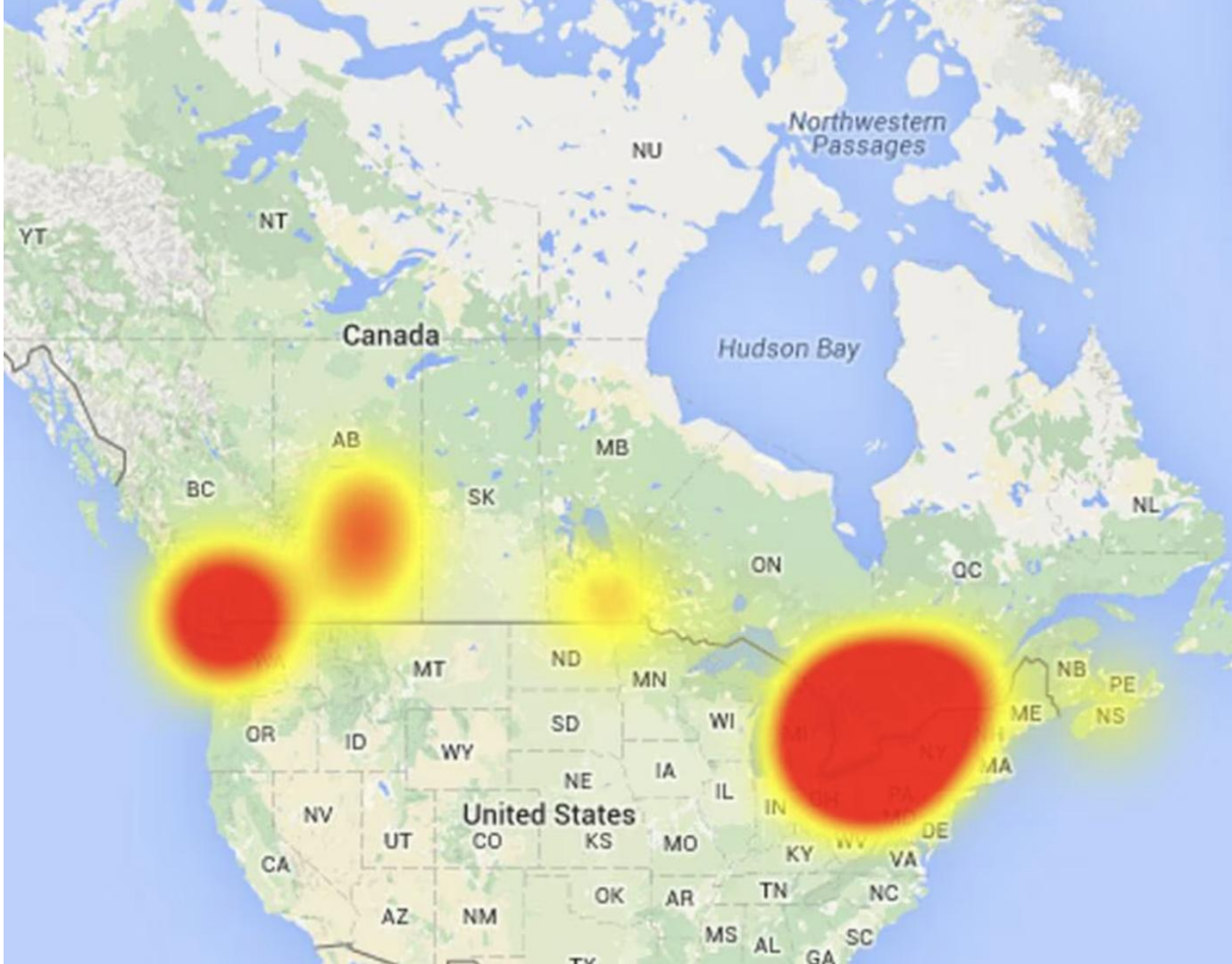
Major Process Safety Incident vs Root Cause Map
(Quick Reference Guide)

		"Natech" Triggers					Root Causes																																									
Abnormal Operations	Escalation Potential	Earthquake	Tsunami	Flood	Cyclone/Hurricane	Extreme Cold/Ice	Hazard Identification	Process Design	Equipment/Piping Design	Matterials of Construction	Instrumentation	Safety Instrumented Systems	Protective Systems	Plant Layout	Occupied Buildings	Process Monitoring	Process Control	Cyber Security Breach	Alarm Management	Creeping Change	Hazard Awareness	Operations Risk Assessment	Preventative Maintenance	Inspection	Material Degradation	Work Planning	Maintenance Risk Assessment	Energy Isolation	Control of Work	Housekeeping	Human Factors	Role Clarity	Personal Protective Equipment	Communication	Procedures	Training	Supervision/Leadership	Contractor Selection	Production over Safety	Normalisation of Deviance	Quality Assurance/Control	Management of Change	Failure to Learn	Emergency Preparedness	Process Safety Management	Design Standards	Land Use Planning	Regulatory Compliance Audits
Context		Natural Hazards					Design Factors									Operations Factors							Maintenance Factors								Personal			Competency					Culture							Regulator		

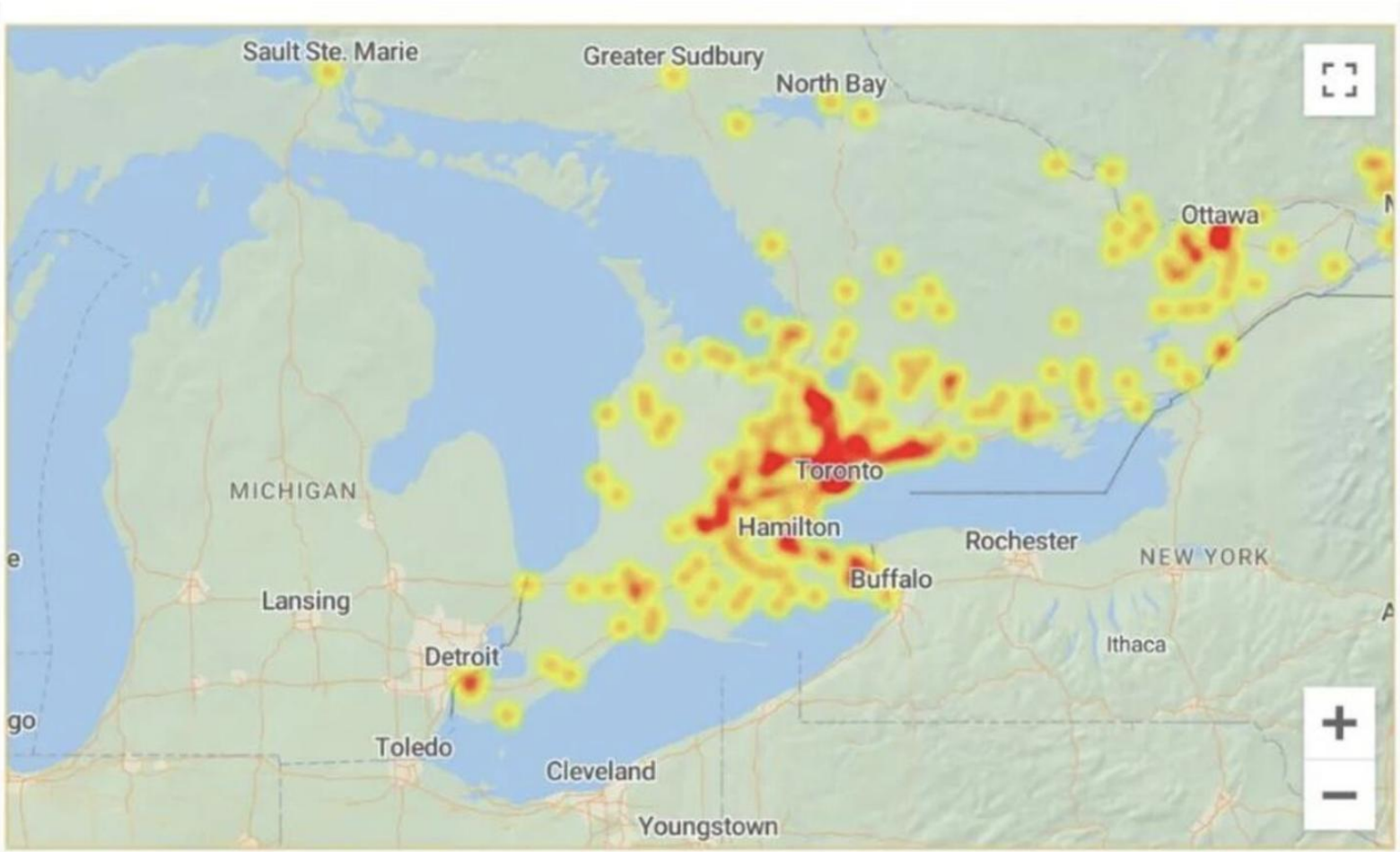
IChemE (2022) Learning from Major Incidents

Sector		Date	Event	Country	Type
Oil & Gas	Upstream	06-Jul-88	Piper Alpha	UK	Explosion
		27-Jul-05	Mumbai High North	India	Explosion
		20-Apr-10	Macondo	USA	Explosion
		11-Feb-15	Camarupim	Brazil	Explosion
	LNG	19-Jan-04	Skikda	Algeria	Explosion
	GPP	25-Sep-98	Longford	Australia	Fire
	Ship	24-Mar-89	Valdez	USA	Pollution
	Rail	06-Jul-13	Lac Mégantic	Canada	Fire
	Downstream	04-Jan-66	Feyzin	France	BLEVE
		23-Jul-84	Romeoville	USA	Explosion
		22-Mar-87	Grangemouth	UK	Explosion
		24-Jul-94	Milford Haven	UK	Explosion
		23-Feb-99	Avon	USA	Fire
		17-Aug-99	Izmit	Turkey	Fire
		16-Apr-01	Humber	UK	Explosion
		23-Mar-05	Texas City	USA	Explosion
		05-Nov-05	Delaware City	USA	Asphyxiation
		16-Feb-07	McKee	USA	Fire
		02-Apr-10	Anacortes	USA	Explosion
		11-Mar-11	Chiba	Japan	BLEVE
		06-Aug-12	Richmond	USA	Fire
		18-Feb-15	Torrance	USA	Explosion
	Terminal	19-Nov-84	San Juan Ixhuatepec	Mexico	BLEVE
		11-Dec-05	Buncefield	UK	Explosion
		23-Oct-09	Bayamón	Puerto Rico	Explosion
Power Gen	Nuclear	28-Mar-79	Three Mile Island	USA	Near Miss
		26-Apr-86	Chernobyl	Russia	Explosion
		11-Mar-11	Fukushima Daiichi	Japan	Explosion
	Coal	08-Apr-99	Gannon	USA	Explosion
		10-Nov-07	Dallman	USA	Explosion
Petrohemical	Manufacture	01-Jun-74	Flixborough	UK	Explosion
		23-Oct-89	Pasadena	USA	Explosion
		21-Sep-92	Castleford	UK	Fire
		01-Feb-94	Ellesmere Port	UK	Fire
		27-Mar-98	Hahnville	USA	Asphyxiation
		13-Jun-13	Geismar	USA	BLEVE
		03-Jun-14	Moerdijk	Netherlands	Explosion
		31-Aug-17	Crosby	USA	Decomposition
Agrochemical	Manuf.	10-Jul-76	Seveso	Italy	Toxic Release
		03-Dec-84	Bhopal	India	Toxic Release
		21-Sep-01	Toulouse	France	Explosion
		15-Nov-14	La Porte	USA	Toxic Release
	Store	17-Apr-13	West	USA	Explosion
Pharma	Manuf.	04-Jan-92	Grimsby	UK	Runaway
		29-Jan-03	Kinston	USA	Explosion
		28-Apr-08	Cork	Ireland	Runaway
Water	Dist	23-May-84	Abbeystead	UK	Explosion
	Treat	06-Jul-88	Camelford	UK	Pollution
		05-Apr-93	Milwaukee	USA	Disease
Food		03-Sep-91	Hamlet	USA	Fire
		11-Apr-03	Louisville	USA	Explosion
		07-Feb-08	Port Wentworth	USA	Explosion

ROGERS OUTAGE 2015



ROGERS OUTAGE 2022



Major Process Safety Incident vs Root Cause Map

(Quick Reference Guide)

IChemE

Safety & Loss Prevention Special Interest Group

Sector	Date	Event	Country	Type	Fatalities	Injuries	Context		"Natech" Triggers – Natural Hazards					Root Causes – Design Factors									Operations Factors							Maintenance Factors								Personal			Competency					Culture							Regulator			Links
							Abnormal Operations	Escalation Potential	Earthquake	Tsunami	Flood	Cyclone/Hurricane	Extreme Cold/Ice	Hazard Identification	Process Design	Equipment/Piping Design	Materials of Construction	Instrumentation	Safety Instrumented Systems	Protective Systems	Plant Layout	Occupied Buildings	Process Monitoring	Process Control	Cyber Security Breach	Alarm Management	Creeping Change	Hazard Awareness	Operations Risk Assessment	Preventative Maintenance	Inspection	Material Degradation	Work Planning	Maintenance Risk Assessment	Energy Isolation	Control of Work	Housekeeping	Human Factors	Role Clarity	Personal Protective Equipment	Communication	Procedures	Training	Supervision/Leadership	Contractor Selection	Production over Safety	Normalisation of Deviance	Quality Assurance/Control	Management of Change	Failure to Learn	Emergency Preparedness	Process Safety Management	Design Standards	Land Use Planning	Regulatory Compliance Audits	Investigation Reports
Oil & Gas – Upstream	06-Jul-88	Piper Alpha	UK	Explosion	167	?										X				X	X													X	X	**X**		X			X	X	X	X					X		X	X				Click
Oil & Gas – Upstream	27-Jul-05	Mumbai High North	India	Explosion	22	?									X						X							X	X									**X**	X		X	X	X												X	
Oil & Gas – Upstream	20-Apr-10	Macondo	USA	Explosion	11	17	X							X	X	X		X	X				X						X	X								X	X		X	X	**X**	X							X	X	X		X	Click
Oil & Gas – Upstream	11-Feb-15	Camarupim	Brazil	Explosion	9	26	X							X	X			X			X							X	X							X		X	X		X	X	X	X		X			**X**		X	X			X	Click
Oil & Gas – LNG	19-Jan-04	Skikda	Algeria	Explosion	27	74		X							X		?	X	?		**X**	X								X	X	X						X					X								X	X	X	X		
Oil & Gas – GPP	25-Sep-98	Longford	Australia	Fire	2	8	X							**X**					X				X			X		X				X						X			X	X	X	X			X				X	X			X	Click
Oil & Gas – Ship	24-Mar-89	Valdez	USA	Pollution	0	0		X					X			X		X					X															**X**			X	X	X	X							X	X			X	
Oil & Gas – Rail	06-Jul-13	Lac Mégantic	Canada	Fire	47	?								X		X				X							X		X			X						X				**X**	X	X		X			X		X	X			X	
Oil & Gas – Downstream	04-Jan-66	Feyzin	France	BLEVE	18	84									X	X				X								X														**X**	X								X		X			Click
Oil & Gas – Downstream	23-Jul-84	Romeoville	USA	Explosion	17	22								X			X											X			X	**X**										X											X			
Oil & Gas – Downstream	22-Mar-87	Grangemouth	UK	Explosion	1	0	X	X						X		X		X	**X**	X								X								X						X	X			X			X	X		X				Click
Oil & Gas – Downstream	24-Jul-94	Milford Haven	UK	Explosion	0	26	X	X								X		X					X			X			X	X	**X**	X				X		X			X		X						X		X	X				Click
Oil & Gas – Downstream	23-Feb-99	Avon	USA	Fire	4	1	X							X													X		X	X	X	X	X		X	**X**						X	X	X		X			X			X				Click
Oil & Gas – Downstream	17-Aug-99	Izmit	Turkey	Fire	0	0		X	X						X	X	X			X	X								X			X						X			X		X								**X**	X			X	Click
Oil & Gas – Downstream	16-Apr-01	Humber	UK	Explosion	0	5		X						X		X														X	X	X									X								**X**			X				Click
Oil & Gas – Downstream	23-Mar-05	Texas City	USA	Explosion	15	180	X							X	X			X				X	X				X		X	X		X				X		X	X		X	**X**	X			X	X		X	X		X			X	Click
Oil & Gas – Downstream	05-Nov-05	Delaware City	USA	Asphyxiation	2	0																						X						X		**X**		X				X	X													Click
Oil & Gas – Downstream	16-Feb-07	McKee	USA	Fire	0	4		X					X	X	X				X	X	X										X			X															**X**				X			Click
Oil & Gas – Downstream	02-Apr-10	Anacortes	USA	Explosion	7	0	X							X		X	**X**	X					X				X		X			X										X					X					X	X		X	Click
Oil & Gas – Downstream	11-Mar-11	Chiba	Japan	BLEVE	0	6		X	X							**X**				X	X						X		X		X		X										X								X	X		X		Click
Oil & Gas – Downstream	06-Aug-12	Richmond	USA	Fire	0	26											**X**												X		X	X														X					X	X	X	X		Click
Oil & Gas – Downstream	18-Feb-15	Torrance	USA	Explosion	0	4	X	X						**X**				X	X				X							X	X	X			X	X						X		X					X	X		X				Click
Oil & Gas – Terminal	19-Nov-84	San Juan Ixhuatepec	Mexico	BLEVE	542	4,248										X		X	X	X	X						X		X	X													X			X			**X**		X	X	X	X		
Oil & Gas – Terminal	11-Dec-05	Buncefield	UK	Explosion	0	43		X						**X**	X			X	X		X		X	X			X			X				X				X			X	X	X			X			X		X	X		X		Click
Oil & Gas – Terminal	23-Oct-09	Bayamón	Puerto Rico	Explosion	0	3		X						**X**	X			X	X		X		X	X				X	X	X								X				X	X			X				X	X	X	X			Click
Power Gen – Nuclear	28-Mar-79	Three Mile Island	USA	Near Miss	0	0		X						X	X			X			X					**X**			X									X			X	X	X								X				X	
Power Gen – Nuclear	26-Apr-86	Chernobyl	Russia	Explosion	> 30	~ 7,000	X	X						X	X	X			X									X	X									X			X	X	X			X			**X**	X	X	X			X	
Power Gen – Nuclear	11-Mar-11	Fukushima Daiichi	Japan	Explosion	0	13		X	X	X				X				X			X								**X**													X	X								X	X			X	
Power Gen – Coal	08-Apr-99	Gannon	USA	Explosion	3	48																							X					X	X	**X**		X			X	X		X								X			X	
Power Gen – Coal	10-Nov-07	Dallman	USA	Explosion	0	0	X	X								X	X	X	X	X		X							X	**X**		X										X	X				X									
Petrochemical – Manufacture	01-Jun-74	Flixborough	UK	Explosion	28	104	X	X													X	X						X	X		X	X		X				X			X	X	X	X		X		X	**X**		X	X		X		Click
Petrochemical – Manufacture	23-Oct-89	Pasadena	USA	Explosion	23	314	X									X		X		X	X									X				X	X	**X**					X	X	X				X		X	X	X	X				
Petrochemical – Manufacture	21-Sep-92	Castleford	UK	Fire	5	201	X														X	X						X						X		**X**		X					X	X					X	X	X	X				Click
Petrochemical – Manufacture	01-Feb-94	Ellesmere Port	UK	Fire	0	18		X						X		X		X										X		**X**	X	X									X	X	X								X	X	X			Click
Petrochemical – Manufacture	27-Mar-98	Hahnville	USA	Asphyxiation	1	1								X														X	X							**X**						X														Click
Petrochemical – Manufacture	13-Jun-13	Geismar	USA	BLEVE	2	167	X							X														X	X												X	X							**X**	X		X				Click
Petrochemical – Manufacture	03-Jun-14	Moerdijk	Netherlands	Explosion	0	2	X							X				X	X					X				X										X			**X**	X	X						X	X	X	X			X	Click
Petrochemical – Manufacture	31-Aug-17	Crosby	USA	Decomposition	0	21					X	X		**X**						X	X						X	X	X									X			X										X	X	X	X		Click
Agrochemical – Manuf.	10-Jul-76	Seveso	Italy	Toxic Release	0	~ 500	X	X						X	X			X	X					X				X	X									X			X	**X**					X				X	X	X			
Agrochemical – Manuf.	03-Dec-84	Bhopal	India	Toxic Release	2153	>200,000	X							X	**X**		X											X	X	X								X				X	X	X		X			X		X	X		X		
Agrochemical – Manuf.	21-Sep-01	Toulouse	France	Explosion	31	2442		X						X			X				X							X	X					**X**			X					X	X							X	X	X		X	X	Click
Agrochemical – Manuf.	15-Nov-14	La Porte	USA	Toxic Release	4	0	X							X		X				X		X				X		X	X	X						X		X		X	X	X	X				X		X	X	X	**X**	X		X	Click
Agrochemical – Store	17-Apr-13	West	USA	Explosion	15	> 160		X						X			**X**				X							X						X									X							X	X			X	X	Click
Pharma – Manuf.	04-Jan-92	Grimsby	UK	Runaway	0	0	X	X						X	**X**			X						X			X		X													X					X		X							
Pharma – Manuf.	29-Jan-03	Kinston	USA	Explosion	6	38								**X**		X				X		X						X	X								X				X	X	X									X	X			Click
Pharma – Manuf.	28-Apr-08	Cork	Ireland	Runaway	1	1								**X**	X	X													X									X				X	X								X		X			Click
Water – Dist	23-May-84	Abbeystead	UK	Explosion	16	28	X							**X**	X			X										X														X	X						X				X			Click
Water – Treat.	06-Jul-88	Camelford	UK	Pollution	1	~ 400								X							X								X									**X**			X	X	X								X	X				
Water – Treat.	05-Apr-93	Milwaukee	USA	Disease	69	>403,000								X	**X**								X	X																			X			X					X					
Food	03-Sep-91	Hamlet	USA	Fire	25	54								X			X	X	X	X	X	X									X			X				X			X		X			X	X		X	X	X	X	X		**X**	Click
Food	11-Apr-03	Louisville	USA	Explosion	1	0		X						**X**		X		X		X			X	X				X		X	X										X	X	X							X					X	Click
Food	07-Feb-08	Port Wentworth	USA	Explosion	14	36								X	X					X								**X**	X								X	X			X	X	X	X			X		X	X	X	X			X	Click

Cause-effect model to latency (weaknesses in management system elements)

Detailed Cause and Effect Model:

Losses Type	Incident Type	Immediate Causes Type	Basic Causes Type	Latent Causes			
				Weaknesses in System Elements	Categories P	S	C
Injury / Illness	**Body Motion:**	**Substandard Work Practices**	**Engineering & Design Factors:**	1) Management Leadership, Commitment and Accountability.			
First Aid	Struck against	Use of Protective Defenses (assumes in place)	inadequate technical design	2) Risk Assessment and Management of Risks.			
Medical Treatment	Struck by	Use of Tools or Equipment (good equipment available)	inadequate ergonomic design	3) Community Awareness and Emergency Preparedness.			
Lost Time	Fall to lower level	Following Procedures General: (assumes sound & exist)	inadequate assessment of loss exposures	4) Management of Change.			
Fatality	Fall on same level	Following Procedures Specific: (assumes sound & exist)	inadequate standards, specifications and/or design criteria	5) Incident Reporting, Investigation, Analysis and Actions.			
	Caught in	Inattention / Lack of Awareness (not focused)	inadequate monitoring of construction	6) Program Evaluation and Continuous Improvement.			
Environment	Caught on		inadequate assessment of operational readiness	7) Design, Construction and Start-up.			
spill / release <25 kg, no adverse impact	Caught between	**Substandard Conditions**	inadequate monitoring of initial operation	8) Operations and Maintenance.			
spill / release >25 kg, no adverse impact	Overexertion	Hardware	inadequate evaluation and/or documentation of change	9) Employee Competency and Training.			
spill / release >25 kg, adverse impact	Overstress	Condition of Safeguards	**Job Factors:**	10) Contractor Competency and Integration.			
regulatory exceedance		Process Exposure	Inadequate maintenance	11) Operations and Facilities Information and Documentation.			
off-plant adverse impact	**Contact with:**	Workspace Hazards	Inadequate job procedures				
	Environmental Heat		Error-inducing conditions				
Assets	Environmental Cold		Organizational factors				
Minor <$5,000	Hot surface		Incompatible goals				
Serious $5,000-$50,000	Cold surface		Inadequate training				
Major $50,000-$500,000	Fire		Inadequate communication				
Catastrophic >$500,000	Electricity						
	Chemical - corrosive		**Personal Factors:**				
Business Interuption *	Chemical - toxic		Inadequate physical / physiological state / capability to do the work.				
Minor <$5,000	Noise		Perceived inadequate mental / psychological state / capability to do the work.				
Serious $5,000-$50,000	Pressure		Physical or physiological stress.				
Major $50,000-$500,000	Radiation		Perceived mental or psychological stress.				
Catastrophic >$500,000			Improper risk taking / improper motivation				
			Lack of knowledge / lack of skill.				

Categories of Latent Causes:

P = inadequate program

S = inadequate standards

C = inadequate compliance

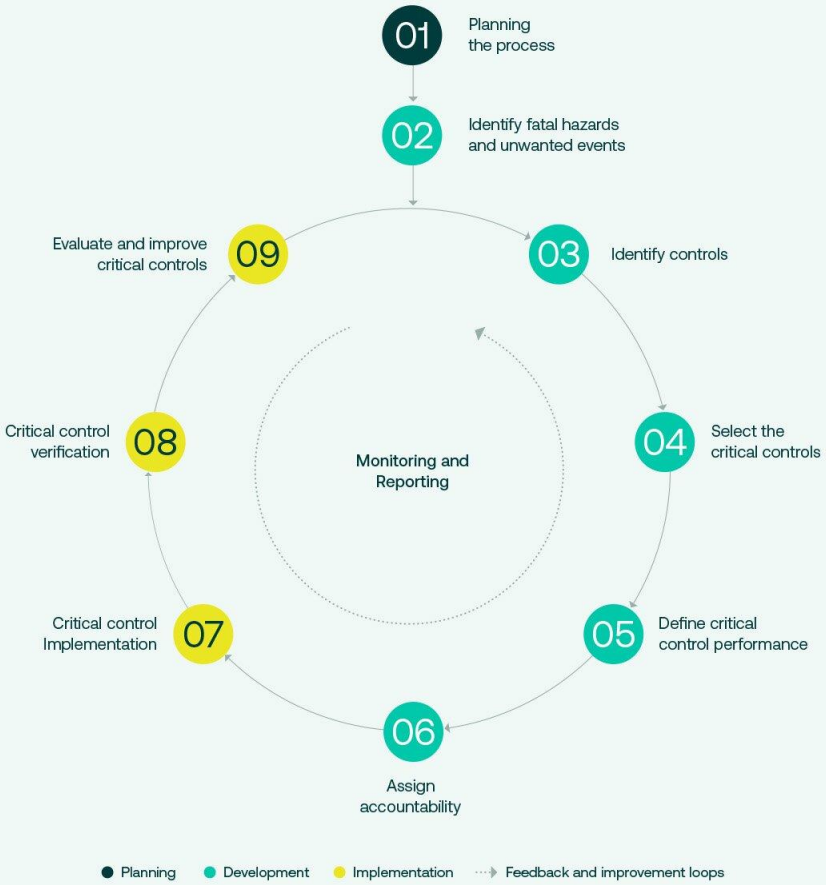
** measured as conversion cost of lost production plus any wasted / lost materials*

This model is based on a model developed by Bird Jr., F.E. and Germain, G.L. (1992). Practical Loss Control Leadership. Loss Control Management. Det Norske Veritas Inc.
Adapted by ESRM Program at The U of Alberta, including the APEGA Model for Management System Elements.

RISK MANAGEMENT SYSTEM ELEMENTS (APEGA)

1) Management Leadership, Commitment and Accountability.
2) Risk Assessment and Management of Risks.
3) Community Awareness and Emergency Preparedness.
4) Management of Change.
5) Incident Reporting, Investigation, Analysis and Actions.
6) Program Evaluation and Continuous Improvement.
7) Design, Construction and Start-up.
8) Operations and Maintenance.
9) Employee Competency and Training.
10) Contractor Competency and Integration.
11) Operations and Facilities Information and Documentation.

ICMM THE CRITICAL CONTROL MANAGEMENT PROCESS

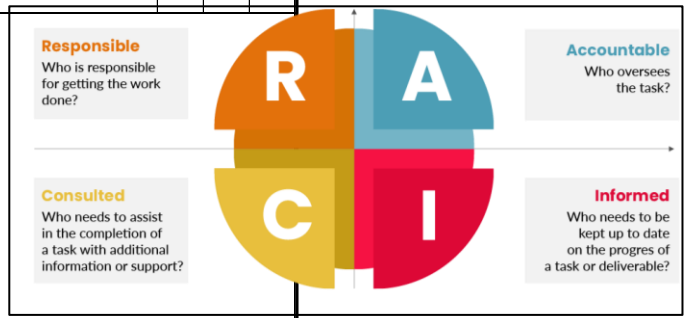


Cause-effect model to latency (weaknesses in management system elements)

Detailed Cause and Effect Model:

Losses Type		Incident Type		Immediate Causes Type		Basic Causes Type	
Injury / Illness		**Body Motion:**		**Substandard Work Practices**		**Engineering & Design Factors:**	
First Aid		Struck against		Use of Protective Defenses (assumes in place)		inadequate technical design	
Medical Treatment		Struck by		Use of Tools or Equipment (good equipment available)		inadequate ergonomic design	
Lost Time		Fall to lower level		Following Procedures General: (assumes sound & exist)		inadequate assessment of loss exposures	
Fatality		Fall on same level		Following Procedures Specific: (assumes sound & exist)		inadequate standards, specifications and/or design criteria	
		Caught in		Inattention / Lack of Awareness (not focused)		inadequate monitoring of construction	
Environment		Caught on				inadequate assessment of operational readiness	
spill / release <25 kg, no adverse impact		Caught between		**Substandard Conditions**		inadequate monitoring of initial operation	
spill / release >25 kg, no adverse impact		Overexertion		Hardware		inadequate evaluation and/or documentation of change	
spill / release >25 kg, adverse impact		Overstress		Condition of Safeguards		**Job Factors:**	
regulatory exceedance				Process Exposure		Inadequate maintenance	
off-plant adverse impact		**Contact with:**		Workspace Hazards		Inadequate job procedures	
		Environmental Heat				Error-inducing conditions	
Assets		Environmental Cold				Organizational factors	
Minor <$5,000		Hot surface				Incompatible goals	
Serious $5,000-$50,000		Cold surface				Inadequate training	
Major $50,000-$500,000		Fire				Inadequate communication	
Catastrophic >$500,000		Electricity					
		Chemical - corrosive				**Personal Factors:**	
Business Interuption *		Chemical - toxic				Inadequate physical / physiological state / capability to do the work.	
Minor <$5,000		Noise				Perceived inadequate mental / psychological state / capability to do the work.	
Serious $5,000-$50,000		Pressure				Physical or physiological stress.	
Major $50,000-$500,000		Radiation				Perceived mental or psychological stress.	
Catastrophic >$500,000						Improper risk taking / improper motivation	
* measured as conversion cost of lost production plus any wasted / lost materials						Lack of knowledge / lack of skill.	

Latent Causes			
	Categories		
Weaknesses in System Elements	P	S	C
1) Management Leadership, Commitment and Accountability.			
2) Risk Assessment and Management of Risks.			
3) Community Awareness and Emergency Preparedness.			
4) Management of Change.			
5) Incident Reporting, Investigation, Analysis and Actions.			
6) Program Evaluation and Continuous Improvement.			
7) Design, Construction and Start-up.			
8) Operations and Maintenance.			
9) Employee Competency and Training.			
10) Contractor Competency and Integration.			
11) Operations and Facilities Information and Documentation.			



Categories of Latent Causes:

P = inadequate program

S = inadequate standards

C = inadequate compliance

This model is based on a model developed by Bird Jr., F.E. and Germain, G.L. (1992). Practical Loss Control Leadership. Loss Control Management. Det Norske Veritas Inc. Adapted by ESRM Program at The U of Alberta, including the APEGA Model for Management System Elements.

APPLICATION THREAT MODELING ACTIVITIES per STAGE	BU/Product Groups						Corporate Functions							3rd Party	
	MGT	PMO	BA	ARC	SWE	QA	SYS	SOC	RL	PC	SA	EA	CTO	VA	PT
STAGE 1 - DEFINE BUSINESS OBJECTIVES - Est. New TM = 2-4 hours | Est. Repeat TM = < 1 hour	A	R	R	A	I	I	I	-	I	R	I	I	R	-	-
Obtain business objectives for product or application	A	I	R	A	I	I	I	-	I	-	-	I	I	-	-
Identify regulatory compliance obligations	A	I	I	A	I	I	I	-	I	R	-	I	I	-	-
Define a risk profile or business criticality level for the application	A	I	I	A	I	I	I	-	I	C	I	I	R	-	-
Identify the key business use cases for the application/product	A	R	R	A	I	I	I	-	I	-	-	I	I	-	-
STAGE 2 - TECHNICAL SCOPE - Est. New TM = 3-4 hours | Est. Repeat TM = 1-3 hours	I	I	C	A	R/A	C	I	-	I	-	I	C	I	-	-
Enumerate software applications/database in support of product/application	I	I	C	A	R/A	C	I	-	-	-	-	C	I	-	-
Identify any client-side technologies (Flash, DHTML5, etc.)	I	I	C	A	R/A	C	I	-	-	-	I	C	I	-	-
Enumerate system platforms that support product/application	I	I	C	A	R/A	C	I	-	-	-	I	C	I	-	-
Identify all application/product actors	I	I	C	A	R/A	C	I	-	-	-	I	C	I	-	-
Enumerate services needed for application/product use & management	I	I	C	A	R/A	C	I	-	-	-	I	C	I	-	-
Enumerate 3rd party COTS needed for solution	I	I	C	A	R/A	C	I	-	-	-	I	C	I	-	-
Identify 3rd party infrastructures, cloud solutions, hosted networks, mobile devices	I	I	C	A	R/A	C	I	-	-	-	I	C	I	-	-
Obtain business objectives for product or application	I	I	C	A	R/A	C	I	-	I	-	I	C	I	-	-
STAGE 3 - APPLICATION DECOMPOSITION - Est. New TM = 8 hours | Est. Repeat TM = 4 hours	I	I	I	A	R	C	C	-	I	-	-	C	-	-	-
Perform data flow diagram of application environment	I	I	I	A	R	I	C	-	-	-	-	C	-	-	-
Define application trust boundaries/trust models	I	I	I	A	R	C	C	-	-	-	-	C	-	-	-
Enumerate application actors	I	I	I	A	R	C	C	-	-	-	-	C	-	-	-
Identify any stored procedures/batch processing	I	I	I	A	R	C	C	-	-	-	-	C	-	-	-
Enumerate all application use cases (ex: login, account update, delete users, etc.)	I	I	I	A	R	C	C	-	-	-	-	C	-	-	-
STAGE 4 - THREAT ANALYSIS - Est. New TM = 6 hours | Est. Repeat TM = 2 hours	I	I	R/A	A	R/A	R/A	C	C	-	-	-	I	-	-	-
Gather/correlate relevant threat intel from internal/external threat groups	I	I	R/A	A	C	I	C	C	-	-	-	C	-	-	-
Review recent log data around application environment for heightened security alerts	-	-	I	A	R	R/A	I	C	-	-	-	C	-	-	-
Gather audit reports around access control violations	-	I	I	A	R	C	I	C	-	-	-	C	-	-	-
Identify probable threat motives, attack vectors & misuse cases	I	I	I	A	R/A	C	I	C	-	-	-	C	-	-	-
STAGE 5 - VULNERABILITY ASSESSMENT - Est. New TM = 12 hours | Est. Repeat TM = 6 hours	I	I	I	A	R	C	I	C	I	-	-	I	-	R/A	R
Conduct targeted vulnerability scans based upon threat analysis	-	-	-	A	R	C	I	C	I	-	-	I	-	R	R
Identify weak design patterns in architecture	-	-	-	A	R	C	I	-	-	-	-	C	-	R	C
Review/correlate existing vulnerability data	I	I	I	A	R	I	I	C	-	-	-	I	-	R/A	I
Map vulnerabilities to attack tree	-	I	I	A	R	I	I	-	-	-	-	C	-	C	I
STAGE 6 - ATTACK ENUMERATION - Est. New TM = 10 hours | Est. Repeat TM = 5 hours	I	I	I	A	R	R	-	-	I	-	-	C	I	I	R/A
Enumerate all inherent and targeted attacks for product/application	I	I	I	A	R	C	-	-	I	-	-	C	I	I	R/A
Map attack patterns to attack tree vulnerability branches (attack tree finalization)	-	-	-	A	R	C	-	-	I	-	-	C	-	I	A
Conduct targeted attacks to determine probability level of attack patterns	-	-	-	A	C	R	-	-	I	-	-	C	-	I	R/A
Reform threat analysis based upon exploitation results	I	I	I	A	R	C	-	-	I	-	-	C	I	I	C
STAGE 7 - RESIDUAL RISK ANALYSIS - Est. New & Repeat TM = 5 days (inc. countermeasure dev.)	C	I	I	A	R	C	C	C	I	I	C	C	I	I	R
Review application/product risk analysis based upon completed threat analysis	I	I	I	A	R	C	I	C	I	I	C	C	I	I	R
List recommended countermeasures for residual risk reduction	I	I	I	A	R	C	C	C	I	I	C	C	I	I	R
Re-evaluate overall application risk profile and report.	C	I	I	A	R	C	I	I	I	C	C	C	I	I	I

MGT *Product Mgmt*
PMO *Project Mgmt*
BA *Business Analyst*
ARC *Architect*
SWE *Software Engineer*
QA *Quality Assurance*
SYS *SysAdmin*
SOC *Security Operations*
RL *IT Risk Leader*
PC *Product Compliance*
SA *Software Assurance*
EA *Enterprise Architect*
CTO *Administration*
VA *Vuln Assessor*
PT *Pen Tester*

Corporate Functions

Office of the CTO
Compliance
Security (ISRM)

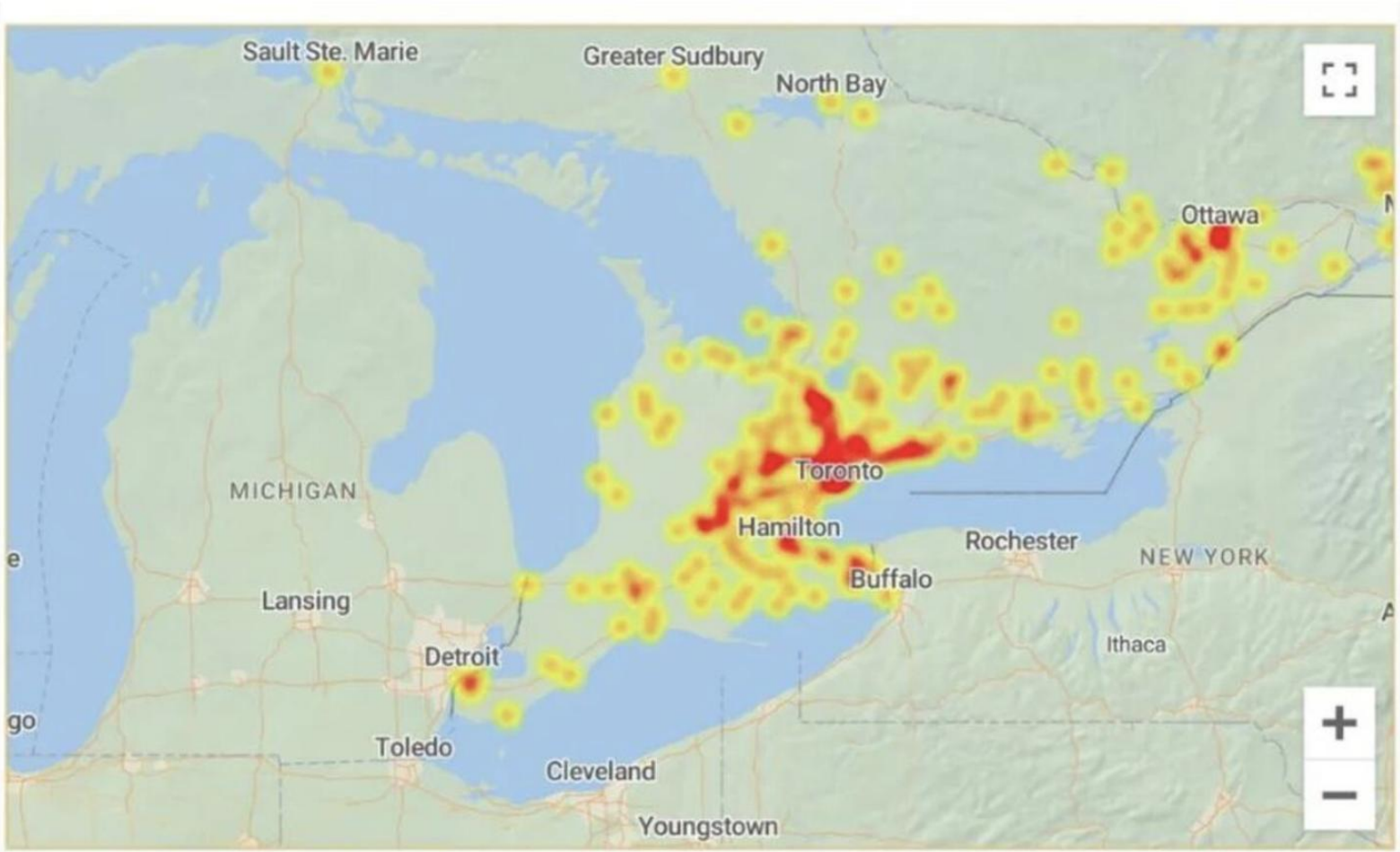
RACI Legend

R	Responsible
A	Accountable
C	Consulted (2 way)
I	Informed (1 way)

VERSPRITE

VerSprite's Process for Attack, Simulation and Threat Analysis (PASTA) benefits stakeholders by assessing threats to your application environment by designing secure applications and deciding how to mitigate risks by applying risk mitigation strategies. Examples include Architects, Developers, Security Testers, Project Managers, Business Managers, and Information Risk Officers. Learn more >>

ROGERS OUTAGE 2022



ROGERS OUTAGE 2022

The July 8, 2022 Rogers network outage was caused by a routing error during a system upgrade when Rogers staff inadvertently removed an Access Control List (ACL) policy filter from distribution routers. This missing ACL allowed a flood of IP routing data to crash the core network.

This critical network failure, which impacted roughly 12 million customers:

The Root Cause: Removing the ACL filter caused routing information to flood the core network routers. This triggered a massive system crash within minutes.

Flawed Risk Assessment: The configuration change was the sixth phase of a seven-phase network upgrade. Because earlier phases went smoothly, Rogers' algorithm downgraded the change to "Low risk," bypassing crucial laboratory testing and higher levels of approval.

Outage Impact: The combined wireless and wireline networks shared this common IP core. This resulted in a near-total blackout of internet, wireless, and 911 services, and completely disabled the Interac payment network across Canada.

Delayed Recovery: Incident management was hampered because staff lost access to error logs and lacked backup communication channels (Rogers staff even had to send SIM cards from rival network operators to communicate). Following the subsequent investigations by the Canadian Radio-television and Telecommunications Commission (CRTC), Rogers was ordered to implement router overload protection, separate data networks from network management layers, and use third-party backup systems.

Pranuthi V · 3rd

Network Security Engineer | Firewall Operations | Network Monitoring| DNS/IPAM | F5 | Incident Response | Security Policy Management |

Hyderabad, Telangana, India · Contact info

What is an ACL?

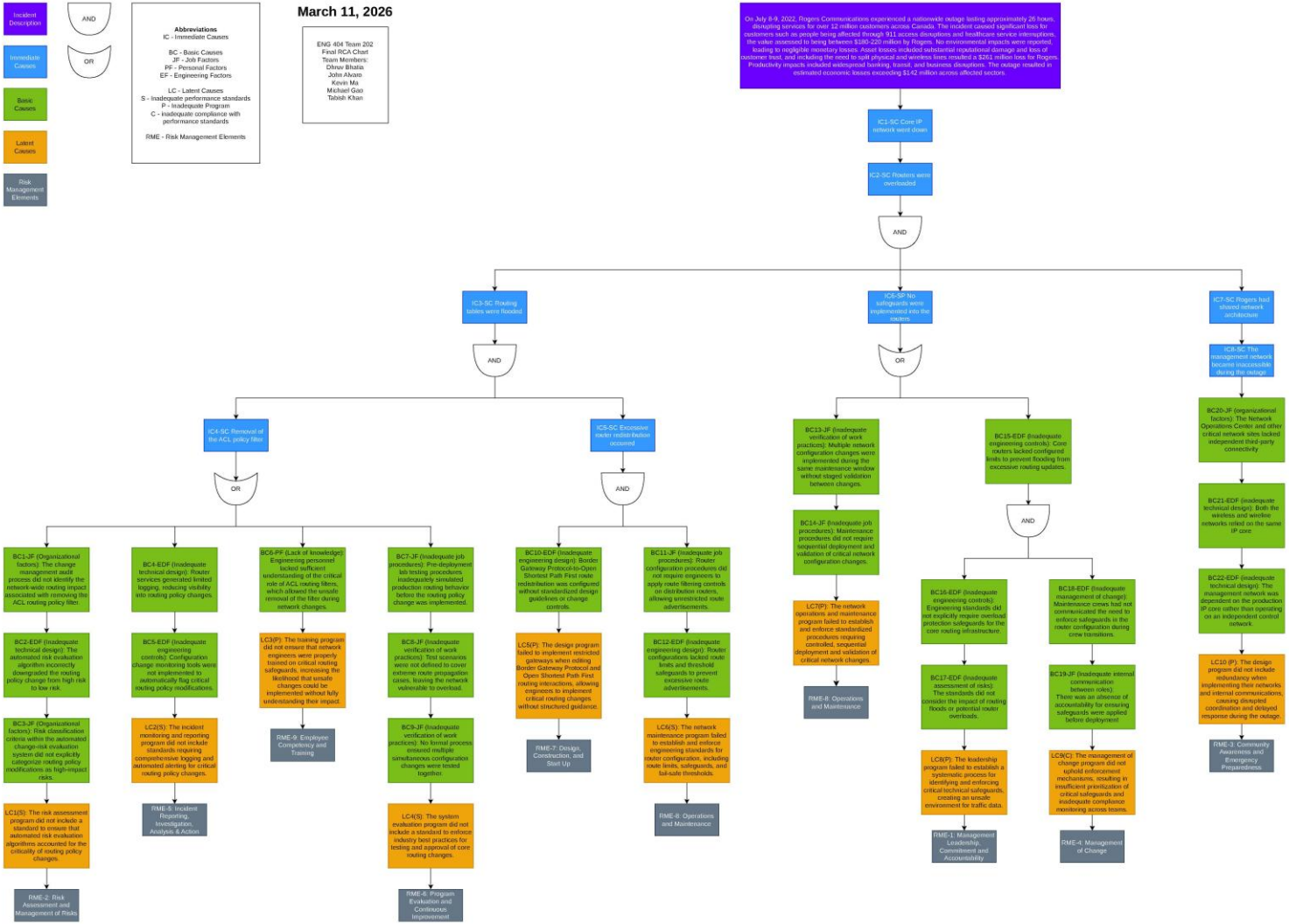
An Access Control List (ACL) is used to control the traffic flowing through a network by defining which packets are permitted or denied.

Standard ACL: Controls traffic using source IP addresses

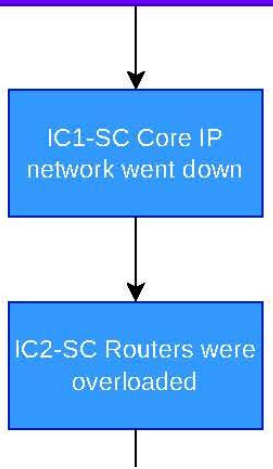
Extended ACL: Controls traffic using both source and destination IP addresses, along protocols and port numbers

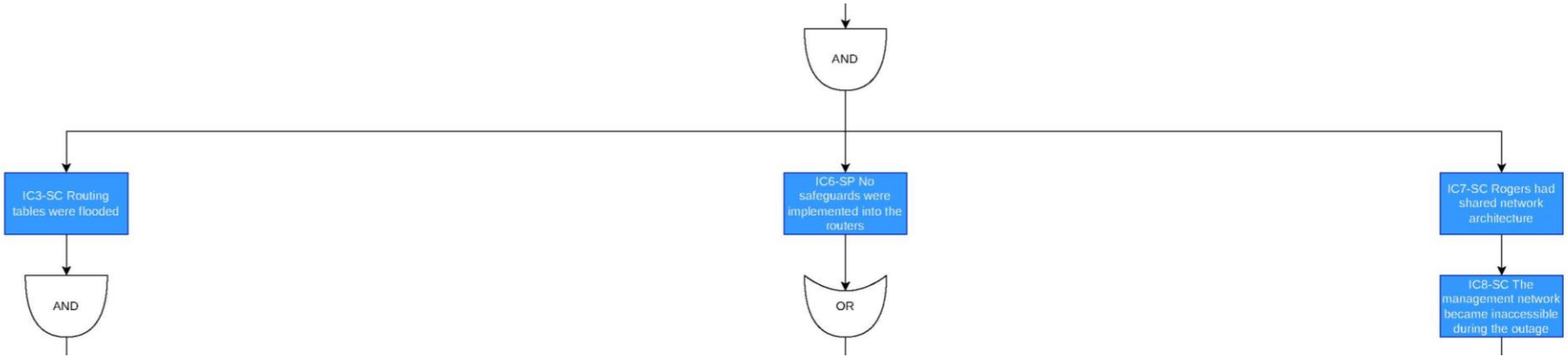
IPv6 ACL: Filter traffic on IPv6 networks

Named ACL: Create ACLs that are defined with a name, instead of a number

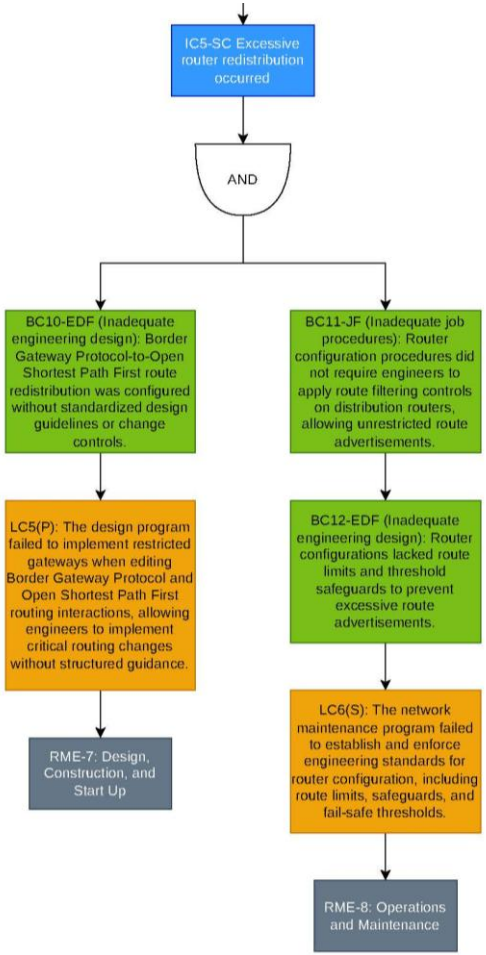

Incident Description
Immediate Causes
Basic Causes
Latent Causes
Risk Management Elements
AND
OR
Abbreviations
IC - Immediate Causes
BC - Basic Causes
JF - Job Factors
PF - Personal Factors
EF - Engineering Factors
LC - Latent Causes
S - Inadequate performance standards
P - Inadequate Program
C - inadequate compliance with performance standards
RME - Risk Management Elements
March 11, 2026
ENG 404 Team 202
Final RCA Chart
Team Members:
Dhruv Bhatia
John Alvaro
Kevin Ma
Michael Gao
Tabish Khan
On July 8-9, 2022, Rogers Communications experienced a nationwide outage lasting approximately 26 hours, disrupting services for over 12 million customers across Canada. The incident caused significant loss for customers such as people being affected through 911 access disruptions and healthcare service interruptions, the value assessed to being between $180-220 million by Rogers. No environmental impacts were reported, leading to negligible monetary losses. Asset losses included substantial reputational damage and loss of customer trust, and including the need to split physical and wireless lines resulted a $261 million loss for Rogers. Productivity impacts included widespread banking, transit, and business disruptions. The outage resulted in estimated economic losses exceeding $142 million across affected sectors.
IC1-SC Core IP network went down
IC2-SC Routers were overloaded
AND
IC3-SC Routing tables were flooded
AND
IC4-SC Removal of the ACL policy filter
OR
BC1-JF (Organizational factors): The change management audit process did not identify the network-wide routing impact associated with removing the ACL routing policy filter.
BC2-EDF (Inadequate technical design): The automated risk evaluation algorithm incorrectly downgraded the routing policy change from high risk to low risk.
BC3-JF (Organizational factors): Risk classification criteria within the automated change-risk evaluation system did not explicitly categorize routing policy modifications as high-impact risks.
LC1(S): The risk assessment program did not include a standard to ensure that automated risk evaluation algorithms accounted for the criticality of routing policy changes.
RME-2: Risk Assessment and Management of Risks
BC4-EDF (Inadequate technical design): Router services generated limited logging, reducing visibility into routing policy changes.
BC5-EDF (Inadequate engineering controls): Configuration change monitoring tools were not implemented to automatically flag critical routing policy modifications.
LC2(S): The incident monitoring and reporting program did not include standards requiring comprehensive logging and automated alerting for critical routing policy changes.
RME-5: Incident Reporting, Investigation, Analysis, &Action
BC6-PF (Lack of knowledge): Engineering personnel lacked sufficient understanding of the critical role of ACL routing filters, which allowed the unsafe removal of the filter during network changes.
LC3(P): The training program did not ensure that network engineers were properly trained on critical routing safeguards, increasing the likelihood that unsafe changes could be implemented without fully understanding their impact.
RME-9: Employee Competency and Training
BC7-JF (Inadequate job procedures): Pre-deployment lab testing procedures inadequately simulated production routing behavior before the routing policy change was implemented.
BC8-JF (Inadequate verification of work practices): Test scenarios were not defined to cover extreme route propagation cases, leaving the network vulnerable to overload.
BC9-JF (Inadequate verification of work practices): No formal process ensured multiple simultaneous configuration changes were tested together.
LC4(S): The system evaluation program did not include a standard to enforce industry best practices for testing and approval of core routing changes.
RME-6: Program Evaluation and Continuous Improvement
IC5-SC Excessive router redistribution occurred
AND
BC10-EDF (Inadequate engineering design): Border Gateway Protocol-to-Open Shortest Path First route redistribution was configured without standardized design guidelines or change controls.
LC5(P): The design program failed to implement restricted gateways when editing Border Gateway Protocol and Open Shortest Path First routing interactions, allowing engineers to implement critical routing changes without structured guidance.
RME-7: Design, Construction, and Start Up
BC11-JF (Inadequate job procedures): Router configuration procedures did not require engineers to apply route filtering controls on distribution routers, allowing unrestricted route advertisements.
BC12-EDF (Inadequate engineering design): Router configurations lacked route limits and threshold safeguards to prevent excessive route advertisements.
LC6(S): The network maintenance program failed to establish and enforce engineering standards for router configuration, including route limits, safeguards, and fail-safe thresholds.
RME-8: Operations and Maintenance
IC6-SP No safeguards were implemented into the routers
OR
BC13-JF (Inadequate verification of work practices): Multiple network configuration changes were implemented during the same maintenance window without staged validation between changes.
BC14-JF (Inadequate job procedures): Maintenance procedures did not require sequential deployment and validation of critical network configuration changes.
LC7(P): The network operations and maintenance program failed to establish and enforce standardized procedures requiring controlled, sequential deployment and validation of critical network changes
RME-8: Operations and Maintenance
BC15-EDF (Inadequate engineering controls): Core routers lacked configured limits to prevent flooding from excessive routing updates.
AND
BC16-EDF (Inadequate engineering controls): Engineering standards did not explicitly require overload protection safeguards for the core routing infrastructure.
BC17-EDF (Inadequate assessment of risks): The standards did not consider the impact of routing floods or potential router overloads.
LC8(P): The leadership program failed to establish a systematic process for identifying and enforcing critical technical safeguards, creating an unsafe environment for traffic data.
RME-1: Management Leadership, Commitment and Accountability
BC18-EDF (Inadequate management of change): Maintenance crews had not communicated the need to enforce safeguards in the router configuration during crew transitions.
BC19-JF (Inadequate internal communication between roles): There was an absence of accountability for ensuring safeguards were applied before deployment
LC9(C): The management of change program did not uphold enforcement mechanisms, resulting in insufficient prioritization of critical safeguards and inadequate compliance monitoring across teams.
RME-4: Management of Change
IC7-SC Rogers had shared network architecture
IC8-SC The management network became inaccessible during the outage
BC20-JF (organizational factors): The Network Operations Center and other critical network sites lacked independent third-party connectivity
BC21-EDF (Inadequate technical design): Both the wireless and wireline networks relied on the same IP core
BC22-EDF (Inadequate technical design): The management network was dependent on the production IP core rather than operating on an independent control network.
LC10 (P): The design program did not include redundancy when implementing their networks and internal communications, causing disrupted coordination and delayed response during the outage.
RME-3: Community Awareness and Emergency Preparedness

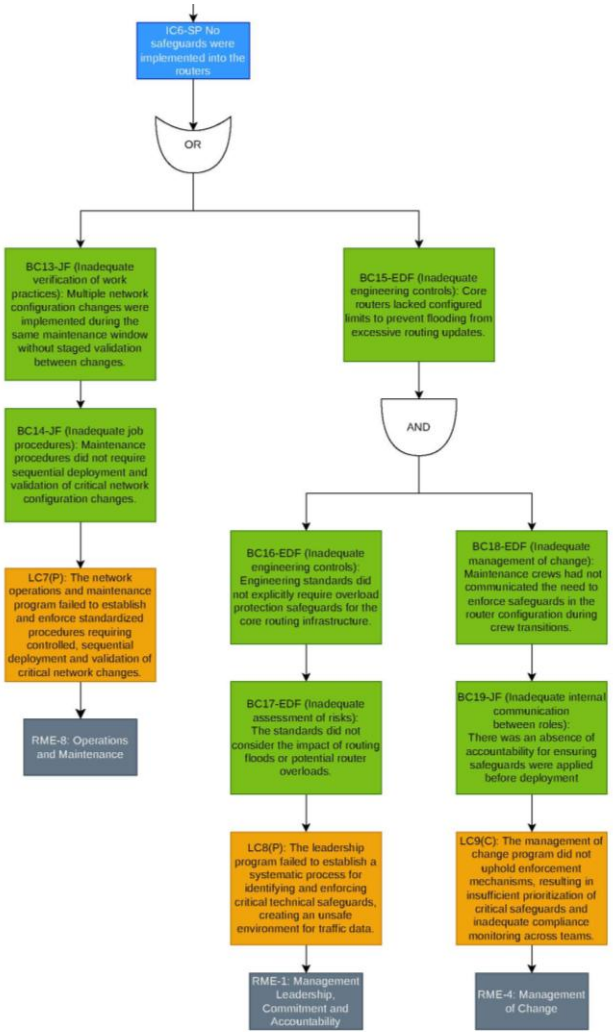
On July 8-9, 2022, Rogers Communications experienced a nationwide outage lasting approximately 26 hours, disrupting services for over 12 million customers across Canada. The incident caused significant loss for customers such as people being affected through 911 access disruptions and healthcare service interruptions, the value assessed to being between $180-220 million by Rogers. No environmental impacts were reported, leading to negligible monetary losses. Asset losses included substantial reputational damage and loss of customer trust, and including the need to split physical and wireless lines resulted a $261 million loss for Rogers. Productivity impacts included widespread banking, transit, and business disruptions. The outage resulted in estimated economic losses exceeding $142 million across affected sectors.

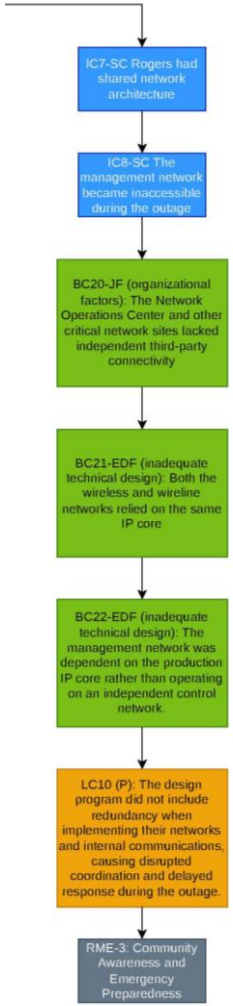


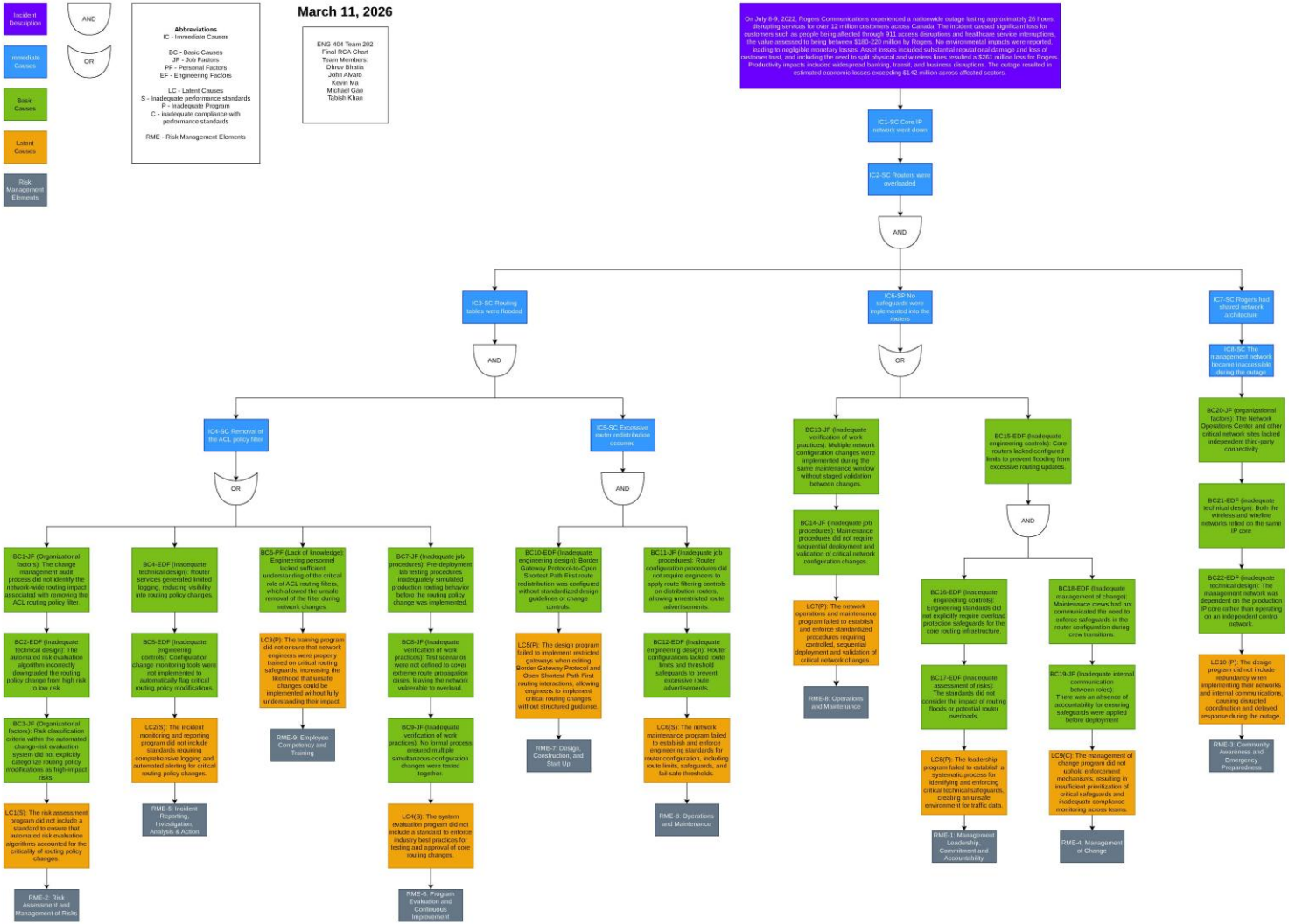

AND
IC3-SC Routing tables were flooded
AND
IC6-SP No safeguards were implemented into the routers
OR
IC7-SC Rogers had shared network architecture
IC8-SC The management network became inaccessible during the outage


IC4-SC Removal of the ACL policy filter
OR
BC1-JF (Organizational factors): The change management audit process did not identify the network-wide routing impact associated with removing the ACL routing policy filter.
BC2-EDF (Inadequate technical design): The automated risk evaluation algorithm incorrectly downgraded the routing policy change from high risk to low risk.
BC3-JF (Organizational factors): Risk classification criteria within the automated change-risk evaluation system did not explicitly categorize routing policy modifications as high-impact risks.
LC1(S): The risk assessment program did not include a standard to ensure that automated risk evaluation algorithms accounted for the criticality of routing policy changes.
RME-2: Risk Assessment and Management of Risks
BC4-EDF (Inadequate technical design): Router services generated limited logging, reducing visibility into routing policy changes.
BC5-EDF (Inadequate engineering controls): Configuration change monitoring tools were not implemented to automatically flag critical routing policy modifications.
LC2(S): The incident monitoring and reporting program did not include standards requiring comprehensive logging and automated alerting for critical routing policy changes.
RME-5: Incident Reporting, Investigation, Analysis & Action
BC6-PF (Lack of knowledge): Engineering personnel lacked sufficient understanding of the critical role of ACL routing filters, which allowed the unsafe removal of the filter during network changes.
LC3(P): The training program did not ensure that network engineers were properly trained on critical routing safeguards, increasing the likelihood that unsafe changes could be implemented without fully understanding their impact.
RME-9: Employee Competency and Training
BC7-JF (Inadequate job procedures): Pre-deployment lab testing procedures inadequately simulated production routing behavior before the routing policy change was implemented.
BC8-JF (Inadequate verification of work practices): Test scenarios were not defined to cover extreme route propagation cases, leaving the network vulnerable to overload.
BC9-JF (Inadequate verification of work practices): No formal process ensured multiple simultaneous configuration changes were tested together.
LC4(S): The system evaluation program did not include a standard to enforce industry best practices for testing and approval of core routing changes.
RME-6: Program Evaluation and Continuous Improvement

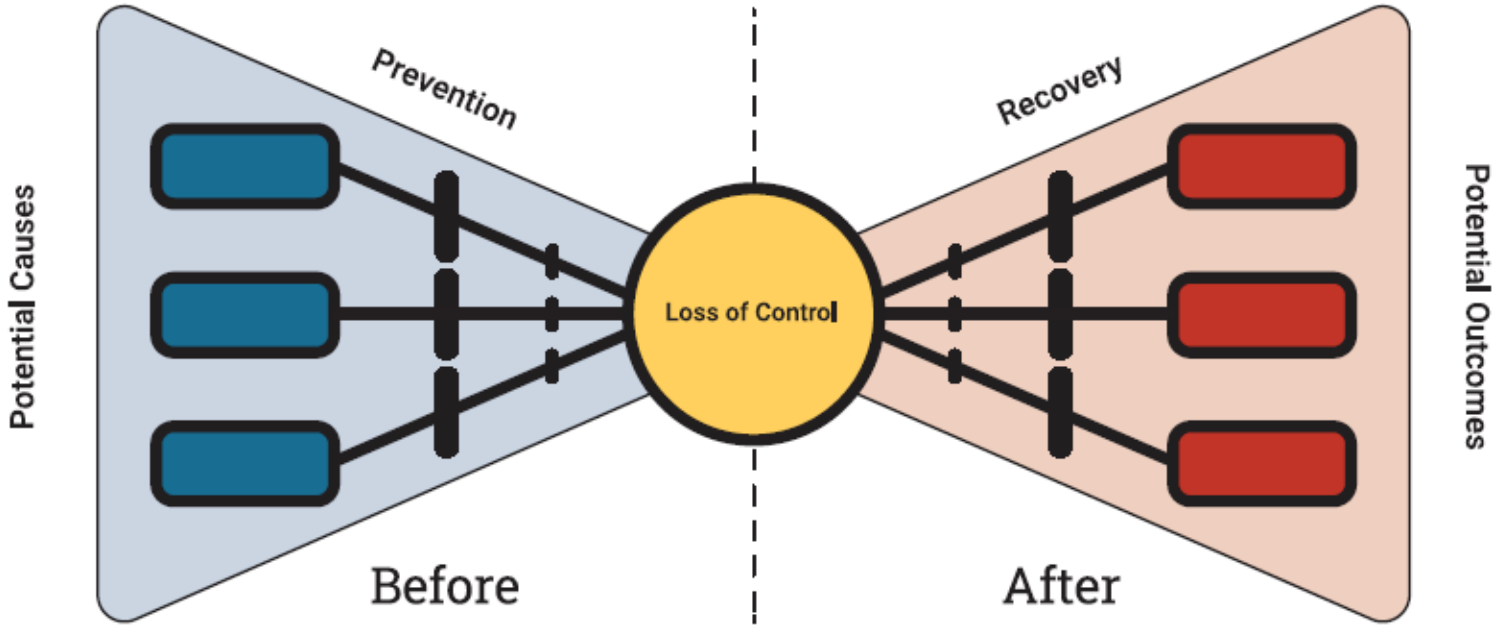

IC5-SC Excessive router redistribution occurred
AND
BC10-EDF (Inadequate engineering design): Border Gateway Protocol-to-Open Shortest Path First route redistribution was configured without standardized design guidelines or change controls.
BC11-JF (Inadequate job procedures): Router configuration procedures did not require engineers to apply route filtering controls on distribution routers, allowing unrestricted route advertisements.
LC5(P): The design program failed to implement restricted gateways when editing Border Gateway Protocol and Open Shortest Path First routing interactions, allowing engineers to implement critical routing changes without structured guidance.
BC12-EDF (Inadequate engineering design): Router configurations lacked route limits and threshold safeguards to prevent excessive route advertisements.
RME-7: Design, Construction, and Start Up
LC6(S): The network maintenance program failed to establish and enforce engineering standards for router configuration, including route limits, safeguards, and fail-safe thresholds.
RME-8: Operations and Maintenance


IC6-SP No safeguards were implemented into the routers
OR
BC13-JF (Inadequate verification of work practices): Multiple network configuration changes were implemented during the same maintenance window without staged validation between changes.
BC14-JF (Inadequate job procedures): Maintenance procedures did not require sequential deployment and validation of critical network configuration changes.
LC7(P): The network operations and maintenance program failed to establish and enforce standardized procedures requiring controlled, sequential deployment and validation of critical network changes.
RME-8: Operations and Maintenance
BC15-EDF (Inadequate engineering controls): Core routers lacked configured limits to prevent flooding from excessive routing updates.
AND
BC16-EDF (Inadequate engineering controls): Engineering standards did not explicitly require overload protection safeguards for the core routing infrastructure.
BC17-EDF (Inadequate assessment of risks): The standards did not consider the impact of routing floods or potential router overloads.
LC8(P): The leadership program failed to establish a systematic process for identifying and enforcing critical technical safeguards, creating an unsafe environment for traffic data.
RME-1: Management Leadership, Commitment and Accountability
BC18-EDF (Inadequate management of change): Maintenance crews had not communicated the need to enforce safeguards in the router configuration during crew transitions.
BC19-JF (Inadequate internal communication between roles): There was an absence of accountability for ensuring safeguards were applied before deployment
LC9(C): The management of change program did not uphold enforcement mechanisms, resulting in insufficient prioritization of critical safeguards and inadequate compliance monitoring across teams.
RME-4: Management of Change

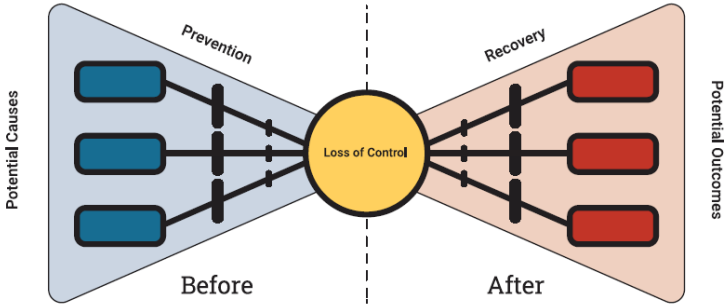

IC7-SC Rogers had shared network architecture
IC8-SC The management network became inaccessible during the outage
BC20-JF (organizational factors): The Network Operations Center and other critical network sites lacked independent third-party connectivity
BC21-EDF (inadequate technical design): Both the wireless and wireline networks relied on the same IP core
BC22-EDF (inadequate technical design): The management network was dependent on the production IP core rather than operating on an independent control network.
LC10 (P): The design program did not include redundancy when implementing their networks and internal communications, causing disrupted coordination and delayed response during the outage.
RME-3: Community Awareness and Emergency Preparedness

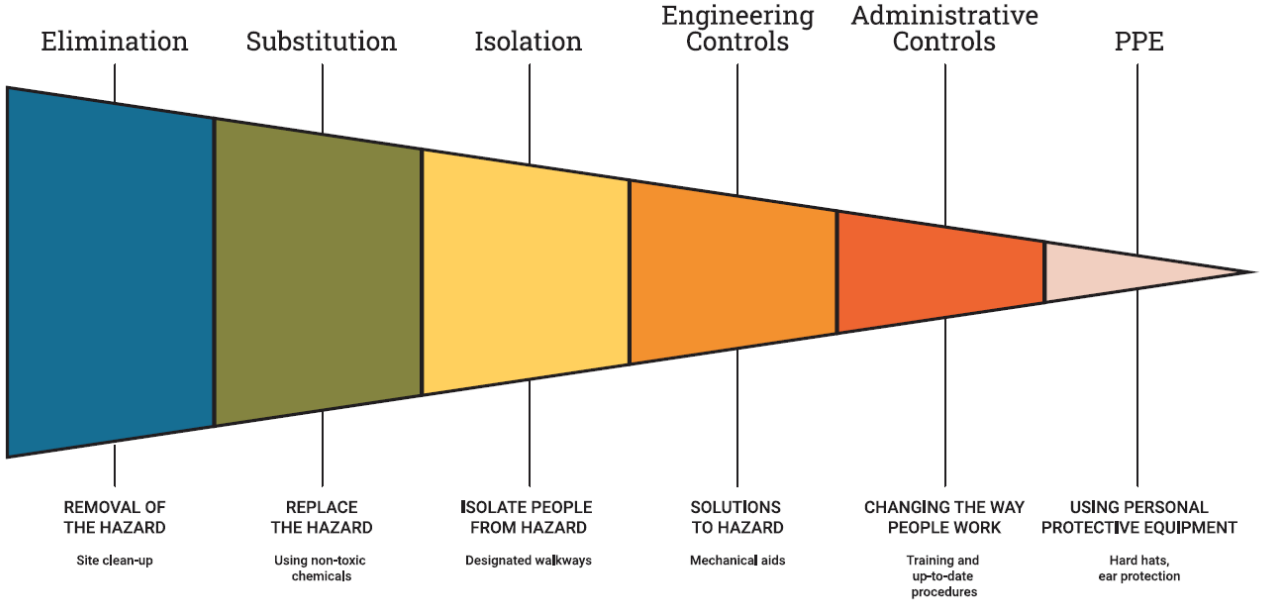

Incident Description
Immediate Causes
Basic Causes
Latent Causes
Risk Management Elements
AND
OR
Abbreviations
IC - Immediate Causes
BC - Basic Causes
JF - Job Factors
PF - Personal Factors
EF - Engineering Factors
LC - Latent Causes
S - Inadequate performance standards
P - Inadequate Program
C - inadequate compliance with performance standards
RME - Risk Management Elements
March 11, 2026
ENG 404 Team 202
Final RCA Chart
Team Members:
Dhruv Bhatia
John Alvaro
Kevin Ma
Michael Gao
Tabish Khan
On July 8-9, 2022, Rogers Communications experienced a nationwide outage lasting approximately 26 hours, disrupting services for over 12 million customers across Canada. The incident caused significant loss for customers such as people being affected through 911 access disruptions and healthcare service interruptions, the value assessed to being between $180-220 million by Rogers. No environmental impacts were reported, leading to negligible monetary losses. Asset losses included substantial reputational damage and loss of customer trust, and including the need to split physical and wireless lines resulted a $261 million loss for Rogers. Productivity impacts included widespread banking, transit, and business disruptions. The outage resulted in estimated economic losses exceeding $142 million across affected sectors.
IC1-SC Core IP network went down
IC2-SC Routers were overloaded
AND
IC3-SC Routing tables were flooded
AND
IC4-SC Removal of the ACL policy filter
OR
BC1-JF (Organizational factors): The change management audit process did not identify the network-wide routing impact associated with removing the ACL routing policy filter.
BC2-EDF (Inadequate technical design): The automated risk evaluation algorithm incorrectly downgraded the routing policy change from high risk to low risk.
BC3-JF (Organizational factors): Risk classification criteria within the automated change-risk evaluation system did not explicitly categorize routing policy modifications as high-impact risks.
LC1(S): The risk assessment program did not include a standard to ensure that automated risk evaluation algorithms accounted for the criticality of routing policy changes.
RME-2: Risk Assessment and Management of Risks
BC4-EDF (Inadequate technical design): Router services generated limited logging, reducing visibility into routing policy changes.
BC5-EDF (Inadequate engineering controls): Configuration change monitoring tools were not implemented to automatically flag critical routing policy modifications.
LC2(S): The incident monitoring and reporting program did not include standards requiring comprehensive logging and automated alerting for critical routing policy changes.
RME-5: Incident Reporting, Investigation, Analysis, &Action
BC6-PF (Lack of knowledge): Engineering personnel lacked sufficient understanding of the critical role of ACL routing filters, which allowed the unsafe removal of the filter during network changes.
LC3(P): The training program did not ensure that network engineers were properly trained on critical routing safeguards, increasing the likelihood that unsafe changes could be implemented without fully understanding their impact.
RME-9: Employee Competency and Training
BC7-JF (Inadequate job procedures): Pre-deployment lab testing procedures inadequately simulated production routing behavior before the routing policy change was implemented.
BC8-JF (Inadequate verification of work practices): Test scenarios were not defined to cover extreme route propagation cases, leaving the network vulnerable to overload.
BC9-JF (Inadequate verification of work practices): No formal process ensured multiple simultaneous configuration changes were tested together.
LC4(S): The system evaluation program did not include a standard to enforce industry best practices for testing and approval of core routing changes.
RME-6: Program Evaluation and Continuous Improvement
IC5-SC Excessive router redistribution occurred
AND
BC10-EDF (Inadequate engineering design): Border Gateway Protocol-to-Open Shortest Path First route redistribution was configured without standardized design guidelines or change controls.
LC5(P): The design program failed to implement restricted gateways when editing Border Gateway Protocol and Open Shortest Path First routing interactions, allowing engineers to implement critical routing changes without structured guidance.
RME-7: Design, Construction, and Start Up
BC11-JF (Inadequate job procedures): Router configuration procedures did not require engineers to apply route filtering controls on distribution routers, allowing unrestricted route advertisements.
BC12-EDF (Inadequate engineering design): Router configurations lacked route limits and threshold safeguards to prevent excessive route advertisements.
LC6(S): The network maintenance program failed to establish and enforce engineering standards for router configuration, including route limits, safeguards, and fail-safe thresholds.
RME-8: Operations and Maintenance
IC6-SP No safeguards were implemented into the routers
OR
BC13-JF (Inadequate verification of work practices): Multiple network configuration changes were implemented during the same maintenance window without staged validation between changes.
BC14-JF (Inadequate job procedures): Maintenance procedures did not require sequential deployment and validation of critical network configuration changes.
LC7(P): The network operations and maintenance program failed to establish and enforce standardized procedures requiring controlled, sequential deployment and validation of critical network changes
RME-8: Operations and Maintenance
BC15-EDF (Inadequate engineering controls): Core routers lacked configured limits to prevent flooding from excessive routing updates.
AND
BC16-EDF (Inadequate engineering controls): Engineering standards did not explicitly require overload protection safeguards for the core routing infrastructure.
BC17-EDF (Inadequate assessment of risks): The standards did not consider the impact of routing floods or potential router overloads.
LC8(P): The leadership program failed to establish a systematic process for identifying and enforcing critical technical safeguards, creating an unsafe environment for traffic data.
RME-1: Management Leadership, Commitment and Accountability
BC18-EDF (Inadequate management of change): Maintenance crews had not communicated the need to enforce safeguards in the router configuration during crew transitions.
BC19-JF (Inadequate internal communication between roles): There was an absence of accountability for ensuring safeguards were applied before deployment
LC9(C): The management of change program did not uphold enforcement mechanisms, resulting in insufficient prioritization of critical safeguards and inadequate compliance monitoring across teams.
RME-4: Management of Change
IC7-SC Rogers had shared network architecture
IC8-SC The management network became inaccessible during the outage
BC20-JF (organizational factors): The Network Operations Center and other critical network sites lacked independent third-party connectivity
BC21-EDF (inadequate technical design): Both the wireless and wireline networks relied on the same IP core
BC22-EDF (inadequate technical design): The management network was dependent on the production IP core rather than operating on an independent control network.
LC10 (P): The design program did not include redundancy when implementing their networks and internal communications, causing disrupted coordination and delayed response during the outage.
RME-3: Community Awareness and Emergency Preparedness

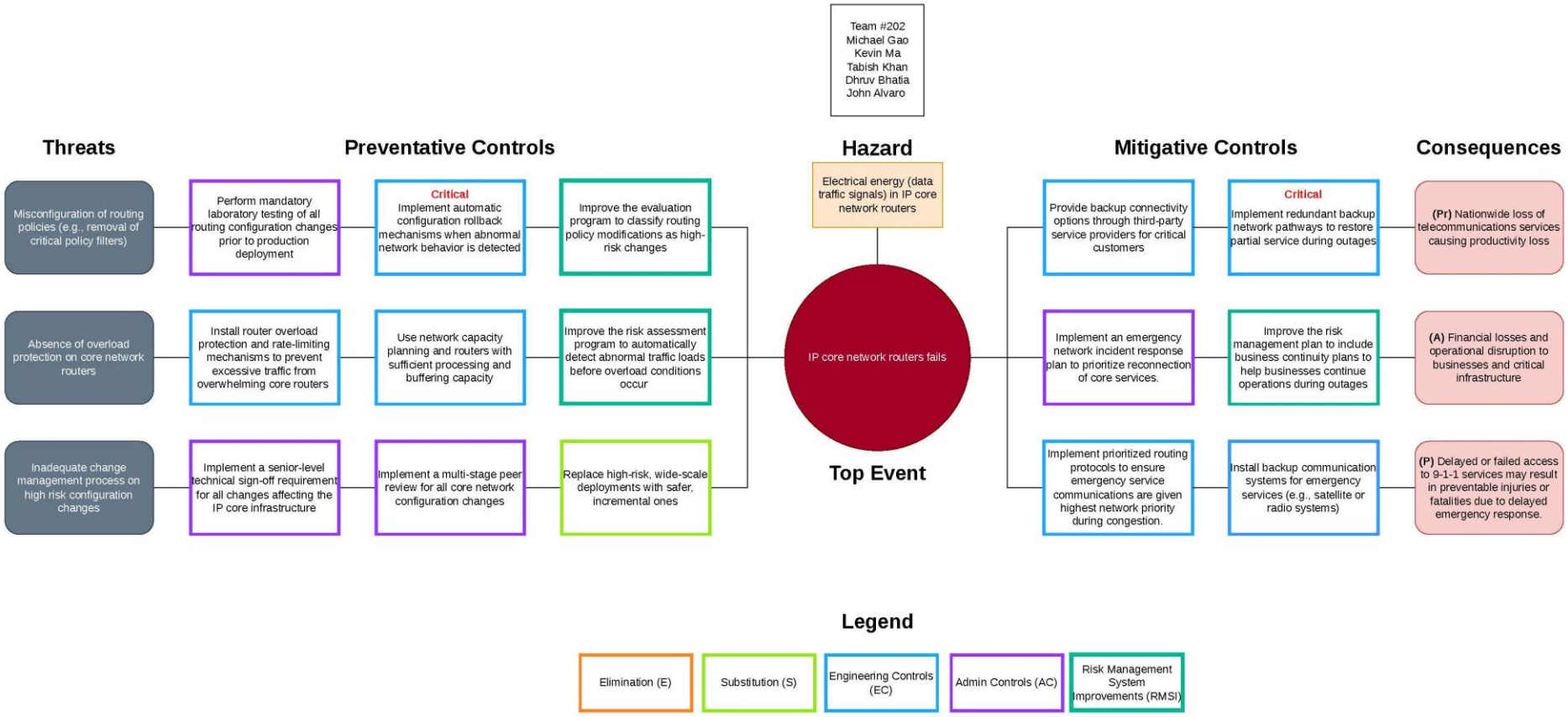
Use Bowties to examine causes for loss of control, outcomes, preventions, and recovery/mitigations



Bowties show that safety is the presence of layers of controls, so we are more likely to fail safely than fail lucky






Team #202
Michael Gao
Kevin Ma
Tabish Khan
Dhruv Bhatia
John Alvaro
Threats
Preventative Controls
Hazard
Mitigative Controls
Consequences
Misconfiguration of routing policies (e.g., removal of critical policy filters)
Perform mandatory laboratory testing of all routing configuration changes prior to production deployment
Critical
Implement automatic configuration rollback mechanisms when abnormal network behavior is detected
Improve the evaluation program to classify routing policy modifications as high-risk changes
Electrical energy (data traffic signals) in IP core network routers
Provide backup connectivity options through third-party service providers for critical customers
Critical
Implement redundant backup network pathways to restore partial service during outages
(Pr) Nationwide loss of telecommunications services causing productivity loss
Absence of overload protection on core network routers
Install router overload protection and rate-limiting mechanisms to prevent excessive traffic from overwhelming core routers
Use network capacity planning and routers with sufficient processing and buffering capacity
Improve the risk assessment program to automatically detect abnormal traffic loads before overload conditions occur
IP core network routers fails
Implement an emergency network incident response plan to prioritize reconnection of core services.
Improve the risk management plan to include business continuity plans to help businesses continue operations during outages
(A) Financial losses and operational disruption to businesses and critical infrastructure
Inadequate change management process on high risk configuration changes
Implement a senior-level technical sign-off requirement for all changes affecting the IP core infrastructure
Implement a multi-stage peer review for all core network configuration changes
Replace high-risk, wide-scale deployments with safer, incremental ones
Top Event
Implement prioritized routing protocols to ensure emergency service communications are given highest network priority during congestion.
Install backup communication systems for emergency services (e.g., satellite or radio systems)
(P) Delayed or failed access to 9-1-1 services may result in preventable injuries or fatalities due to delayed emergency response.
Legend
Elimination (E)
Substitution (S)
Engineering Controls (EC)
Admin Controls (AC)
Risk Management System Improvements (RMSI)

In sum:

- Process safety techniques – root cause analysis, risk management element failures, bowties are supremely helpful for examining non-chemical/process safety incidents

- Linking root causes to failures in risk management elements generates very specific recommendations for improvements
- Tying these to RACI supports organizational learning and change

- Bowties also demonstrate that a “layers of protection” approach ensures organizational fail safely and not ‘fail lucky’ or, worse, unlucky

- We teach this to 1000+ engineering undergraduates/year

Thank you!

"Bowtie Primer"

"Using Key Risk Indicators"

"What is the Value of Risk Management"

"Why is the Value of Risk Management so Difficult to Measure?"

Lianne M. Lefsrud, PhD, PEng, lefsrud@ualberta.ca
Risk, Innovation, and Sustainability Chair (RISC)
Professor, Engineering Safety and Risk Management
E: lefsrud@ualberta.ca, W: liannelefsrud.com