Using software development standards to analyse incidents involving E/E/PE systems: The blade mill PLC case study

Mark Bowell
Health and Safety Executive

Chris Johnson
University of Glasgow

IRIA 03 17 September 2003

Glasgow Accident Analysis Group

Overview

- **Background and objectives**
- **PARCEL**
- **Case study**
- **Way forward**

UK Health and Safety Executive Mission statement

To ensure that risks to people's health and safety from work activities is properly controlled

Management of Health and Safety at Work Regulations 1999

The Approved Code of Practice requires that employers:

Adequately investigate the immediate and underlying causes of incidents and accidents to ensure that remedial action is taken, lessons are learnt and longer-term objectives are introduced.

It may be appropriate to record and analyse the results of monitoring activity, to identify any underlying themes or trends, which may not be apparent from looking at events in isolation.

Industry today

- Fragmentation – impedes holistic root cause analysis and information sharing
- Contractors – lack of competence and experience
- Standards – main technical influence
- Existing systems – little knowledge of design history
- E/E/PES involvement – difficult for users to determine
- "Openness" culture – non-confidential reporting

Industry today

- Causal analysis techniques
  - Timelines, event trees and checklists
  - Accident trees plus structured checklists
  - Event chain modelling
  - Textual elaboration by experts
- Formal classification of causes is rare
- Focus on necessary immediate changes
- Good tracking of safety recommendations

Objectives

- To analyse the cause of E/E/PES incidents
- Incremental adoption
- Proportionality
- Trend analysis
- Information sharing
- Collation
- Match existing standards/guidance – IEC 61508
- Inform standard revision

Participants

- Adelard
- Glasgow Accident Analysis Group
- Blacksafe Consulting
- UK Health and Safety Executive

Industry sectors

- Onshore and offshore oil and gas
- Chemical plant
- Nuclear installations
- Railways
- Mines and quarries
- Factories

- Pharmaceuticals
- Marine
- Aviation

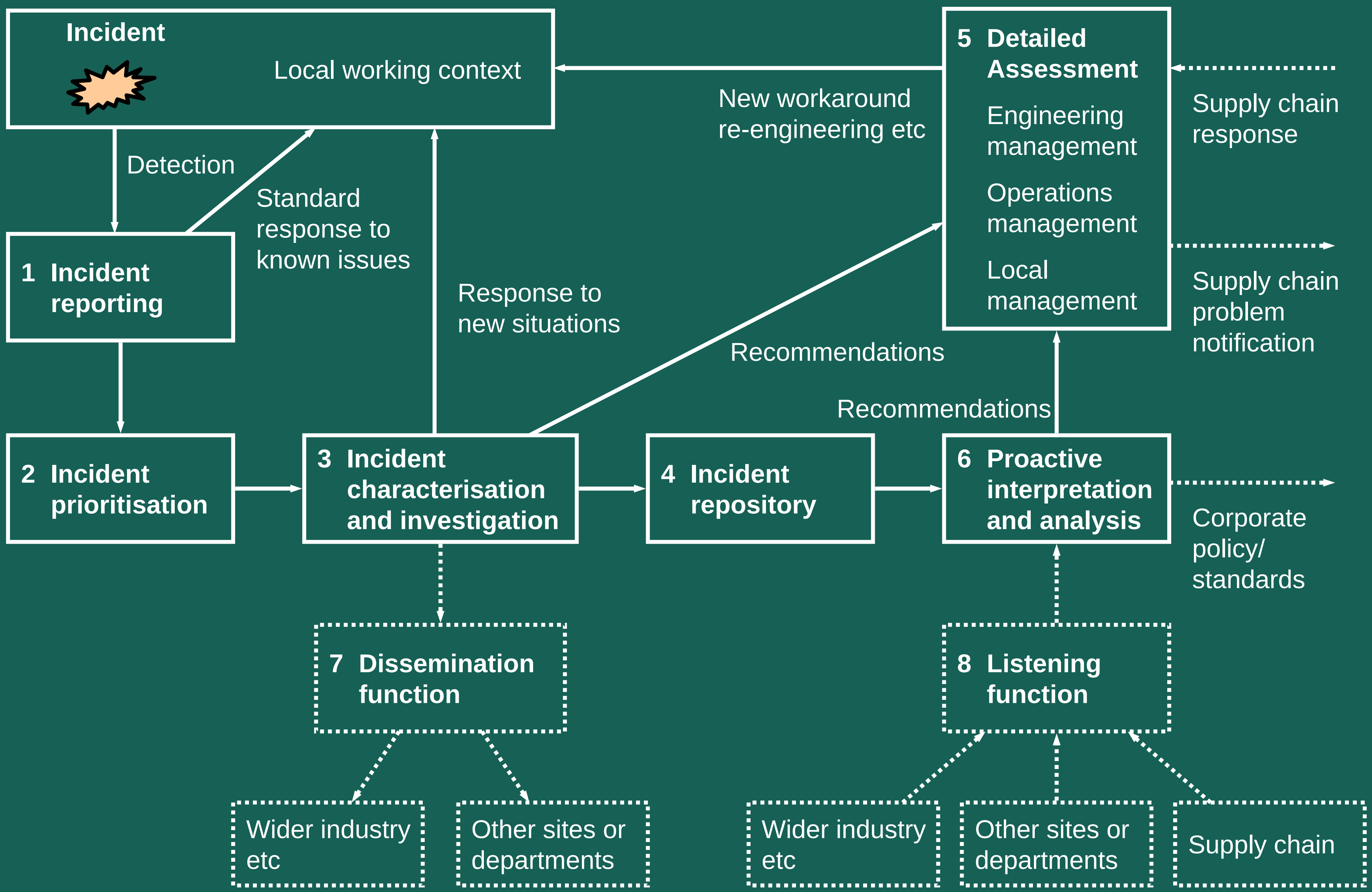
Roles

- End users
- Designers
- System suppliers/integrators
- Maintainers

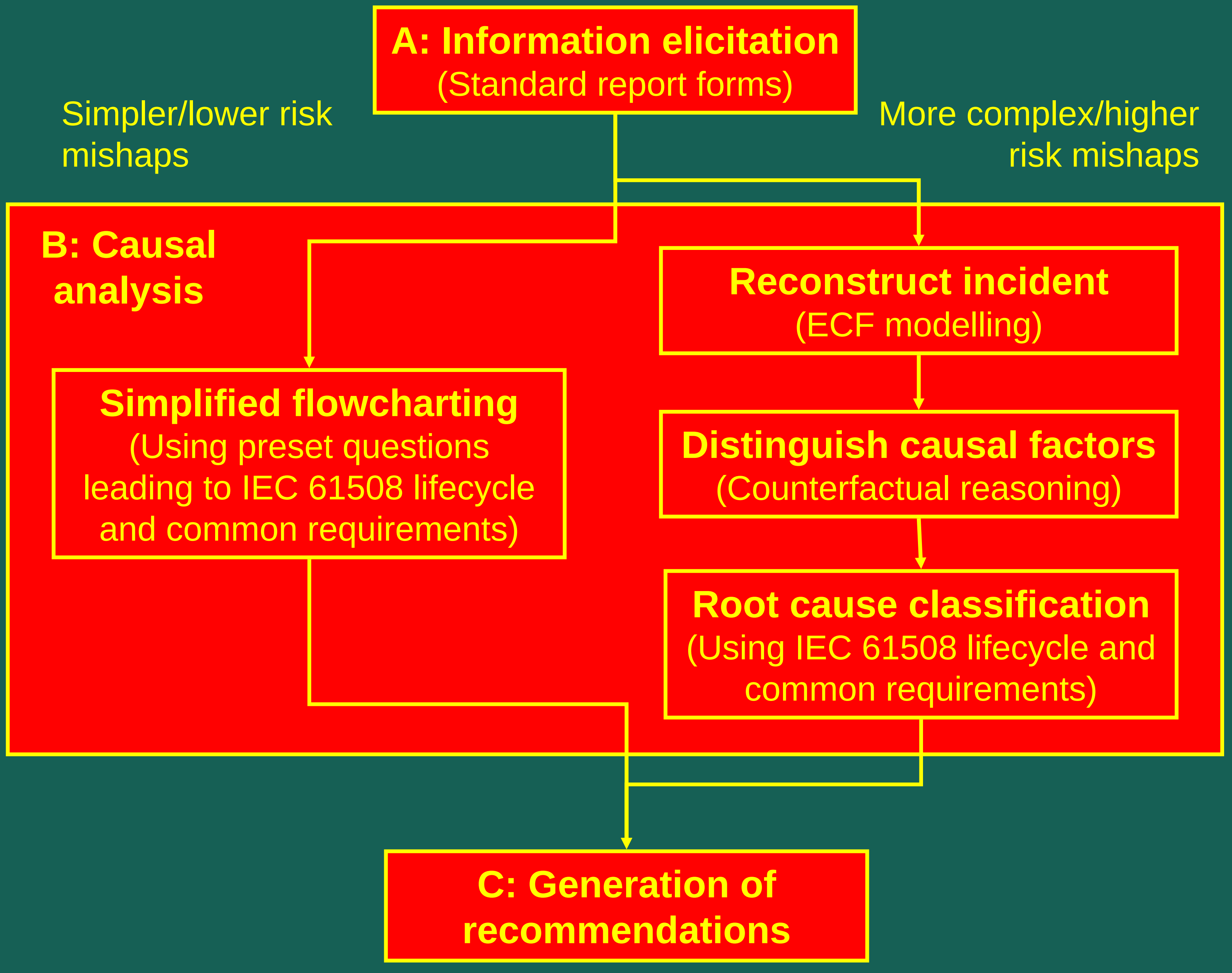
PARCEL

Programmable electronic systems
Analysis of
Root
Causes for
Experience-based
Learning

Overall learning process



	Elicitation and analysis techniques	Barrier analysis	Change analysis	**Event based techniques**	Timelines	Accident fault trees	Events and causal factors charting	**Flowcharts and taxonomies**	MORT	PRISMA	**Accident models**	TRIPOD	STAMP	**Argumentation techniques**	Why-Because analysis	CAE diagrams
IEC 61508 lifecycle phase																
Concept		**S**	**S**		-	-	s		**S**	s		**S**	s		-	**S**
Overall scope		**S**	**S**		-	-	s		**S**	s		**S**	s		-	**S**
Hazard and risk assessment		s	s		s	s	s		**S**	s		s	**S**		-	**S**
Overall safety requirements		**S**	**S**		-	-	s		s	s		**S**	**S**		-	**S**
Allocation		**S**	s		s	-	**S**		s	s		**S**	s		-	-
Planning of I & C, V and O & M		-	s		s	s	**S**		**S**	**S**		-	s		s	-
Realisation		-	**S**		**S**	s	**S**		-	s		-	**S**		**S**	-
Installation and commissioning		-	s		**S**	s	**S**		s	s		s	s		**S**	s
Validation		s	s		s	s	**S**		s	s		s	-		**S**	s
Operation and maintenance		s	**S**		**S**	s	**S**		s	s		**S**	**S**		**S**	s
Modification		-	**S**		**S**	s	**S**		s	s		-	**S**		**S**	s
IEC 61508 common requirements																
Competence		s	s		s	s	**S**		s	s		**S**	s		s	s
Lifecycle		-	s		s	s	**S**		s	s		s	s		s	s
Verification		s	s		s	s	**S**		s	s		s	s		s	s
Safety management		s	s		s	s	**S**		s	s		s	s		s	s
Documentation		s	s		s	s	**S**		s	s		s	s		s	s
Functional safety assessment		s	s		s	s	**S**		s	s		s	s		s	s


A: Information elicitation
(Standard report forms)
Simpler/lower risk mishaps
More complex/higher risk mishaps
B: Causal analysis
Reconstruct incident
(ECF modelling)
Simplified flowcharting
(Using preset questions leading to IEC 61508 lifecycle and common requirements)
Distinguish causal factors
(Counterfactual reasoning)
Root cause classification
(Using IEC 61508 lifecycle and common requirements)
C: Generation of recommendations

End user classification

IEC 61508 lifecycle reference
System assessment
Safety requirements and allocation
E/E/PES installation and commissioning planning
E/E/PES validation planning
E/E/PES operation and maintenance planning
E/E/PES realisation
E/E/PES installation and commissioning
E/E/PES validation
E/E/PES operation and maintenance
E/E/PES modification

IEC 61508 common requirement
Safety management
Lifecycle
Competence
Verification
Documentation
Functional safety assessment

IEC 61508 lifecycle phase	Classification	IEC 61508 reference
System assessment	1 LTA hazard and risk assessment	7.2, 7.3, 7.4
E/E/PES operation and maintenance	1 LTA operation procedures 2 Operation procedures not impact assessed 3 Operation procedures not applied 4 LTA maintenance procedures 5 Maintenance procedures not impact assessed 6 Maintenance procedures not applied 7 No routine operation or maintenance audits 8 Test interval not sufficient 9 LTA permit/hand over procedures 10 LTA procedures to monitor system performance 11 Tools incorrectly selected or applied	7.6.2.1/2/5 (2) 7.6.2.4 (2) 7.15.2.1/2 7.6.2.1/2/3/5 (2) 7.6.2.4 (2) 7.15.2.1/2 7.15.2.3, 7.6.2.1/2 (2) 7.6.2.3 (2) 7.6.2.1 (2) 7.6.2.1f (2) 7.6.2.1g (2)
E/E/PES modification	1 LTA procedures applied to initiate modification in the event of systematic failures or vendor notification of faults 2 LTA authorisation procedure 3 LTA impact analysis 4 LTA modification plan (including sufficient lifecycle activities) 5 LTA implementation of modification plan 6 LTA manufacturers information 7 LTA verification and validation	6.2.11, 7.8.2.2 (2) 7.16.2.2/5, 7.8.2.1c (2) 7.16.2.3/6, 7.8.2.1b (2) 7.16.2.1/6, 7.8.2.3 (2) 7.16.2.1 7.8.2.1 (2) 7.8.2.4 (2)

Blade Mill PLC case study

- Details from http://www.msha.gov/fatals/1997/ftl97m01.htm

- Gravel wash plant
- Blade mill to ‘precondition’ aggregates prior to wet screening
- Mill consisted of two interlocking screws driven by two 40-horse power motors
- Motors operated from a control center in a trailer 30 metres away

Blade Mill PLC case study

- At the start of this day, material was frozen inside mill and broken paddle tips and wearing shoes needed replacing
- Material thawed using a propane burner, mechanic signalled to foreman to start motors to check that blades are free
- Foreman switches buttons to ‘off’ and moves to another task elsewhere
- Foreman returns to help carry out repairs, but is then called to assist an electrician working on a faulty circuit breaker
- Circuit breaker in control center had been tripping out after 10-15 minutes of operation, resulting in loss of control power to the wash plant components

Blade Mill PLC case study

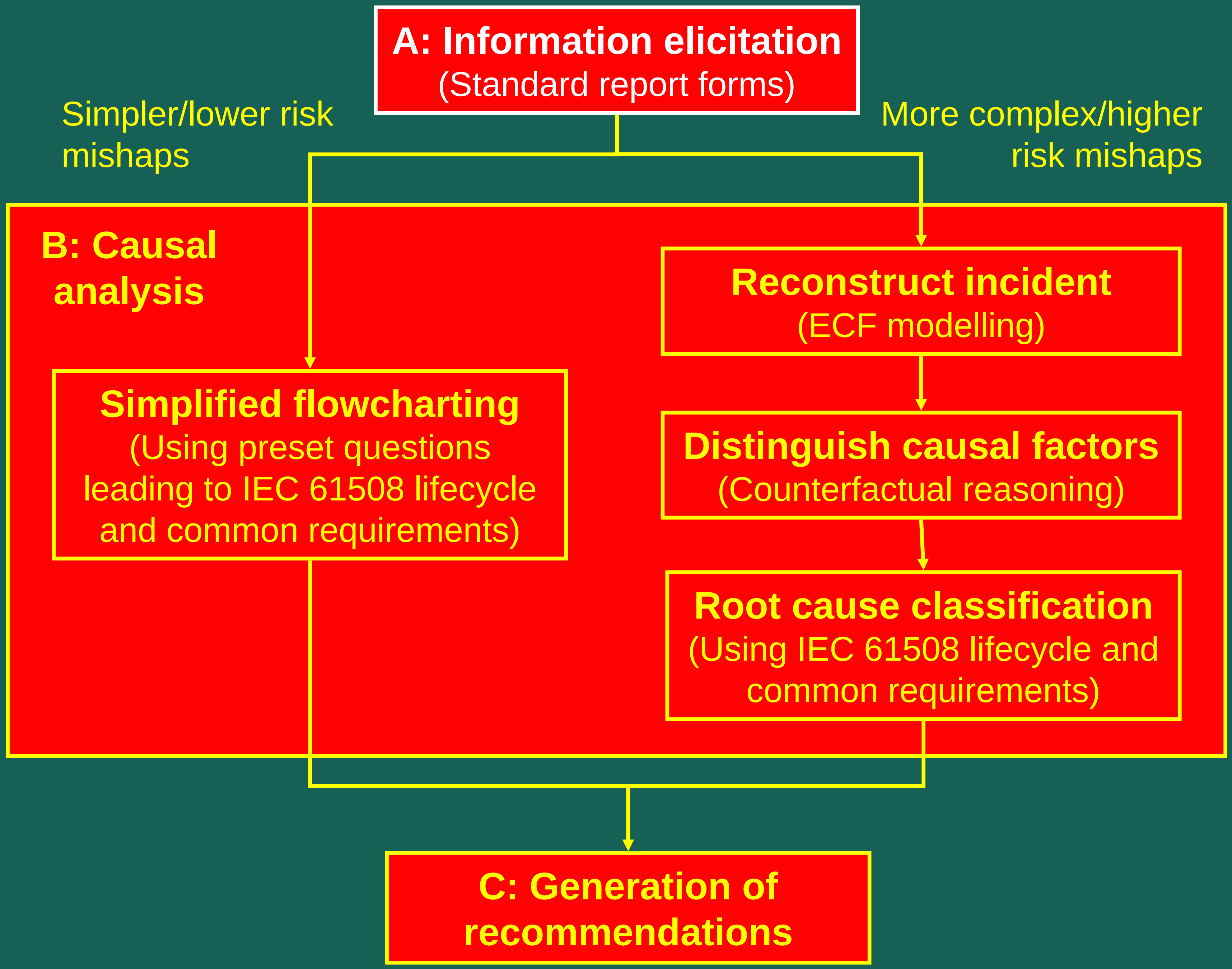
- The electrician switched the breaker on and together with the foreman watched it for several minutes without observing a trip
- The electrician then switched it off and began diagnosing the problem
- Meanwhile the foreman returned to check on the mechanic
- As he was leaving the control center, he noticed that the blade mill buttons were in the ‘run’ position
- He pushed them off and continued to the mill where he found the mechanic entangled in the blades
- Paramedics later pronounced the mechanic dead at the scene

Blade Mill PLC case study

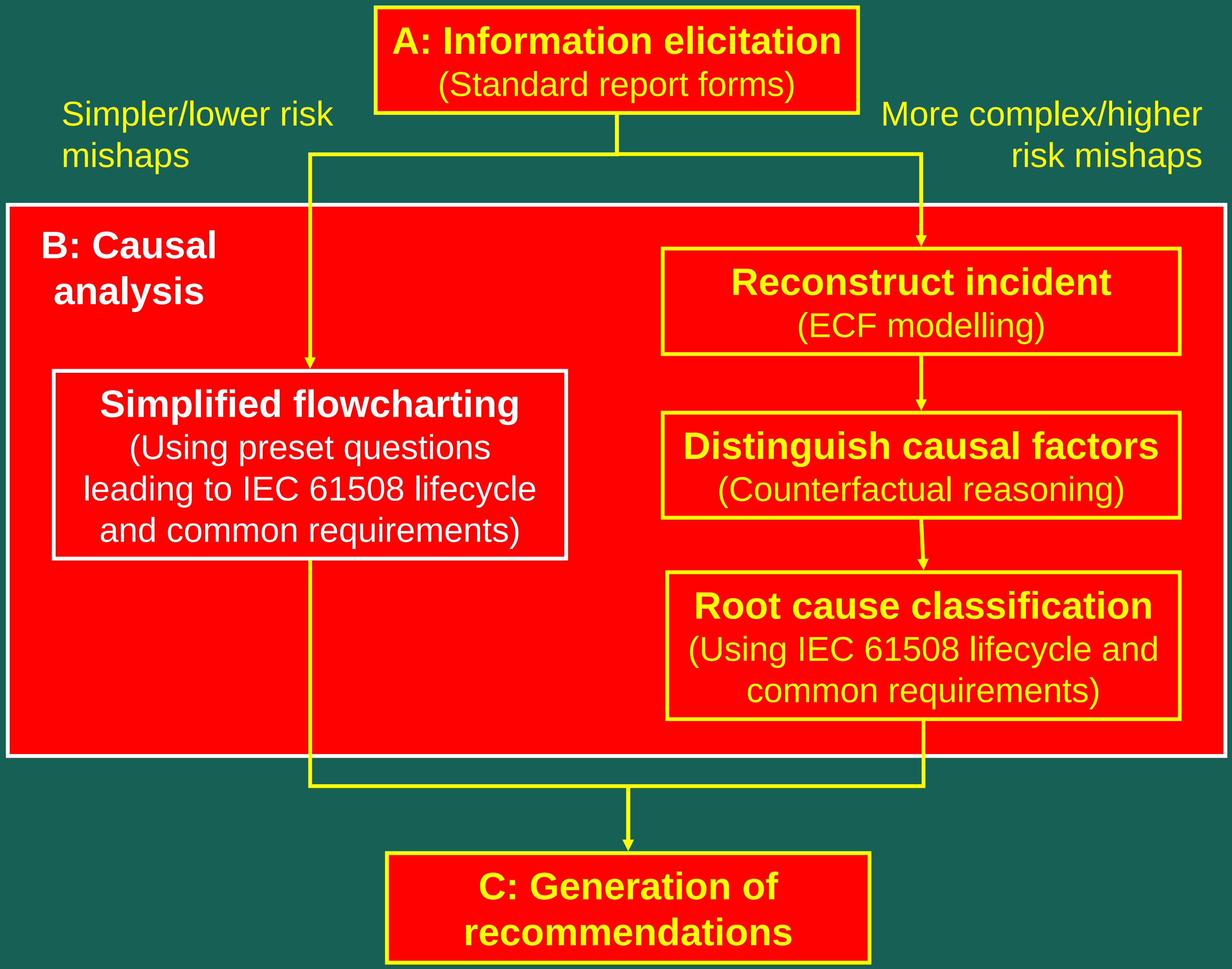
- A modification to the PLC three months earlier had resulted in power being unintentionally returned to components following a power failure, if their switches had been left 'on'.

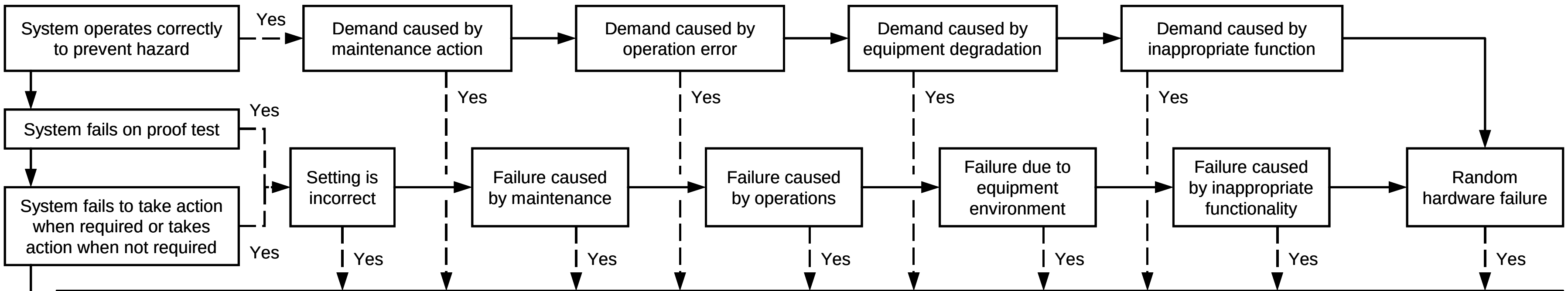
Investigators concluded:

- The mechanic turned the mill back on to clear some remaining frozen material while the foreman was away the first time
- The mill operated until the circuit breaker tripped out
- The mechanic went back to work on the mill without shutting off any switches


A: Information elicitation
(Standard report forms)
Simpler/lower risk mishaps
More complex/higher risk mishaps
B: Causal analysis
Reconstruct incident
(ECF modelling)
Simplified flowcharting
(Using preset questions leading to IEC 61508 lifecycle and common requirements)
Distinguish causal factors
(Counterfactual reasoning)
Root cause classification
(Using IEC 61508 lifecycle and common requirements)
C: Generation of recommendations

Initial incident report	
Your name	Mark Bowell
Date of report	9 January 1997
Date of incident	8 January 1997
Time of incident	12.30 pm
Title	Blade mill fatality
Reference number	97/01
Location of Incident	Pre-conditioning blade mill
Was any person hurt?	Yes – fatality
Did any damage or loss of production occur?	Not significant
Could this have led to more serious consequences?	No – already a fatality
Has this problem occurred before?	No
Electrical/electronic equipment involved	Kolberg Products Model 6500 blade mill GE Fanuc 90-30 Programmable Logic Controller
Electrical/electronic equipment cause or failure	Unwarranted blade mill start-up
Describe the incident	Mechanic assigned to thaw frozen material inside the blade mill and then replace broken and worn paddle tips and wearing shoes. He was found entangled in the blades. Controls were found in 'run' position and circuit breaker had been reset after previously tripping out, so mill must have restarted while he was working.


A: Information elicitation
(Standard report forms)
Simpler/lower risk mishaps
More complex/higher risk mishaps
B: Causal analysis
Reconstruct incident
(ECF modelling)
Simplified flowcharting
(Using preset questions leading to IEC 61508 lifecycle and common requirements)
Distinguish causal factors
(Counterfactual reasoning)
Root cause classification
(Using IEC 61508 lifecycle and common requirements)
C: Generation of recommendations



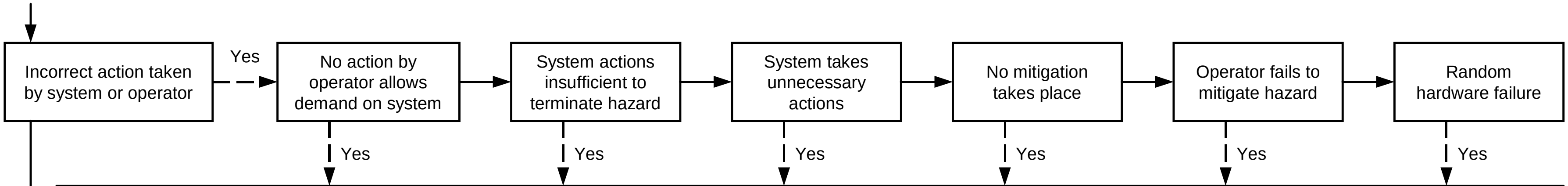
Would the incident have been prevented if

System concept	– hazard and risk analysis had considered all modes of operation and causes	– hazard and risk analysis had considered all modes of operation and causes	– hazard and risk analysis had considered all modes of operation and causes			Log failure and check – if dangerous failure rate is in line with design assumptions – if all expected actions occurred and no unexpected actions occurred – if safe failure causes any unexpected actions Log demand and check – if demand rate is in line with design assumptions – if demand cause was predicted in hazard and risk analysis
Design	– different equipment had been selected – the installation design had been different – specification was correct	– maintenance facilities had been designed adequately	– operation facilities had been designed adequately	– different equipment had been selected – the installation design had been different	– different equipment had been selected – the installation design had been different – configuration was correct	
Installation & commissioning	– the equipment had been installed according to design	– the maintenance facilities had been installed according to design	– the operation facilities had been installed according to design	– the equipment had been installed according to design	– the equipment had been installed according to design	
Validation	– the setting had been checked during validation	– maintenance facilities had been fully checked	– operation facilities had been fully checked	– equipment condition had been fully checked	– equipment condition had been fully checked	
Operation & maintenance	– maintenance procedures were applied – maintenance procedures were improved – test interval was reduced	– correct maintenance procedure had been used – maintenance procedure was improved – permit procedures were improved	– correct operation procedure had been used – operation procedure was improved – permit procedures were improved	– maintenance procedures were applied – maintenance procedures were improved – test interval was reduced – additional protection was provided	– maintenance procedures were improved – maintenance tools were improved – test interval was reduced – additional protection was provided	
Modification	– setting had been reviewed during impact analysis	– maintenance facilities or procedures had been reviewed during impact analysis	– operation facilities or procedures had been reviewed during impact analysis	– equipment used or installation design had been reviewed during impact analysis	– equipment used or installation design had been reviewed during impact analysis	

Would the incident have been prevented if

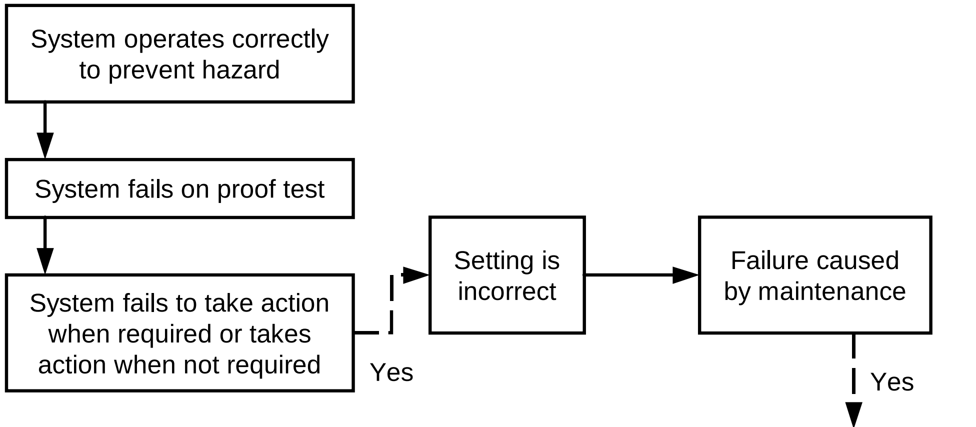
	Competence	**Lifecycle**	**Verification**	**Safety management**	**Documentation**	**Safety assessment**
Operation & maintenance	– operation or maintenance staff were more competent	– responsibilities were defined better	– a better verification scheme had been in place	– safety culture was improved – audits were more frequent	– documentation was clear and sufficient	– operation and maintenance phase had been assessed
Modification	– modification had been carried out by more competent staff	– modification lifecycle was better defined	– a better verification scheme had been in place	– accountabilities were better defined – suppliers had been reviewed	– documentation had been updated	– modification had been assessed

Continued from previous page



	Would the incident have been prevented if					
System concept	– hazard and risk analysis had considered all modes of operation and causes	– hazard and risk analysis had considered all modes of operation and causes	– hazard and risk analysis had considered all modes of operation and causes	– hazard and risk analysis had considered all modes of operation and causes	– hazard and risk analysis had considered all modes of operation and causes	Log failure and check – if dangerous failure rate is in line with design assumptions – if all expected actions occurred and no unexpected actions occurred – if safe failure causes any unexpected actions Log demand and check – if demand rate is in line with design assumptions – if demand cause was predicted in hazard and risk analysis
Design	– operator facilities had been designed better – the installation design had been different	– additional actions had been specified – actions had been faster – final actuation device were improved	– design requirements were better documented	– mitigation system had been specified – mitigation system had been better designed	– operator facilities had been designed better – the installation design had been different	
Installation & commission-ing	– the equipment had been installed according to design	– the equipment had been installed according to design	– the equipment had been installed according to design	– mitigation system had been installed according to design	– the equipment had been installed according to design	
Validation	– operator facilities had been checked during validation	– operation facilities had been checked during validation	– operation facilities had been fully checked	– mitigation system had been fully checked	– operator facilities had been fully checked	
Operation & maintenance	– operation procedures were applied – operation procedures were improved	– correct maintenance procedure had been used – maintenance procedure was improved – proof testing was more frequent	– correct operation procedure had been used – operation procedure was improved – permit procedures were improved	– mitigation procedures were applied – mitigation procedures were improved – mitigation system was proof tested more frequently	– operation procedures had been applied – operation facilities or procedures were improved	
Modification	– operation facilities had been reviewed during impact analysis	– necessary system actions had been reviewed during impact analysis	– necessary system actions had been reviewed during impact analysis	– need for mitigation had been reviewed during impact analysis	– need for mitigation had been reviewed during impact analysis	

	Would the incident have been prevented if					
	Competence	**Lifecycle**	**Verification**	**Safety management**	**Documentation**	**Safety assessment**
Operation & maintenance	– operation or maintenance staff were more competent	– responsibilities were defined better	– a better verification scheme had been in place	– safety culture was improved – audits were more frequent	– documentation was clear and sufficient	– operation and maintenance phase had been assessed
Modification	– modification had been carried out by more competent staff	– modification lifecycle was better defined	– a better verification scheme had been in place	– accountabilities were better defined – suppliers had been reviewed	– documentation had been updated	– modification had been assessed

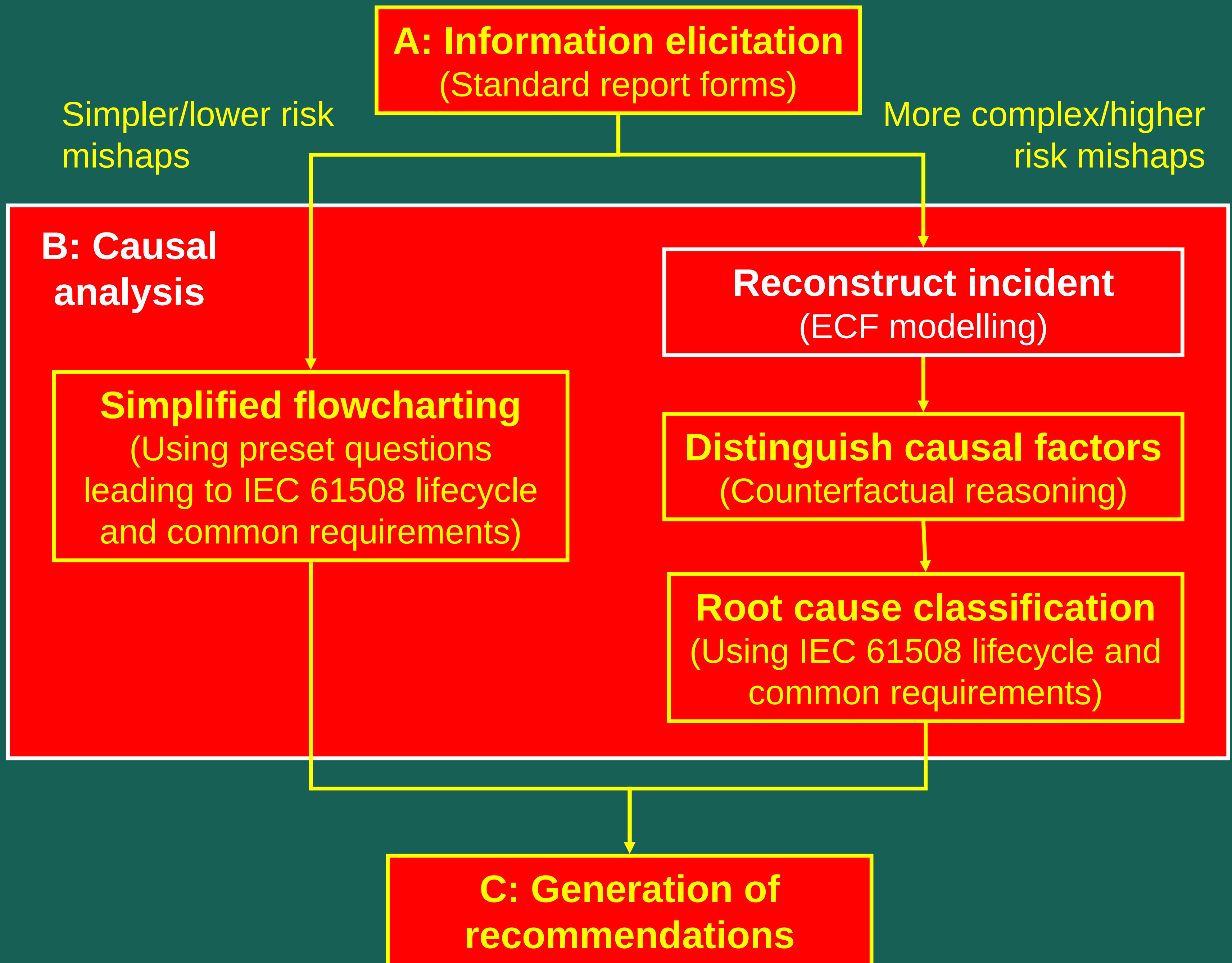


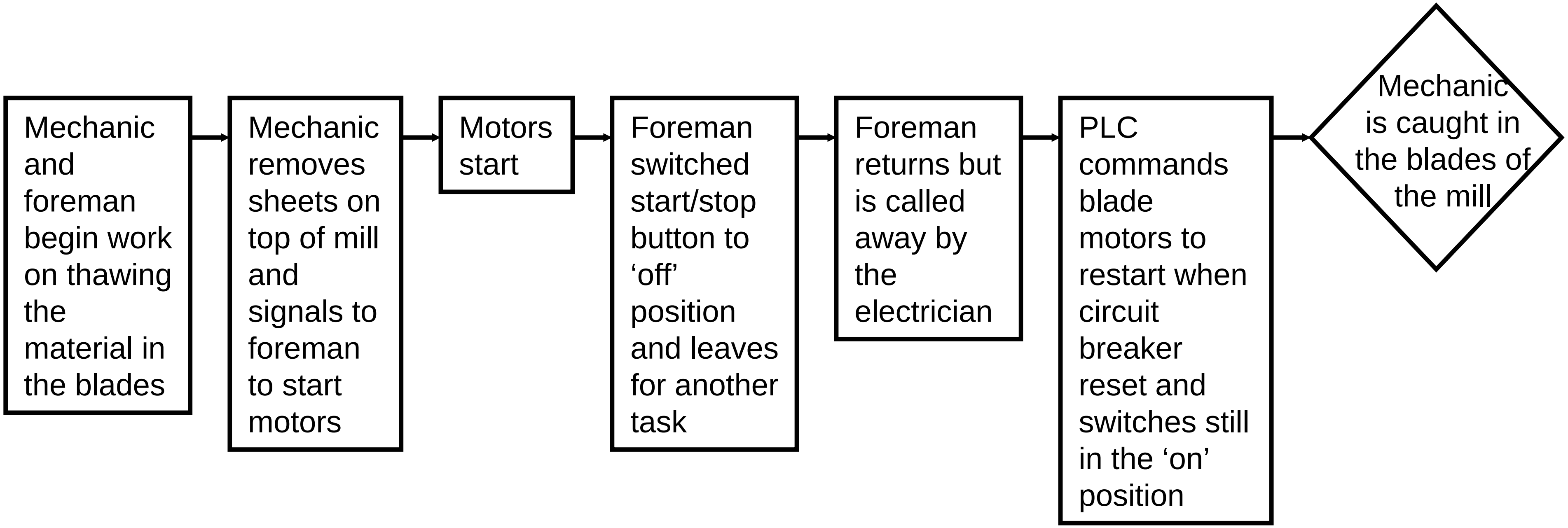
Would the incident have been prevented if	
System concept	– hazard and risk analysis had considered all modes of operation and causes
Design	– maintenance facilities had been designed adequately
Installation & commission-ing	– the maintenance facilities had been installed according to design
Validation	– maintenance facilities had been fully checked
Operation & maintenance	– correct maintenance procedure had been used – maintenance procedure was improved – permit procedures were improved
Modification	– maintenance facilities or procedures had been reviewed during impact analysis

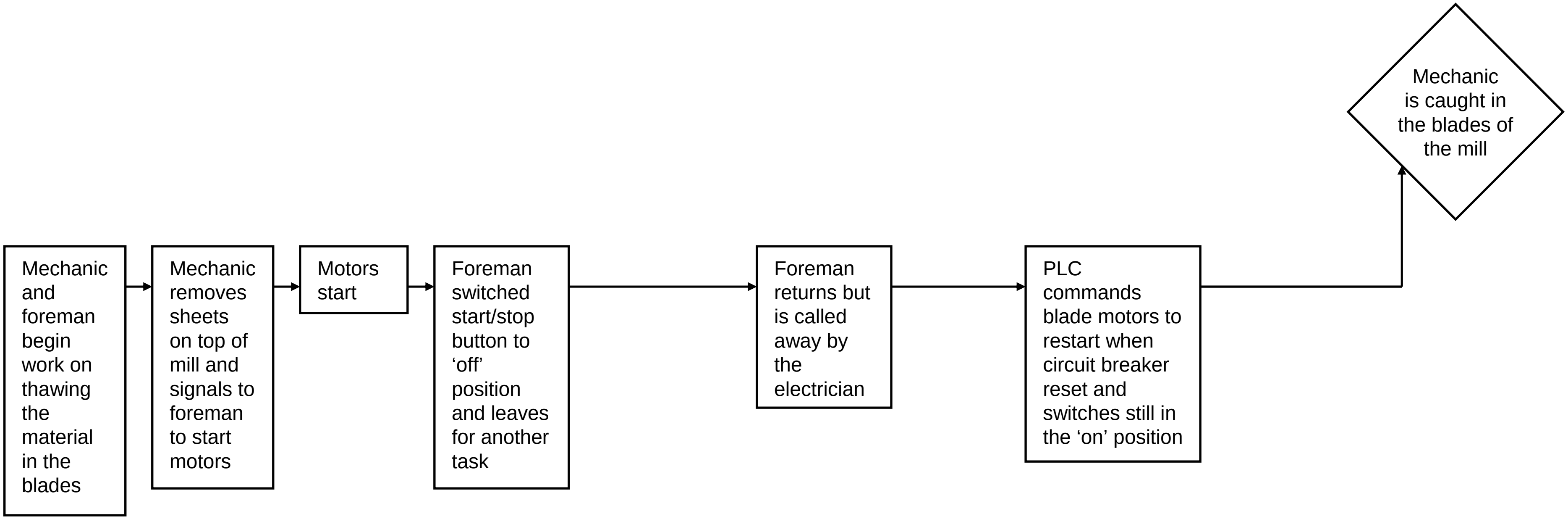
Causal Event	IEC 61508 Classification	Route through flow chart	Rationale
PLC allows automatic restart of equipment following power trip	**Hazard and risk assessment**	System fails to take required action -> Failure caused by maintenance -> Hazard and risk analysis had not considered all modes of operation.	The reprogramming of the PLC allowed for a situation in which equipment was automatically restarted following a power trip. Reprogramming is likely to have prevented a restart without operator intervention had this potential hazard been recognised. (Note: if there were evidence that this hazard had been considered during the reprogramming then the causal analysis might have focussed more on validation to ensure that the PLC prevented the automated restart hazard.)
Failure to warn mechanic that power circuits not locked out during maintenance on circuit breaker.	**Operation and maintenance**	System fails to take required action -> Failure caused by maintenance -> Accident would have been avoided if maintenance procedure were improved.	On-site investigators argued that the foreman was aware of the relationship between the circuit breakers and the mill. The incident might have been avoided if they had followed a documented maintenance procedure or permission to work scheme that would have locked out all equipment affected by the maintenance on the circuit breakers.

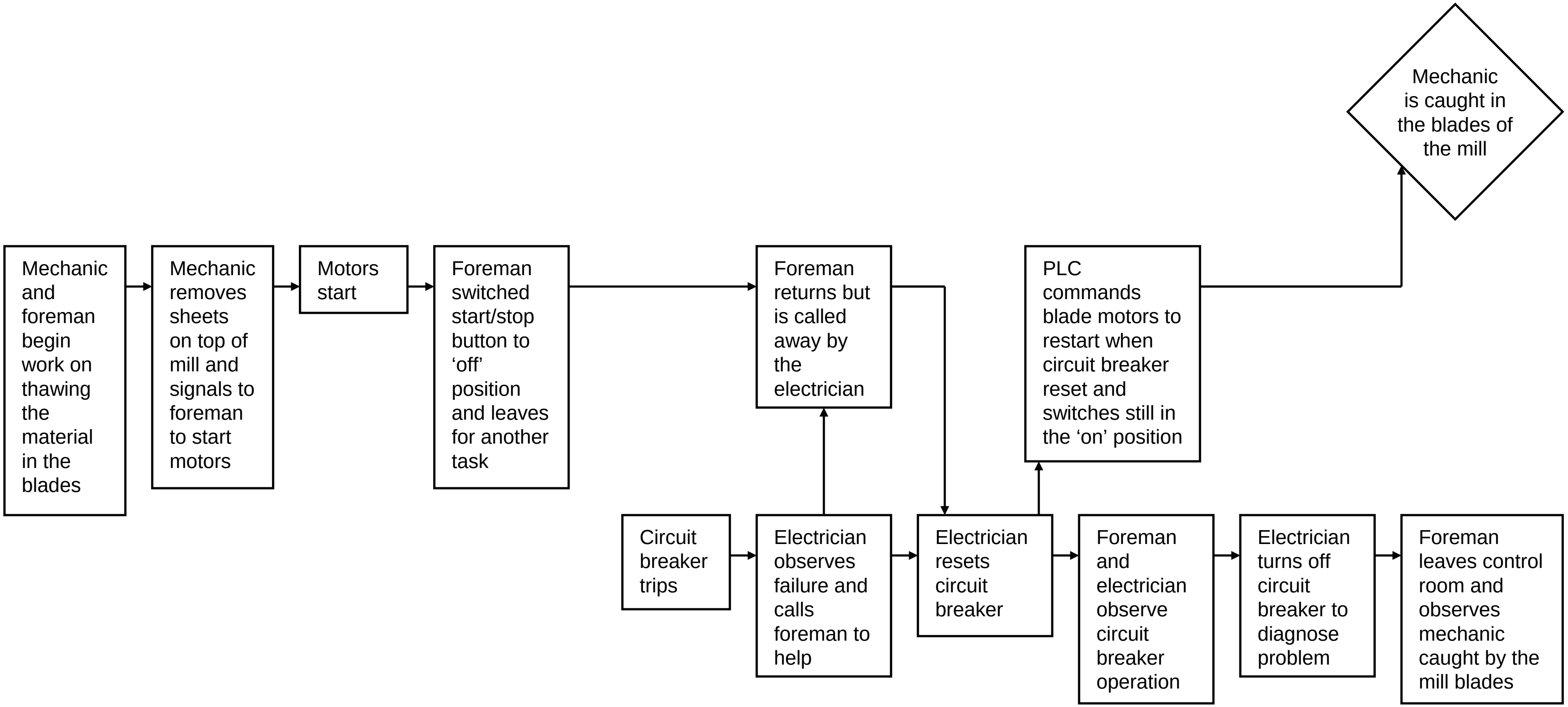
Flow chart issues

- Need several passes for multiple causes
- Protocol can increase consistency
- Order bias
- User refinement necessary
- Complete for every scenario?

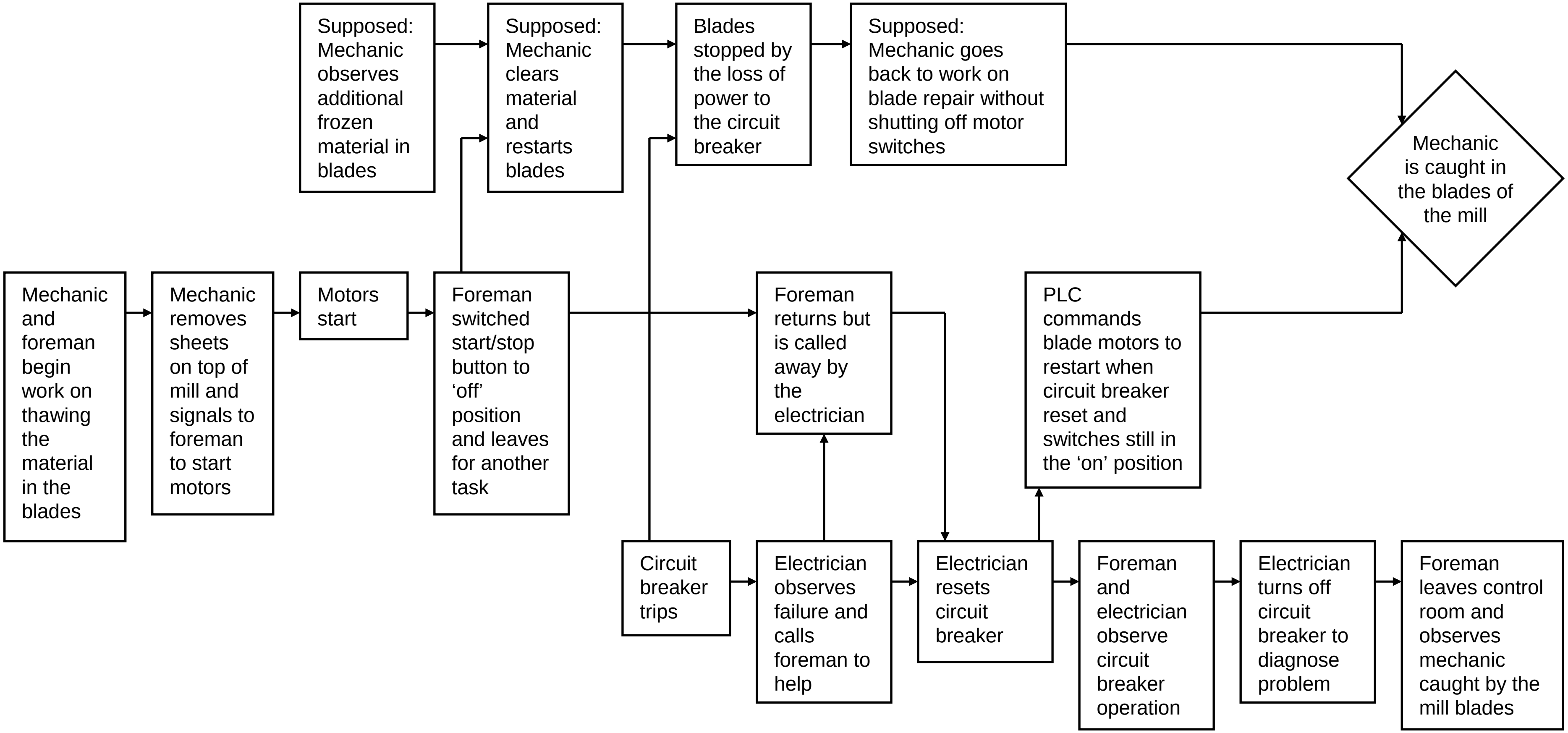

A: Information elicitation
(Standard report forms)
Simpler/lower risk mishaps
More complex/higher risk mishaps
B: Causal analysis
Reconstruct incident
(ECF modelling)
Simplified flowcharting
(Using preset questions leading to IEC 61508 lifecycle and common requirements)
Distinguish causal factors
(Counterfactual reasoning)
Root cause classification
(Using IEC 61508 lifecycle and common requirements)
C: Generation of recommendations

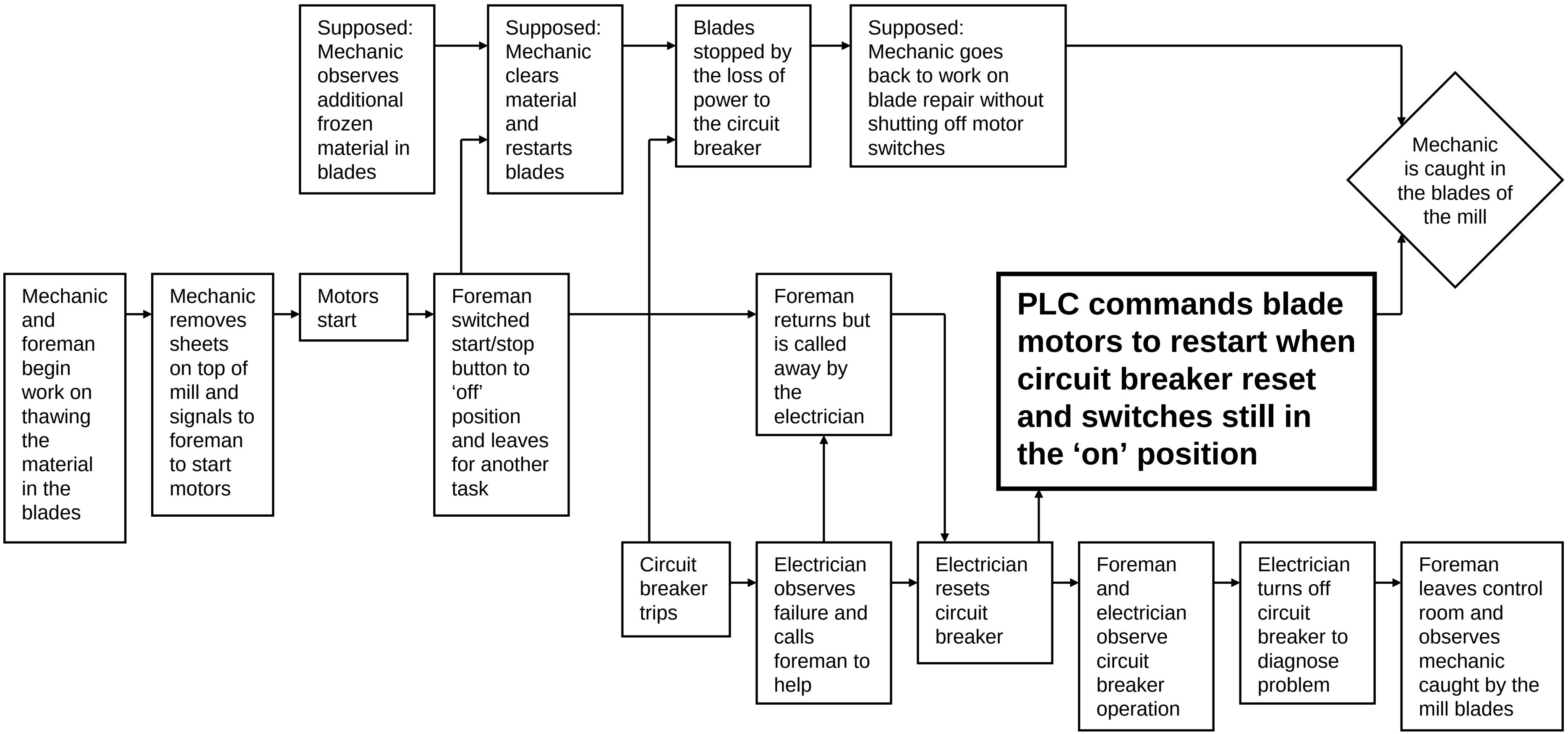

Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to ‘off’ position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position
Mechanic is caught in the blades of the mill

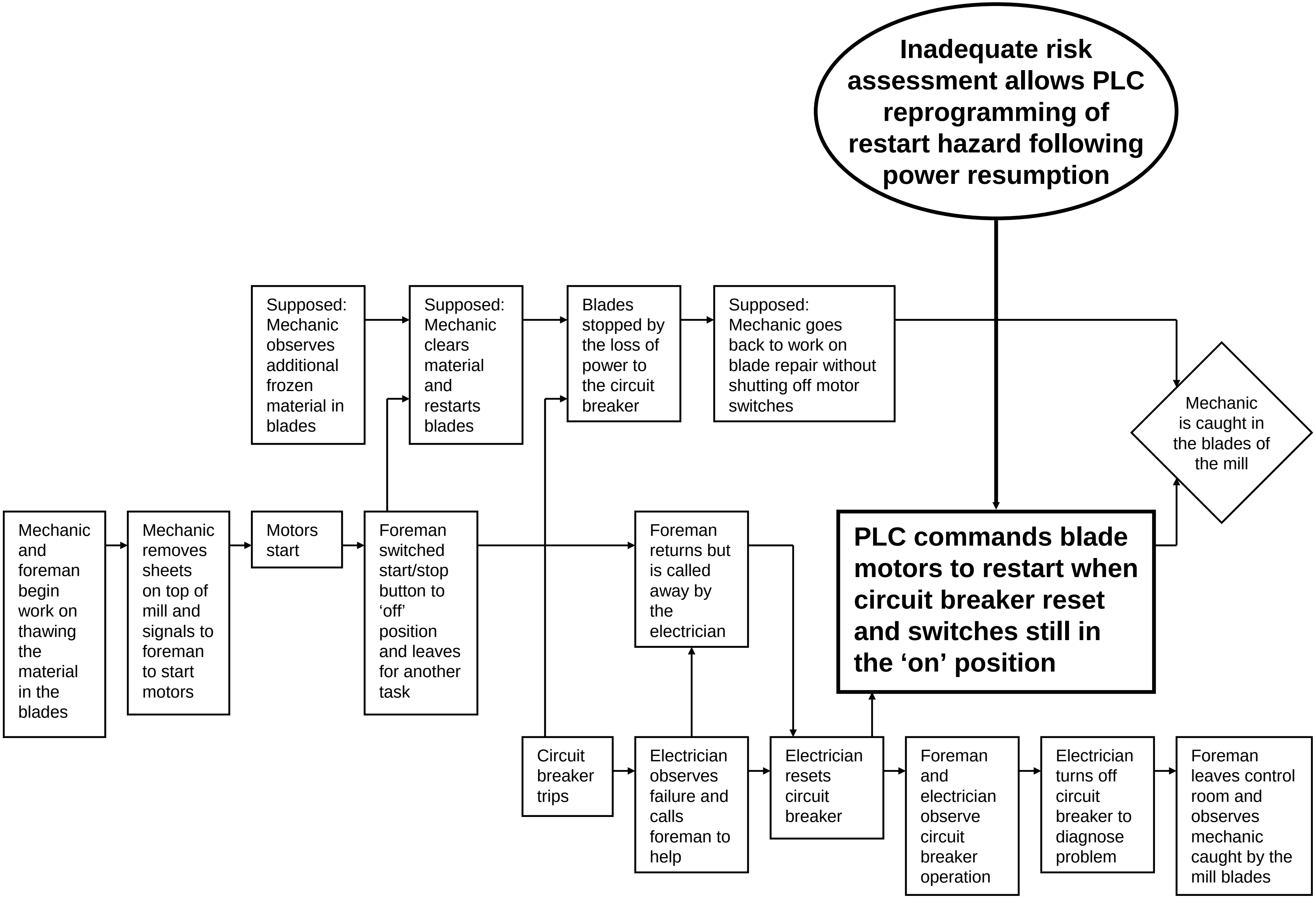

Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to ‘off’ position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position
Mechanic is caught in the blades of the mill

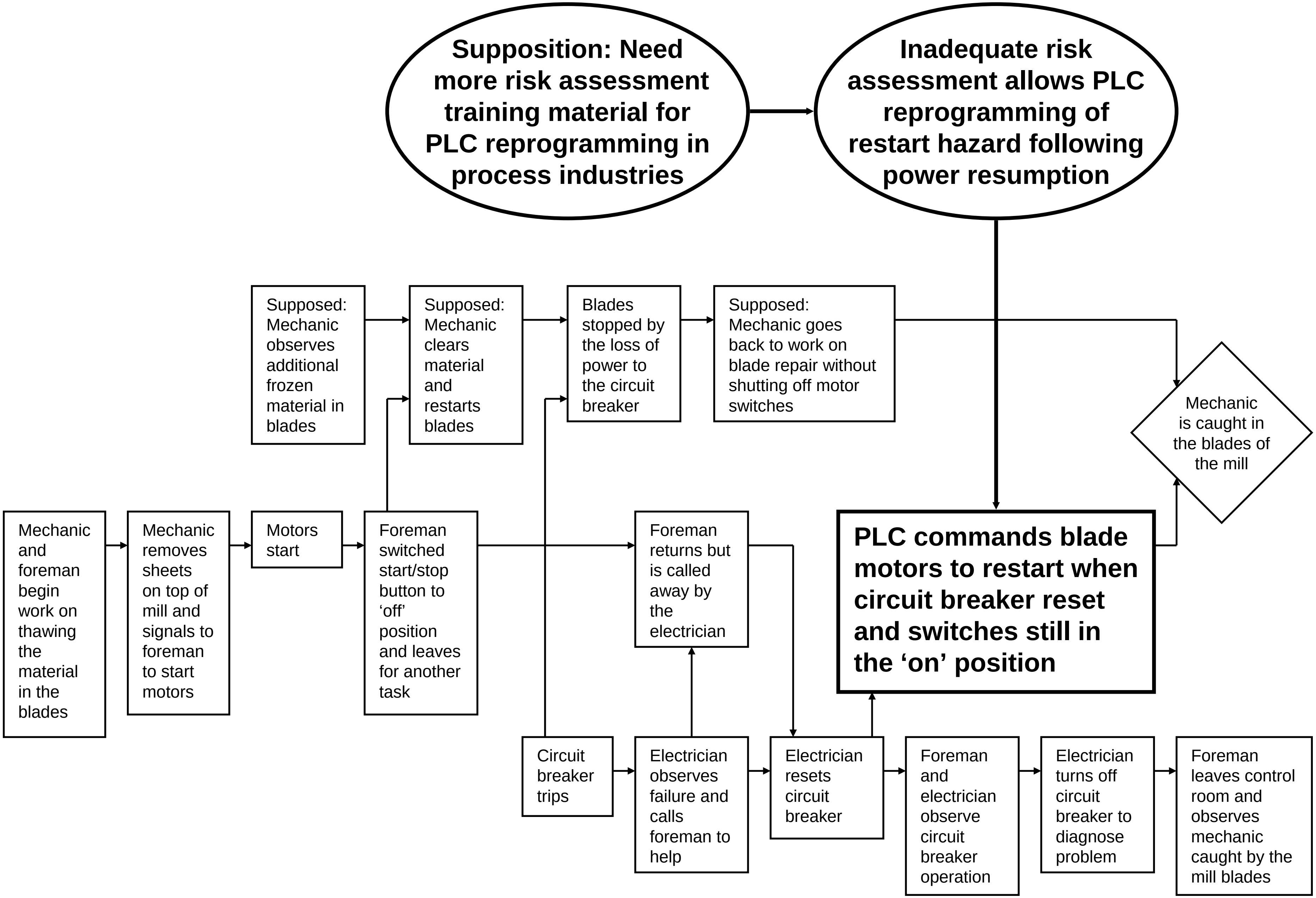


Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to ‘off’ position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position
Mechanic is caught in the blades of the mill
Circuit breaker trips
Electrician observes failure and calls foreman to help
Electrician resets circuit breaker
Foreman and electrician observe circuit breaker operation
Electrician turns off circuit breaker to diagnose problem
Foreman leaves control room and observes mechanic caught by the mill blades

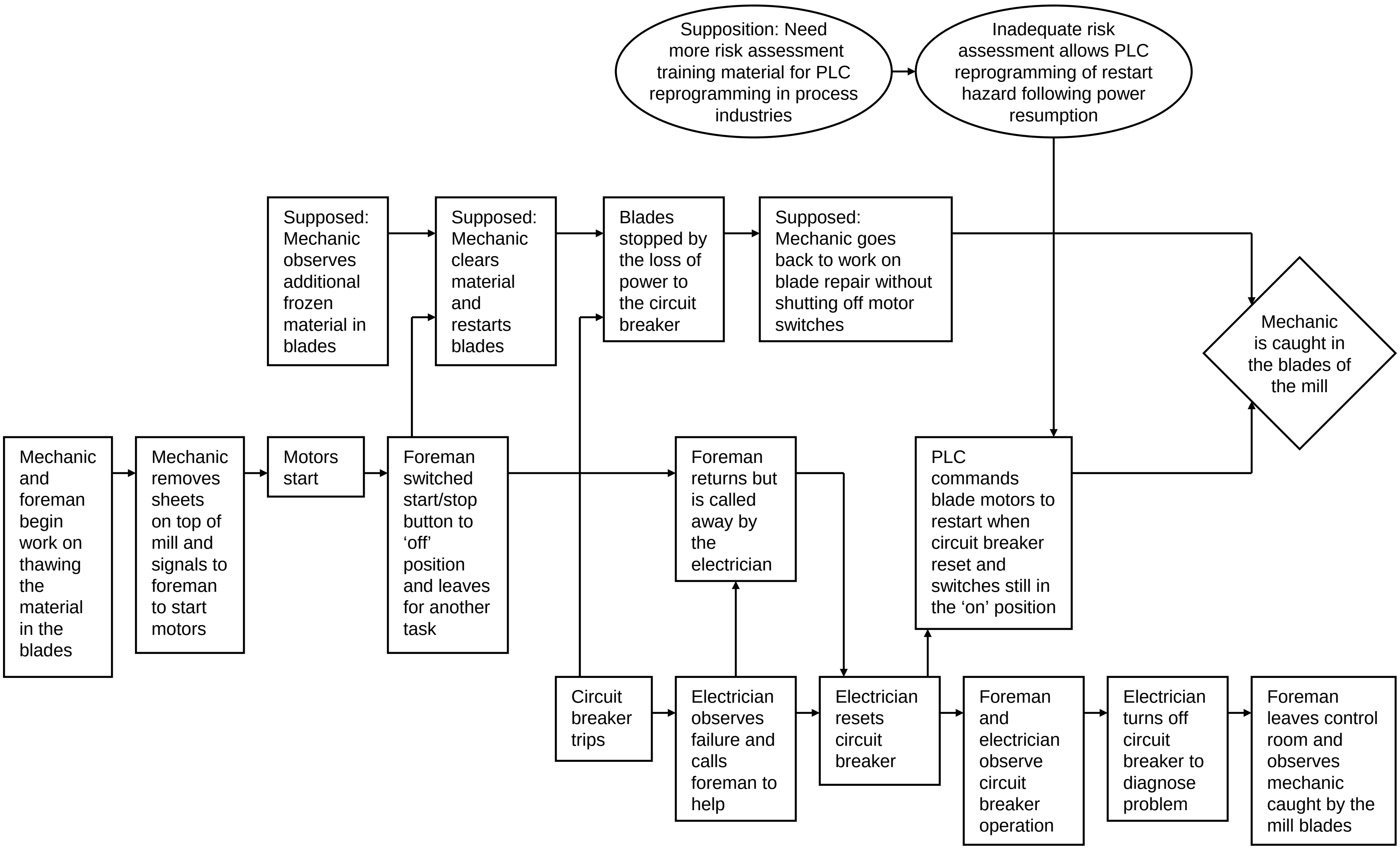

Supposed: Mechanic observes additional frozen material in blades
Supposed: Mechanic clears material and restarts blades
Blades stopped by the loss of power to the circuit breaker
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches
Mechanic is caught in the blades of the mill
Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to ‘off’ position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position
Circuit breaker trips
Electrician observes failure and calls foreman to help
Electrician resets circuit breaker
Foreman and electrician observe circuit breaker operation
Electrician turns off circuit breaker to diagnose problem
Foreman leaves control room and observes mechanic caught by the mill blades


Supposed: Mechanic observes additional frozen material in blades
Supposed: Mechanic clears material and restarts blades
Blades stopped by the loss of power to the circuit breaker
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches
Mechanic is caught in the blades of the mill
Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to 'off' position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position
Circuit breaker trips
Electrician observes failure and calls foreman to help
Electrician resets circuit breaker
Foreman and electrician observe circuit breaker operation
Electrician turns off circuit breaker to diagnose problem
Foreman leaves control room and observes mechanic caught by the mill blades

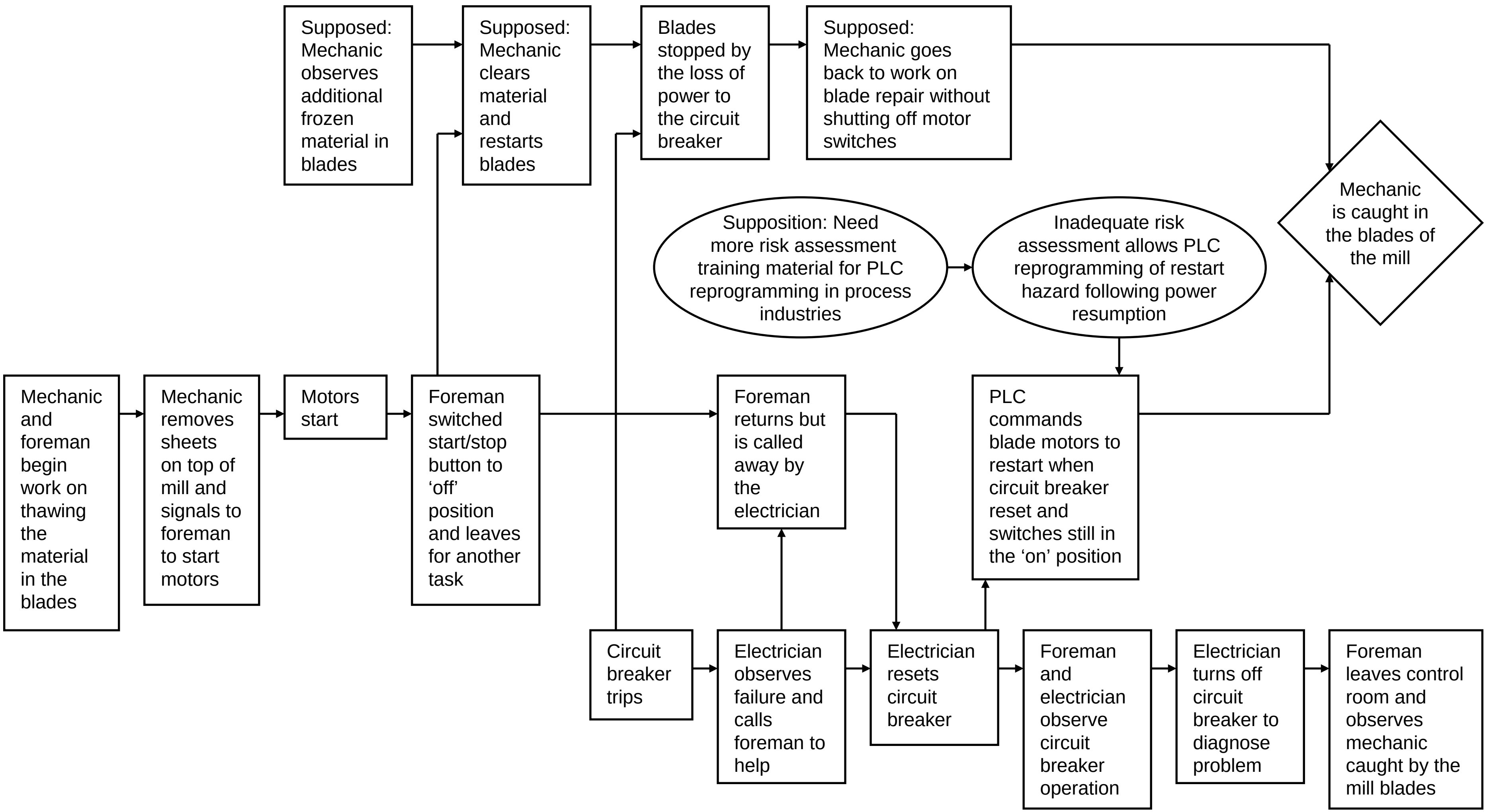

Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption
Supposed: Mechanic observes additional frozen material in blades
Supposed: Mechanic clears material and restarts blades
Blades stopped by the loss of power to the circuit breaker
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches
Mechanic is caught in the blades of the mill
Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to 'off' position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position
Circuit breaker trips
Electrician observes failure and calls foreman to help
Electrician resets circuit breaker
Foreman and electrician observe circuit breaker operation
Electrician turns off circuit breaker to diagnose problem
Foreman leaves control room and observes mechanic caught by the mill blades

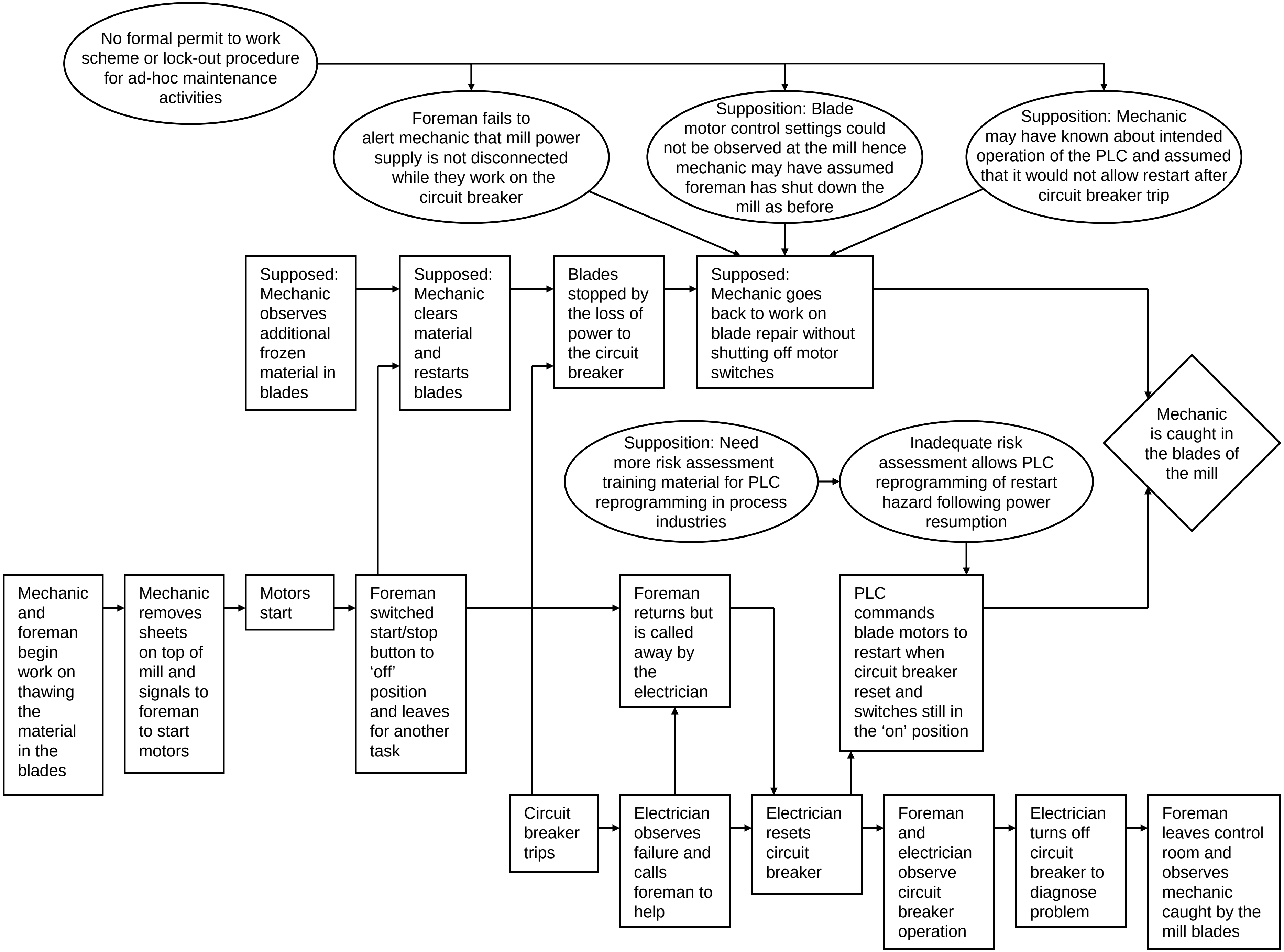


Supposition: Need more risk assessment training material for PLC reprogramming in process industries
Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption
Supposed: Mechanic observes additional frozen material in blades
Supposed: Mechanic clears material and restarts blades
Blades stopped by the loss of power to the circuit breaker
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches
Mechanic is caught in the blades of the mill
Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to 'off' position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position
Circuit breaker trips
Electrician observes failure and calls foreman to help
Electrician resets circuit breaker
Foreman and electrician observe circuit breaker operation
Electrician turns off circuit breaker to diagnose problem
Foreman leaves control room and observes mechanic caught by the mill blades



Supposition: Need more risk assessment training material for PLC reprogramming in process industries
Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption
Supposed: Mechanic observes additional frozen material in blades
Supposed: Mechanic clears material and restarts blades
Blades stopped by the loss of power to the circuit breaker
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches
Mechanic is caught in the blades of the mill
Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to 'off' position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position
Circuit breaker trips
Electrician observes failure and calls foreman to help
Electrician resets circuit breaker
Foreman and electrician observe circuit breaker operation
Electrician turns off circuit breaker to diagnose problem
Foreman leaves control room and observes mechanic caught by the mill blades


Supposed: Mechanic observes additional frozen material in blades
Supposed: Mechanic clears material and restarts blades
Blades stopped by the loss of power to the circuit breaker
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches
Mechanic is caught in the blades of the mill
Supposition: Need more risk assessment training material for PLC reprogramming in process industries
Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption
Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to ‘off’ position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position
Circuit breaker trips
Electrician observes failure and calls foreman to help
Electrician resets circuit breaker
Foreman and electrician observe circuit breaker operation
Electrician turns off circuit breaker to diagnose problem
Foreman leaves control room and observes mechanic caught by the mill blades


No formal permit to work scheme or lock-out procedure for ad-hoc maintenance activities
Foreman fails to alert mechanic that mill power supply is not disconnected while they work on the circuit breaker
Supposition: Blade motor control settings could not be observed at the mill hence mechanic may have assumed foreman has shut down the mill as before
Supposition: Mechanic may have known about intended operation of the PLC and assumed that it would not allow restart after circuit breaker trip
Supposed: Mechanic observes additional frozen material in blades
Supposed: Mechanic clears material and restarts blades
Blades stopped by the loss of power to the circuit breaker
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches
Mechanic is caught in the blades of the mill
Supposition: Need more risk assessment training material for PLC reprogramming in process industries
Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption
Mechanic and foreman begin work on thawing the material in the blades
Mechanic removes sheets on top of mill and signals to foreman to start motors
Motors start
Foreman switched start/stop button to 'off' position and leaves for another task
Foreman returns but is called away by the electrician
PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position
Circuit breaker trips
Electrician observes failure and calls foreman to help
Electrician resets circuit breaker
Foreman and electrician observe circuit breaker operation
Electrician turns off circuit breaker to diagnose problem
Foreman leaves control room and observes mechanic caught by the mill blades

Causal event	Associated conditions	Lifecycle classification	Justification	Common reqs classification	Justification
PLC commands blade motors to restart when circuit breaker reset and switches still in the ‘on’ position	Supposition: Need more risk assessment training material for PLC re-programming in process industries.	**Modification** 6 LTA manufacturers information 7 LTA verification and validation	The company responsible for the PLC update arguably did not appreciate the need to formally consider the implications of the changes on the operation of the mill. Hence the potential restart hazard was not adequately tested for.	**Safety Management** 4 LTA safety management: external suppliers **Documentation** 1 documentation absent/ incomplete	The reprogramming of the PLC does not seem to have been supported by a detailed consequence assessment. Again, additional documentation may be required from regulatory organisations to guide E/E/PES suppliers about the best means of performing such a hazard assessment. The operators of the mill might also use such guidance to validate any maintenance activities by suppliers.
	Inadequate risk assessment allows PLC re-programming of restart hazard following power resumption	**Modification** 1 LTA modification plan (including sufficient lifecycle activities) 3 LTA impact analysis			

Recommendation	**Priority**	**Responsible authority**	**Deadline for response**	**Date accepted/ rejected**
Develop training material for E/E/PES suppliers and for operators on necessary hazard identification during PLC programming	Medium	Industry regulator	1 Sep 1997	
Conduct formal hazard identification process to determine if there are any additional threats posed by reprogramming of PLC on this plant and supplier's other installations	High	PLC supplier Safety manager	1 Jun 1997	Accepted 15 Feb 1997

PARCEL summary

- Two approaches depending on consequence and complexity
- IEC 61508 classification
- Supports end users, designers, suppliers/integrators, maintainers
- Several industry sectors

Next steps

- **Publish HSE research reports**
- **Internal HSE consultation**
- **Published HSE guidance document**

Further information

- www.hse.gov.uk/research/rrhtm/index.htm
- www.dcs.gla.ac.uk/~johnson/hse

- mark.bowell@hse.gsi.gov.uk
- johnson@dcs.gla.ac.uk