BAKERRISK

Boats, Bridges and Back-ups

Roger Stokes BSc CEng FIChemE MIE

EPSC European Conference on Plant & Process Safety
December 2024

Contents

- Boats and Bridges
- Why do we need a back-up?
- Some causes of power / energy supply failure
- Consequences of power / energy failure
- Understanding the hazards and risks
- Types of back-up systems
- Human Factors
- Design and testing of back-ups
- Process Industry examples where back-ups didn't work
- Conclusions

BOATS AND BRIDGES

MV Dali/ Francis Scott Key Bridge, Baltimore
26 Mar 2024 at 0129 hrs

- 6 Fatalities / 1 major injury (roadworkers)
- 1 injury on board

Sources of data

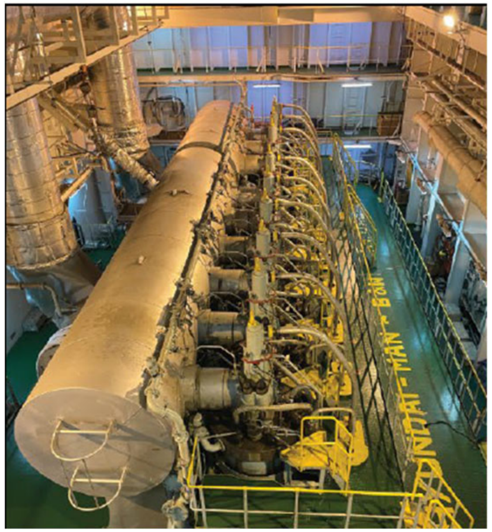
- NTSP Preliminary Report - 14 May 2024
- Investigation update - 24 June 2024
- Dali Shipboard Machinery Examination and Record of Electrical Testing on April 1–29, 2024 – 11 Sep 2024
- US Claim against MV Dali owners - 18 Sep 2024
- WGOW Shipping (Sal Mercogliano, YouTube)

Changes expected as investigation continues

ntsb.gov/investigations/Documents/DCA24MM031_PreliminaryReport%203.pdf

MV Dali

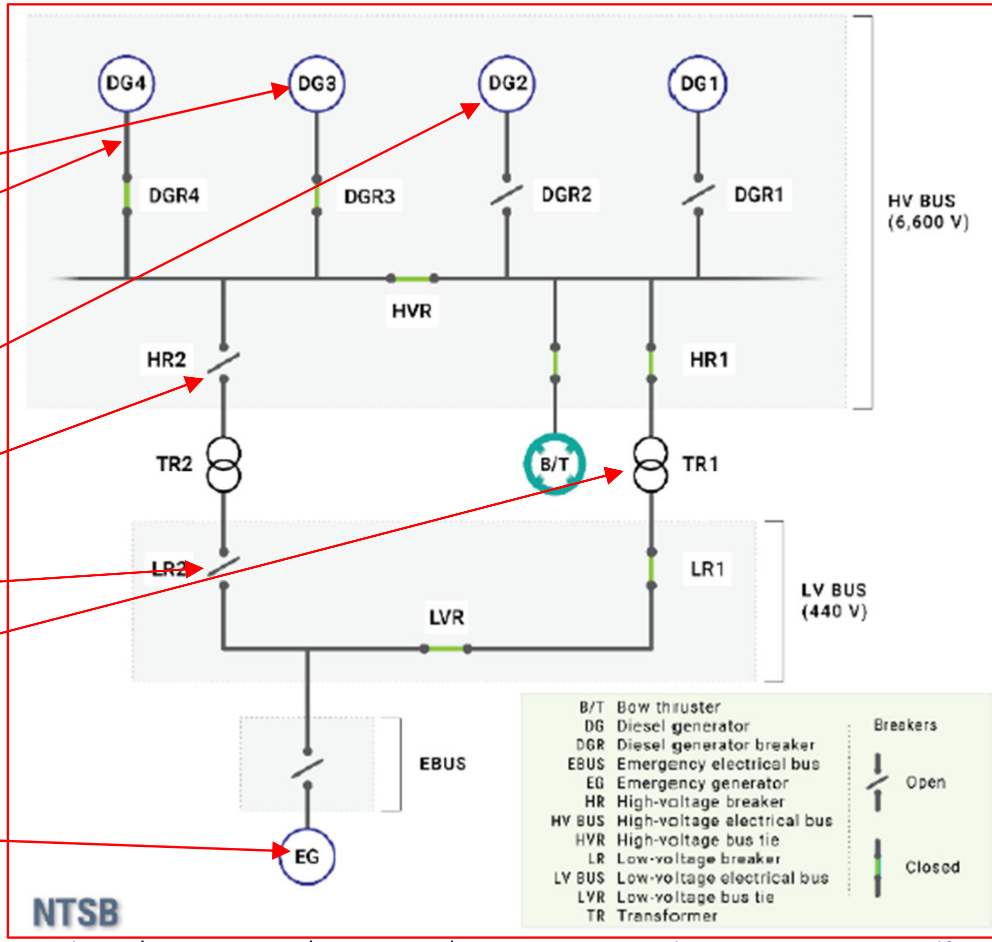
- Registered: Singapore
- Length: 289 metres ~ 100,000 tonnes (gross)
- Engine: single 41,480 kW low-speed two-stroke diesel engine
- No gearbox/ clutch
- Compressed air to start/ reverse
- Propeller 27 rpm – 80 rpm
- Single rudder
- Fuel: Light oil (Low sulphur) and heavy fuel (outside emissions control areas)



NTSB Preliminary Report

Electrical Systems

- HV power (6.6kV) to HV bus by up to four diesel generators
- Two operating (DG3 and DG4) at the time of the incident.
- DG2 “on automatic standby”
- Transformer TR2 isolated
- Transformer TR1 on line
- Emergency generator on LV bus



ntsb.gov/investigations/Documents/DCA24MM031_PreliminaryReport%203.pdf

Critical Systems

Some key electrical systems

HV system

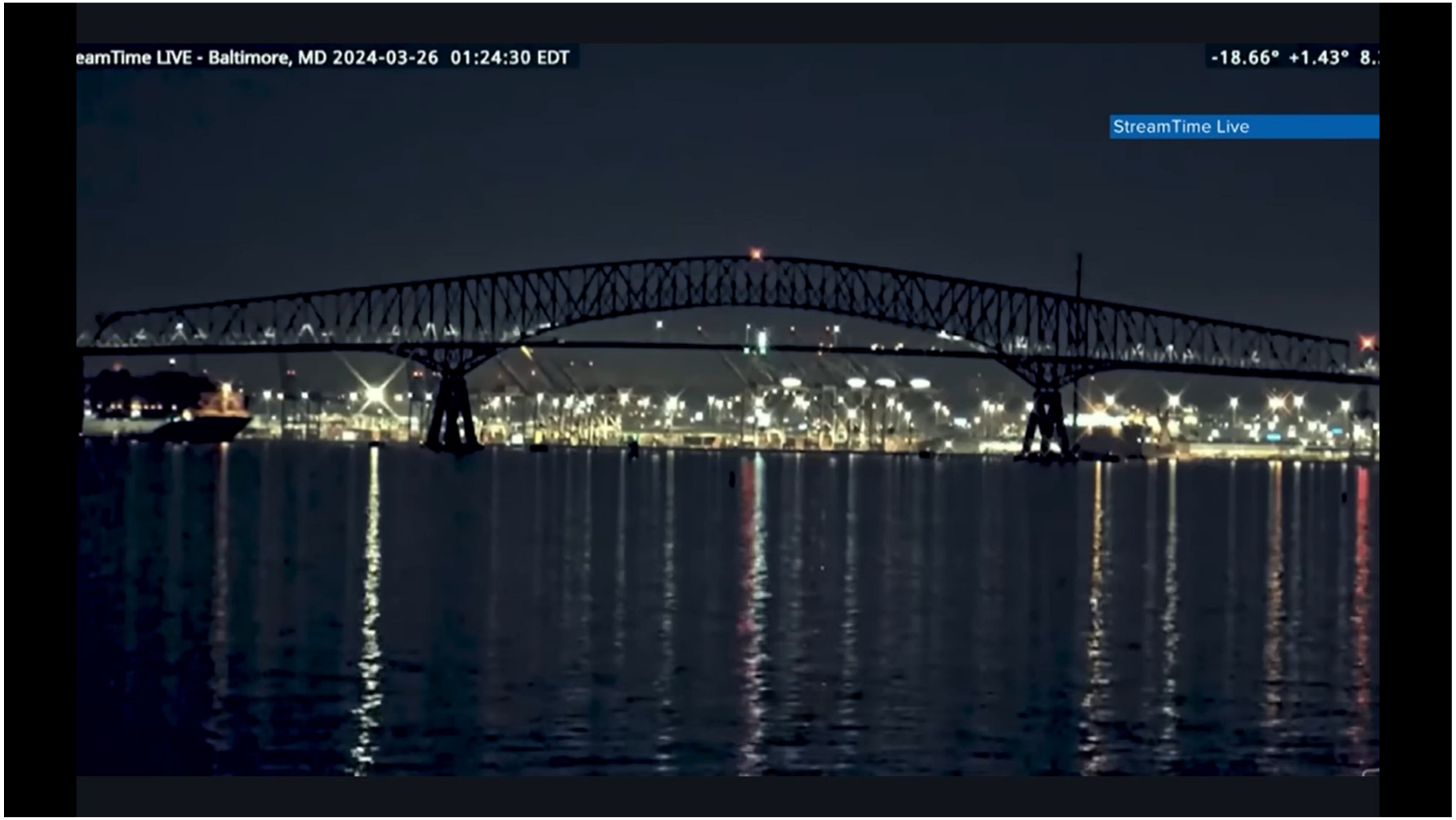
- Engine lube oil pumps
- Bow thruster (B/T)
- Refrigerated containers

LV system

- Lighting
- Steering Gear pumps (x3)
- Engine cooling water pumps

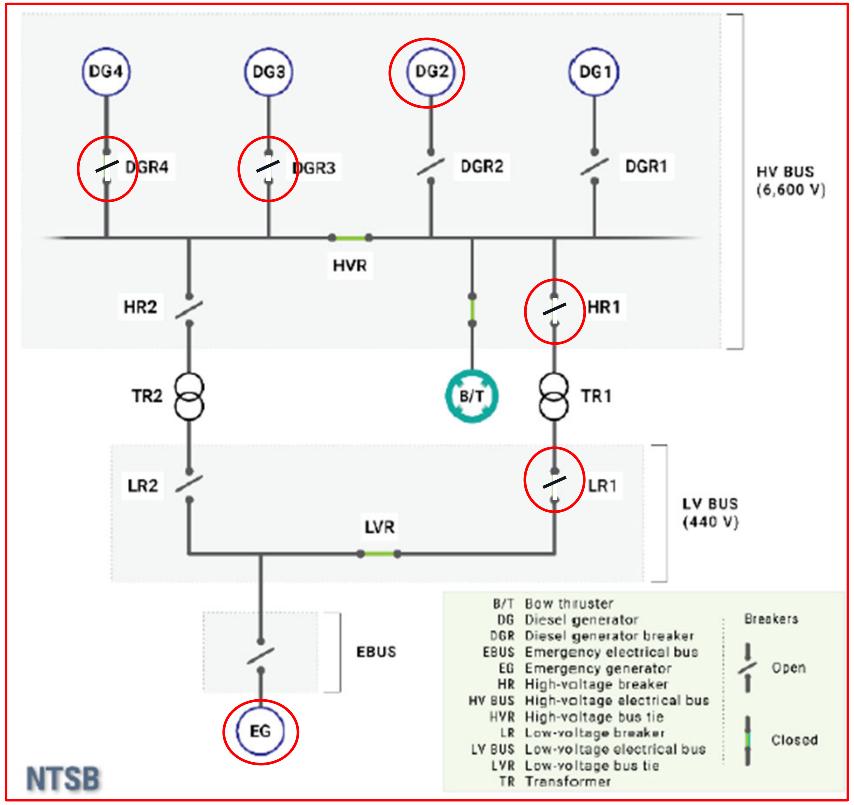
- Fuel Pumps – engine, generators

MV Dali, Baltimore Bridge collapse, 26 Mar 2024



Events (Preliminary Report, subject to change)

- 01:24:58 hrs SOG ~ 9 knots[1]
  - HR1 and LR1 tripped – LV systems lost power
  - Most bridge systems lost power
  - Engine shuts down (fuel/ lube/ cooling)
  - Steering pumps (x3) lost power
- 01:25:57 power restored ("Manual reset HR1, LR1"[2])
- EG started – timing tbc ("over 1 minute")
- DG2 started – timing tbc
- 01:26:13 pilot orders 20° port rudder
- 01:27:01 pilot ordered anchor drop
- 01:27:03 second power failure HV and LV bus
  - DGR3 and DGR4 opened due to fuel starvation to generator
- 01:27:23 pilot ordered 35° port rudder
- 01:27:36 power restored
- 01:29:10 Dali strikes pier 15 of Francis Scott Bridge



[1] Video times showing power failure adjusted to match NTSB report
[2] US Claim against MV Dali owners

Consequences of power loss – cascade failure

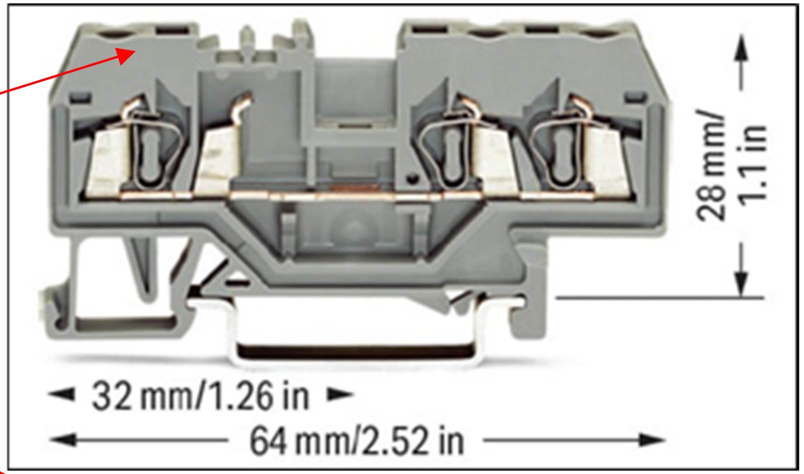
- Engine stop - not self-sustaining for fuel, lube or cooling
  - Common cause failure
  - Not quick to restart / put astern
- Loss of hydraulic oil to rudder – slow movement
- Loss of effectiveness of rudder - less flow over it
- Loss of HV to bow thruster - not very effective at speed anyway
- Anchor drop attempt – required local attendance as bridge approaching, so dropped but not locked off

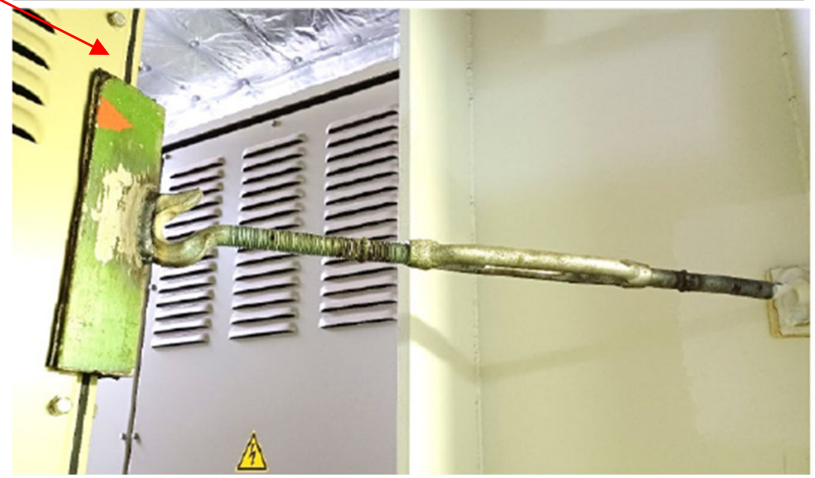
Pier Fender

- 100 ft x 84 ft crushable concrete box and timber fender system
- Clearly not sufficiently large/ robust

Cause – Power outages

- First undervoltage release blackout: Loose connections on HR1's termination block
  - Possibly vibration
- Auto-switchover to No.2 transformer not operating "disabled"
- Second blackout : No 3 and 4 generators for US ECA areas – burn marine gas oil
  - Set up "temporary" fuel pump for 3 & 4, to use low sulphur fuel - that could not recover automatically after first black-out. (MOC)
  - Fueled only by a small emergency air-driven pump, the generators were starved of fuel and slowed down until switchgear tripped out.



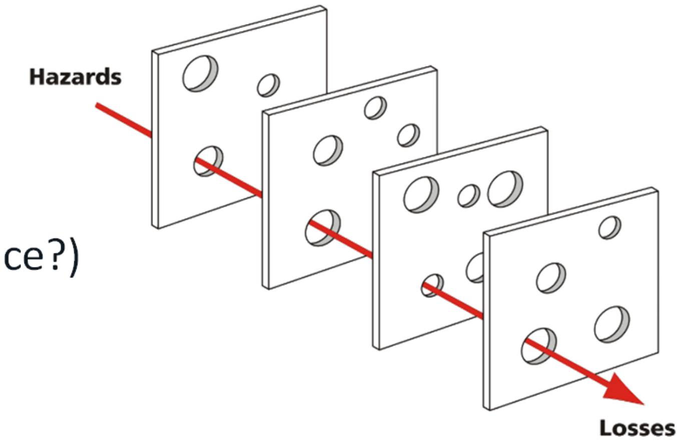


Vibration reduction measures !

Drone footage (NTSB)

MV Dali – The Barriers that failed

- Tugboat
  - Not available at critical point of departure (procedure?)
- Power loss due to electrical / vibration problems
  - No available back-up to allow main engine to run (design / maintenance?)
- Transformer not set to auto-changeover
  - Or set up on shared 50:50 load (procedure?)
- Fuel pump for generators
  - Not lined up for restart from power loss (MOC ?)
- Emergency Generator (LV) not started up quickly enough
  - Greater than 45 seconds (design/ testing / procedure ?)
- Pier Fendering system
  - Not effective for speed/ tonnage (creeping change?)
- Plus plus …

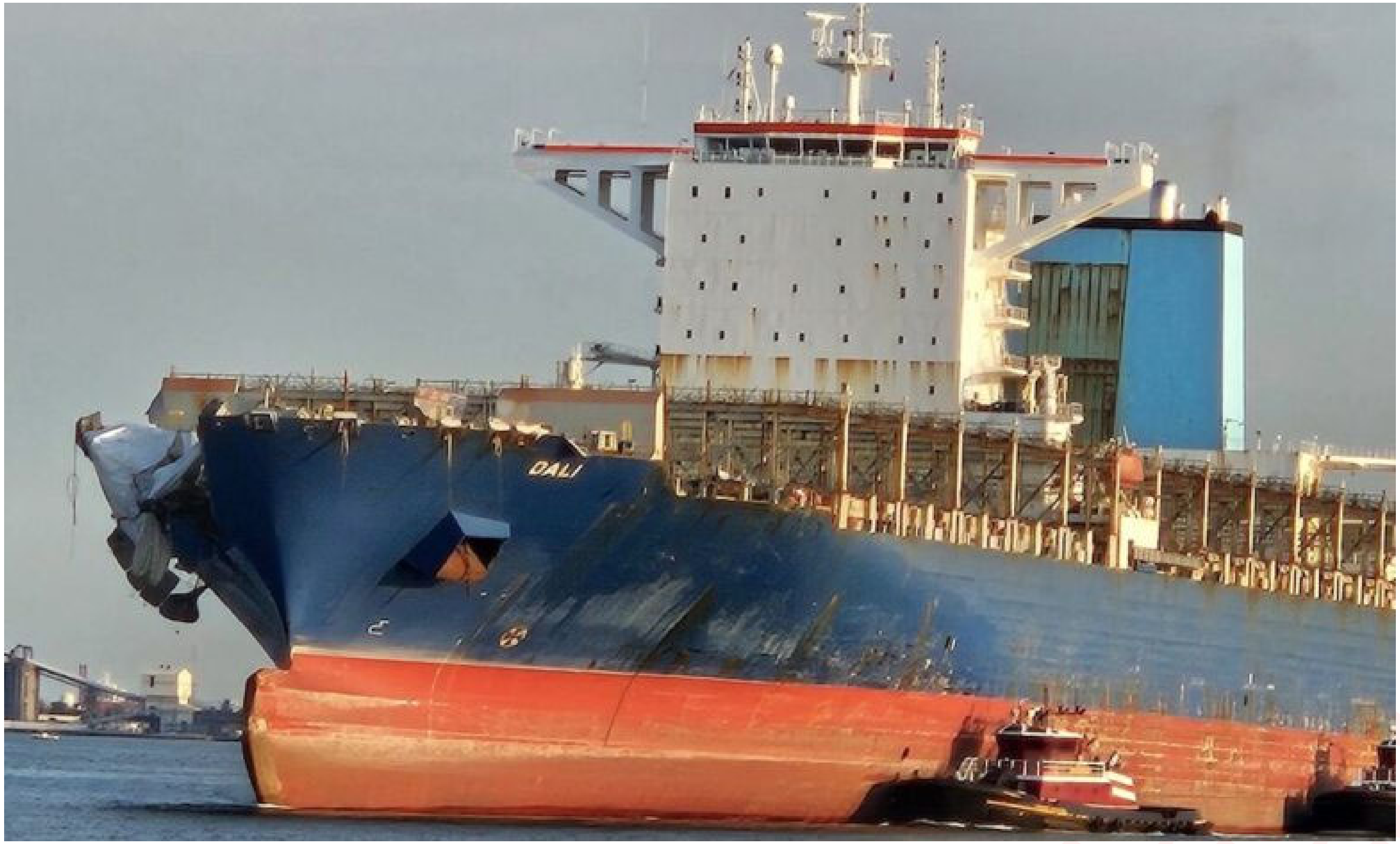


Current Status

- MV Dali arrived Norfolk, Virginia June 25th 2024
- Containers were offloaded by August 20th 2024
- MV Dali sets sail (empty) for repairs in China Sep 20th 2024
  - Avoiding canals (Panama/ Suez) – Costs?
  - Via S Africa / Malacca Straits to Shanghai
- Nov 4 – South China Sea
- Nov 13 – arrived at Fujian Huadong Shipyard, China

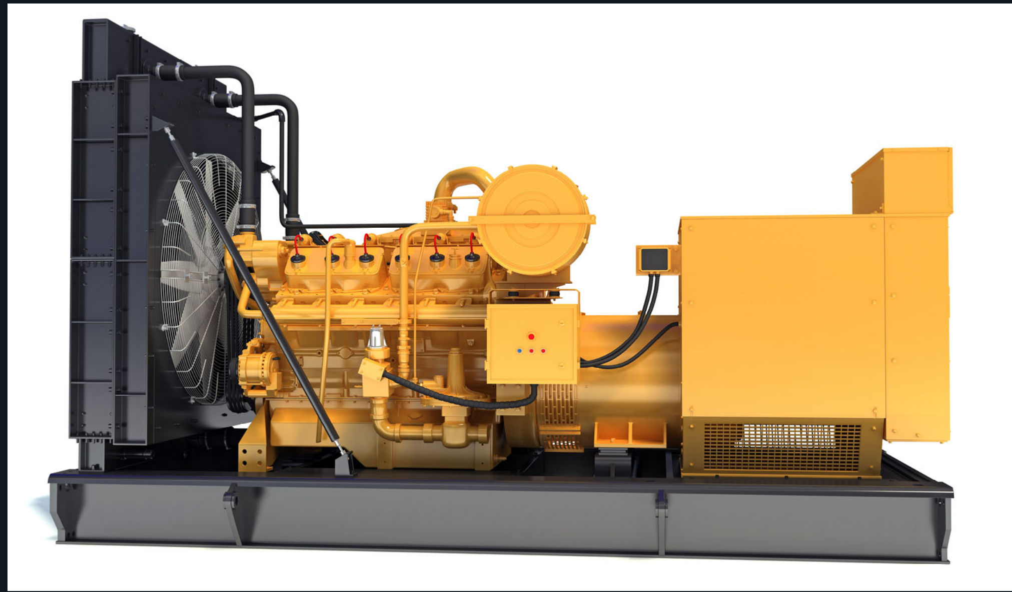
MV Dali – En route to China

MV Dali arrival China – Nov 13th, 2024



BAKERRISK

BACKUPS



Why we need back-ups

- Industrial processes at risk due to a sudden loss of energy supply (mainly, but not wholly electrical power)
  - Physical damage/ injury and/or environmental incidents
- Require a continuous supply of energy for the safe operation of “Essential Services” including:
  - Process control computer
  - Plant, machinery and instrumentation
  - Services including
    - Steam
    - Air
    - Water (process water and cooling water)
    - Nitrogen
    - Lubrication
    - Hydraulics
  - Emergency systems
    - Vent scrubbers, fire systems

Essential Services

- Unlikely to be able to sustain operations
- Services that are crucial for safe shutdown
- Identify through HAZOP / LOPA (but not always)
- Identify common cause failures – e.g. “what-if” or FMEA study
- Consider potential for cascade failure

Some causes of power supply failure

- Fires in substations and switch-houses
- Switchgear faults/ human error when working on switchgear
- Underground cable faults
- Excavations and other works damaging underground cables / gas piping
- Cranes/ tipper trucks contacting overhead cables
- Lightning strikes
- Failures in external grid network
- Storm/ flood / tsunami

Some Consequences of Power Failure

Equipment damage and loss of containment/ injury due to:

- Loss of process control
  - Uncontrolled chemical reaction / nuclear reaction
  - Loss of cooling
  - Blockage due to stoppage of solids/ slurry/ plastics
- Rapid cooling of fired equipment
  - Glass Furnaces
  - Fired heaters/ reformers
- Potential for cascade failure

  Power Loss – Control systems – Air systems – Nitrogen systems – Cooling Water – Communication Systems
- Damage during restart
  - Due to unplanned shutdown

Understanding hazards and risks

- Usually at the design stage via HAZID/ HAZOP / LOPA
- Identification of critical services, including:

- Safety Critical instrumentation and electrical drives
- Instrument air compressors
- Emergency scrubbers (vent fans and circulation pumps)
- Steam boilers (feed water pumps and exhaust fans)
- Cooling water pumps

- Refrigeration systems
- DCS control systems
- Emergency lighting
- Firewater pumps
- Seal water pumps
- Reactor agitators
- Nitrogen
- Hydraulic systems

Types of back-up systems

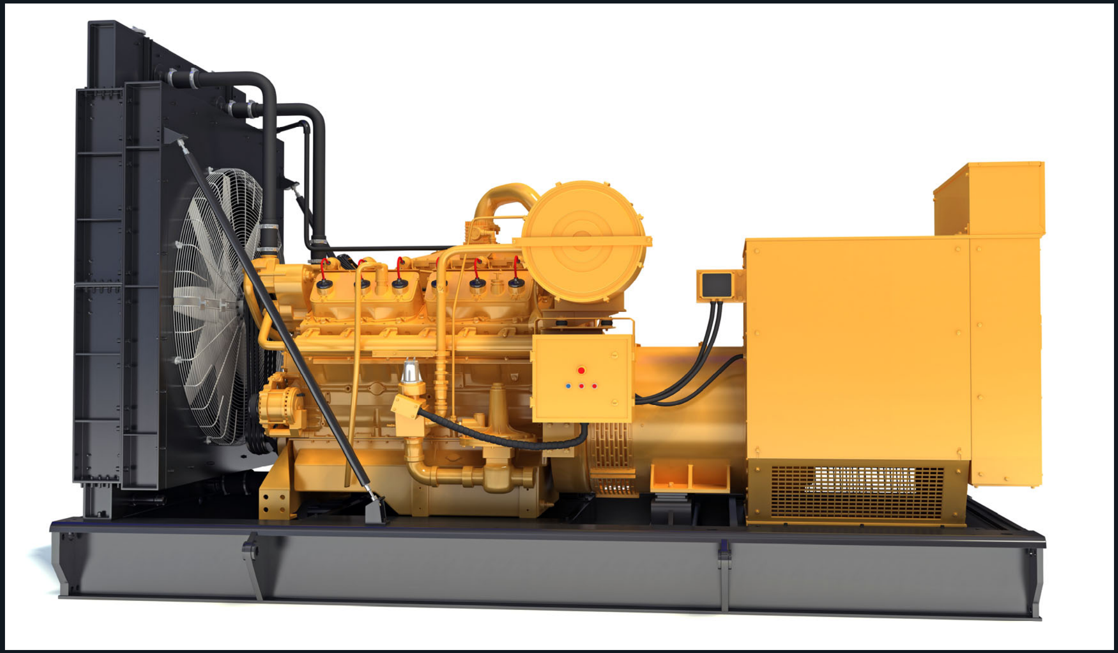
Examples:

- Secondary independent power supply
- UPS
  - Battery, uninterrupted but limited capacity
- Diesel powered standby equipment (pumps, compressors, generators)
  - Longer operating period than UPS
  - Start-up time, synchronisation time
  - Compressed air start for higher reliability, e.g. nuclear
- Compressed air storage
- Nitrogen bottles
- Hydraulic packs
- And many more …

Human Factors

- Procedures may be limited to failure of individual services
  - Not a cascade failure of services
- Operators have little or no experience of power failure
  - Until it happens
- Operator overload
  - Decision making
  - Resources – e.g. requirement to open/ close valves manually
  - Assumptions about status of equipment (blank DCS screen)

- Design and testing of Back-ups



Design Considerations

- Standards are available
  - NFPA 110 , 111, IEEE 446, IAEA SSR-21
- Holistic approach when considering power/ energy failure
  - Include electrical and process specialists, process safety engineers, technicians, and emergency response planners
- Design to allow complete end-end testing
  - Without risking loss of power to process

A testing problem

- If the test fails, there is a risk of tripping the facility
  - To be safe, leave it until the next shutdown
- Perception that the back-up is reliable enough
  - Fingers crossed – The “Titanic approach”
- Testing up to a point…
  - Not synchronized
  - Not run for more than xx minutes
  - Not load tested
  - Faults recorded and fixed, but causes not resolved

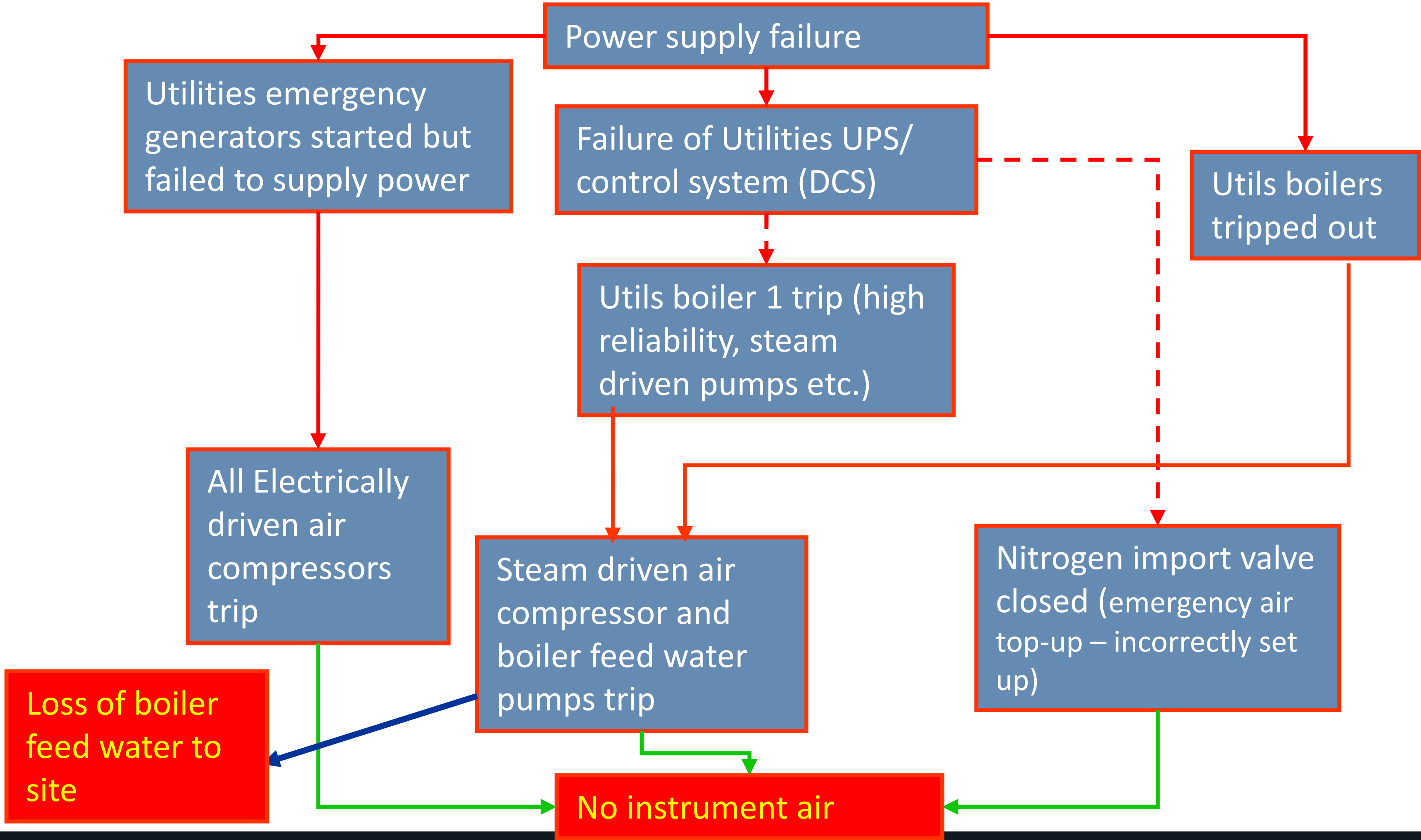
AN EXAMPLE FROM THE PROCESS INDUSTRY

Loss of Power – Major Petrochemical Complex

- Dual, independent power supplies on separate poles
- 14 diesel back-up generators at various locations
  - To allow safe shutdown of facilities
- 56 UPS (battery backups)
- Steam supply includes “high integrity boiler”
  - Steam turbine-driven feed pumps/ combustion air fans
- Steam turbine-driven air compressors
  - With back-up from nitrogen system for instrument air

- Both Power supplies failed
- Only 3 effectively supplied power
- 5 UPSs failed to work
- Boilers tripped
- Air compressors tripped

Key events – cascade failure of power/air/ water



Consequences

- Failure of furnace tubing
  - Thermal stress and overtemperature
- Backflow of hydrocarbons due to downstream pressure control valve failing closed
  - Backpressure on furnaces
  - Operators could not close manual valves in time
- Uncontained fires in multiple furnaces
- £MM repair costs/ environmental damage

Key Learning

- External power supplies were <u>not</u> independent - subject to common cause failure.
- Inadequate design, maintenance and testing of emergency generators
  - Not synchronized – routine test was to mechanically start the generators and verify voltage is generated.
  - No simulated load testing of generators was conducted, and the tests did not include electrical synchronisation.
- Failure mode of the control valve on backup to instrument air supply was incorrect.
- Failure to consider total loss of services in the design/emergency planning/human factors, including inability to manually close outlet valves from each furnace in time.

Conclusions

Conclusions

- Multiple, reliable energy sources are required for safe operations
- Failure of one or more of these energy sources can lead to major incidents.
- Consequences are mitigated by the provision of back-up supplies for critical services.
- Design and testing of backups must be carefully considered to ensure they are sufficiently reliable.
- Emergency procedures should also consider the potential failure of the back-up supplies and include procedures, training, and exercises to minimise the hazardous consequences of such events.
- It is healthy to maintain a "sense of chronic unease" when it comes to emergency back-up systems.

CONTACT US

ROGER STOKES

BakerRisk Europe Limited, Regus House,
Heronsway, Chester, CH4 9QR

+44 (0)1244 792040

rstokes@bakerrisk.com

WE HAVE ANSWERS

SERVICES

Better Risk Management Starts Here

- Accident Investigation
- Functional and Electrical Safety
- Fire Protection and Insurance Risk
- Consequence and Risk Modeling
- Qualitative Hazard Identification and Risk Assessment
- Protective Structures
- Testing
- Low Carbon Energy

BAKERRISK LEARNING CENTER

BAKERRISK LEARNING CENTER

LOCATIONS

San Antonio	Canada
Houston	Egypt
Chicago	United Arab Emirates
Los Angeles	United Kingdom

BAKERRISK