WARNER ENERGY STORAGE SOLUTIONS

Bowtie and Hazard Mitigation (HMA) as a Visual Means for Risk Analysis and Incident Planning

DOE ESS Safety Forum

March 7th, 2019

Albuquerque, New Mexico

Warner ESS and risk analysis

- Warner ESS and DNV GL have worked with industry risk experts over the last two years to apply industry accepted best practices from Oil & Gas, Nuclear, Maritime, and the Utility industries to energy storage
  - Though much of the historic data has been lacking from US operational experience, South Korea may be able to provide this information going forward
  - In the US, we have leveraged power electronic failure rates as well as six sigma principles and human factors rates to make estimates about failure rates

- Uncertainty surrounding risk and failure likelihood has resulted in the delay of installation of systems in crowded urban environments like New York City

What is Risk?

Understanding risk

- Understanding the hazard involves understanding both:
  - Consequence
  - Frequency
- Risk is assessed based on all potential hazards
- Once risk is understood, mitigation measures can be put in place to reduce risk
- These documents are not always helpful to first responders

Risk=Likelihood*Consequence

We know the consequences of energy storage fires are severe, but how common are they?

Prior to the outbreak of fire's in South Korea, very few large scale ESS failures had occurred in the US and the causes of all were quickly understood

Causes have included poor BMS algorithms, inadequate HVAC systems, sensor failure and integration, and human factors

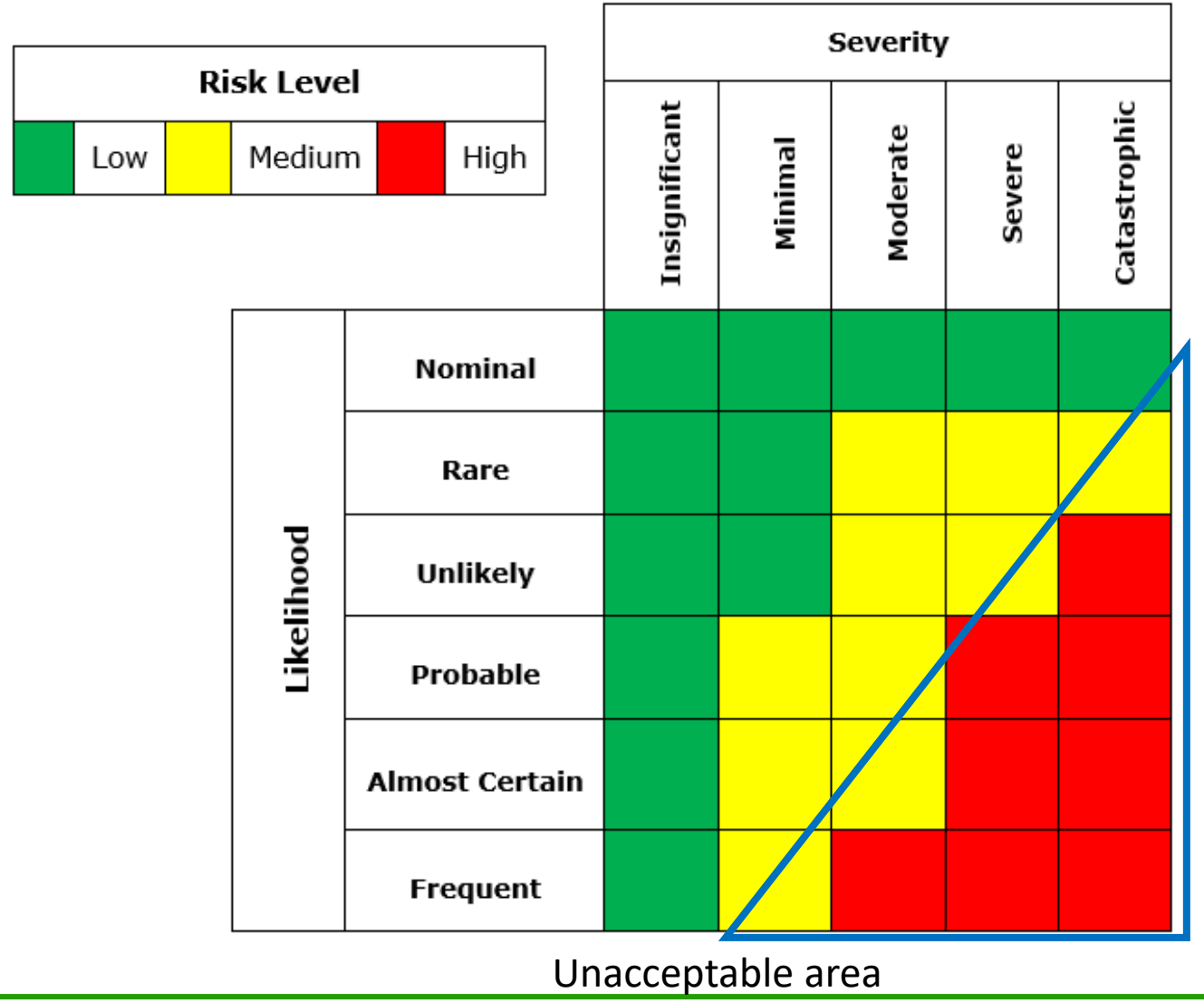
Risk and Hazard Mitigation Analysis

- There are numerous types of qualitative risk, quantitative risk, and hazard mitigation analysis:
  - Safety Independent Layers (SIL)
  - Layers of Protection (LOPA)
  - Event Tree
  - Hazard Identification (HAZID)
  - Hazard Mitigation Analysis (HMA)
  - Matrix Analysis – Popular among utilities
  - Bowtie Analysis – Popular among Oil&Gas and Maritime industries
  - The list goes on and on…

- All have strengths and weaknesses and many can feed into each other
  - As many stakeholders may be involved, a proper analysis should be one easily understood by stakeholders without risk assessment expertise
  - This likely means a qualitative analysis with a clear flow, breakouts for individual cases and a clear but simple quantitative assessment (could be as simple as red, yellow, green)

Understanding risk – Matrix Analysis

- Matrix or tabulated techniques assign a likelihood and severity to every possible failure
- Creates a clear table and results with clearly defined criteria for acceptable versus unacceptable risk
- Does not lend itself to visually understanding the failure pathway
  - Also unclear if “worst case scenario” being evaluated versus a scenario where mitigation is in place



Understanding risk – Bowtie

Threats

Hazard Event

Consequences

Barriers preventing threat inception from reaching “hazard” event

Barriers to mitigate “hazard” event once it has occurred

The more visual “bowtie” method lays out not just the failure but the pathway, highlighting all barrier to prevent it and their relative strengths

Understanding risk – Bowtie

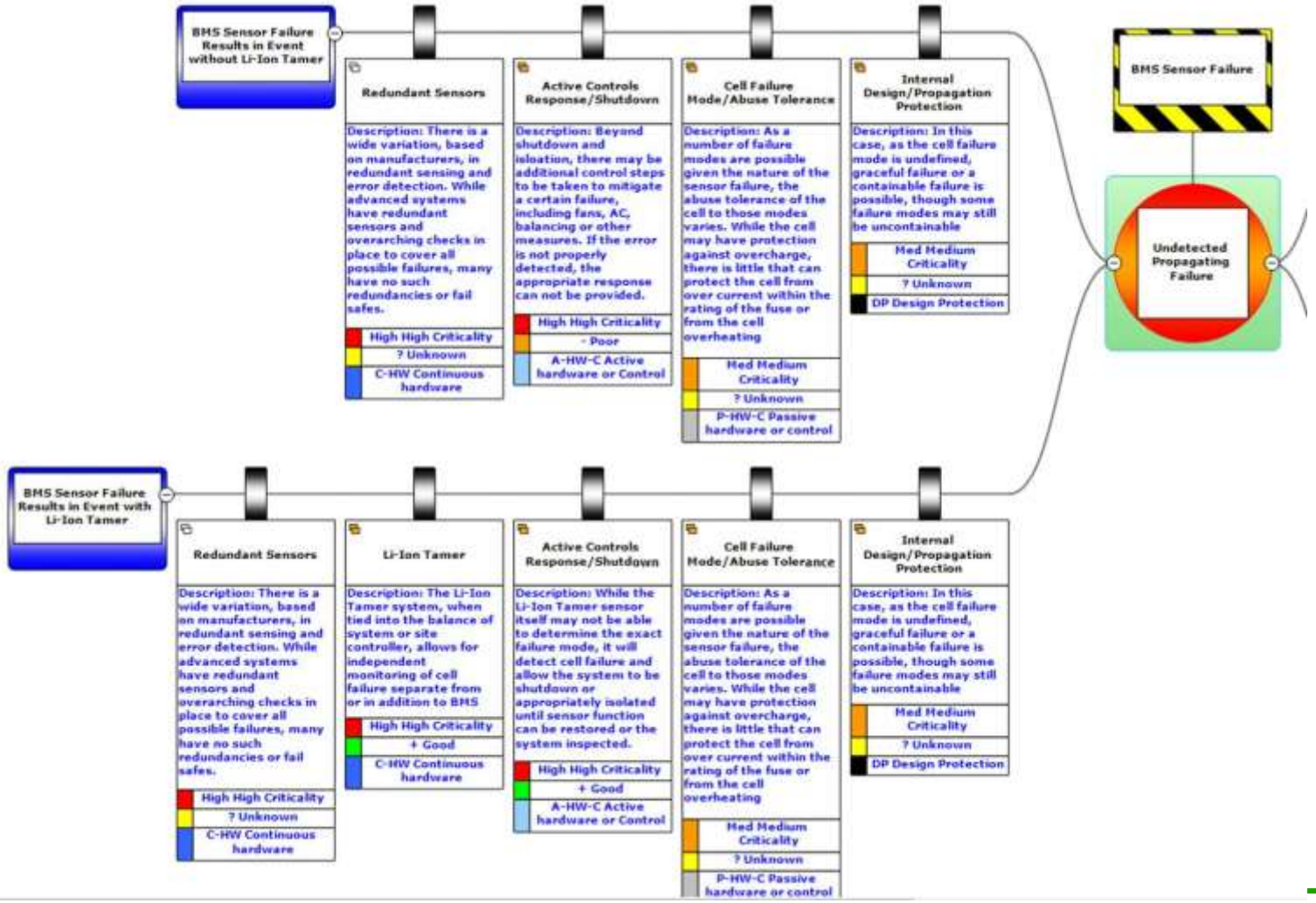
- Bowtie Analysis provides a clear visual analysis with a separate path for every failure type or mode
- Barriers or mitigation techniques may be placed along the path, and the barriers' strength defined, to show what is in place to stop failures
- Additional details about the failures and barriers may be relayed in the description to provide additional information and categorization
- Matrix style analysis (red, green, yellow) can be used as well in each failure mode and consequence
- Allows for independent breakdown between the failure mode or "threat" leading to an event and then again the event leading to a different type of "consequence"
- Weakness: more qualitative and may not lend itself as well to quantifying risk
  - This can be remedied via more detailed approach which may be too complicated for some

Acting on risk

- Once failure pathways are identified and their overall risk assessed, mitigation measures can be installed to reduce risk.
  - This may be accomplished by reducing the likelihood or the magnitude of the consequence
  - With lithium ion batteries, this could be accomplished by increasing the time between or likelihood of propagation to adjacent cells, modules, or racks or even preventing the failure altogether
  - This can be accomplished by detecting the failure as early as possible which may allow it to be avoided entirely
  - However, in many cases it was a BMS failure that allowed the system to reach this point, thus making the BMS equally unable to stop it or provide warning of the failure
    - In these cases, a redundant failure detection mechanism could detect the failure and shut the system off through the PLC or balance of system controller
    - One must not completely forget relationships when performing a risk assessment

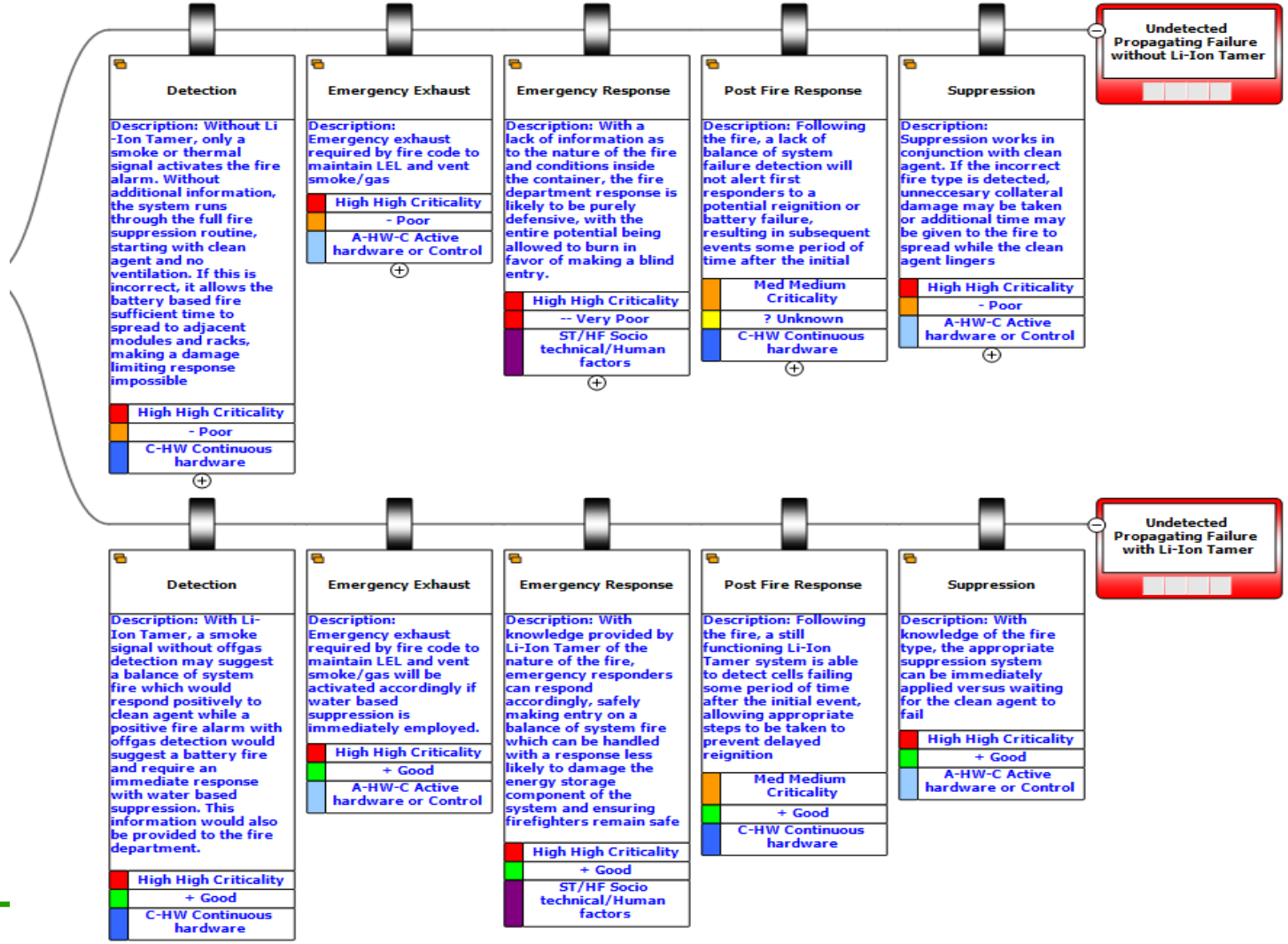
Acting on risk

-Reducing likelihood



Acting on risk

-Mitigating consequence



What Risk Assessment Isn't

- Risk assessment is not a box checking exercise for code compliance
  - All applicable codes and standards apply regardless of outcome
  - A component, design or system being code compliant doesn't necessarily make it a strong barrier or failure proof
  - Codes and standards are great and necessary, but represent the minimum generic requirements
  - Risk assessment should exceed code requirements and focus on actual strengths and weaknesses independently.
- Risk assessment is not about fudging or manipulating numbers to pass a requirements
  - Risk assessment done in a less than intellectually honest manner serves no one

Key Points and Proposals

- Risk Assessment need not be pass/fail
  - It may qualitatively show weaknesses throughout the process and design

- Risk assessment can and should be a living document
  - It need not be performed once and forgotten about
  - It should encompass the system, the balance of plant, and the surrounding built environment
  - We are working to development a guidance document on risk assessment from proposal to disposal
  - Could help evaluate intangibles of system against mismatched cost