Reliability Analysis

Module 6C: Failure Modes and Effects Analysis (FMEA/FMECA)

Probability Class				
	High	M	H	H
	Medium	L	M	H
	Low	L	L	M
		Minor	Moderate	Critical
		Severity Class		

Prof. Katrina M. Groth

Mechanical Engineering Department

Center for Risk and Reliability

University of Maryland

kgroth@umd.edu

#	Failure Mode	Effect	Severity	Likelihood
ASV1	External Leak	H2 accumulation above leak	3 - Critical	4 - Frequent
Tubing	External Leak	H2 accumulation above leak	3 - Critical	4 - Frequent
	Rupture/separation	Large H2 release if HV2 and N1 also fail	4 - Catastrophic	2 - Occasional
F1	Flow blockage	Potential overpressure at filter induces filter separation	2 - Marginal	3 - Reasonably probable
	Fluid contamination	Contaminated H2	2 - Marginal	3 - Reasonably probable
	External Leak	Accumulation of H2 above F1	3 - Critical	4 - Frequent
R1	External Leak	Accumulation of H2 in building	3 - Critical	4 - Frequent

Why FMEA?

- Pros
  - Valuable qualitative insights
  - Facilitates participation of multiple types of expertise
  - Comprehensive
  - Scalability to different design stages
  - Early insight into potential problems
  - Feedback process to address problems
  - Enables initial reliability analysis on low-maturity systems.
- Cons
  - “Not probabilistic” in the textbook. Meaning: Simplistic quantification results in high uncertainties, subjectivity, limited “big picture” insights
  - Limited insight into system-level failures
  - Can only address one failure at a time
  - High time, effort, expertise required

Anything else?

Types

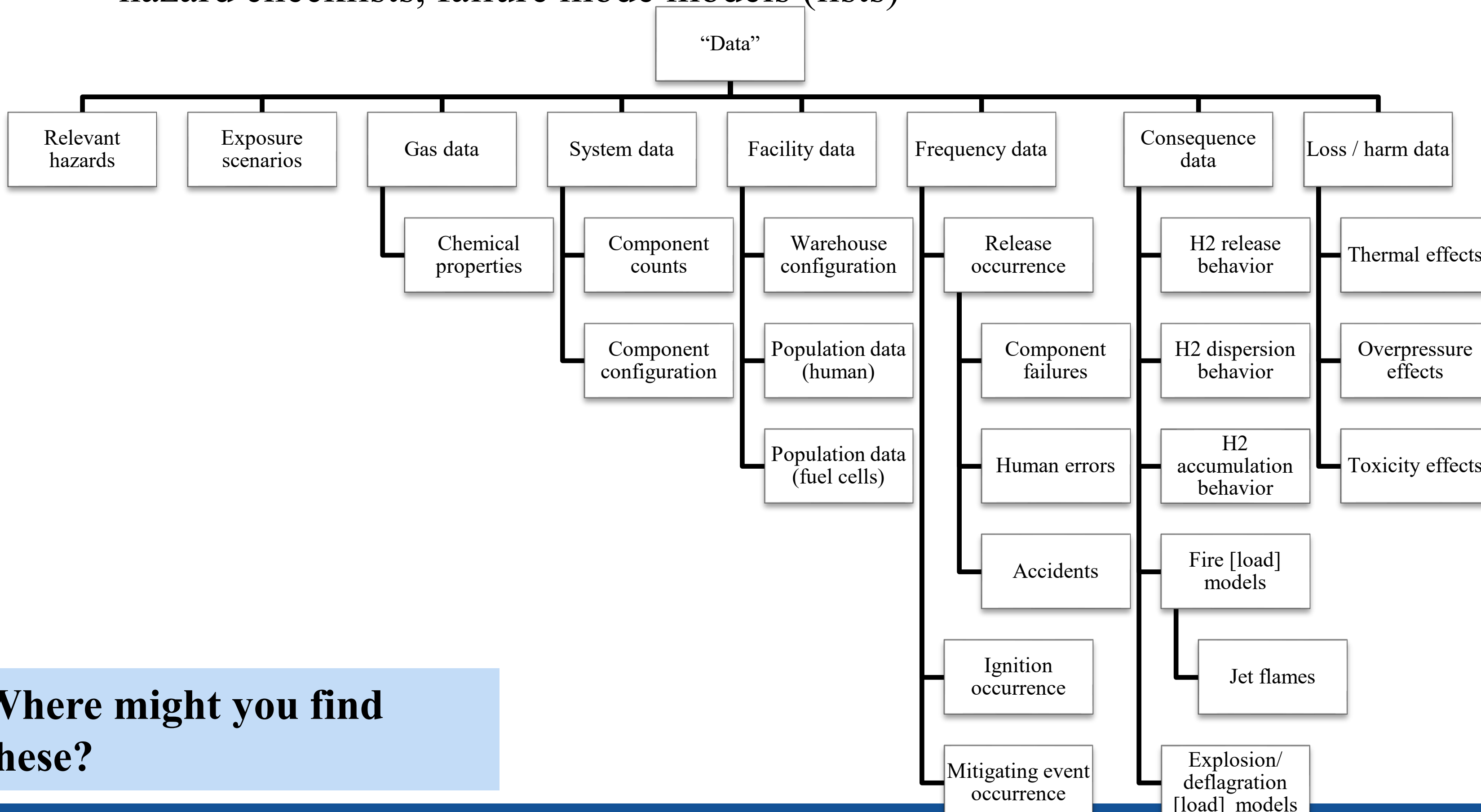
- Types of FMEA: See text or published procedures
  - Design FMEA
  - Process FMEA
  - Concept FMEA
- Published FMEA procedures:
  - **MIL-STD-1629A**. Procedures for Performing Failure Mode, Effects and Criticality Analysis. 1980.
  - SAE RP J1739
    - Ford FMEA Handbook- based on SAE RP J1739 http://www.quality.ford.com/cpar/fmea/
  - **SAE ARP5580**. Aerospace Recommended Practice-Recommended Failure Modes and Effects Analysis Practices for Non-Automobile Application. SAE International. Updated May 2012.
  - **IACS Rec No. 138**. Recommendation for the FMEA process for diesel engine control systems. Dec 2014. http://www.iacs.org.uk/media/2644/rec_no_138_pdf2553.pdf
  - **Other well-documented procedures exist**. Others you work with?

Planning an FMEA (1)

- **<u>Define goal</u>**. Options from SAE ARP5580 include:
  - Enhancing system safety by uncovering failure modes that result in hazardous conditions
  - Assessing the mission related effects of critical and/or undetectable failures
  - Influencing the design engineer to select a design with a high probability of operation success
  - Assisting the design engineer to select a design with a high probability of operation success
  - Providing data for development of effective maintenance support
- **<u>Define method and ground rules</u>**
  - Terminology, assumptions, worksheet format, end effects categories, severity definitions, boundary conditions, failure criteria, level of detail
    - An FMEA standard will define many of these
- **<u>Assemble the team</u>**
  - 2-5 core team members plus access to experts from risk analysis, design, manufacturing, operations, maintenance, etc.
  - Experienced members + newer engineers; diverse perspectives

Planning an FMEA (2)

- **<u>Assemble the information basis</u>**
  - System diagrams, system descriptions, system breakdowns, data sources, hazard checklists, failure mode models (lists)



Where might you find these?

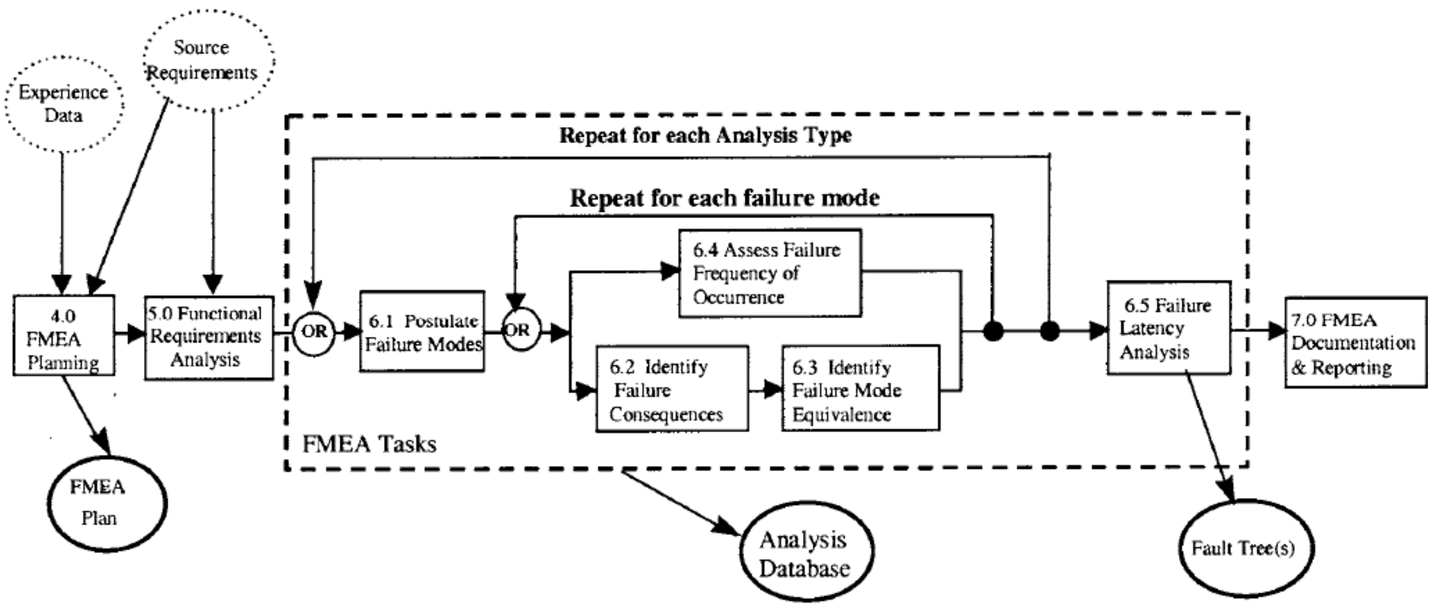
(A variant of this figure has subsequently been published in: R. Moradi, & KM Groth. 2019. “Hydrogen Storage and Delivery: Review of the State of the Art Technologies and Risk and Reliability Analysis.” *International Journal of Hydrogen Energy*, 44 (23): 12254–12269. doi:10.1016/j.ijhydene.2019.03.041.

General Procedure for FMEA/FMECA (after planning…)

- **Define the system to be analyzed**
  - System boundaries
  - Internal and interface functions
  - Failure definitions
- **Construct a block diagram of the system**
  - Structural (hardware)
  - Functional block diagram
  - Reliability block diagram (RBD)
- **Complete FMEA worksheet**
  - Identify failure modes and effects
  - Assign severity and likelihood
  - Identify compensation provisions, design corrections
- **Document the analysis (!)**

FMEA Methodology: SAE ARP 5580

- For an FMEA for the LNG Locomotive/Tender System, SAE ARP 5580 is recommended
  - "*Aerospace Recommended Practice—Recommended Failure Modes and Effects Analysis Practices for Non-Automobile Application*." (May 2012 v.)
  - Based on level of available design details [*conceptual design phase*], a "Product Design Hardware" "functional analysis" approach was used (see Table 2 in ARP5580)



FMEA Worksheets- SAE ARP 5580

Product Design Hardware Functional Failure Mode and Effects Analysis

System: LNG Tender Supplying Fuel to a Locomotive diesel/LNG Internal Combustion Enginee | **Operating Mode:** Operation

Date: 12/9/2017 | **Analysts:** [redacted] K. Groth

Version: Draft | **Affiliation:** University of Maryland

Unit Indenture Level	Assembly Indenture Level	Item/Functional Identification	Function	Failure Mode ID	Failure Modes and Causes	Failure Mode Model	Failure Effects: Local Effects	Failure Effects: Next Higher Level	Failure Effects: End Effects	Severity Class	Item Failure Rate	Failure Mode Distribution Ratio	Failure Mode Rate	Probability Class
30	37	Shutoff Valve	Controls flow to fuel into [39]	37.02	Valve operates spuriously due to control issues, short, etc.	Premature operation	GNG flow stopped prematurely	Low flow of GNG to engine	Locomotive performance is compromised	1	1.37	0.001	0.00	Low
30	37	Shutoff Valve	Controls flow to fuel into [39]	37.03	Leakage from valve due to seal failure, mechanical damage, etc	Failure to meet functional specs	Leakage		Potential release of GNG	2	1.37	0.668	0.92	Low

Worksheet Format: MIL-STD

SYRRA

- MIL-STD 1629, Task 101

System:
Indenture Level:
Reference Drawing:
Mission:

Data:
Sheet Number:
Compiled by:
Approved by:

ID	Item/ Functional Identification	Function	Failure Modes and Causes	Mission Phase Operational Mode	Failure Probability and Data Source	Failure Effects			Failure Detection Method	Compensating Provisions	Severity Class	Remarks
						Local	Next Higher	End				

- MIL-STD 1629, Task 102

System:
Indenture Level:
Reference Drawing:
Mission:

Data:
Sheet Number:
Compiled by:
Approved by:

ID	Item/ Functional Identification	Function	Failure Modes and Causes	Mission Phase Operational Mode	Severity Class	Failure Probability and Data Source	Failure Effect Prop.	Failure Mode Ratio	Failure Rate, 1/hour	Mission Duration hour	Failure Mode Criticality	Item Criticality $C = 3 C_m$	Remarks

FMEA + Criticality Analysis = FMECA

- **FMEA (MIL-STD 1629, Method 101)**
  - Standard: **Severity classification of Failure Mode Occurrence** on a 1 to 4 scale
  - Variation: **Risk Priority Number (RPN)** = Occurrence * Severity * Detection
    - **All above estimates evaluated on a <u>relative</u> 1 to 5 scale**
- **FMECA (MIL-STD 1629, Method 102)**
  - Qualitative: **Severity of Failure Mode Occurrence** on a 1 to 5 relative scale
  - Quantitative: Criticality Number =Part Failure Rate * Failure Mode Ratio * Probability of Function Loss * Operating Time.
    - **All above estimates are obtained through generic (field) failure data**

Failure mode criticality number

- A numerical value used to rank each potential failure mode based on its likelihood of occurrence and the consequence of its effect.

$$C_m = \lambda t \alpha \beta$$

- Where,
  - λ = *Part Failure Rate* (estimated by an appropriate failure data analysis or calculated from MIL-HDBK-217)
  - t = *the estimated mission time* of the unit (system)
  - α = *Failure Mode Ratio* as the fraction of the part failure rate related to a particular failure mode (estimated by an appropriate failure data analysis or calculated from MIL-HDBK-217)
  - β = *Failure Effect Probability*

Failure Effect	$\boldsymbol{\beta}$
Actual loss	1.0
Probable loss	0.1 - 1.0
Possible loss	0.0 – 0.1
No loss	0.0

Failure mode criticality number (cont.)

- The unit criticality number is the sum of criticality numbers for all individual failure modes of that unit: $C_{unit} = \sum C_{fm}$
- Notes:
  - Use the RBDs to evaluate the failure effect probability β for non-series systems.
  - The notion of the failure mode ratio assumes that **independence** of individual failure modes ($\sum \alpha_i = 1$).

Failure mode by criticality number (cont.)

- **Example**
  - A 1 kV varistor has a generic failure rate of $\lambda_p = 1 \times 10^{-6}/hour$ and the "short-circuit" failure mode ratio is $\alpha = 0.8$. The "short-circuit" failure mode results into the probable loss of a High Voltage protection circuit with $\beta = 0.001$. For all other failure modes, $\beta = 0.01$.
  - Determine the criticality number for the 10 month (7200 hour) period of the system operating time.

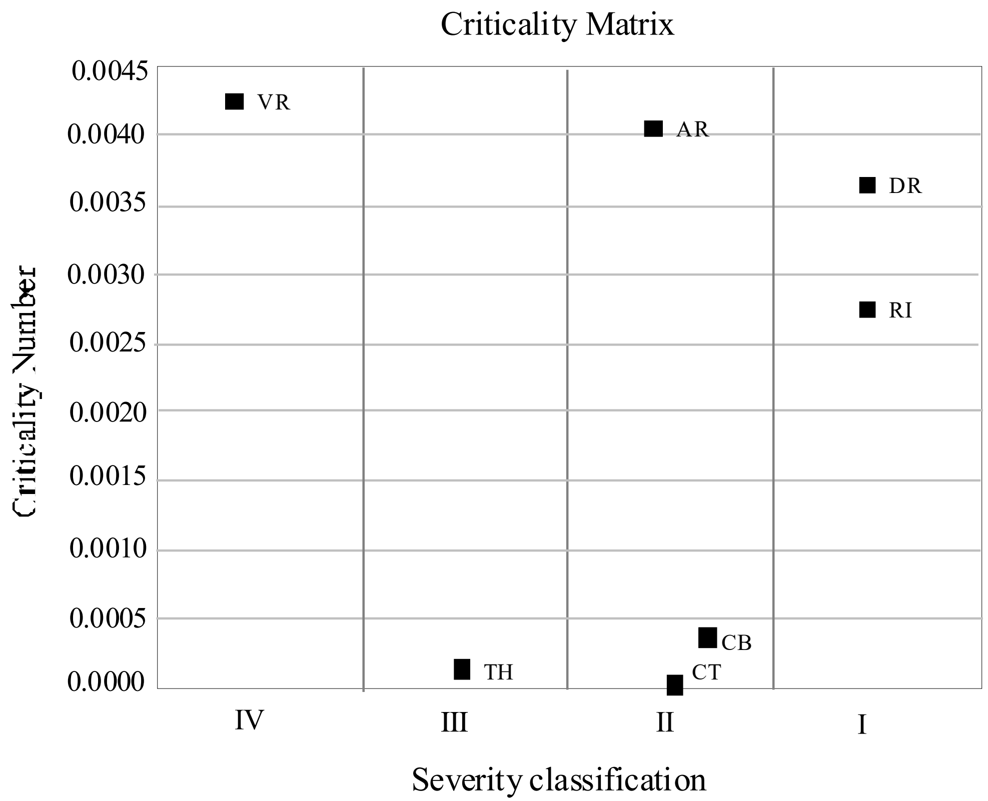
Failure mode by criticality number (cont.)

- **Example**
  - A 1 kV varistor has a generic failure rate of $\lambda_p = 1 \times 10^{-6}/hour$ and the "short-circuit" failure mode ratio is $\alpha = 0.8$. The "short-circuit" failure mode results into the probable loss of a High Voltage protection circuit with $\beta = 0.001$. For all other failure modes, $\beta = 0.01$.
  - Determine the criticality number for the 10 month (7200 hour) period of the system operating time.
- **Solution**
  - For short circuit: $C_m = (1 \times 10^{-6})(7200)(0.8)(0.001) = 5.76 \times 10^{-6}$
  - For the other failure modes: $C_m = (1 \times 10^{-6})(7200)(0.2)(0.01) = 1.44 \times 10^{-5}$

$$C_{varistor} = \sum C_m = 2.02 \times 10^{-5}$$

Criticality matrix

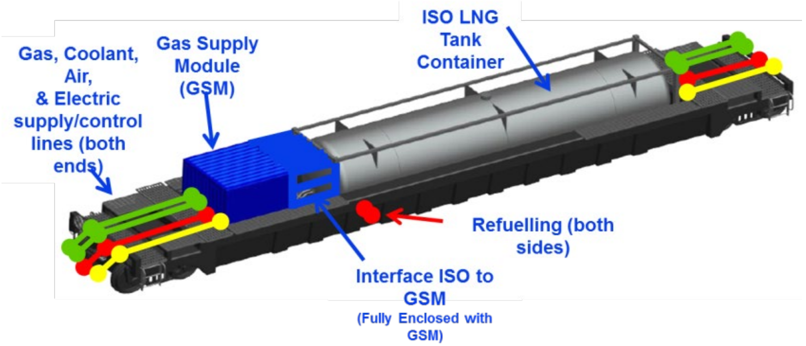
- A visual method to compare (and prioritize) the failures with respect to their severity and criticality (may also involved red/yellow/green coloring to support visualization.



FMEA- What are some attributes of success?

- Repeatability and traceability
  - Defined objectives and scope
  - Clear definitions of failure modes, consequences, the system, and criteria (or data used) to assign severity and likelihood
  - Final analysis reflects actual product (document the system)
  - Documentation of all of the above (and below)
- Diverse, representative team
  - Experts from all aspects of the system
    - Hardware, process, design, operations, maintenance
  - Experienced risk analysts
  - And beyond the team…honest reviewers
- To get there…follow a *rigorous* or *standardized* approach
  - Level of detail matched to type of technology, maturity, goals

Inspired in part by a true analysis



Case Study: Modified FMEA for LNG rail

System overview

- System elements:
  - LNG Tender (Intended to fuel an LNG/diesel dual fuel locomotive)
- Non-system elements: (Relevant for interfaces)
  - Track system
  - Human operators
  - Interface system
- Operating modes
  - Line-haul operation (“Operation phase”)
  - Refueling
  - Maintenance
  - Storage

FMEA Plan for today's exercise

- **Goals**
  - Enhancing system safety by uncovering failure modes that result in hazardous conditions
  - Influencing the design to mitigate the impact of failure on the final product
- **Define method and ground rules**
  - Defined in next few slides + handout
- **Assemble the team**
  - Members from risk analysis, design, manufacturing, operations, maintenance, etc.
    - **Reflect: what role do you fill on your team?**
- **Assemble the information basis**
  - Illustrative example attached.
    - System diagrams, system descriptions, system breakdowns, data sources, hazard checklists, failure mode models (lists).

Basis and Assumptions

- Analysis focused on the Line-haul operation phase
  - System is expected to spend a majority of time in this phase.
  - Operation phase includes: mainline travel and siding. We are not addressing switching or classification.
- System definition was based entirely on readily available public information
  - Based on Canadian Patent published in 2013.
  - No detailed system information was otherwise available.
- Focused on the Tender system
- The only hazard considered is release of natural gas (in any form) from any part of the system. (Defines ‘failure’)

Hazard identification

- Hazard: "A condition or physical situation with a potential for harm" (SFPE) [or loss]
  - What *could* go wrong?
  - …And which ones are you including in the risk analysis?

What are the hazards?
• Mechanical • Thermal • Chemical • Electrical • Biological • Radiation • Digital • …

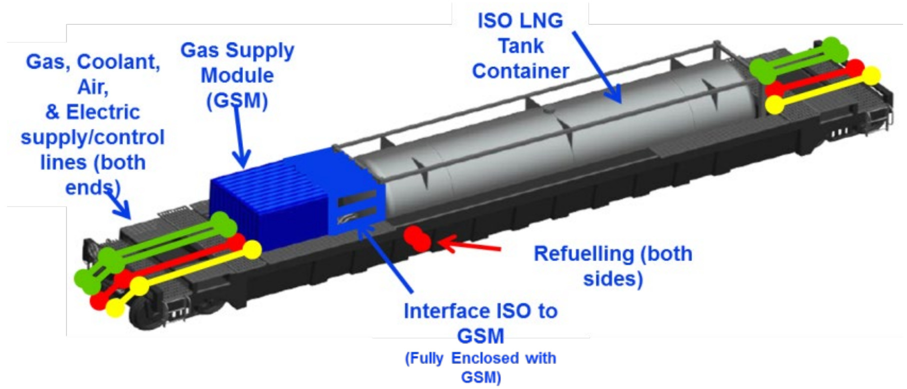
How do they manifest?
• Pressure? Impacts? • Fire? Freezing? • Corrosion? Oxidation? • Toxicity? Tenability? • Bacteria, virus, plant? • ..

Which of these apply for LNG/GNG?

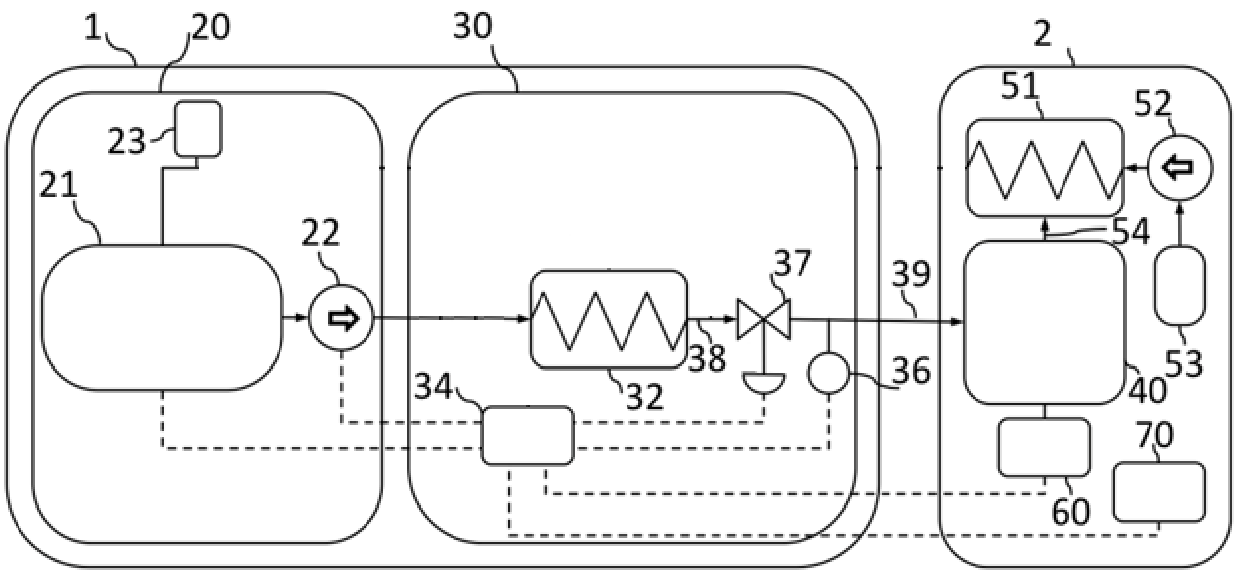
Hazards for the LH2 tanker

- Mechanical
  - Effects of overpressure (direct or indirect)
  - Impact from debris/projectiles
- Thermal
  - Heat flux (from various types of fires and smoke)
  - Freezing from exposure to cryogenic fluids
- Chemical
  - Tenability (asphyxiation (From NG or from smoke))

System drawing



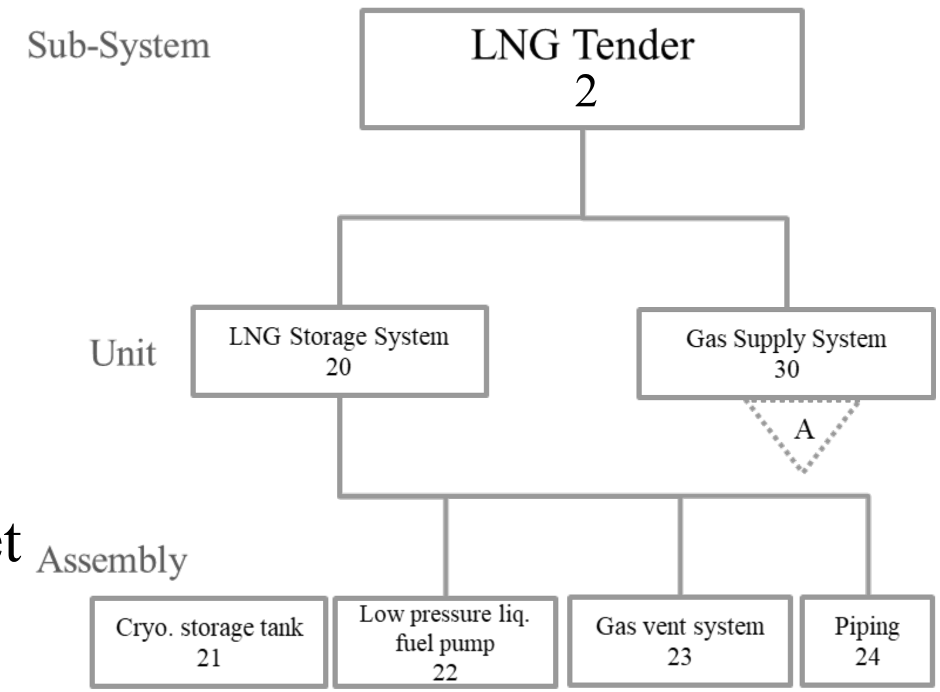
- See handout for a P&ID
- The drawing has been modified and simplified from the original to create a more simplified example for discussion purposes



System diagram source: Canadian Patent Document 2762697- Figure 1 – "Preferred embodiment." Full description of systems, parts, and interfaces provided in patent document

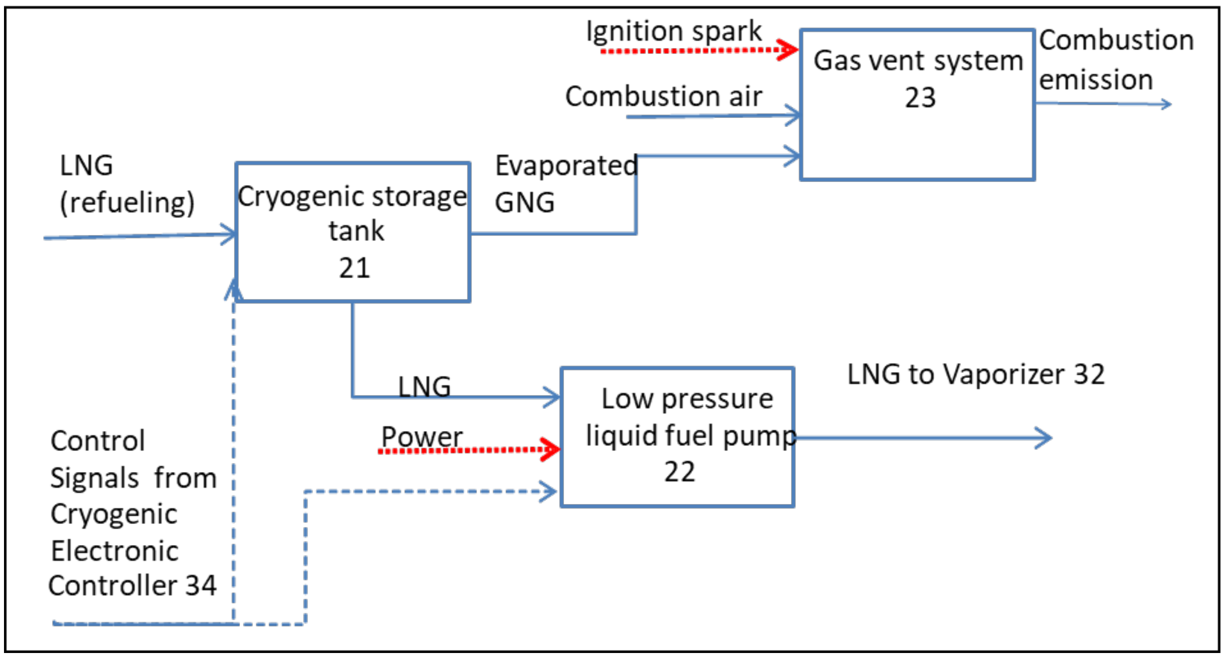
Break into 3 teams

- **Team 21** Cryogenic storage tank
- **Team 22** Low pressure liquid storage pumps
- **Team 23** Gas vent system
- Over the next several slides: you will fill in the elements of the ARP5580 FMEA worksheet for your component.
- Assemble results from each group to get the “final” FMEA for the class.



***Notice hierarchical numbering system in an FMEA**

LNG storage system block diagram



Identification of failure modes

SYRRA

- Systematic analysis of each assembly level component.
- Examination of assembly inputs and outputs

Failure Mode Models
Premature operation Failure to operate at prescribed time Failure to cease operation at prescribed time Failure to meet functional specifications Failure conditions caused by the operational environment

- Focused on failures that could lead to a release of GNG or LNG
- Note (Beyond current scope: Credible failure scenarios could also be identified from the Reliability Information Analysis Center (RIAC) Non-Electric Parts Reliability Database (NPRD) and Failure Mode Distribution (FMD) and previously published FMEAs of LNG vehicles and facilities.)

Identification of Failure Effects

- Failure Effects analyzed by identifying the consequence of each failure mode on operation of the assembly operation as well as the next higher indenture level
- The end effect on the system should also be identified
  - Consider specifically whether LNG or GNG could potentially be released in an uncontrolled manner

Severity Class	Criteria: Severity of Effect
1. Minor	No potential release of LNG or GNG (e.g., from failure of a component that does not process LNG or GNG)
2. Moderate	Potential leak or small-scale release of LNG or GNG (e.g., from a leaking seal, breach of line carrying vented GNG)
3. Critical	Potential for catastrophic release of LNG or GNG (e.g., from a breach of a line carrying LNG, from a rupture of storage tank, from failure of a tank relief valve)

Probability characterization

- To characterize the probability that a given failure mode occurs, it is common to use a failure rate as an approximation
- Failure Rate Source Priority
  - Field Data from exact equipment in exact environment
  - Failure rates from similar systems
  - Tables of generic component failure rates
- (RIAC) Non-Electric Parts Reliability Database (NPRD) was used as a standardized approach for estimating failure rates for the assemblies in this analysis
- Assumed to be constant over lifetime of component

Failure rate calculation

- Failure Rate: $\lambda = \alpha\beta t\lambda_p$ where
  - λ_p is the failure rate for all failure modes for a specific component
  - α is the fraction of component failure corresponding to the failure mode
    - (Ignore this part for the class exercise example; data not provided; just calculate it as $\frac{1}{\#\, failure\ modes\ you've\ identified}$).
    - $\beta, t\!: treat\ as\ 1\ for\ this\ exercise$
- $\lambda_p(per\ million\ hrs) = \frac{Number\ of\ failures}{Total\ hours\ (million)}$
- If no failures were reported, a Jeffrey's prior = 0.5 failures (half of an event) was used
- For failure modes involving an accident:

Railroad Accident Failure Modes and Frequencies

	Human Factors	Track and Infrastructure Defects	Rolling Stock Defects	Miscellaneous Causes	Total
Cars Derailed per Million Car-Miles	0.055	0.151	0.128	0.055	0.389

Probability classes

- The calculated failure rates were grouped into ranges to identify a qualitative characterization
- An order of magnitude scale was used
- A qualitative class was chosen due to uncertainty of failure rates from applying rates for similar equipment in different environments

Probability Class	**Criteria: Failure Rate**
High	$\lambda > 10.0$ per Million Hours or Million Track Miles
Medium	$\lambda =$ between 1 and 10 per Million Hours or Million Track Miles
Low	$\lambda < 1.0$ per Million Hours or Million Track Miles

Risk Priority

- Simple 3x3 Matrix
- Used to prioritize the failure events

Probability Class		Severity Class		
		Minor	Moderate	Critical
	High	M	H	H
	Medium	L	M	H
	Low	L	L	M

FMEA Conclusions

- Four of the failure modes were scored as high risk in the risk priority matrix in (LaFleur et al 2017):
  - **21.01—An over pressurization of the LNG storage tank due to failure of the relief valve,** either by failure to open or failure to vent at the rate of methane boil-off. Because the relief valve penetrates both inner and outer tanks, it is a single point failure mechanism that could lead to the uncontrolled release of the LNG tank contents.
  - **21.02—A leak of LNG due to a failure of a fitting or outlet in the LNG tank**. The fitting or outlet failure could be due to mechanical, installation or material defect or mechanical damage. Detailed specifications for the ports and outlets on the tank have not been designed; however, they also represent single points of failure through the double-walled tank that could lead to a release of the bulk of the LNG contents.
  - **21.07—This failure mode involved the embrittlement or cracking of the outer tank due to leakage or failure of the inner tank**. The outer tank is typically made of carbon steel and is not rated for cryogenic storage. Although this is a compound failure mode, requiring a failure of two components, it could result in a release of the tank contents and should be targeted for engineered safety in the design process.
  - **22.04—This failure mode involves a liquid LNG fuel pump scenario that experiences cavitation**. Cavitation is especially dangerous as it involves localized areas of low pressure which could cause boiling of the LNG and ultimately lead to rupture of the pump resulting in uncontrolled release of LNG or an explosion.

LaFleur, C. B.; Muna, A. B.; Groth, K. M.; St. Pierre, M. & Shurland, M. "Failure analysis of LNG rail locomotives." *Proceedings of the 2017 Joint Rail Conference (JRC2017),* The American Society of Mechanical Engineers (ASME), 2017