Improvement and Change Management

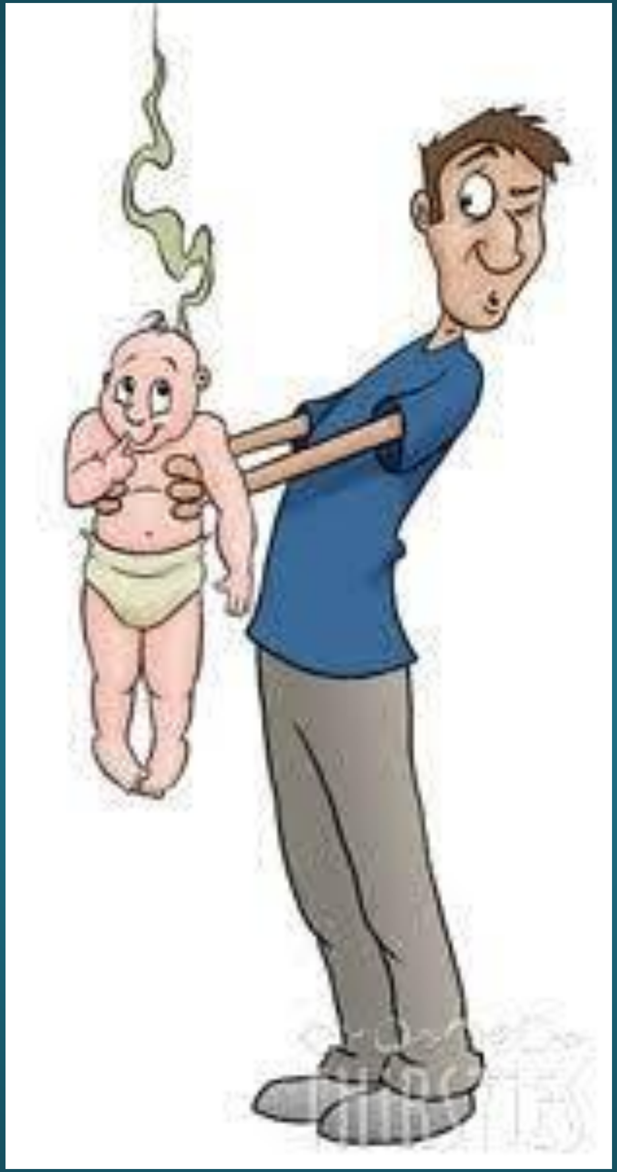
Jay G Standish, Rescar Companies

MxV Rail
350 Keeler Pkwy | Pueblo, CO 81001
www.mxvrail.com
A subsidiary of the Association of American Railroads

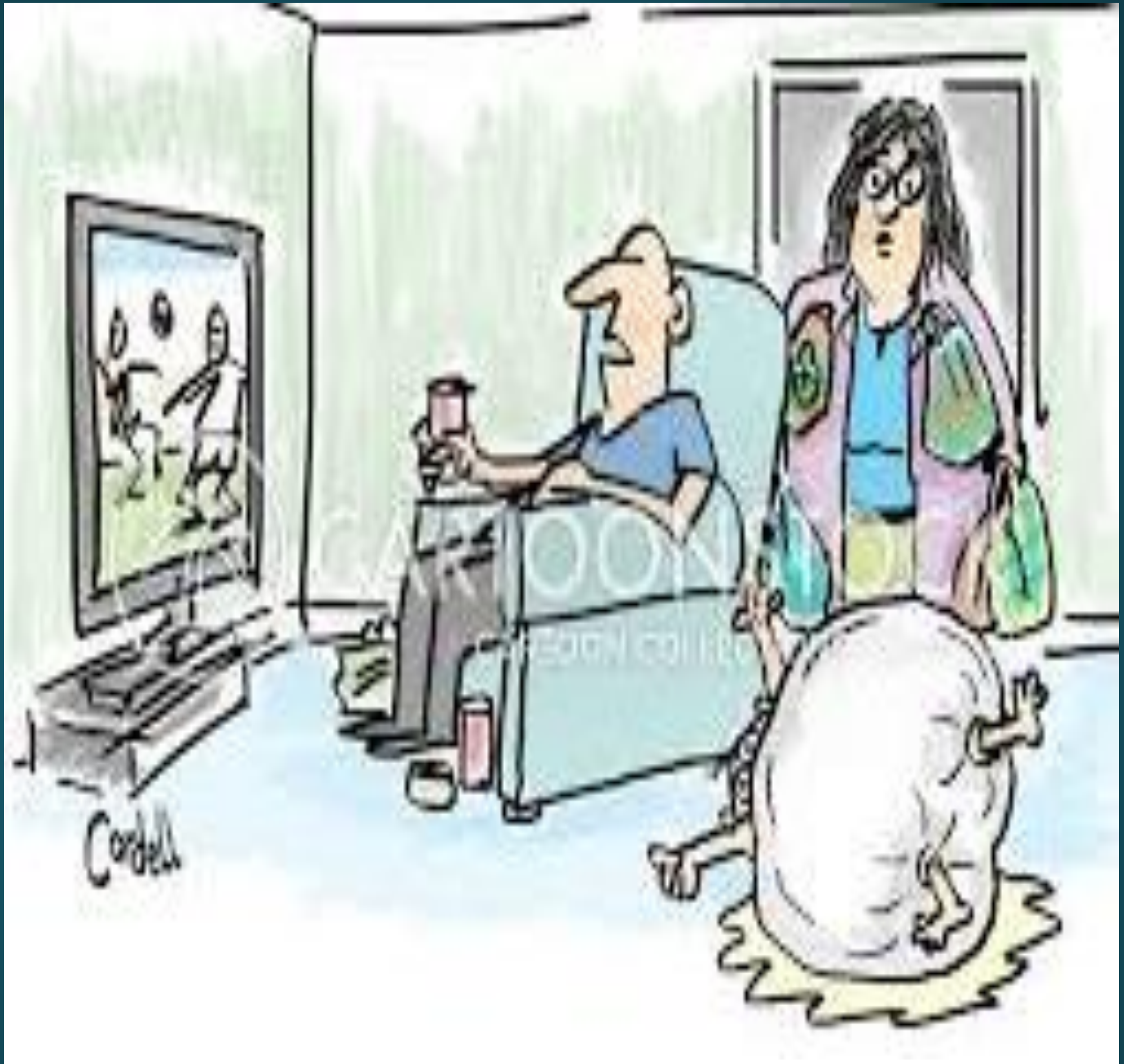
CHANGE?

I hate change!

Sometimes, change is needed.

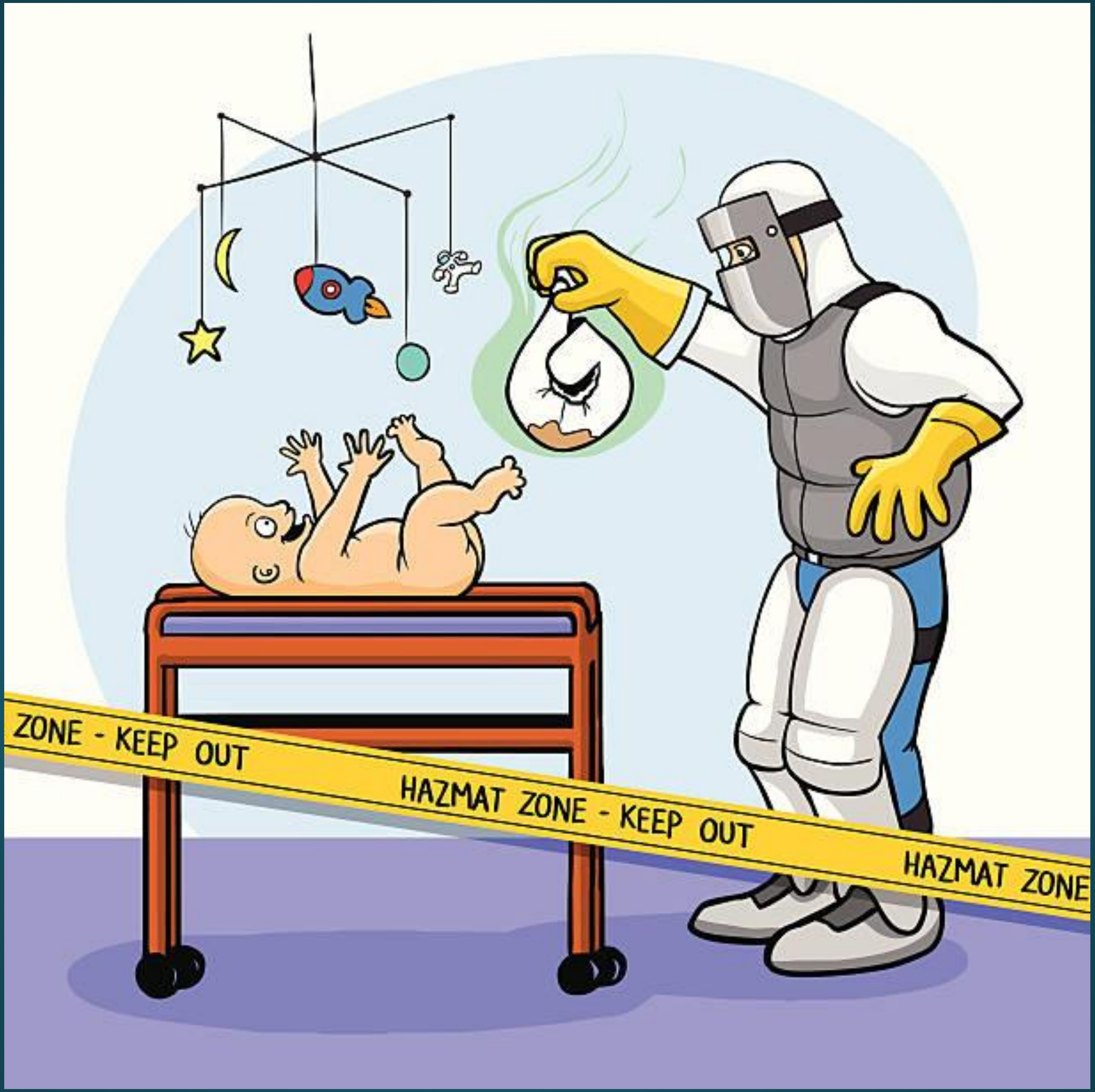


Some avoid it.



“He’s been fine – I haven’t had to do a thing”

Others adapt.



With most changes, the result is usually good.

Imagine the phone. And the changes embraced over time.

Material

Method

Technique

Environment

Machine

Tools / Equipment

Change is needed.
We can’t avoid it or
hope that it happens.
We have to adapt

2.19 Improvement and Change Management

- **2.19 Improvement and Change Management**
  - 2.19.1 The facility should maintain an effective change management program.
  - 2.19.2 The facility should utilize quantifiable risk analysis tools on activities to mitigate potential quality issues.
  - 2.19.3 The facility should retain documentation of changes

QAC’s Intent:

- The QAC would like facilities to implement a system/process to manage changes within their quality assurance programs and operations. This systematic approach should consist of structured processes to control change. Tools should include communication with all stakeholders, providing both an understanding and a path to the desired outcome. Communications should solicit feedback and track identified obstacles to address concerns. Some examples of changes could be adding a new product line, adding critical machinery, adding a new shift, etc. The QAC would like to encourage facilities to develop their own change management program.

- Almost every element in the M-1003 is about change. The elements require procedures and records for the given change.

- What to audit? Shift change, model year, equipment (major equipment projects) or scope of work.

Risk

- **Quantitative risk analysis – The process of numerically analyzing the combined effect of risks and other sources of uncertainty.**
- **Two key factors – probability and impact (best guesses)**

Risk Analysis Tools

- **Failure Mode Effects Analysis (FMEA) –** Severity, occurrence, detection = RPN – Critical + RPN/Detection. Design, process and product.
- **Overall Equipment Effectiveness – OEE.** Utilization x Yield x Efficiency. Utilization considers the availability. And you can include cost. OEE - the gold standard for measuring manufacturing productivity, quality, and availability.
- **Qualitative Analysis Tools-** high/medium/low or very likely/possible/not likely scale.
- **Expected monetary value (EMV) –** probability %; cost when it definitely occurs; multiply the two – then use simple pareto for risk exposure. Add them all up for a cumulative effect.
- **Delphi Technique -** form of expert brainstorming for risk identification.

Risk Analysis Tools

- **SWIFT Analysis -** The Structured What-If Technique (SWIFT) is a simplified version of a Hazard and Operability Analysis (HAZOP), or a structured and systematic technique for system examination and risk management.
- **Decision Tree Analysis-** A Decision Tree Analysis is similar to an Event Tree Analysis, but a Decision Tree does not provide a fully quantitative output.
- **Bow-tie Analysis -** One of the most practical techniques available for identifying methods for risk mitigation. In Bow-tie Analysis, you start by looking at a singular risk event and projecting it in two directions. On the left, you'll list all the potential causes of the event; on the right, all the potential consequences.
- **Probability/Consequence Matrix -** Risk matrices (also called risk heatmaps) all do essentially the same thing: provide a practical means of assessing the overall severity of a risk by multiplying the likelihood of a risk occurring against the impact of the risk, should it occur.

Even the most precise risk analysis is open to error simply because there is no way to predict the future with 100 percent certainty. Additionally, data is never perfect. Together, these uncertainties make it difficult to measure risk in a way that contributes to more meaningful decisions.

- To perform a risk assessment, organizations need to do the following:

1. Identify threats, vulnerabilities, and risks.
2. Understand the impact of these threats, vulnerabilities, and risks on the organization.
3. Create or use a model for risk analysis.
4. Sample the model to understand the threats, vulnerabilities, and risks more fully.
5. Analyze the results obtained from the above steps.
6. Implement a risk management plan to manage the threats, vulnerabilities and risks based on the results of the risk analysis.

A Congressional sub-committee meeting.

“What if we don’t change at all …
and something magical just happens?”

EMPLOYEE INTERVIEW	**Speak to the employees involved. What needs to change? How will that change impact them?**
LOOK-ACROSS	**What other employees, processes, practices, parts, equipment are in the same condition?**
PROCESS CONSIDERATIONS (Ishikawa Diagram)	**Identify items that may be impacted by the change based on the categories below.**
People	
Materials	
Measures	
Method	
Technique	
Tools and Equipment	
Procedures	
Forms / Drawings / Records	
Environment	

M-1003 Requirement

- **2.19 Improvement and Change Management**
  - 2.19.1 The facility should maintain an effective change management program.
  - 2.19.2 The facility should utilize quantifiable risk analysis tools on activities to mitigate potential quality issues.
  - 2.19.3 The facility should retain documentation of changes

Auditing!

- **What improvement and change management programs does your organization have in place?**
  - How does it work?
  - Is that process documented?
  - Are risks identified and quantified?
  - What happens if something goes wrong?
  - What records are kept?

MxV™

MxV RAIL

THANK YOU