Operating & Support Hazard Analysis (O&SHA)

MIL-STD-882E Task 206

Integrating elements of
System-of-Systems (SoS)

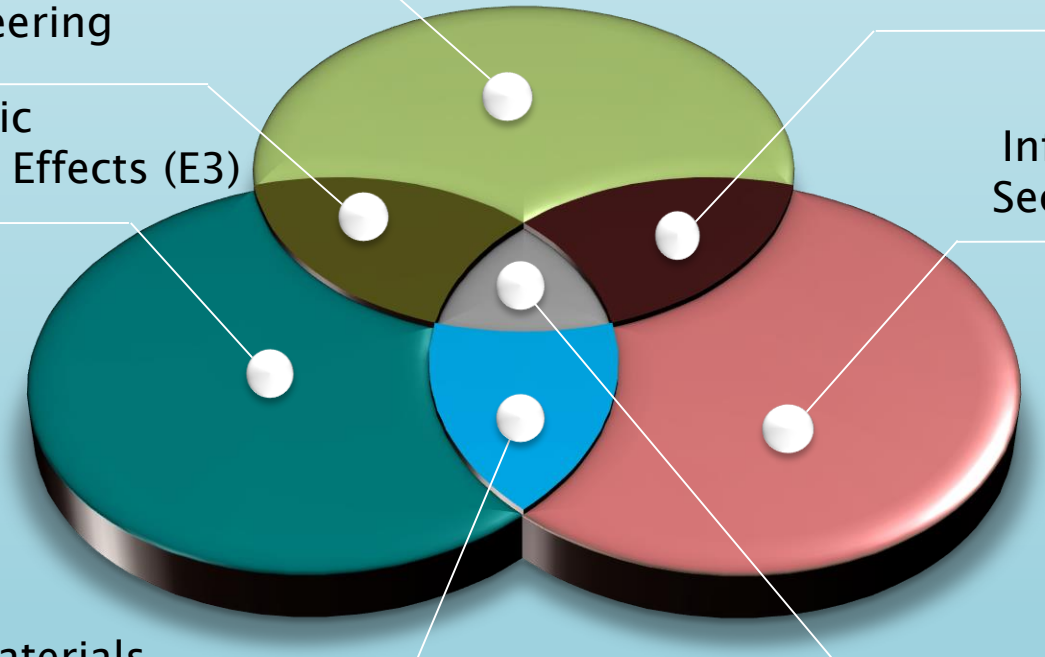
Workshop
International System Safety Society – Ottawa
13 December 2017

CMTIGroup Inc & Associates
Sue Cox P. Eng.
Tony Zenga BSc. Eng.

Agenda

- Specialty Engineering
- Managing System Safety
- DoD Standard Practice System Safety MIL-STD-882E
- What is an O&SHA
- Purpose & Challenges of O&SHA
- Cowboy After O.S.H.A
- O&SHA Findings
- O&SHA, How it is done
- Regulations in Canada
- O&SHA, Scope, Lessons Learned and Incidents
- Operational Hazard (participants inputs)
- Operations, Facilities & Maintenance Flow down – SoS, SHA, SSHA
- Mitigation Effectiveness
- Hazard Log, O&SHA V&V, Closeout
- O&SHA Planning Misconception & Summary
- Questions / Comments

Specialty Engineering



Managing System Safety for a System-of-Systems

- Despite the progress made in the System Safety Engineering discipline we continue to see safety related issues such as:

  - Automobile Equipment Safety Recalls
  - Train Derailments or Collisions
  - Aviation Incidents
  - Environmental Impact

  - Equipment failures
  - Operational hazards
  - Contingency plan
  - Planet Earth

- System Safety challenges facing the industry include:

  - System Complexity
  - Competitive marketplaces
  - Quick deployment time
  - Geographically diverse subsystem suppliers
  - Outsourcing of engineering activities & Cultural differences
  - Timing of Safety Information sharing

DEPARTMENT OF DEFENSE STANDARD PRACTICE SYSTEM SAFETY MIL-STD-882E

TASK SECTION 100 - MANAGEMENT

TASK SECTION 200 - ANALYSIS

- TASK 201 PRELIMINARY HAZARD LIST
- TASK 202 PRELIMINARY HAZARD ANALYSIS
- TASK 203 SYSTEM REQUIREMENTS HAZARD ANALYSIS
- TASK 204 SUBSYSTEM HAZARD ANALYSIS
- TASK 205 SYSTEM HAZARD ANALYSIS
- **TASK 206 OPERATING AND SUPPORT HAZARD ANALYSIS**
- TASK 207 HEALTH HAZARD ANALYSIS
- TASK 208 FUNCTIONAL HAZARD ANALYSIS
- TASK 209 SYSTEM-OF-SYSTEMS HAZARD ANALYSIS
- TASK 210 ENVIRONMENTAL HAZARD ANALYSIS

TASK SECTION 300 – EVALUATION – Safety Assessment Report ……

TASK SECTION 400 - VERIFICATION

O&SHA – What is it ?

- A systematic analysis of the controlling documents (e.g., procedures and tasks) to ensure hazard elimination or control with emphasis on the performance of people and their relationship to hazards within the tasks.

- The O&SHA focus is on the:
  - Operation & Maintenance
  - Installation
  - Testing
  - Special Tools & Test Equipment
  - Facilities
  - Transportation
  - Storage
  - Disposal
  - Emergency Egress & Rescue
  - Training

  of the system rather than system components.

O&SHA

Purpose:

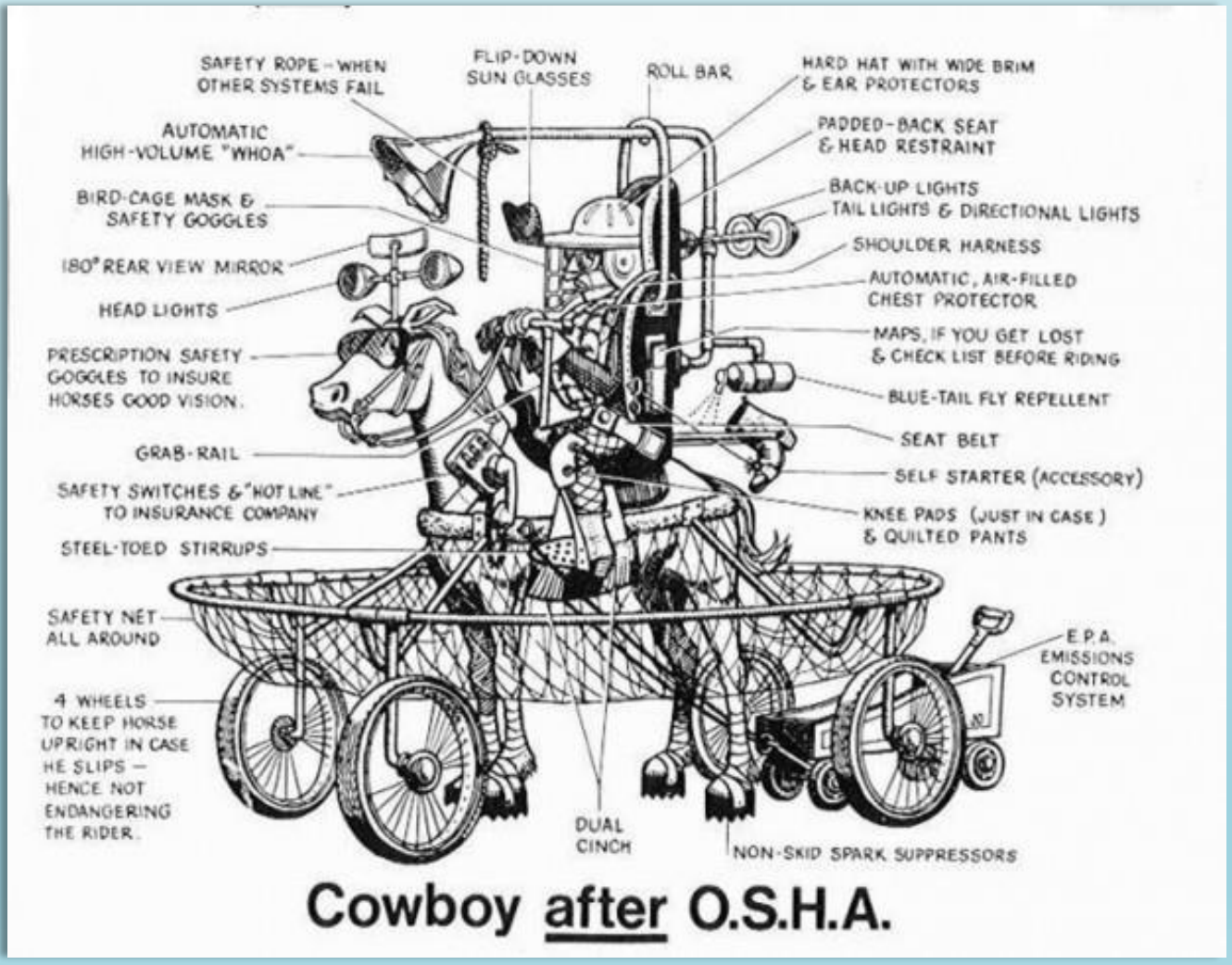
- To identify and assess hazards introduced by operation and support activities; and
- Evaluate the procedures, facilities, and equipment used during operation and support activities.

Challenges:

- The human is an element of the system, both receiving inputs and initiating outputs. O&SHA needs to create an effective link between Human Factors Engineering and System Safety.

- O&SHA is typically one of the poorest performed system safety analyses. Subject Matter Expert (SMEs) and documented procedures are not always available to support O&SHA.

O&SHA should not result in a "Cowboy"



OSHA drawn by J.N. Devin 1972

O&SHA – Findings

- Identify the activities that involve a known hazard
- Identify the hazards the risk and controls for each activity
- Identify design changes or functional changes needed to reduce risk
- Identify procedure changes needed to reduce risk
- Identify Personal Protective Equipment (PPE) and any limitations
- Identify Warnings and Cautions on equipment and in procedures
- Identify Emergency procedures.

O&SHA, How is it done?

- HAZOP is a planned, structured and systematic examination of procedures, processes and facilities
  - -sample ref. IEC 61882 Ed. 2.0 b:2016 "Hazard and operability studies (HAZOP studies) – Application guide"

SIEVERT. MATERIAL SAFETY DATA SHEET

SIEVERT AB — POWERGAS 220383, 220483

Revision: 1.0 — Date: 05/11/2012

1. IDENTIFICATION OF THE SUBSTANCE/PREPARATION AND OF THE COMPANY/UNDERTAKING

Product identifier: Sievert Powergas disposable cartridge 2203, 175g, 300ml – 2204,336g, 600ml

Relevant identified uses: Professional, heating, shining and cooling for do it yourself purpose.

Supplier: Sievert AB

Address: P.O Box 1366, Hemvärnsgatan 22, SE-171 26 Solna, Sweden, +46 8 629 22 00 (office hours 08:00 to 16:30)

Emergency telephone number: 112 (Sweden)

E-mail: info@sievert.se

2. HAZARDS IDENTIFICATION

Classification of the substance or mixture

Classification according to Regulation (EC) No 1272/2008 (CLP): : Extremely flammable gas (H220)

Classification according to Directive 67/548 ECC or EC 1999/45: : F_+; R12

Label elements

Labeling according to Regulation (EC) No 1272/2008 (CLP)

Signal Words: Danger
Hazard statements: H 220 : Extremely flammable gas
Precautionary statements:
- General: P 102: Keep out of the reach for children
- Prevention: P 210: Keep away from heat/sparks/open flames/hot surfaces - No smoking
- Storage: P 403: Store in a well ventilated place.

Labeling according to Directive 67/548 ECC or EC 1999/45

R-Phrases: : R12 Extremely flammable
S-Phrases: : S2 Keep out of the reach for children; : S9 Keep container in a well-ventilated place.; : S16 Keep away from sources of ignition - No smoking

Gas cartridge - do not expose to temperatures exceeding 50 °C, protect from direct sunlight. Assemble or dismantle cartridge from appliance outdoors only, free from ignition sources. Gas cartridge - store in a cool dry place. Large gas leak in non-ventilated areas could cause lack of oxygen.

Other hazards: : None

Page 1 of 4 — Print date: 16/11/2012

- Methods:
  - comparison of similar operations/facilities,
  - information review (e.g. MSDS),
  - checklists,
  - "what if?" scenarios,
  - guide words,
  - FMEA
- Method selection depends upon factors such as Regulatory requirements, complexity, similarity, history, engagement of operations/support representatives.

Regulations in Canada

- **Canada – Bill C-45, March 31st 2001**
  - Established new legal duties for workplace health and safety
- **Ontario Occupational Health and Safety Act**
  - Occupational health and safety awareness training
  - Workplace Hazardous Materials Information System (WHMIS)
- **Alberta OHS Act, Part 2 Hazard Assessment.**
  - Prepare a report of the results of a hazard assessment and the methods used to control or eliminate the hazards identified.
  - Ensure that the hazard assessment is repeated ...
  - Involve affected workers in the hazard assessment and in the control or elimination of the hazards identified.
  - Ensure that workers affected by hazards identified in a hazard assessment report are informed of the hazards and of the methods used to control or eliminate the hazards.

O&SHA, Scope

Operations	Operating Rules, Operating Manuals, MANOPS – ATC, Flight Operations Manual – Airlines . Safety Review of Operational Procedures.
Maintenance	Removal, Assembly, Calibrating, Maintenance Frequency, Number of Personnel Involved. Safety Review of Maintenance Procedures & Tasks.
Installations	Installation of Systems or Equipment. Safety review of installation procedures.
Test	Testing under hazardous conditions. Safety review of Test Procedures.

O&SHA, Scope Cont'd

Special Tools	Test Equipment, Support Tools, Tools Calibration.
Facilities	Facilities Interface with systems, Special grounding (ordnance static grounds), Conductive flooring of non-sparking material.
Transportation	(Air, Rail, Water) – Safety of systems or equipment during transport
Storage	Storage of hazardous equipment e.g., Missiles, Ordnance, Chemical agents, Oils, Solvents. Missile storage in Shipboard Magazine.

O&SHA, Scope Cont'd

Training	Training completeness – e.g., explosive safety Training for personnel who produce, handle, transport, store, inspect, test, maintain, use, or dispose dangerous goods.
Disposal	Substances, solvents or other agents, munitions or materials harmful to personnel or environment
Emergency Egress & Rescue	Emergency escapes, First respondents accessibility to rescue access, Communications.

O&SHA Lessons Learned

Operations

Mass Transit, Space, Military

- Mass Transit – Crew failure to follow exit procedures. Crew key used to open train doors at train end of line drops train lines. The propulsion software was designed to continue in its last known direction when train lines were dropped. Train moved in the opposite direction of intended motion.

- Space – Astronaut skips steps in operating procedures during EVA close call with ISS Antenna.

- Military – Unsafe Hoist motor during power loss requires manual cranking by the operator – becomes unsafe when power is inadvertently restored.

O&SHA Lessons Learned

Maintenance

Mass Transit, Navy

- Maintenance engineer runs a test to ensure the doors are in proper working conditions after door leaf replacement. Fails to see that they are not in their lower roller track. Train enters operation with doors not in their lower tracks. The doors collide with the platform.

- Equipment Damage – Subsystems interface – Doors interference with vehicle bogie side panels.

- Fire on board the aircraft carrier USS Forrestal (1967). An electrical anomaly (ungrounded ordinance) had caused the discharge of a Zuni rocket on the flight deck, triggering a chain-reaction of explosions.

O&SHA Lessons Learned

Installation — Rail, Navy ship

- Incorrect wiring of Traction Motors.
- Fire – Welding on upper deck caused sparks falling to decks below, where painting was in progress.

Testing — Rail, Aero

- Train fatality during test run – train derailed during testing of the AirTrain, Kennedy Airport.
- Missile release Relay was replaced with Solid State technology, Testing successfully passed the "Iron Bird" testing. While in flight the missile was fired but remained attached to the aircraft.

Special Tools & Test Equipment — Missile Launch, Aero

- Missile System – Energizing a sequence of Pins on Connector X results in missile inadvertent Launch sequence.
- Aircraft Engine – Use of fork lift to install engine on wing instead of the OEM specified special tool. Fork lift upward force stressed the engine mounting bolt. The aircraft loses engine during takeoff.

O&SHA Lessons Learned

Facilities — Mass Transit

- Vehicle in Maintenance Depot In Reduced Operation Mode the vehicle can be driven while it is connected to 600V overhead power shop plug (*the why is on slide 21*).

Transportation — Saturn V Rocket, Military

- Ensure payload pyros do not energize (appendages do not deploy) during launch.
- Equipment or systems Activation during flight.
- Transportation of HazMat,
- Transportation of explosives or other dangerous articles.

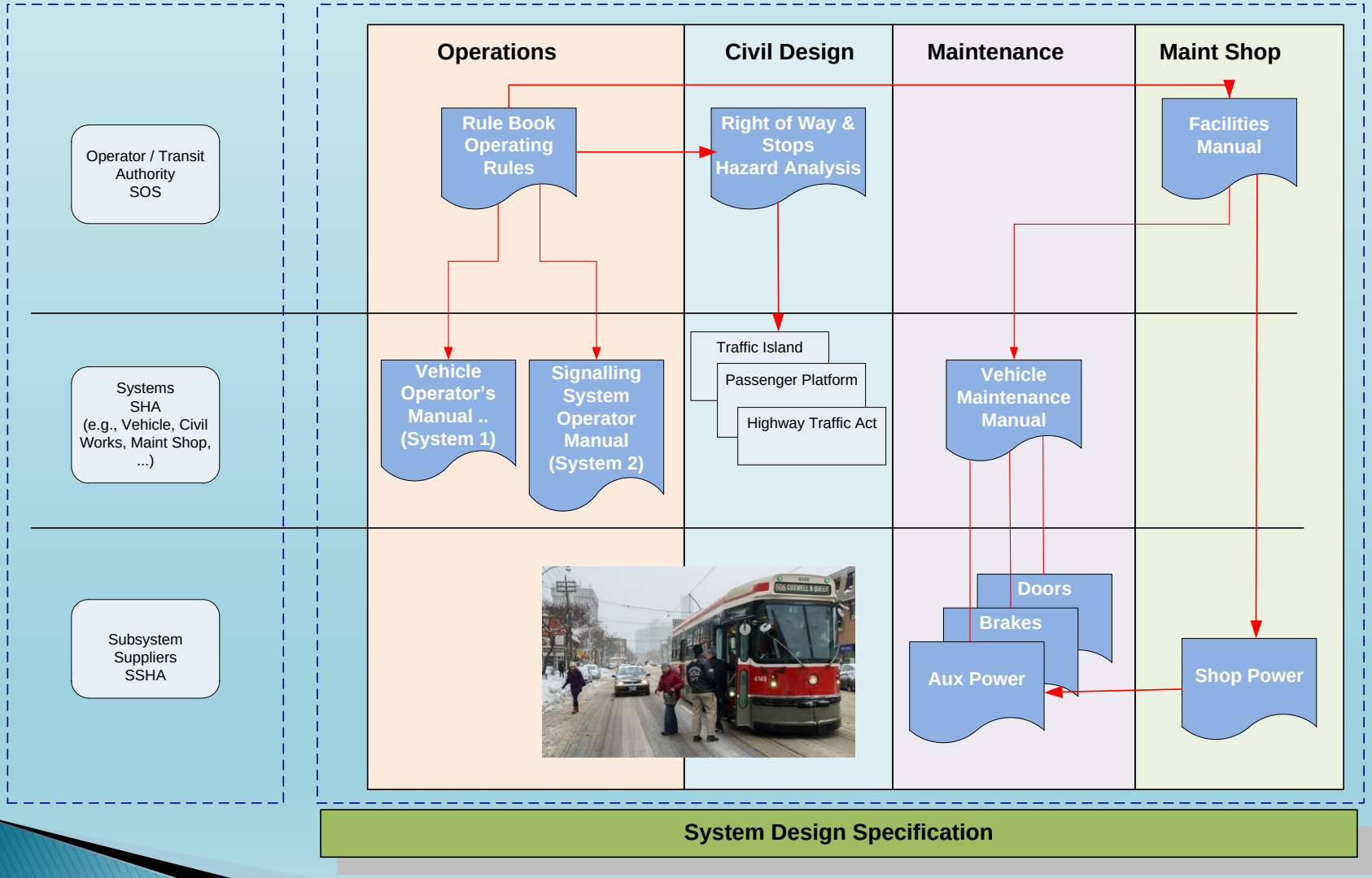
Storage — General

- Equipment can be sensitive to temperature and humidity during storage.
- Shock and vibration during storage, e.g. storage onboard a ship.
- Materials deteriorate, limited shelf life.

O&SHA Incidents

Operational Hazard ?

Operations, Facilities & Maintenance



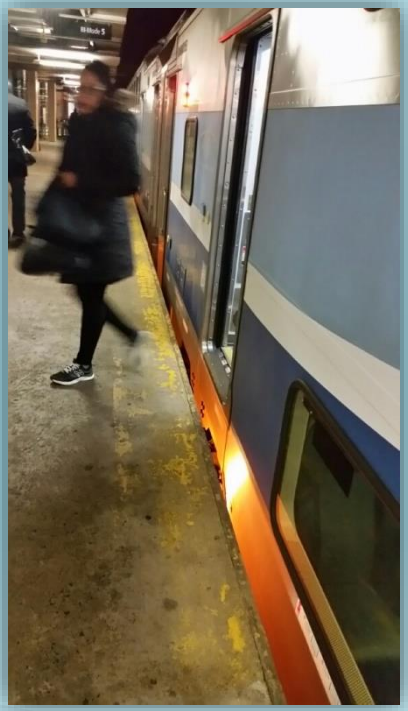
Operational Hazard ?

"Toronto city councillor Mike Layton wants the TTC to use cameras to nab drivers who ignore open streetcar doors."

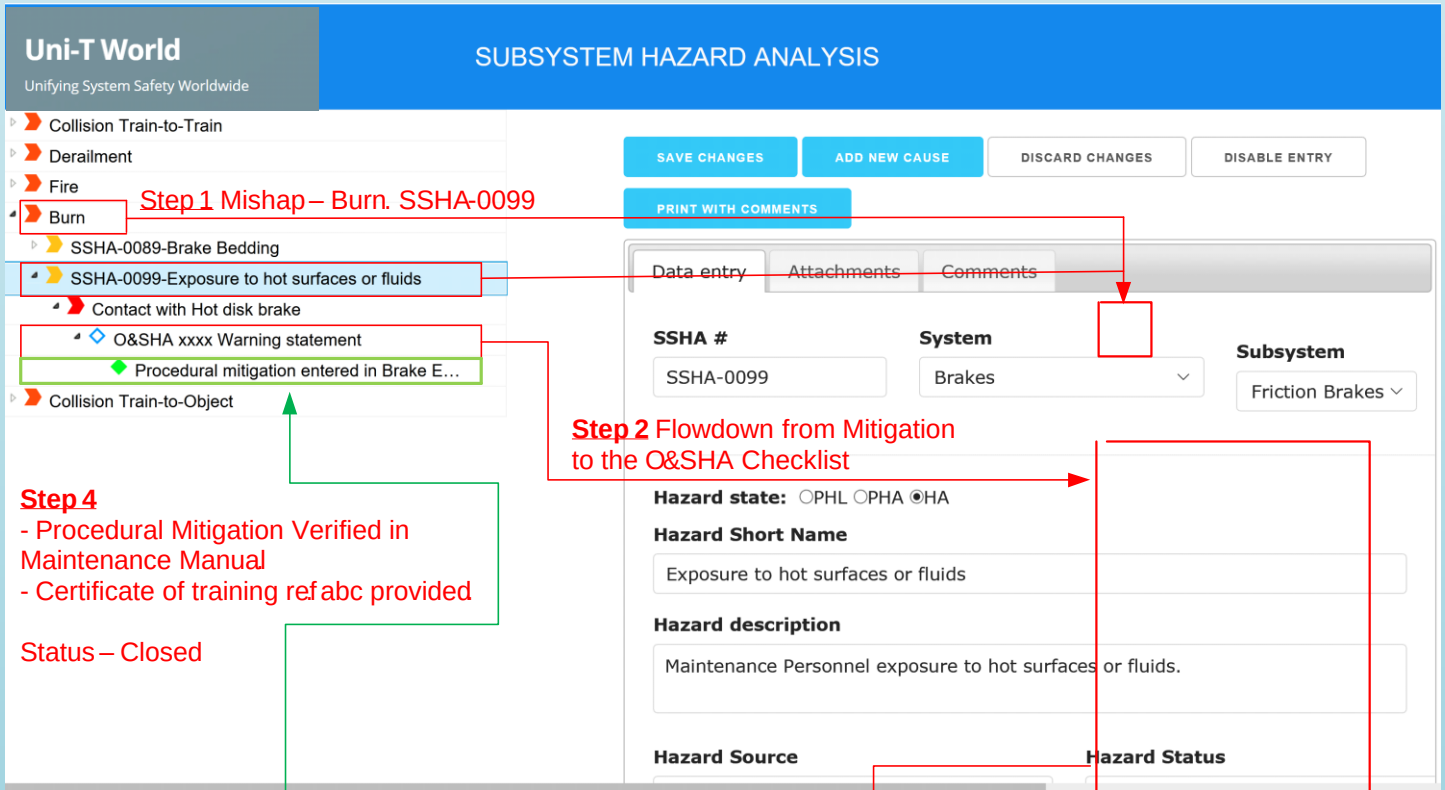
(RICHARD LAUTENS / TORONTO STAR FILE PHOTO)

Mitigation Effectiveness ?

Watch gap between car and platform



Hazard Log, O&SHA V&V, Closeout



Step 1 Mishap – Burn. SSHA-0099

Step 2 Flowdown from Mitigation to the O&SHA Checklist

Step 3 Procedural Mitigation applicable to checklist

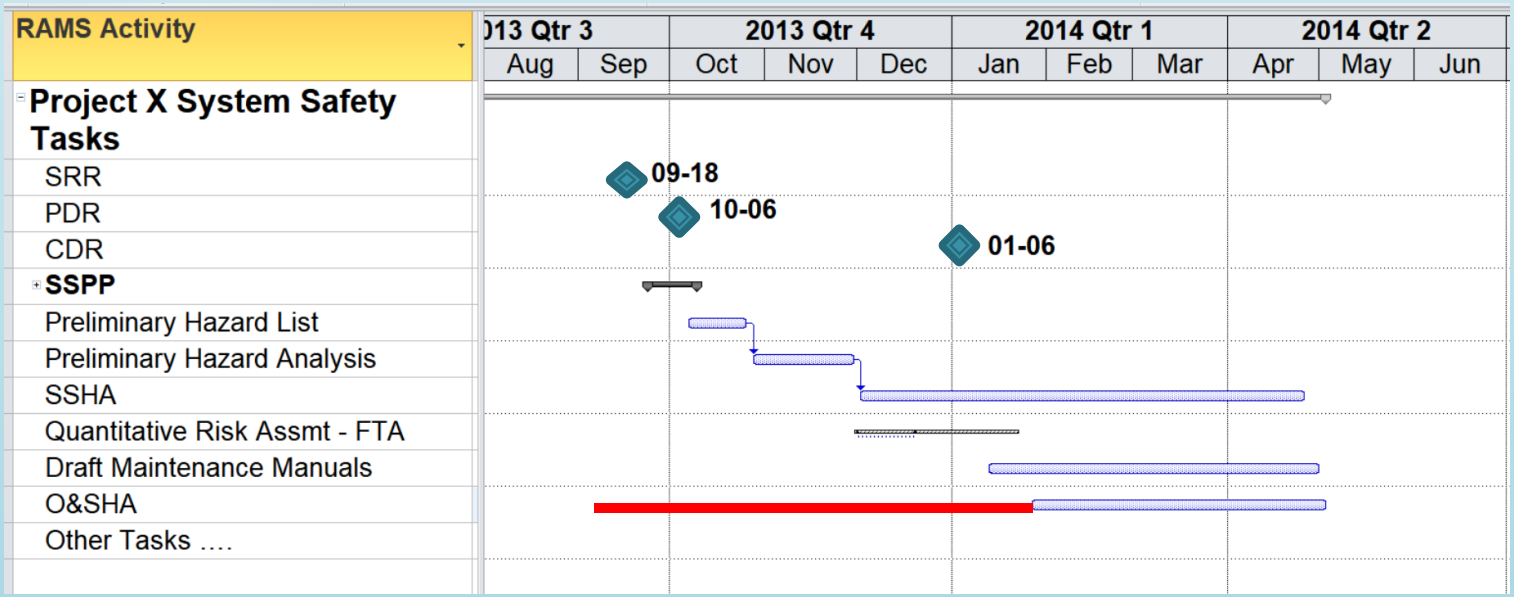
Step 4
- Procedural Mitigation Verified in Maintenance Manual
- Certificate of training ref abc provided

Status – Closed

WARNING

Risk of Sever Burn Disc Brake can be extremely hot when the vehicle enters the shop
Allow time for equipment to cool before performing any maintenance

O&SHA Planning Misconception & Summary



1	2	3	4	5	6	7
O&SHA to be initiated early in the program	All elements analyzed by O&SHA shall be considered	SOS integration sequence influences O&SHA activities	Written procedures and tasks are a necessary input for O&SHA	SMEs need to participate in O&SHA	O&M manuals need to reflect O&SHA findings	O&SHA shall follow the V&V process

Questions / Comments ?

Thank You
for your attendance and participation

Sue Cox P. Eng.
Tony Zenga BSc. Eng.

www.cmtigroup.com
www.uni-tworld.com

Backup Slides

O&SHA activity Exclusions

- Human Factors
  - Operator
    - Omits required actions
    - Failure to recognize actions when required
    - Improper response (early, late, wrong)
    - Failure to follow Procedures
- Designers
  - Lack of System Safety / Hazard Awareness
  - Provides inadequate or Faulty documented Procedures
  - Quick Operator Response for hazard recognition
  - Requires Intense Operator Attention
  - Designing or providing improper tools
- Common Errors
  - Inadequately Rested
  - Human exposure to extremes (temperature, noise, adequate space, etc.…)