www.mwftr.com/CS2.html

CS^2
(Computers and Safety Critical Systems)

Safety Interface
(Safety related subjects)

Dr. Charles Kim

Fall 2014

Language of Safety

- Latin " Salvus"
  - **Safe, whole, healthy**
  - Try Google Translate: "Salvus Sis" → "**Be Safe"**
- Definition(s):
  - SAFE: "**freed from harm, injury, or risk**; no longer threatened by danger or injury; secure from threat of danger, harm or loss"
  - SAFETY1: "**the condition of being safe; freedom from exposure to danger; exemption from hurt, injury or loss**"
  - SAFETY2: "**Freedom from those conditions that can cause injury or death to personnel, or damage to or loss of equipment of property**"
- Interface of "Safety"
  - Definition is very **genera**l: **people and things**
  - Definition is **qualitative** rather than quantitative
  - Definition permits a natural **interface** between safety and other disciplines closely aligned with safety: **reliability, maintainability, human factor, and Value Engineering**

How to write well for the class

- **Background**
  - People are more likely to read subjects/writings/emails that create curiosity or provide utility
  - When they are busy
    - Curiosity fades in importance
    - They read only the ones with practical importance ["utility"]
- **How to write your essay and report?**
  - Write as if you are a staff writer (targeting for busy people) for a newspaper, who has an editor behind whose job is to cut his/her article to fit into a limited space, maybe just 1 inch in a column.
  - Practical Guide
    - (1) Important things [Conclusions and summary] in the first paragraph
      - Summary of the event/thing first so that it delivers message even though the rest is not read or cut by the editor --- "**Summary survives the "cutting""**
      - Then expand your story (with paragraphs and paragraphs) after the First Paragraph
    - (2) Use your own words --- Be aware of plagiarism !!!! --- F grade !!

Compare this

www.cbsnews.com/8301-202_162-57600384/syria-strike-seems-inevitable-as-u.n-warns-against-unilateral-military-action-hunt-

Updated at 6:48 a.m. Eastern

DAMASCUS, SYRIA | U.N. chemical weapons experts investigating an alleged poison gas attack near Damascus left their hotel again Wednesday hoping to carry out their second field trip, which was delayed Tuesday for security reasons.

The team of about 20 inspectors left their hotel in the Syrian capital in a convoy of cars to visit the eastern Ghouta suburbs, where the Obama administration says President Bashar Assad's forces unleashed a chemical weapons attack on Aug. 21 that killed hundreds of people.

Local opposition activists told CBS News that the convoy had reached the town of Mleiha, in the sprawling Ghouta area, and videos posted online by the activists showed the U.N. inspectors interviewing patients at clinics in Mleiha and the nearby town of Zamalka.

Play VIDEO

Intercepted communications, tissue samples prove Syrian regime responsible for gas attack

On Tuesday, Vice President Joe Biden made it clear that regardless of what the U.N. inspectors find, the White House is now convinced the attack was carried out by Assad's forces.

The American government's assessment is based on the circumstantial evidence from videos posted on the internet, and, as CBS News correspondent David Martin reported Tuesday, intelligence -- much of it still classified -- ranging from intercepted Syrian communications to tests of tissue samples taken from victims.

Another key piece of circumstantial evidence which has been cited by both officials and analysts for days is the simple fact that the regime is the only entity in Syria known to have chemical weapons and the means to disperse them.

With this

By Oliver Holmes and Erika Solomon
BEIRUT | Wed Aug 28, 2013 7:59am EDT

(Reuters) - The United Nations Security Council was set for a showdown over Syria on Wednesday after Britain sought authorization for Western military action that seems certain to be vetoed by Russia and probably China.

U.N. chemical weapons experts investigating an apparent gas attack that killed hundreds of civilians in rebel-held suburbs of Damascus made a second trip across the front line to take samples. Secretary-General Ban Ki-moon pleaded for them to be given the time they need to complete their mission.

But the United States and European and Middle East allies have already pinned the blame on Assad and, even without full U.N. authorization, U.S.-led air or missile strikes on Syria look all but certain, though the timing is far from clear.

That has set Western leaders on a collision course with Moscow, Assad's main arms supplier, as well as with China, which also has a veto in the Security Council and disapproves of what it sees as a push for Iraq-style "regime change" - despite U.S. denials that President Barack Obama aims to overthrow Assad.

Uncertainty over how the escalation of the conflict at the heart of the oil-exporting Middle East will affect trade, and the world economy sent oil prices, and gold, to their highest levels in months while stocks fell. Fears over the economy of Syria's hostile neighbor Turkey pushed its lira to a record low.

Analysis & Opinion

Western powers could strike Syria within days

West mustnâ€™t rush into Syrian conflict

Related Topics

World »
Russia »
United Nations »
Syria »

Related Video

U.N. resumes Syria chemical attack probe
4:20am EDT

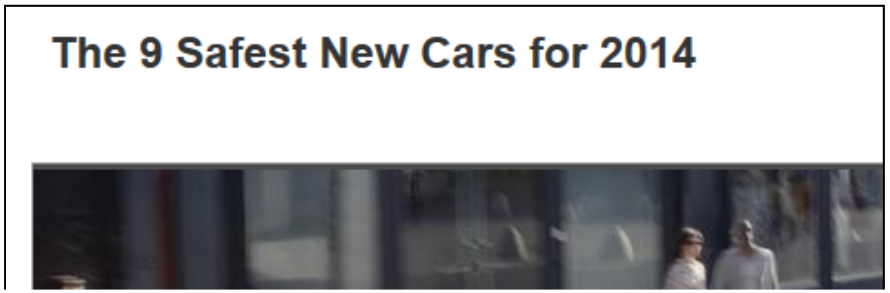
Rebels gain ground in Northern Syria

Israel will respond with force to any attack from Syria

Biden: No doubt Syrian regime used chemical weapons

Reliability vs Safety

- Most Reliable Car vs. Safest Car



- Most reliable and safest car?

Interface with Reliability

- Safety is most closely related with Reliability than other components
- Reliability: "Probability that the system will perform its intended function for a specified period of time under a set of specified environmental conditions"
- Safety: "Freedom from those conditions that can cause injury or death to personnel and damage to, or loss of, equipment or property."
- "Hazards which occur without causing injury or death to personnel" → domain of safety or reliability?
- "A hazard which affects only personnel" → domain of safety or reliability?
- Fusion of safety and reliability:
  - Quantification of safety: Safety expressed in probability that injury or damage does not occur.

Safety-Reliability Interface – "Drive-to-Work" case

- S: Safe event
- $\overline{S}$: Unsafe Event
- R: Reliable event
- $\overline{R}$: Unreliable Event
- Example (sample point marking??)
  - Safe arrival
  - Damage to car but no injury
  - Injury but no damage to car
  - Injury plus damage to car
- How about this?
  - An engine does not start → no driving & no accident
  - A collision caused by careless driving

$\overline{R}$

$\overline{S}$

Reliability vs. Survivability

Reliability vs. Survivability

- Survivability
  - A variant of reliability
  - Definition: “The measure of the degree to which a **system wil withstand the environment in** which it is placed and not suffer abortive impairment of its ability to accomplish the designated mission.”
- Reliability vs. Survivability
  - Reliability: relates to activity carried out **prior to the appearance of failures or degradation** in accordance with *a* priori standards
  - Survivability: relates to activities conducted **subsequent to the occurrence of failure or degradation**
  - What can be unreliable and still survive?
- Situation Dependency (example. Multi-engine commercial aircraft): Conflict and Compromise
  - **Reliability requirement**: each engine must assure the safety of the aircraft
  - **Survivability criteria**: the aircraft must survive in the event of a failure of an engine

Reliability and Maintainability

What is a nice looking and easily maintainable car (Used) that one can buy with $10K? ★

- 10 year warranty program?

Interface with Maintainability

- Definition: "**The probability that the system will be retained in, or restored to, a specified condition** within a given period of time, presuming that the maintenance is performed in accordance with a set of prescribed procedures and allocated resources.
- Maintenance: "all actions necessary for retaining the system in, or restoring it to, a specified condition"
- Maintenance for retaining a system in sound condition → preventive in nature
- Maintenance carried out for restoring a system from difficulty → corrective in nature
- Fundamental role of maintainability is to **increase system life** without necessarily enhancing safety

Safety-Maintainability-Reliability Interface

- Mark the following guidelines in the diagram:
  - Direct removal and replacement of faulty components, or their repair by personnel
  - Switching to redundant equipment through the use of built-in, self-checking circuits
  - Use of redundant elements and use of majority voting

Interface with Human Factors

- Personnel activities and incidences of human error
- **Human factor:** "A body of scientific facts about human characteristics. It includes, but is not limited to, principles and applications in the areas of human engineering, personnel selection, training, life support, job performance aids, and human performance evaluation"
- **Human Engineering:** "The area of human factors which applies scientific knowledge to the design of items in order to achieve effective man-machine integration and utilization"

Safety and Human Factor

- Problems (in safety enhancement)
  - Much of the biological and psychological information needed for the purpose is not yet available
  - The mathematical tools for quantifying and optimizing in a formal fashion are just now being developed
- **Fundamental areas in which human factors and system safety interface**
  - The mechanisms by which the body regulates and maintains an optimal internal environment
  - Person's ability to adapt to specific work-sleep schedules while maintaining effectiveness.
  - Human tolerance to physical forces such as shock, vibration, and noise
  - Human tolerance to long-term effects of irreversible, or slowly reversible, pollutants expended into the environment.

Design for Human Factor

Interface with Value Engineering (or value Analysis)

- **Value Engineering**: “an organized effort to analyze the functions of systems, equipment, facilities, services, and supplies for the purpose of achieving essential functions **at the lowest life-cycle cost** consistent with required performance, quality and safety.”
- Safety has a value
  - Problem of a relative value as a factor to be quantified
  - Transformation of relative safety values to absolute values – complete safety analysis

Value of Safety

- Value = Function/Cost
- Absolute Value: "Cost(price) value is equal to the amount of money needed for purchasing labor, material, and overhead that are required to produce a given item or establish and explicit system output"
- Relative Value: subjective (use value or esteem value)
  - "Use value (or function value) relates to the properties and qualities of an item or system output that permit a task, work, or a service to be performed."
  - "Esteem value relates to the characteristics of an item or a system output that make the system desirable or attractive and, consequently, valuable."
- Combined meaning with absolute and relative values
  - "Exchange value is determined by the intrinsic properties of an item or system output which enables it to be exchanged or traded for some other item or output"
- Transformation of relative value into absolute value?
  - In all, some quantitative assessment of the risks must be preceded before taking any action → need some transformation of relative safety values into absolute ones.

Value Engineering and Safety

- Some explicit dollar value is assigned to a system for each significant inherent hazard known to exist → All relative values which affect the inputs or outputs of the system have been transformed into absolute values.
- The cost of eliminating a single hazard is relatively small when there are a large number of hazards inherent in a system
- The cost becomes relatively large as the number of inherent hazards remaining in the system approaches zero.
- It would need an infinite amount of money to eliminate all hazards
- Assessment of the value of safety in absolute terms – cost

Example with car's safety features