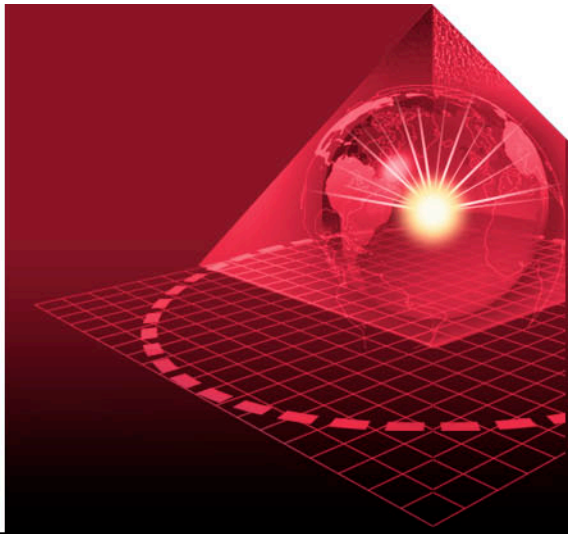
Systems theoretic safety in a Process Safety world



Simon Lucchini & Stephen Johnson

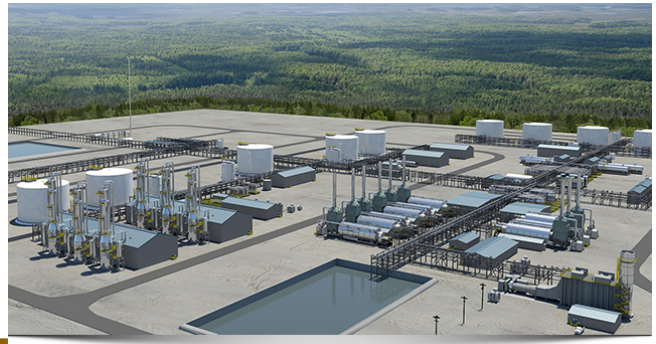
ESW Oct 2015

FLUOR®

Energy and Chemicals Facilities

← Refineries

Liquified Natural Gas (LNG) plants →



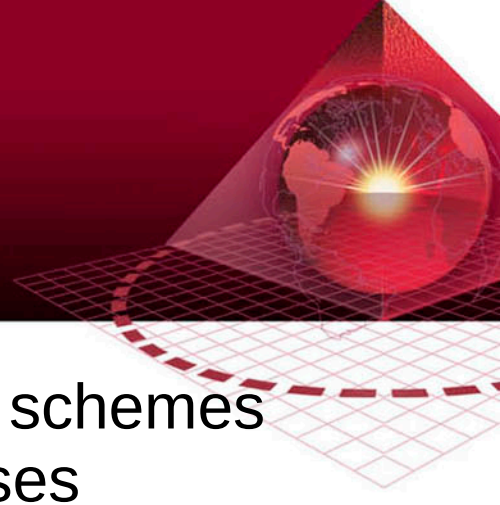
←Oil Sands

Chemical plants →

Terms of art

- Process Hazard (PHA) – one of the principal reviews used in the industry. A brainstorming analysis performed at multiple stages of design development, typically focused on error & failure propagation. HAZOP, Fault tree and “What-If?” are types of PHA.
- Process safety – A means for preventing and mitigating accidents. (Fires, explosions, toxic releases, spills , pollution, and economic losses)

Design HSE in Energy & Chemicals Industries



- Most operating companies (OPCOs) have schemes to maintain information about their processes including:
  - Basis of design data on safe operating limits
  - Hazard analyses, both qualitative and quantitative
  - Means for orderly management of change
  - Some analysis of systems interaction (functional safety, etc.)
  - Maintenance and performance testing systems (reliability calculations, etc)

The spectrum of Design HSE capabilities

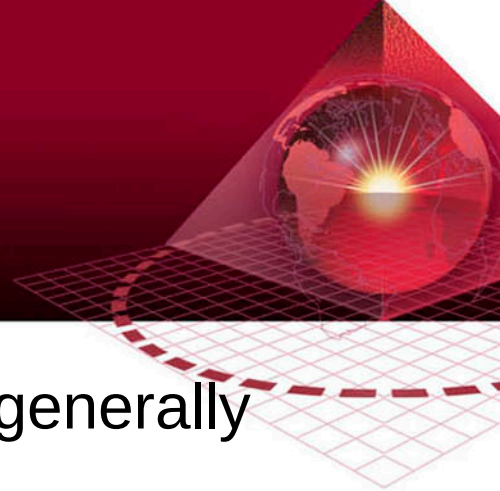
- Design HSE capabilities range from fairly sophisticated corporate level programs to very limited ad-hoc responses. They may be summarized as:

1. Opinion based safety
2. Math, models and methodology
3. Constraints and sociotechnical systems

Challenge of large scale capital projects

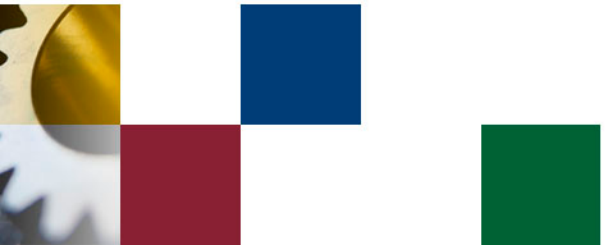
- Major Engineering firms works primarily in new build large capital projects, with some sustaining and revamp scope.
- This presents an opportunity to escape past bad practices, challenges to overcome
  - pressure to reduce capital costs
  - compressed schedules and out of sequence execution
  - globally distributed design & fabrication
- Quality of the facility (equipment and of design) can often be impacted adversely

Barriers to progress



- What prevents operating companies from generally adopting the safety theoretic approach?
- Issues to address:

1. Unknown unknowns
2. Hollowing out of expertise
3. The paradox of sophistication
4. Real world versus ideal behavior



Unknown unkowns

- Applies principally to less sophisticated OPCOs, and relates to their not being very aware of even the considerations associated with process safety, let alone the concepts of the systems theoretic approach
- Problem of risk (and perceived risk) as a function of organisational scale – a single plant new operator may see risk very differently than a company with a long history of global operations

Hollowing out of expertise

- At one time, most OPCOs had significant expert groups who had fairly significant organizational reach to ensure that design norms were followed.
- In many cases, such central authority groups may still exist, but often with much mores slender resources, and far more limited authority.
- The net result of this is that organizations have much less incentive / ability to progress towards more sophisticated techniques

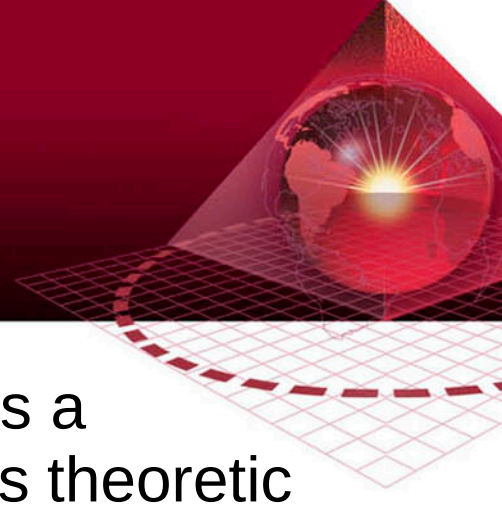
The paradox of sophistication

- For organizations which do retain reasonable levels of expertise, a paradoxical situation may arise,
- Well implemented traditional programs may well have (relatively) high performing results,
- There is a reduced incentive to take on new approaches

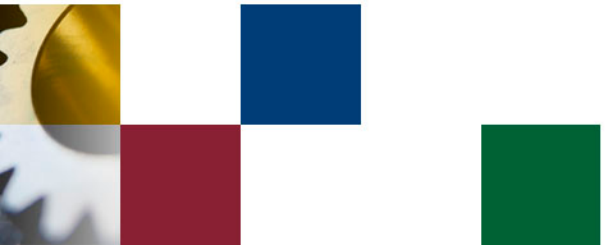
Real world versus ideal behavior

- A real problem for OPCOs is acknowledging that many unsafe conditions arise from real incentives that may push organizations into unsafe states
- A significant example from the hydrocarbon processing industry being the relentless pressure to reduce maintenance costs and avoid capital upgrades, which can lead over time to incidents such as Bhopal and Texas city.

Opportunities for improvement



- The whole world of process safety provides a reasonable basis for evolution into systems theoretic approaches by incremental change
- Process Hazard Analyses – and, especially, HAZOP were developed for use in sequenced engineering projects –out of sequence project execution is increasingly problematic
- Semi-quantitative techniques represent a place to introduce more systemic thinking



A framework to update

- First and foremost, a process safety program provides a systematic approach to design safety which can be co-opted towards a systems theoretic approach,
  - by integration of theory of constraints
  - recognition of the interactions of systems and people within a sociotechnical matrix

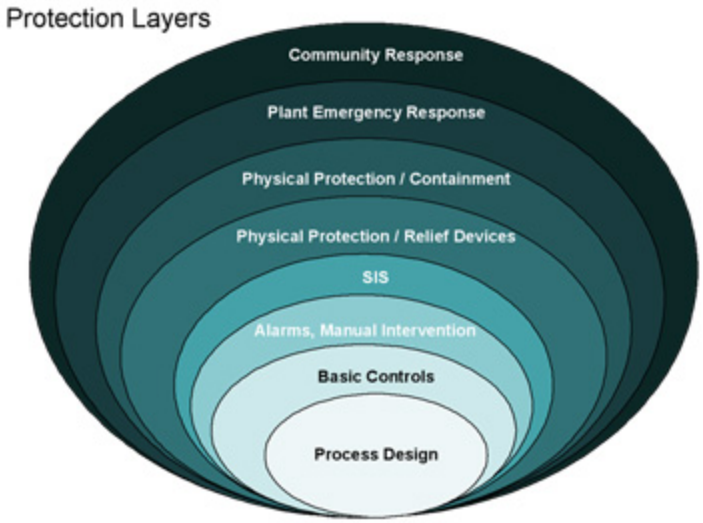
Process Hazard Analysis

- Process hazard analysis reviews – and particularly the HAZOP technique sit at the core of a lot of corporate design HSE programs.
- Schedule and resource constraints, however, often dilute such programs into limited utility.
- STPA offers a potentially more time efficient approach, as well as the benefit of potentially improving safety performance.

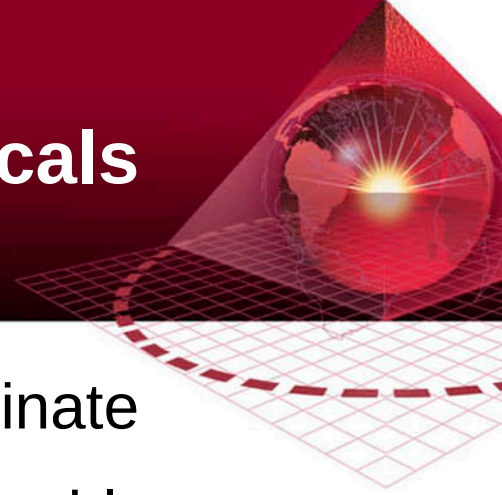
Semi-quantitative opportunities

- These are a fairly new technique in E&C, which have achieved considerable acceptance, not least because they can be used where risk matrices break down
- Currently heavily integrated with PHA, we believe it's desirable to separate them, especially if we are to push towards bowtie techniques preferentially to LOPA

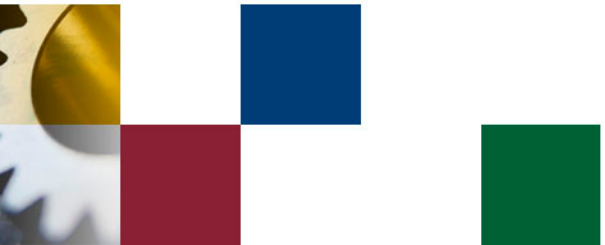
Comparison of LOPA and Bowtie



The near future, in Energy & Chemicals



- Statistical risk models will continue to dominate
- Semi-quantitative techniques offer considerable room for methodological improvement
- There is room for introduction of STPA as a replacement for PHA, especially in areas of particular concern or sensitivity



Ethylene Oxide example