A simple end-to-end guide to COMAH report writing and Management

Mark Manton & Brad Eccles, ABS Consulting, Warrington, UK

There are hundreds, if not thousands, of pages of regulation and guidance on the Control of Major Accidents and Hazards Regulations, 1999 (COMAH), but it is all actually quite simple. COMAH just demands that you "demonstrate" that you have:

1. Assessed the risks of fatalities and Major Accidents to the Environment (MATTE), i.e. performed:
   - HAZOPs and/or developed BowTies to identify the major accident hazards (MAH), and
   - Consequence modelling to determine the maximum number of potential fatalities, or the extent of potential MATTEs, from the unmitigated MAH events.
2. Identified and implemented the barriers to firstly reduce the frequency of the MAH event and secondly to mitigate the consequences should it occur. Plans are also required to maintain barrier effectiveness, e.g.:
   - preventative maintenance of critical equipment and
   - correct execution of Critical Activities, including competence assurance of relevant personnel.
3. Defined actions to take if all barriers fail, i.e.
   - incorporated the worst case scenarios in your emergency response plans

Overall this approach is best described by the schematic at the heart of the presentation (Figure 1).

The summary of the above process should be the COMAH Safety Report and this needs to be a "live" and practical document rather than one that sits on a library shelf. Our recommendation is to break the report down in to logical sections between the site-wide issues, owned by the HSE Manager, and separate sections "owned" by each unit manager with appropriate delegation of the upkeep to the unit's process engineer.

By considering the three elements above and keeping the safety report "live", COMAH compliance should be a straight-forward exercise.

Introduction – Understanding Process Safety Management

Process safety management (PSM) involves two primary components:

- **Process safety culture** which encompasses all aspects of how humans interact with the plant. Examples include a company's process safety policy, leadership by site management and site-wide processes and procedures such as Permit to Work (PtW), Management of Change (MoC) and Competence Management
- **Technical process safety**, covers the issues of identifying the MAH scenarios, determining the threats and consequences, implementing sufficient mitigation and maintaining the effectiveness of safety critical equipment and critical activities.

Managing these two aspects is key to achieving safe operation. Once the site management have a PSM baseline in place a further stage is to justify to the CA (Competent Authority of the HSE and the Environment Agency (in England)/Scottish Environment Protection Agency/Natural Resources Wales) that the residual risks have been reduced to as low as is reasonably practicable (ALARP). This will typically involve some Quantitative Risk Assessments (QRA) or Layer of Protection Analysis (LOPA) and cost-benefit analyses (CBA). A summary of this process is then the COMAH Safety Report.

COMAH is simple, but with thousands of pages of guidance and, superficially conflicting opinions, it can appear complex. For example, the COMAH report for a simple site such as a terminal with only a few tanks can reach 400 pages. For a top tier COMAH site such as a chemical complex or refinery it is no longer possible to cover each scenario in depth, so representative sets are needed and even then the reports may be many volumes long. An objective is to demonstrate that the risks have been reduced to ALARP for the entire system, but the reports can be so cumbersome, that they can be difficult to comprehend to all but the most dedicated interpreters. Those who really need to understand PSM - senior managers and front-line operators - need help to overcome the complexities so that they can perform their activities which are critical to preventing the MAHs.

Background: PSM in the UK

The key regulatory driver for safety management in the UK is the Health and Safety at Work Act, 1974, (HSWA, UK Government, 1974) where Articles 2.1 and 3.1 state:

> "It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees."

And

> "It shall be the duty of every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health or safety"

The remaining 116 pages of the Act just support these requirements which in effect mean:

- "We" are not going to tell you what to do, and
- If anyone gets hurt, then, by definition, you have not done your **duty**.

In effect you are in breach of the Act unless you can demonstrate that you have implemented "All Measures Necessary" (so far as is reasonably practicable) to manage the risk.

Since the promulgation of the HSWA, the UK became part of the EU which brought a slightly different approach. Safety legislation in other European countries is more compliance-driven with regulators telling operators what to do rather than the UK's risk-based approach which set goals rather than prescribing solutions. The combination of the two cultures led to the EU's Seveso-II directive (EC, 1996) with the key clause referring to the Safety Report (Article 9) being that:

1. Member States shall require the operator to produce a safety report for the purposes of:
    a) demonstrating that a major-accident prevention policy and a safety management system for implementing it have been put into effect …
    b) demonstrating that **major-accident hazards have been identified** and that the necessary measures have been taken to prevent such accidents and to limit their consequences for man and the environment;
    c) demonstrating that adequate safety and reliability have been incorporated into the … **operation** and **maintenance** of any … equipment … connected with its operation which are linked to major-accident hazards …
    d) demonstrating that internal emergency plans have been drawn up and supplying information to enable the external plan to be drawn up in order to take the necessary measures in the event of a major accident;

So HSWA simply tells you not to hurt anyone and Seveso-II (or COMAH, as it is implemented in the UK), tells you to "demonstrate" that you have

- really thought about how you could hurt someone
- done something about it in terms of [safety critical] equipment and [safety critical] activities/operations
- plan for the possibility that the preventative measures don't work and everything goes wrong

And that is all you ever really need to know about PSM and COMAH in the UK!

However:

- operators "needed" more guidance so we have the L111: Guide to COMAH Regs (HSE, 2006), HSG-190 Preparing Safety Reports (HSE, 1999), Off-site Emergency Planning guide (CA, 2010), PSLG (Buncefield) guidance (PSLG, 2009), ALARP Suite of Guidance (HSE, 2003) and SPC-PERM-37 (HSE, 2012), etc., etc.
- we have top tier and lower tier COMAH sites and
- the CA have to read the many reports they receive and to judge them. The outcome then is the Safety Report Assessment Manual (SRAM; HSE, 2011) a 109 page document to tell CA personnel how to assess the reports, which effectively acts as further guidance on how to write the report.

So it is not surprising that COMAH is perceived as complicated.

The provision of more detailed guidance from the regulator can lead to a conflict between how the CA want the information presented and how the operators function and operate and, for multinationals at least, how they follow corporate process safety policies.

One way out of this conflict is to delegate the writing of the COMAH report to consultants. Unfortunately, while simple for the operator, it can have devastating consequences. An extreme example of this was the crash of the RAF Nimrod that cost 14 lives. The Nimrod Review (Haddon-Cave, 2009) summarised the issues with the Safety Case as follows (pg 11):

14. The Nimrod IPT [Integrated Project Team]

- inappropriately delegated project management of the Nimrod Safety Case task to a relatively junior person without adequate oversight or supervision;
- failed to ensure adequate operator involvement in BAE Systems' work on Phases 1 and 2;
- failed to project manage properly, or to act as an 'intelligent customer' at any stage;
- failed to read the BAE System Reports carefully or otherwise check BAE Systems' work;
- failed to follow its own Safety Management Plan;
- failed properly to appoint an Independent Safety Advisor to audit the Nimrod Safety Case; and
- signed-off BAE Systems' work in circumstances where it was manifestly inappropriate to do so.

Subsequently, the Nimrod IPT sentenced the outstanding risks on a manifestly inadequate, flawed and unrealistic basis, and in doing so mis-categorised the catastrophic fire risk represented by the Cross-Feed/SCP duct (Hazard H73) as 'Tolerable' when it plainly was not. The Nimrod IPT was sloppy and complacent and outsourced its thinking.

And (p 259):

3. Unfortunately, the Nimrod Safety Case was a lamentable job from start to finish. It was riddled with errors. It missed the key dangers. It was essentially a 'paperwork' exercise. It was virtually worthless as a safety tool. The defining features of the four years it took to produce the Nimrod Safety Case are high levels of incompetence, complacency and cynicism by the organisations and key individuals involved.

And so recommended (p 533):

7. Safety Cases should be renamed "Risk Cases" and conform in the future to the following six Principles:
    - Succinct;
    - Home-grown;
    - Accessible;
    - Proportionate;
    - Easy to understand; and
    - Document-lite.

So the risks of getting it wrong are real, substantial and potentially fatal. The rest of this document proposes a way out of this malaise and to ensure that "operations" is involved in its creation but not overwhelmed by it.

The COMAH Report

Schematic Overview for Managing PSM & Facilitating COMAH Reports

In ABS Consulting in the UK we developed the schematic shown in Figure 1 to define the overall flow of information for process safety management. We believe that this gives a good overview from the initial scenarios through to the COMAH (Safety) Report for full compliance with the COMAH Regulations. Visual bowties greatly facilitate communication and "simplify" the process.

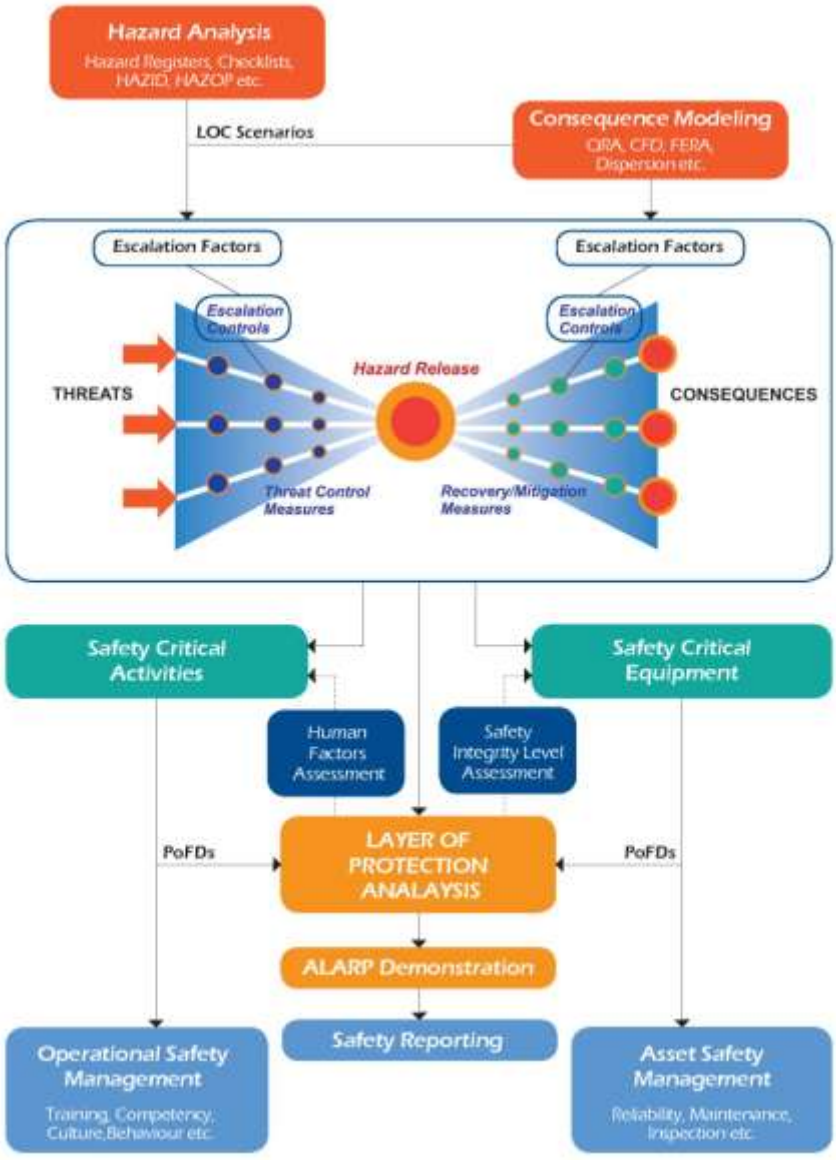

Figure 1: End to end process safety management schematic

The COMAH report is divided in to two main sections, a generic site-wide section and then unit-specific sections.

Generic Section of COMAH Report

The generic section provides the simple statements of facts such as operator name and address, volumes of materials stored on site and the generic issues such as the Hazard Registers, corporate risk assessment matrix (RAM) and methodologies used to "demonstrate" that the risks have been reduced to ALARP. These aspects should not change much with time.

Hazard Register

The hazard register is a simple list of the hazardous material on a site that have the potential for significant people and environmental consequences. The data is extracted from Material Safety Data Sheets (MSDSs) and ranked according to the corporate RAM.

Unit-Specific Section of COMAH Report

The unit-specific sections are the heart of the report and the parts that need to be kept "live". They contain the actual definitions of the MAHs and how they are managed. We highly recommend that the unit-specific sections are "owned" by each unit manager with maintenance of the document (e.g. when modifications are made to the unit via the Management of Change process) delegated to the process (chemical) engineer responsible for that section.

Scenario definition

HSG-190: Preparing Safety Reports (HSE, 1999) clearly defines this element as follows:

> 293 There are three steps in preparing information about all major accident scenarios:
>
> a) identify all the possible major accidents;
>
> b) give a realistic estimate of the likelihood of each major accident hazard or an adequate summary of initiating events to support (a); and
>
> c) produce an adequate assessment of the extent and severity of the consequences for each identified major accident hazard.

There are two possible approaches to defining the MAHs:

- Brainstorming: using a very experienced team, following guidelines, e.g. HAZID, and then identifying the MAH scenarios.
- HAZOPs: these provide a line-by-line review of the units and so a clear bottom-up definition of all possible MAHs. The advantage of HAZOPs are the clear demonstration, to the CA, that all potential MAHs have been considered. The demonstration may be logged via a simple spreadsheet or using commercially available software. The advantage of using software, such as ABS Consulting's Leader™ software (ABS, 2012), is that it acts as a structured database for logging the discussions and extracting the lists of follow-up actions, critical equipment and critical activities. Other commercial packages performing similar functions are also available.

The CA is only concerned with MAHs that affect people or the environment (the M in MAH stands for major). The list of scenarios that have potentially fatal consequences for people or environment therefore constitute the list of all MAHs. We would typically expect a simple chemical plant unit to have an order of magnitude of 50 potential MAHs and increasing up to an order of magnitude of 1,000 for a complex site such as a refinery or chemicals complex.

Bowties

The strength of HAZOPs is in their in-depth review of the unit's process safety risks. A downside of HAZOPs is the volume of tables produced and the complexity of communicating the content to the people who really count, i.e. those who could be killed by the MAH (mainly unit operators) and those who have roles in preventing the fatalities (i.e. management, maintenance and the operators themselves). Bowties are a useful means of facilitating this communication in that they visually display the MAH scenario and the threats, controls, risk reduction measures and potential consequences. These may be drawn by hand or by using commercial software packages such as ABS Consulting's THESIS software (ABS, 2012). An advantage of using both Leader™ and THESIS BowTie™ is that they are integrated so THESIS effectively acts as the graphical interface for the HAZOPs produced via Leader™.

Tank overfill Bowtie example

Figure 2 shows an example of a bowtie for the MAH scenario of tank overfill from materials that can form vapour cloud explosions (*à la* Buncefield). This MAH was investigated as a follow-up to the Buncefield Report (PSLG, 2009) by a working group of the Chemicals and Downstream Oil Industry Forum (CDOIF) with representatives of both the trade associations and the CA and recently published in the "Other Products in Scope" guidance (CDOIF, 2012). The threats and barriers are taken from that guidance.

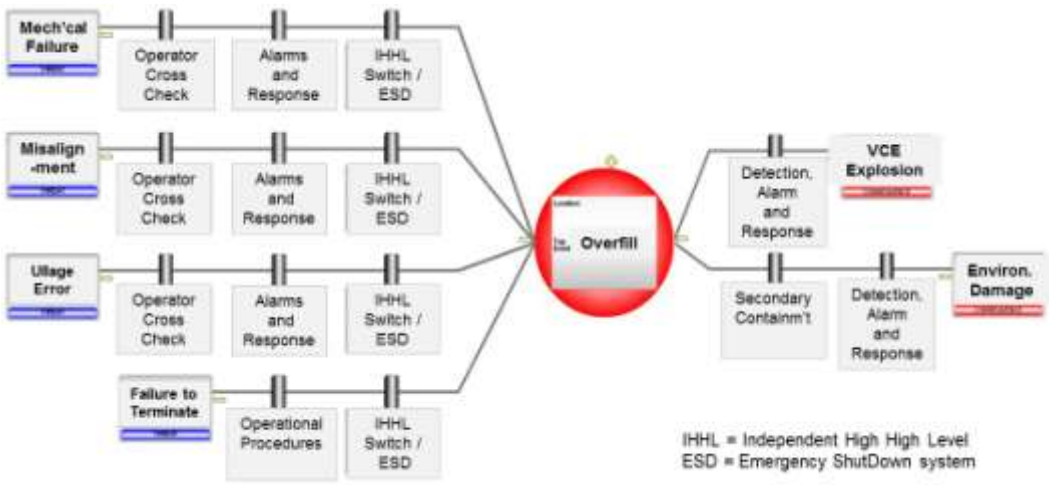

Figure 2: THESIS BowTie™ schematic of the MAH of tank overfill, as per the CDOIF "Other Products in Scope" guidance (CDOIF 2012)

Critical Equipment

Equipment listed as safeguards in HAZOP threatlines with potentially fatal consequences and/or the barriers, or threat control measures, in the bowtie therefore constitute the list of [safety] critical equipment (CE) to prevent the potential consequence from arising. These may be readily extracted from the databases.

Typically there will be an order of magnitude 100 items of critical equipment per unit. These will be instrument alarms, process controllers, critical non-return valves, trip systems and relief valves.

Other Critical Equipment

HAZOPs mainly detail the scenarios and barriers that lead to the top event, typically, of a loss of containment (LOC). The barriers on the right hand side of the bowtie, the recovery mitigation measures, are present to minimise the consequences of an LOC. They are largely associated with Emergency Response (ER) and need to be identified via a separate review. Examples of such equipment include pumps to supply and remove firewater, snuffing steam, critical insulation & fireproofing, restriction orifices and sewers for removal of firewater.

Tank overfill example

The CEs for the tank overfill example (Figure 2) are the tank level gauges, tank level alarms, the independent high-high level (IHHL) alarm/switch/shut-down system, and, as part of the mitigation barriers, the leak detection and alarm (when present) and the bunds/secondary containment surrounding the tank.

Critical Activities

Where the safeguards in the BowTies and HAZOPs refer to procedures then these are the critical activities (CActs) associated with the MAHs. There may again be grouped:

- Operator actions where human intervention is the primary barrier (threat control measure) to prevent an MAH, e.g. operator activities during start-ups, shut-downs and emergencies.
- Monitoring longer term trends that if not managed could lead to an MAH, e.g. fouling monitored by process engineers and corrosion rates monitored by corrosion engineers
- Maintenance procedures to ensure that critical equipment is correctly scheduled for maintenance, correctly maintained and correctly returned to service after maintenance
- Site-wide process safety management processes and procedures such as: management of change, control of area occupancy, permit to work process, Learning from Incidents (LFI), etc.

The approach for these CActs (for logging in the COMAH report), is to:

- Extract all activities and actions performed by people which appear as safeguards in HAZOPs and BowTies with threatlines potentially leading to fatal consequences
- Check that all activities are documented in written work instructions, or write such instructions when missing.

- Recover the list of work instructions associated with preventative maintenance (PM) tasks on critical equipment
- Have a business processes in place to ensure appropriate training and refresher training for these critical activities and also for auditing of the procedures.

Tank Overfill Example

The CActs for the tank overfill example (taken from Figure 2) are:

- Operator actions: calculation of the available ullage, switching the tanks at the start and end of a run/batch and responding to alarms.
- Monitoring: operator cross-checks
- Maintenance: scheduling PM of the tank level gauge and IHHL alarms/switch and correct returning to service

ALARP Screening

Having defined the MAHs, the next step is to "demonstrate" to the CA that risks of fatalities and MATTEs have been reduced to ALARP. HSE guidance on the risk assessment methodology as originally described in the "Reducing Risks, Protecting People" (R2P2; HSE, 2001) and has been expanded upon in the ALARP Suite of Guidance (HSE, 2003) and SPC-37 (HSE, 2012) and shown schematically in Figure 3. This figure also suggests the different levels of analysis required with QRA when near the tolerability boundary through semi-quantitative methods (SQ, e.g. LOPAs) to qualitative (Q) approaches as the level of risk reduces. This covers the issues for potential fatalities. The approach for MATTEs has recently been developed by another CDOIF Working Group (CDOIF, 2013) and is also being presented by the EA, on behalf of CDOIF, in this conference (EA, 2014).

The different tools for risk assessment were summarised in the PSLG report (PSLG, 2009) as shown in Figure 4.

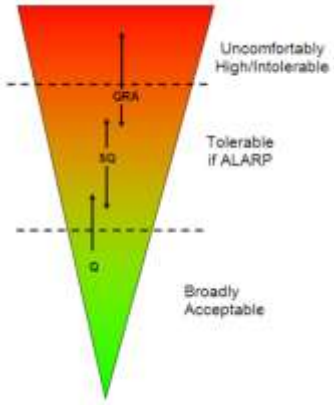

Figure 3: HSE guidance on risk assessment

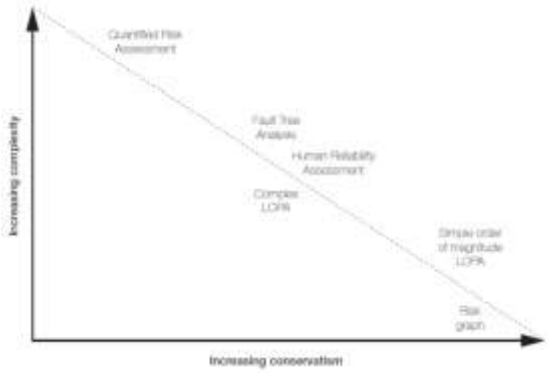

Figure 4: Relationship between different risk assessment methodologies (Figure 21 in PSLG Report)

Simple qualitative risk assessment, as used in HAZOPs, provides a good screening for residual risk from each scenario. It would therefore be suitable for those risks that are low and close to the broadly acceptable range (10^{-6} fatalities per year). However, it may not be sufficient to demonstrate that the residual risks have been reduced to ALARP for risks that are closer to the Tolerability limit (10^{-4} fatalities per year). Detailed demonstration of ALARP is not normally required on the complete set of MAHs but rather only on a smaller representative set. A key element will therefore be defining the representative set and to perform the consequence modelling on these scenarios.

Representative Set

The first step in defining the representative set is to extract the list of all MAHs with fatal people/environmental consequences from the existing BowTie or HAZOP reviews. Once these have been combined then there may well be common root causes for the MAHs (e.g. corrosion leading to an LPG leak on different units) or common consequences (pool fire, BLEVE's, etc.). Cross-referencing and reviewing the MAHs will logically lead to a set that cover most issues. It is important that these should include some of the largest MAHs but also some of the smaller MAHs (resulting in non-fatal injuries and small MATTEs).

ALARP Demonstration

The process to be followed would then be to:

- Develop the representative set. For a complex site of up to 1,000 scenarios we would expect there to be about 100 scenarios for the representative set
- Integrate the resulting list with existing fire and explosion consequence modelling and site-wide Environmental Risk Assessments (ERAs; CDOIF, 2012) and perform the required consequence modelling when not available.
- Perform LOPAs or QRAs for the MAHs in the representative set. If the residual risk is "Intolerable" as per HSE guidance (HSE, 2003 and HSE, 2012) then improvements are mandatory.
- Cost-Benefit Analysis (CBA) for the LOPAs and QRAs in the representative set to determine whether the costs of adding another barrier are Justified, or Grossly Disproportionate, to the risk reduction that would result.
- If improvements are Justified then these need to be included in the Action Plan of the COMAH Report.

This output would then provide the complete risk assessment for the COMAH for individual risk. Work would then be required for Societal Risk.

Societal Risk

The CA guidance for societal risk is not fully clear and consistent. For people risk this may well most easily be satisfied by using an Occupied Buildings Risk Assessment (OBRA). For the environment the desire of the EA is to combine the various scenarios that could result in a MATTE in order to arrive at the sum of the possibilities for each receptor, i.e. the CDOIF methodology (CDOIF, 2013)

Conclusions

Overall the ideal approach for the development and management of a COMAH report for a substantial site is then:

- Generic sections: typically only needing an update from earlier versions of the COMAH Report
- Unit-specific sections:
    - HAZOPs for each unit
    - extract MAHs from the HAZOPs
    - extract Critical Equipment and Critical Activities from each HAZOP
- Representative set
    - Combine all MAHs
    - Determine the Representative Set.
    - Define all possible consequences using existing or new consequence modelling
- Societal Risk
    - Extrapolate from the representative set to the site as a whole and compare to acceptable levels as per R2P2

This is shown schematically in Figure 5.

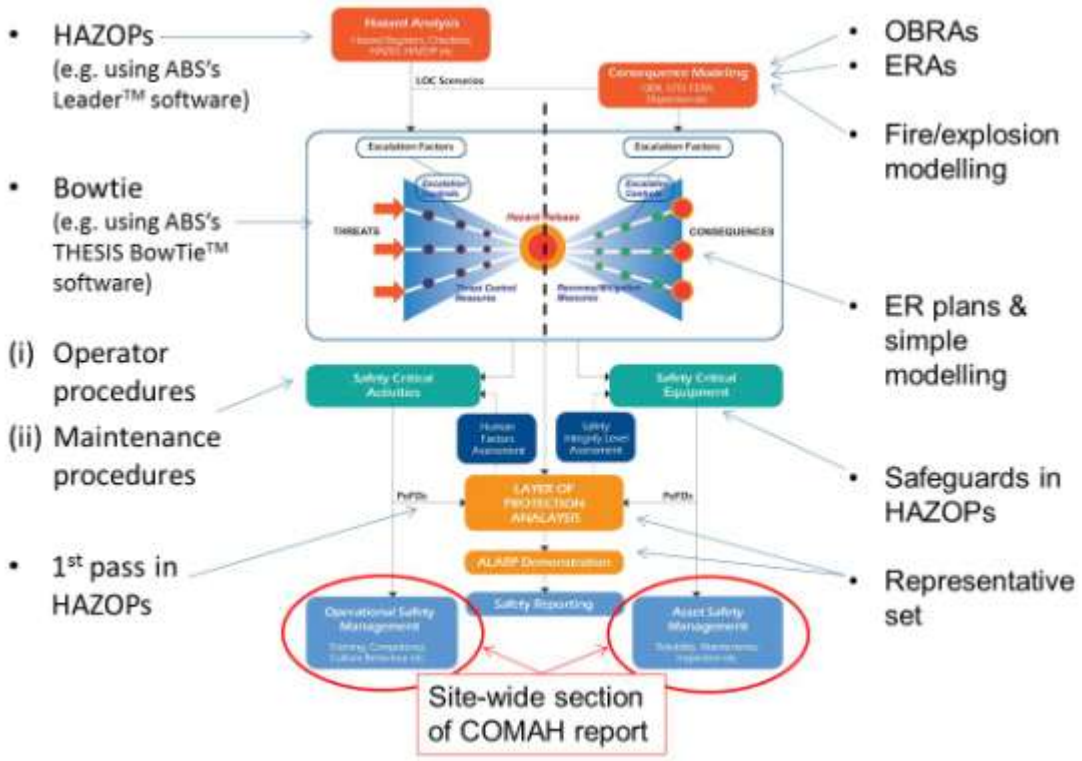

Figure 5: Overview schematic with guidance on solutions per step

- Practically the best approach would be to produce the draft report for a single unit and share with the CA before starting the further effort to rewrite the whole COMAH report

References

1. UK Government, "The Health and Safety at Work Act" (1974): http://www.hse.gov.uk/legislation/hswa.htm and http://www.legislation.gov.uk/ukpga/1974/37/contents
2. European Commission (EC), Seveso-II Directive, European Council Directive 96/82/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1996L0082:20031231:EN:PDF
3. HSE, "L111 Guide to the COMAH Regulations", 2006: http://www.hse.gov.uk/pubns/books/l111.htm
4. HSE, "HSG-190 Preparing Safety Reports", 1999: http://www.hse.gov.uk/pubns/books/hsg190.htm
5. CA, "Off Site emergency planning", 2010: http://www.hse.gov.uk/comah/guidance/off-site-emergency-planning.pdf
6. PSLG, "Safety and Environmental Standards for Fuel Storage Sites", 2009: http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf
7. HSE, "ALARP Suite of Guidance", 2003, http://www.hse.gov.uk/risk/theory/alarp.htm (accessed Jan 2014)
8. HSE, Semi-Permanent Circulars-Permissioning-37: Guidance on ALARP Decisions in COMAH, 2012 (accessed Jan 2014), http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/
9. HSE, "Safety Report Assessment Manual (V2)", 2011: http://www.hse.gov.uk/comah/sram/index.htm (accessed Jan 2014)
10. Charles Haddon-Cave QC, The Nimrod Review, October 2009: http://www.official-documents.gov.uk/document/hc0809/hc10/1025/1025.pdf
11. ABS Consulting, Leader™ software (2013): http://www.absconsulting.com/leadersoftware/index.cfm (accessed Jan 2014)

12. ABS Consulting, THESIS BowTie™ software (2012): http://www.absconsulting.com/%5C/thesis/index.cfm (accessed Jan 2014)

13. CDOIF, "Other Products in Scope", Version 5, issued 3/12/2012: http://www.hse.gov.uk/aboutus/meetings/committees/cif/pslg-other-products.pdf

14. HSE, "Reducing Risks and Protecting People (R2P2)", 2001: http://www.hse.gov.uk/risk/theory/r2p2.pdf

15. CDOIF, "Environmental Risk Assessment", Version 1 issued 18/9/2013: http://www.hse.gov.uk/aboutus/meetings/committees/cif/environmental-risk-assessment.pdf

16. EA: M Nicholas, Environment Agency; I Brocklebank, SEPA; J Coates, CIA; P Davidson, UKPIA; H Bray, TSA: Environmental Risk Tolerability for Major Accident Hazard Sites - A Method for Quantifying and Assessing Environmental Risk. Hazards 24, Edinburgh, May 2014