

Formalising Communication On Potentially Catastrophic Safety Projects



Nicholas Hales examines the retrospective and thereby hypothetical use of portions of a seven layer data safety model in the design, implementation and operation of the Chernobyl RBMK reactor, and how that would have made avoidance of the disaster far more probable. Nicholas proposes a model for the safety issues in all potentially catastrophic projects, stretching from Board Room to safety experts and operators.

On Saturday 26 April 1986, the No. 4 nuclear reactor in the Chernobyl Nuclear Power Plant exploded. The reactor had entered a meltdown situation which was entirely preventable. Like many catastrophic accidents, a whole series of oversights, mistaken behaviours, design faults and communication failures led to the accident.

The main data related reasons are as follows:

1. Operational problems in the earlier small prototype were not advised to the Chernobyl project manager. (Data missing)
2. Disagreements among experts in the reactor design agency about the safety of the design were not resolved and the fact that disagreements existed was suppressed. (Data suppressed)
3. The Chernobyl reactor was so large that what was going on in one part, about which there was sensor-supplied understanding, did not necessarily reflect what was happening in another area of the reactor. (Data not available)
4. Tests to be conducted went ahead late at night after management with safety responsibilities, that should have been consulted, had gone home. (Data maintaining safety processes ignored)
5. The shutdown process was much slower than necessary, so that the material on the tips of the control rods actually allowed acceleration of the reactions for a few critical seconds when emergency shutdown of the runaway reaction was absolutely essential. (Reported design and operation data ignored)

This article examines the retrospective, and thereby, hypothetical use of portions of a seven layer data safety model in the design, implementation and operation of the Chernobyl RBMK reactor, and how that would have made avoidance of the disaster far more probable. In doing so, a model for the safety issues in all potentially catastrophic projects is proposed, stretching from Board Room to safety experts and operators, and which is compatible with actual engineered projects. The comprehensive source document for much historical fact comes from "Midnight in Chernobyl", [1]. The recommendation is for openness about safety data and principles, both between members of an enterprise and stakeholders in associated enterprises, notwithstanding the need for secrecy in cyber-attack capability etc. In short, communication is what it is all about, but safe communication.



Layers previously not considered formally safety-critical are engaged in the on-going safety process, namely layers 7-6, running from Enterprise to Organisational Unit as illustrated in Figure 1. Layer 5, known as the 'Optimising' layer in the original Data Safety Guidance version 1.3 document [2], is also reviewed. The safety issues are isolated by considering the idea of a vertical tranche in an organisation, like an annex, such that the ordinary working of the Enterprise is unaffected by the necessity for the higher two data safety layers 7 and 6 to be involved in safety-critical data issues without all working becoming absurdly cumbersome. The use of it brings a quasi-military approach to command structures with feedback, as in modern military command structures. It is not dissimilar to how machines operate, where we humans input commands at a high level and expect that our intent will not alter, no matter how deep into the machine the command goes, via various translations to

machine code and binary numbers, to communication with another machine and the sending of the data back up to the Human Computer Interface of another machine. Thus, the data model provides a template for process and procedure dissemination, command, maintenance process approval and design, whenever critical safety is involved.

The question of how to engage responsible management is answered. The top layers 7-6 are considered part of the safety related aspects. This then assigns responsibility ultimately, and in all cases, to the Enterprise. This is akin to how a Field Marshall has responsibility for the behaviour of sub-ordinates, such as a Colonel who gets his regiment captured. It thereby becomes a recommended model for financial Enterprises such as banks, where a lack of concern can lead to catastrophic consequences. An example of this is a Gaussian related theory refinement developed by Merton and Scholes, which won them the Nobel Economics prize in 1997. One year later, in 1998, their bank, the ironically named Long Term Capital Management,(LTCM), collapsed, taking a lot of Wall Street with them, because they had taken massive risks based on the infallibility of their model [4]. In this latter case the ultimate Enterprise is the financial regulating authority, which should have taken evidence from the doubters that enabled it to take a view on how much risk LTCM could take.

To recall, the seven layer data model that appeared in the first version of the Data Safety Guidance document, [2] is shown in Figure 1:

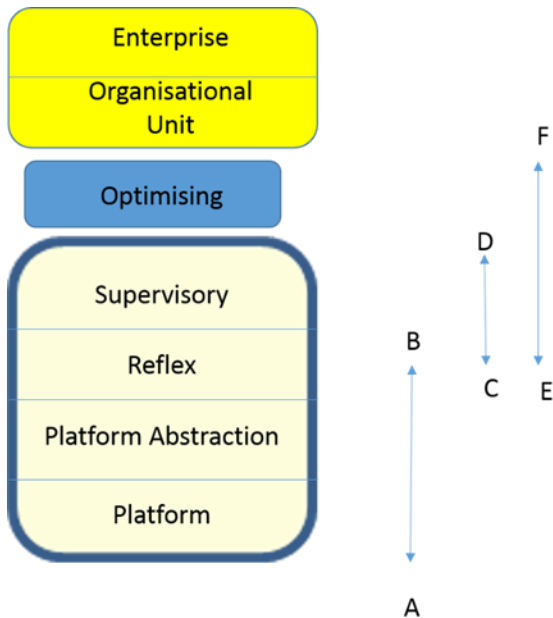


Figure 1

In the figure, as given in the original Data Safety Guidance document, line A-B represents the maximum jurisdiction of SILs 3 and 4, line C-D represents the maximum jurisdiction of SILs 1 and 2 and line E-F represents the combined SIL in a Computer Based Technology and/or human system. The proposition is that, in the context of data, that can simply be a piece of paper passed down through a hierarchy, some level of safety criticality must be assigned. Thus, in some future enquiry into a disaster, the degree of effort made to maintain safety integrity even up to the managerial layer can be asserted through the provision of evidence. It is not easy to prove 'best efforts' by all those involved in each of the Enterprises that makes up a project like Chernobyl, but the complex paths safe data needs to travel from initiation of a project at Government level, to the operational level many years later, are far more visible and thereby better assured than under some current business practices where management, having delegated, wishes not to be troubled by voiced concerns. The Boeing 737 MAX programme being one such where airline pilots and test pilots raised issues [5].

In starting a project, to minimise investment that may result in no return, some Enterprises involved may be linked to others in a minimal form or only using one or not all layers, until the full commitment is developed from established interactions. It should always be the case though that, initially, an Enterprise at layer 7 is created. People can be layers; the important principle being that, as in the 7 layer electronic model, they must be able to supply guaranteed data and receive dependent data safely. The principles can be applied at any abstraction level in safety engineering. It should be seen as a method of maintaining rigour in all aspects of safety related system production.

Due regard to data safety using this model should, as well as defining management responsibility, also ensure management awareness of the safety commitment required. The intention is that arguments over responsibility will not occur as the evidence will be available. That evidence should show that the full enterprise from layer 1 to layer 7 was cognisant of the risks and who was responsible so that all personnel would know exactly who to communicate with whenever issues arose.

It is possible to envisage situations where the Enterprise Layer has not been created. Then, the Enterprise considering setting up an Enterprise at a sub-ordinate layer (the Soviet Government in the Chernobyl case), would have communicated with experts, (from all-encompassing nuclear issue scientists at Sredmash, discussed later), who in time would remain consultants to an, as yet, not established Enterprise, Chernobyl, dedicated to the construction of the reactors. Thus, communication and the tasks of assuring data exchange is safe, begins with the Soviet Enterprise layer 1 communicating with Sredmash at layer 3 Optimising layer and above, without finalised evidence of the need for an Enterprise. Just as with staff turnover in safety cells in industry, there would need to be assurance that data safety expertise from this Enterprise was passed safely to the new Optimising, Organisational Unit and Enterprise layers in the new Enterprise that was to construct and operate Chernobyl.

None of what is written here in any way detracts from the principles of the latest edition of the Data Safety Guidance [3] document. It is intended to broaden the scope out to encompass the wider risks, where a narrow engineering view of software and electronics may lead to inadvertent exclusion of those risks.

The definitions of the model and their relation to the nuclear command structure in 1980s Russia are examined next. These are base starting point definitions, but as this theory progresses, the definitions may alter:

Layer 7 – The ‘Enterprise’ layer

The enterprise layer is the corporate entity, which in the case of the Soviet Union under the Communist Party, can be taken as the entire country as it saw itself as having a common purpose. The layer is defined as being responsible for the planning and execution of large scale changes to the infrastructure, responding to changes in legislation, setting and maintaining standards, procedures and competency requirements.

In terms of a communist monolith, the changes to the infrastructure and responding to changes in legislation equate to influences outside the enterprise forcing competition to produce cheap electricity, in other words, other countries. Setting and maintaining standards, procedures and competency requirements, more than educational and experience requirements at this level, implied membership of the communist party. This of course meant some talent would never achieve greatness for those who were considered less than committed to the party. The cracks then begin to show because data has a source and a sink and if the source is less than competent, the sink, whether human or machine, will not operate to best intent, though one may get away with it for a while.

Layer 6 – The ‘Organisational Unit’ layer

This layer is described originally as being responsible for delivery of the planned service. In the communist world this naturally describes the “Government”, as described in the Cast of Characters in [1]. The layer is described as not playing any part in the day to day running of the system, whatever it may be. Of course, in authoritarian societies that is exactly what happens and unfortunately the second level of cracks start to show as authoritarian means an understanding of the enterprise layer above but very little hands on understanding of the problems those delivering these dreams, in the lower layers of the system, have to deal with. The Data Safety Guidance further describes this layer as likely to become “involved in the short term operation of the system in response to a serious incident that causes substantial impact on the delivery of the system”. In the case of the explosion in reactor 4 at Chernobyl, this definition precisely describes the substantial impact on the Soviet Enterprise intent, to create machines that a perfect society could rely on to run smoothly and be able to outcompete the West. Hence what was required, was much closer safety data definition and communication, but that did not happen.

Layer 5 - The ‘Optimising’ layer

The optimisation layer is described as the most sophisticated control layer. The optimisation layer respects the performance and safety constraints of the underlying system and the information contingency plans. Crucially, this layer is described by the words “information demands on the optimising layer are high requiring a full understanding of the underlying system, the planned service and contingency plans.” This, in Chernobyl terms, represents “The Nuclear Experts” as also given in the Cast of Characters in [1]. They are spread over a number of organisations illustrated in Figure 2.

The Chernobyl Disaster

Below are some of the involved characters and Enterprises as defined by this article:

- Anatoly Aleksandrov – Chairman of the Soviet Academy of Sciences, responsible for nuclear technology development. – **Classed as an Enterprise** and also Director of the Kurchatov Institute – **Classed as an Enterprise**
- Nikolai Dollezhal - director of The Scientific Research and Design Institute of Energy Technology (Russian acronym NIKIET) – **Classed as an Enterprise**
- Victor Brukhanov – Director of Chernobyl plant – **Classed as an Enterprise**
- Efim Slavsky - Ministry of Medium Machine Building (Russian acronym 'Sredmash') – **Classed as an Enterprise**
- Leningrad Nuclear Plant (1st RBMK design) – **Classed as an Enterprise**
- Leonid Brezhnev - The Soviet Union – **Classed as an Enterprise**

So here we have one engineered Enterprise, (The Leningrad Prototype Reactor), four engineering Enterprises, an engineering project barely underway, (Chernobyl itself), and a political Enterprise that all the others serve, though there would be more in time, such as the Enterprises providing components and cement for the construction of the Chernobyl reactors. All of whom could have functioned more efficiently, had data safety level Enterprise analysis been a design criteria throughout the industries involved.

Early in the development of the Chernobyl Plant, when only the director had been appointed, the 7 layer data model may have looked something like figure 2. As can be seen, Victor Brukhanov has been appointed director but without sub-ordinate levels at this stage. This then dates to early 1970. Problems with the first RBMK, the Leningrad Reactor, needed to be reported by the operator to whomsoever had taken the role of optimising at Layer 5. To recap, that person must understand how it should operate, the planned service and contingency plans, how the operations are to be achieved and what the safety plans were. Where that information should have gone is shown on the diagram. What actually happened and the relation to data types is given in the discussion below.

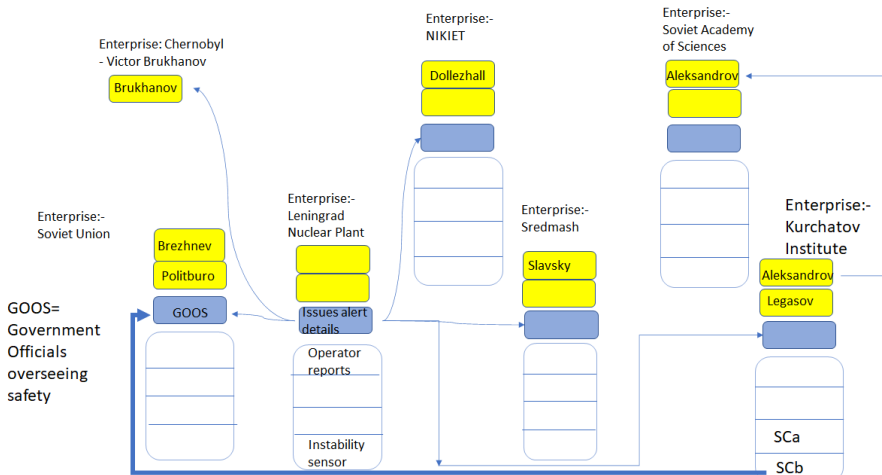


Figure 2 - Chernobyl Related Enterprises in 1970 and Some Illustrative Links

Here are some examples to illustrate how 7 layer diagrams simplify the visualisation of what should have happened and if used from the design stage, could help prevent disaster in the future. It is proposed that this type of diagram will enable the construction of safety cultures by the simplicity that pictures afford, (the actual story of Chernobyl, in written words only, is quite complex to grasp). The simple idea is to observe where data should have gone and where it either did not leave, was not received or was suppressed on the journey.

Note:

- a) The Politburo is used as an embracing term in the Soviet Union Enterprise to include the Soviet Council of Ministers and the Central Committee of the Communist Party.
- b) Aleksandrov had a position as director of both the Academy and the Kurchatov Institute so a link is given there
- c) The Leningrad reactor lower layers, (1-3) are actual machines producing data for the layer 4 operator.

The Leningrad Reactor problem

By 1973, the first ever RBMK reactor had started up. Its construction had been ordered by Sredmash. Aleksandrov and Dollezhall were there witnessing it. Soon after start up, faults became apparent. Earlier at the Kuchatov Institute a scientist, (SCa in Fig 2), warned that the design was too dangerous and another, (SCb), warned that the positive void coefficient made the reactor susceptible to explosions. This latter scientist has been positioned at the bottom of the



Enterprise to bear some resemblance to the original 7 layer data model intent in Figure 1, i.e. dealing with the highest Data Safety Assurance Levels or DSALs in the lower orders. The positive void coefficient made the Leningrad reactor harder and harder to control as it reached the latter part of its three year maintenance cycle. In terms of the Data Safety Guidance document there are issues for 'training', 'design' and other data types, which did not change despite the known problems emerging at the Leningrad plant, thus nothing was added to the manuals for the reactors. The alarm bells rung by SCb were ignored and although attempts were made to sack him, his letters eventually reached the Soviet Council of Ministers (the thick line on the diagram). Too late though, as the decision to build the 4 Chernobyl reactors had already been taken. Sredmash made the fateful decision after redesigning the RBMK as best they could but rejected a prototype and went straight into building the Leningrad reactor. The point of using diagrams like these, as proposed by this article, is that those who read SCb's earliest letters, on looking at these diagrams, would be more likely to realise that the alarm bell was not a case of crying wolf but had been issued by the trusted data integrity layer.

The Technology Development and Design Authority Problem

Aleksandrov believed that big was beautiful and ignored the problems of scale that occur when handling dangerous materials, especially nuclear materials. That size meant reactivity in the core in one measured area may have little to do with the reactivity elsewhere in the core. The problems were not explored further by either Aleksandrov or Dollezhall. Brukhanov had no idea of the problems he was to face at Chernobyl because the suppression of the information by Sredmash meant all design data was out of date or just plain wrong. That compounded the problem as the scale of the machines increased. Whatever the data type, suppression of important information on the poor performance of a prototype is never going to help.

NIKIET’s lack of comprehensive training initiatives

No reasons were given for new procedures by NIKIET, so operators were less likely to stick to those rules as they were not explicit safety instructions. Although in nuclear power stations perhaps one should have assumed that operators would take care, trust in shutdown systems was high since NIKIET had approved the designs. Of course, any data on accidents would never reflect anything other than the false information that the reactors were considered safe. [Data Safety ‘Instructional’ type defined as “data used to warn, train, or instruct users about the system”]

The exclusion of communication to the Chernobyl Enterprise

In the typical manner of Soviet paranoia and secrecy, there is clearly a line of communication that could have gone straight to Brukhanov from the Leningrad plant, as shown in Figure 2. In fact, the information did get to Sredmash but they suppressed it. Thus, vital design and operation data became data destined never to be used again.

Using extracts from Table 4 of the Data Safety Guidance Document Version 3.2, [3], the following becomes clear as shown in Table 1 here below:

Table 1: Data Types

Nos	Title	The Problems Caused
1	Predictive	Lost because lessons were not learnt from the Leningrad reactor.
6	Design and Development	Lost because scientists at the Kurchatov Institute were ignored.
11	Behavioural	The larger RBMK’s at Chernobyl could never be controlled accurately. Operators could only guess and rely on the trusted shutdown systems, which in the event could not be trusted.
13	Staffing and Training	Training was totally inadequate as the reactor’s behaviour was not predictable.
16	Release	The data to ensure safe operations was more appropriate for the smaller Leningrad reactor.
17	Instructional	Warnings were not in any way clear.
+1	Trustworthiness	This meta-data could never be delivered because the Chernobyl reactor could not be trusted. How can one trust something one knows nothing about?

Conclusion

By preparedness of necessary communication, any project can be made much safer. Greater care over communication will be necessary as systems that humans depend on become more integrated, aka the internet of things. Increasing complexity also demands better communication. In a world of increasingly limited resources, cost miscalculations through a lack of understanding of safety may become unbearable and thereby wasteful.

Even with our current epidemic of Covid-19, better communication to co-ordinate the fight would have helped in the initial stages. The military analogy at the beginning of this article holds, in that, recognition of the need for coordination and accuracy of data drives the demand for trustworthy command and control systems. Though there is no reason to doubt the wet market in Wuhan was responsible for the coronavirus epidemic initiation, the same effect could occur from an accident in a laboratory. Much of the near exponential growth has been thought to be due to a lack of co-ordination between stakeholder health agencies. Therefore, there has to be absolute certainty in the future that all programmes with safety related aspects must make all parties aware of all issues and all current understanding of risks involved. This coronavirus and Covid-19, has caused a global economic meltdown, which in severity, matches the effect of Chernobyl on the Soviet Union, and the only way to avoid a repeat is through data safety.

It is proposed that the 7 layer data model, used to identify multi-agency communication and protocols for the safe, timely dissemination of data, could assist greatly in the planning of those necessary command, coordination and control actions.

References

- [1] Adam Higginbottom, "Midnight in Chernobyl", Bantam Press, 2019, ISBN: 9780593076835
- [2] The Data Safety Initiative Working Group, "Data Safety Guidance", The Safety Critical Systems Club, 2016, Version 1.3, ISBN-13: 9781519533579
- [3] The Data Safety Initiative Working Group, "Data Safety Guidance", The Safety Critical Systems Club (SCSC-127E), 2020, Version 3.2, ISBN-13: 9798601577359, scsc.uk/scsc-127E
- [4] Nicholas Taleb, 'The Black Swan', Penguin Books, 2007, 9780141034591
- [5] <https://www.nbcnews.com/news/us-news/u-s-pilots-complained-about-boeing-737-max-8-months-n982651> (last checked 16/04/20)

Author: Nicholas Hales IET Chartered Engineer (retired)

Nicholas Hales is the former Senior Engineer for Critical Avionics in the Defence Engineering and Support agency. He has been involved in Safety Critical Systems Club (SCSC), activities since 1991. He has written a number of articles for the SCSC Newsletter and the IET members Newsletter, and has presented at various associated events.

As a postscript I would like to thank Paul Hampton, the Editor of the SCSC Newsletter, for his patience in the production of this article and the numerous suggestions that have made it more readable.