System Certification: An Alternative to Package Certification?*

Robert E. Luna [1] *and Robert J. Jefferson* [2]

[1] *Sandia National Laboratories, Albuquerque, New Mexico*
[2] *Consultant, Albuquerque, New Mexico*

One precept of the current radioactive material transportation regulations is that the package is the primary protection for the public. A packaging is chosen to provide containment, shielding, and criticality control suitable to the quantity and characteristics of the radionuclide being transported. Occasionally, radioactive materials requiring transport are not of a mass or size that would allow the materials to be shipped in an appropriate packaging. This is a particular problem for materials that should be shipped in a Type B package, but because such packages are designed and certified for specific contents, the package is usually fairly expensive, available in relatively small numbers, and often requires a fairly long period to achieve certification or amended certification for new contents. Where the shipment to be made is relatively infrequent, there may be economic and time penalties that may hamper shipment or force the shipper into uneconomic or high risk options. However, there is recognition of such situations in the International Atomic Energy Agency (IAEA) regulations under the provisions for Special Arrangement.

The principal paragraphs defining Special Arrangement in Regulations for the Safe Transport of Radioactive Material; Safety Series 6 (SS6) [IAEA, 1990a] are 141, 211, 720, and 727. Many national regulations contain similar provisions, but under a variety of terms. For instance, in the US regulations the applicable term is "Exemption." An exemption is obtained from either the United States Department of Transportation (USDOT) or the United States Nuclear Regulatory Commission (USNRC) depending on the character of the needed exemption. The applicable paragraphs are 10CFR71.7 and .41 for the USNRC and 49CFR107 Part B for the USDOT. The essential concept is that some requirements of the regulations that apply in a given situation are not required if the shipment is subjected to other operational controls that provide an equivalent level of risk to that attained if the regulations were observed fully. This paper deals primarily with changing of packaging requirements in Special Arrangements, but it is also true that operational requirements also may be changed as a result of an Exemption or Special Arrangement approval by a regulatory authority.

One problem with Special Arrangement is that not everyone may agree that it is a legitimate application of regulation in the same way that the Competent Authority usually does. The fact that it is a "Special Arrangement" or "Exemption" means that shipments under such arrangements may be looked upon as a risky deal between the regulator and the applicant. This impression is furthered by the fact that little public involvement is sought or required prior to granting the requested Special Arrangement or Exemption. This perception is generally incorrect; Competent Authorities evaluate each exemption application on its face and confirm an appropriate level of safety before granting the request.

*This work performed at Sandia National Laboratories, Albuquerque, New Mexico, supported by the United States Department of Energy under Contract DE-AC04-76DP00789

A change in the IAEA's regulations currently being discussed is to institute a process referred to here as System Certification (SC). While the concept has been discussed in transportation regulatory circles for some time, a proposal for SC seemed to arise as a result of a 1989 action at an IAEA meeting to amend the 1985 edition of SS6 to improve the new Low Specific Activity and Low Contamination Object requirements with a SC concept [Petterson, 1989]. Because the proposal was seen as leading to a major regulation change, it was determined to be outside the scope of that meeting. A meeting of the Standing Advisory Group on the Safety of Radioactive Materials in transport (SAGSTRAM) in 1990[Rolland, 1990] debated the issues without resolution and decided to convene a Consultant Services Meeting (CSM) to consider the issues broadly prior to the 1992 SAGSTRAM meeting in October. The CSM was not funded in 1992, but the 1991 meeting of the first revision panel for the 1995 edition of SS6 was provided information that the CSM would occur in 1993 to provide data for the 1995 Revision Panel meeting [Petterson, 1991].

If it is assumed that SC were to come into wide use, what methods could be used by the Competent Authority (CA) to assess the advisability of certifying the system operation? To a large extent the assessment would be keyed to the content of the application; where there was significant quantitative data offered, confirmation of the information offered and consideration of other features not covered in the application would go forward. Where there was qualitative argument the assessment would, of necessity be qualitative. In such a mode the skill of the applicant to argue the case becomes very important to success. This sets up the opportunity for the CA to be questioned concerning the basis for a decision and makes the proceeding subject to appeal. Note that the system in place for package certification is set within a largely quantitative framework with a binary result. You meet specific design and performance criteria or not. This is not to say that the yes or no is not decided with some measure of subjectivity in some situations, but the result is not often decided by the presentation skills of the applicant. It seems clear that a workable and reliable system certification process must be undertaken with a well defined quantitative framework for application and demonstration of equivalent safety.

The basic precept of SC is similar to Special Arrangement, but differs conceptually in that a set of relatively clear-cut rules would be put into place in order to remove the appearance of an arbitrary decision based on a negotiation outside of public scrutiny. Under SC, the packaging and conveyance as well as all of the operations undertaken to ship a given material in a shipping campaign are evaluated in terms of risk to the public and are approved if the risk measures calculated were within specific acceptable limits. The real difference between the present certification approach and SC would be the consideration of all features of the transport system in addition to the packaging in limiting public risk during safety evaluation of a transportation operation.

As indicated above, exemptions are permitted under USNRC and USDOT regulations. Some exemptions granted by DOT were the following:

- Use of the ATMX railcar for the movement of TRU waste material from Rocky Flats to temporary storage in Idaho [USDOT, 1990].
- Carriage of up to 1000 TI (Transport Index) in radiopharmaceuticals in a single conveyance [USDOT, 1989 & 1990].
- Approval for the DOE and EPA (in separate programs) to transport mill tailings in bulk loads without detailed identification of the nuclide content of each load [USDOT, 1992a] [USDOT, 1992b].

In the first case the special arrangement was a package tradeoff. The ATMX railcar is not a Type B package, but a semi-quantitative risk assessment of the transportation showed sufficiently equivalent risk for approval. In the second case, the usual 50 TI limit per conveyance was waived because the controls put on dose to crew and the low dose to other exposed employees and public resulting from air mode transport, automated handlings and careful controls of proximity of persons to the conveyance. The third case was a waiver of the requirement to fully characterize each shipment since each was a part of a large and relatively homogeneous volume. The first example relates to the type of package/procedure tradeoffs of special interest to this paper. The remaining items relate almost exclusively to operational tradeoffs, but would also need to fit within the guidelines of a viable SC process.

System Certification -- What could it include?

It must be noted that the current version of SS6 and the advisory and explanatory information contained, respectively in SS7[IAEA, 1990b] and SS37[IAEA, 1990c] directly or indirectly validate the concept of SC within the existing framework of Special Arrangement. In fact, the explanatory material for paragraph 211 on Special Arrangement indicates that justification of a Special Arrangement request "ranges from considered judgment ... to probabilistic risk assessment" [IAEA, 1990c]. It is the spectre of defending a decision based on "considered judgment" that makes the need for a new and quantitative method of evaluating Special Arrangement or SC decisions important in the current and growing atmosphere of questioning Competent Authority decisions.

The problem of defending a decision (among others) has caused the IAEA to defer the concept of System Certification until it can be studied by consultants. At the Senior Advisory Group on Safe Transport of RAM (SAGSTRAM) Meeting in June of 1991[Petterson, 1991], it was "envisioned that the 1993 Revision Panel will consider this issue before a final Consultant Services Meeting to be held before the 1995 Revision Panel."

While the impression from the USNRC and USDOT regulations is that any Exemption or SC would include both the package and the conveyance, it is mentioned (and confirmed by the cases cited above) that operational controls are also to be included. If operational controls are included, the possibilities are broadened considerably. For example, in the United States there has been considerable pressure from the railroads to ship spent fuel in "Special Trains" operating under more conservative rules than ordinary freight trains. These "Special Trains" are limited to speeds under 35 mph (56 kph), must yield right of way to all other trains, and must be standing still when being passed in either direction by another train. From the railroad's perspective, these "Special Train" shipments are subject to far lower accident forces than regular train service. Could the accident resistance of the package therefore be reduced or be less well characterized for such shipments without sacrificing overall safety?

Since the risk of shipping high level radioactive materials is at least partially dependent upon the total population along the route, might it be possible to route the shipment to reduce total population exposed along the path and use that reduced risk to offset the added risk of using a packaging that does not fully meet the external dose rate requirements? In a similar way, might shipments be required to be made during low traffic density times of the day so as to reduce the public involvement? For years the City of New York insisted that spent fuel shipments transit Manhattan Island at night while the streets were empty of other vehicles. Routing of shipments of large quantities of radioactive materials over the best available and shortest highways is already a requirement of the DOT in the U.S.

Some states in the United States have insisted on notification of shipments of high level radioactive materials. A communication and tracking system called TRANSCOM allows real time tracking of each such shipment. The TRANSCOM data is available to the states so they may know the exact location of each shipment on a real time basis. In principle, this allows better emergency response and thus lowers risk. Is this reduction of risk available to be applied to the level of competency of the packaging?

Another factor in reducing risk envisioned by most of the public in the U.S. is the state of readiness and competence of the Emergency Response capabilities along the route. If training were instituted (as is being done in the case of the WIPP facility) for fire and police personnel along the transportation routes, could the reduced risk generated by this activity be applied to a reduction in the severity of the regulatory requirements for the packaging?

Before application of SC to situations such as those indicated above, a risk based regulatory concept must be fully defined and accepted. One such concept is that of equivalent safety which might be defined as keeping risk constant by shifting risk between various regulatory control concepts.

System Certification - How might it be used?

It is rather simple to envision, from an operational standpoint, instances where System Certification could be used to great advantage. For example, the regulator might certify the system of shipments for a limited campaign involving a specific package, specific routing, and specific operational controls. The packaging may not be certified for the specific contents involved except for the limited campaign, the routing might be unique to the campaign and the operational controls might be used to attain the level of risk deemed acceptable by the regulators. Included in such a system certification might be requirements for additional Quality Assurance (QA) measures or Compliance Assessment (CoA) inspections by the shipper, the carrier, the States or some independent reviewer acceptable to all three.

Similarly, System Certification might be used to approve a specific package and conveyance for a fixed period irrespective of the number of shipments. This approach might be used to provide an evaluation period of the adequacy of the System Certification before the regulator issued an unlimited System Certification. Alternately, this approach could be used for very short campaigns where time is deemed to be a dominate risk factor.

One possibility that might arise in the U.S.A. and elsewhere involves shipment of storage casks to a repository. Regulators are likely to be uneasy about allowing a cask used to store spent fuel for 20 or more years to then be used for transport with only a relatively simple inspection to find serious problems. System Certification might be used to allow a single trip by such a cask, without inspection. Of course, this assumes that easily obtained measurements confirmed no obvious problems. Certainly the early shipments, if the fuel is unloaded from the cask at the repository, could be used as the basis to confirm satisfactory long term cask behavior thus giving the regulator more data upon which to continue the System Certification, to certify the casks under normal rules, or to discontinue the practice.

If a System Certification is to include a large number of variables, then the regulator must regulate all these variables as well. When training is used as a component of SC, then training must be a regulated component. This would include training covering the QA and CoA requirements applicable to the SC, training covering the operational controls, and training specific to any special conditions involved.

In the United States the most common use of System Certification could be in the movement of materials within the boundaries of a large research site. Most of these sites are several thousand square miles (several thousand square kilometers) and frequently are traversed by public highways. Agreements with the States allow blockage of these highways and the establishment of at least some control over the public at risk. Still, special needs arise that could be quite amenable to SC approaches. SC should not be viewed as an "easy out" somehow relieving the shipper of responsibility. But, if it is to be a viable method of achieving solutions to special problems, it cannot be practically impossible either. To be effective, SC must meet the needs of both the applicant and the regulator while not introducing either significant risk to the public nor spawning widespread public reaction.

Demonstrating Equivalent Safety

A safe activity is one which is perceived as being relatively free of hazard or danger to the person or public affected. Because it includes perception, achieving safety involves more than achieving acceptably low risk. As a result, any SC scheme must preserve the current perception that the regulations provide safety while allowing some risk tradeoff.

Achieving "equivalent safety" would seem to demand specific guides for the protection of the public. Limitation of dose to the public controls consequence; preventing occurrence of an event limits the probability. Since risk is the summation over all events of the products of frequency and consequence of each event,

limiting both is a control on risk. All three measures represent the potential output of risk assessment. Control of risk or achieving "equivalent risk" lays the groundwork for using risk assessment methods and imposing specific risk criteria.

A way of demonstrating equivalent safety is based on the concept of maintaining an equivalent level of risk between the fully regulated activity and that occurring under system certification. The result of such a requirement puts heavy emphasis on being able to calculate risks under both options and being able to show equivalence. Alternately, it would be necessary to meet some absolute risk acceptance criterion that is generally accepted as describing an "acceptable risk." Neither of these options is particularly straightforward given the quality of the data needed to perform risk assessments. Moreover, public experience in interpreting risk assessments is very limited. This means that there might not be high public confidence in risk assessment and its practitioners.

When a decision to use risk criteria in evaluating whether a proposal represents equivalent safety is made, there are several additional problems that become important which relate to using relative or absolute risk criteria, how to handle uncertainty in the basic data needed in each case, and how to handle needed data that may not exist.

Relative vs Absolute Risk - Risk is the summation over all events of the product of an event's frequency and its consequence. Frequency is expressed in terms of expected events per year, events per trip, or events over the duration of a project. Consequence is the outcome from an event in terms of individual dose, population dose, cost or any other quantifiable result of the event. From the definition it is seen that risk is the expected value (or average value) of consequence for the activity. An event tree is usually used to represent the various sequences of events that lead to radiological risks and to guide the risk calculations.

To utilize relative or absolute risk assessment to support an application for system certification requires an event tree(s) that describes the sequences of all possible events affecting the system's risk profile. For relative risks two event trees are constructed; one is for the operation for which a system certificate is desired, the second is for a "reference system" that meets all regulatory requirements. Only the parts of the two event trees which differ between the regulatory and proposed system approval applications need be detailed, since the goal of the calculations is to demonstrate that the ratio of the risk from the proposed operation to what would occur if all regulatory requirements were met is less than unity.

For absolute risk an event tree that describes the sequences of all possible events is constructed, filled in with frequencies and consequences, and evaluated. If one value is used for each parameter in the analysis (a "point estimate"), what results is one numerical estimate of the risk, or one set of points that represents the cumulative probability of exceeding a given consequence level (abscissa) and consequence (ordinate). When plotted, these points become a complementary cumulative density function (CCDF) curve. If each of the parameters in the analysis may have a distribution of values which are selected in a random manner, then many point estimates and a family of CCDF curves will result. These risk assessment results make up the information which can be the basis of all or a part of a decision to certify a system. Finding a criterion on which the CA can accept these risks may have several kinds of formats. Two examples may be instructive:

NRC Reactor Risk Goal - The USNRC has indicated a set of "goals" [USNRC, 1990] for individual reactor risk based on different measures of consequence. One of the goals is that for the population from the reactor fence to a distance of 50 miles, the operation of the reactor should cause no more than a 0.1% increase in individual mortality. This and the other goals were arrived at as a result of a very long process involving much public interaction and staff/consultant effort.

CCDF Goal - A risk limiting goal that was being considered for specific transport operations appears as shown in Figure 1. On the CCDF field, a risk profile that fell below the line would be acceptable. The lines were arrived at in the following way: 1. events that produced or had potential to produce any consequence should not

occur more frequently than 0.001/year; 2. events that could result in 1 latent cancer fatality (LCF) or more should have a probability less than 1 in a million per year; and 3. from the point (1 LCF,10-6) a line of constant risk (probability times consequence) connects to the 0.001 line.

To use these or other absolute risk criteria, the CA must be able to demonstrate that the criterion being used limits the risk for the transportation situation under consideration to that which would occur if conducted under the regulations that are normally in force. This would not be a trivial undertaking for the CA given the number of situations for which system certification is sought. Of course, the CA could require the applicant to provide the comparative estimate of absolute risk under normal regulation events.

Choosing between these two possible absolute risk criteria, the easiest to use is the point estimate (NRC). This is particularly true if variations of parameters or uncertainty analysis is included in the calculations. The CA might require that none, or no more than 5% or as many as 50% of the set of estimated risk values exceed the criterion so long as the median or mean risk is below the criterion line. To use the CCDF criterion will require examining a family of curves for conformance to the requirements and developing a method to determine whether a few exceedences in a small area of the plot disqualifies the applicant.

Data Limitations to the Use of SC

Whether an applicant for SC must meet relative, absolute or even qualitative risk equivalence demonstration, there will be a heavy load of data gathering that must occur. Tradeoffs of package certification for package and conveyance certification or reliance on operational controls implies that the behavior of the containment systems in either case must be known, identical, or reliably estimated in environments below and above the performance limits for the package. Otherwise there is no method for calculating risks for comparison of risk associated with different packaging concepts. Since most packages are not tested to failure above the performance standards, such data tends to be scarce.

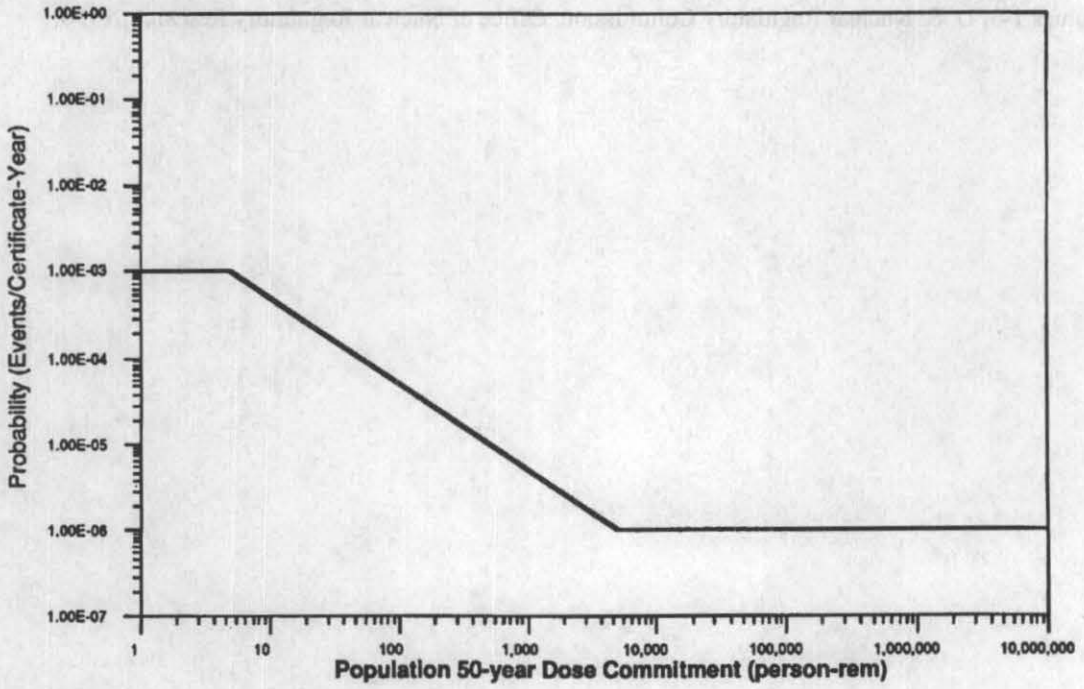
Where there is a tradeoff that involves operational restrictions or modifications, the same problem indicated above occurs; the applicant must present data that suggests a quantified difference in probability or consequence between two operational procedures. Usually such information is not available or is gained only by examining accident records and recalculating rates after accidents caused by specific behaviors and processes are excluded. Where the data does not provide a record that can be so analyzed there is little but qualitative arguments to be used. For example, if transport is restricted to daylight hours, it is relatively easy to find tabulated accident rates for day and night and establish the advantage of daylight travel. To gauge the effect of special driver training or maintenance, however, is a much more difficult restriction to define quantitatively.

Future

The IAEA will examine the issues associated with System Certification in order to determine whether there can be a meaningful elaboration of the SC concept for the 1995 version of SS6. To produce a change which truly embraces the SC concept will take significant effort in resolving the role of risk assessment, the criterion for equivalent risk, and how to account for uncertainty among others. These are non-trivial issues and suggest to the authors that SC inclusion in the 1995 version of SS6 is unlikely. However, there is time to develop the concept for the 2005 version of SS6 if a well conceived plan is put in place soon to develop consensus on need and technical bases for the concept.

A danger in the SC concept is that the process of developing quantitative understanding of the effects of special operational controls will generate a demand for their incorporation in the regulations without specific tradeoff goals. An aligned but slightly different feature of SC is that it represents a change from the current process which states that when you meet the requirements you can proceed with transportation without any additional

permission or approval. Under SC an applicant potentially must demonstrate need and safety for every shipment and incur the possibility of protracted delay.



References

IAEA, 1990a; "Regulations for the Safe Transport of Radioactive Materials (1985 Edition)," (as amended 1990), IAEA Safety Series 6, 1990.

IAEA, 1990b; "Exploratory Material for the IAEA Regulations for The Safe Transport of Radioactive Material (1985 Edition), Second Edition (as amended 1990), IAEA Safety Series 7, 1990.

IAEA, 1990c; "Advisory Material for the IAEA Regulations for The Safe Transport of Radioactive Materials (1985 Edition)," Third Edition (as amended 1990), IAEA Safety Series 37, 1990.

Petterson, 1989; "Chairman's Report on the Technical Committee Meeting on the Continuous Review of the IAEA Regulations for the Safe Transport of Radioactive Materials," TC 405.3, 10-14 July 1989, Vienna, Austria.

Petterson, 1991; "Chairman's Report on Meeting of The Advisory Group on The Revision of SS6," AG 550.2, 10-14 June 1991, Vienna, Austria.

Rolland, 1990; "Chairman's Report on the 8th Meeting of the Standing Advisory Group on The Safe Transport of Radioactive Material (SAGSTRAM), TC 407.6, December 1990, Vienna, Austria

USDOT, 1989 & 1990; DOT Exemptions (DOT-E7060 & DOT-E 10045) 1989 & 1990.

USDOT, 1990; DOT Exemption (DOT-E5948), Sixth Revision, November 1990.

USDOT, 1992a; DOT Exemption (DOT-E10594), First Revision, May 1992.

USDOT, 1992b; DOT Exemption (DOT-10727), September 1992.

USNRC, 1990; NUREG 1150, "Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants," Volumes 1-3, U. S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 1990.