THE ALLOCATION OF FAILURE RATES TO CONTAINMENT COMPONENTS, WITH PARTICULAR REFERENCE TO HYDRAULIC TRANSIENTS

A.G. Rushton
Department of Chemical Engineering, Loughborough University of Technology, Loughborough, LE11 3TU.

Failure frequencies of containment components are widely used in quantitative risk assessment (QRA) of chemical plants.
The amorphous data on failure frequencies of containment components is indicative that the failures are strongly dependent on the context in which the components are employed and are not intrinsic to the components.
This paper questions the validity of using generic failure frequency data without qualification and cites the example of possible exposure to hydraulic transients as one variable, characteristic of the context, which deserves examination.
The difficulty of discounting hydraulic transients as potentially important events, even in small bore and short pipework is highlighted.
Hydraulic transients - because they are transient - are probably under-recorded as being instrumental in containment component failure.
The consideration of contextual factors should be a necessary part of the qualifying conditions for using generic failure frequency data in QRA.

Key Words : Fault, containment, waterhammer, risk assessment.

INTRODUCTION

Quantitative risk assessment (QRA) and the need for failure frequencies

Quantification of risk, (1), requires the logical relations between failure events and consequences to be established. Usually, the intermediate concept of *hazard* is used. First, hazards are identified and enumerated. Then the logical relations between failure events and hazards are obtained, often represented as fault trees, and the logical relations between hazards and consequences are obtained, often represented as event trees.

In the logical relations between the failure events and the hazards, the hazard can be considered as a construct of intermediate events, each of which in turn is ultimately a construct of identifiable and declared failure events (or *basic* events).

For practical purposes, it is desirable to limit the detail, or *resolution*, to which failure events are explored and declared. That is, there is a decision not to resolve a description of a basic event into a more elaborate construct with new and more detailed failure events. For example, the event classified as 'leakage of a stem seal on a valve' could be the limit of resolution for a particular purpose.

There are many justifications for limiting the resolution:

- there is no definite limit to the further refinement that could be undertaken and so some stopping rule is necessary
- the extra complexity of more refined constructs is likely to lead to errors
- the constructs, which are intended to aid judgement, need to be interpreted and excessive detail would make scrutiny and assimilation of the constructs too difficult
- an over-elaborate statement of the relations could lead to unwarranted confidence in the outcome, which the uncertainty in the elements (however detailed), and in the structure and its analysis, do not support.

However the strongest imperative for not resolving basic events is simply that the data related to failure frequencies cannot support more detailed descriptions. This will usually be because the recorded data on failures is not resolved to the necessary extent.

In QRA of chemical processes many of the basic events that have to be considered are often declared to be the failure of various equipment to maintain containment of process materials. In the following discussion a piece of equipment which has, as one of its functions, the containment of process materials is termed a *containment component.*

DEVELOPMENT OF RELIABILITY PRACTICE:

Contrasting features of electronic and process components and systems

Early development of reliability prediction using component failure frequencies focussed on electronic components (2). Operating experience, necessary for the generation of failure data, was often accomplished by simultaneous testing of many components in controlled environments. As new products became available, data could be generated for these quite readily. It was recognised that the environment in which the component operates can affect its failure behaviour, and so data is normally classified according to the operating conditions. Where particularly severe conditions are expected, then tests to generate the necessary data can be performed.

It is natural that the level of resolution of basic events in the analysis of chemical plants is often at the level of individual, identifiable components; these are the elements which the designer has brought together and are often the focus for reliability data collection. This elemental approach has been successful in application to electronic systems, but there are important differences between electronic and process systems.

Characteristics of electronic components include:

- mass production
- dedicated function
- finite range of inputs and outputs
- small
- controlled (or controllable) environment (as a result of being small)

- low unit cost
- (often) a high wear-out life to mission ratio

These contrast with the characteristics of containment components in chemical processes, which include:

- variation in materials of construction (body, trim and seals)
- multiple function (e.g. pipework support, campaign production)
- infinite range of inputs (process fluid mixtures)
- external environment controllable only at high cost and subject to effects of other equipment failures
- internal environment controllable only within the constraints of the process and subject to variation due to other equipment failures and abnormal operation (perhaps an intended response such as trip valve closure, but nevertheless detrimental)
- large
- expensive

The problems for reliability assessment of process systems that arise from these characteristic differences include:

- extensive testing of containment components is usually prohibitively expensive
- extensive control of the operating environment in working applications of the components can be prohibitively expensive (it can also lead to aggravated consequences in the event of failure - e.g. by confinement of explosions)
- even if extensive testing in controlled environments were undertaken the range of operating condition in working applications of the components would make the data of limited use
- the creation of extensive new data in response to technical changes and innovations is usually prohibitively expensive
- differences in primary function (such as material processed and operating temperature) and in ancillary functions such as support of pipework and connections to instrumentation lead to differences, in quality and quantity, in the stress to which a component is normally exposed.

In a special class is the exposure of containment components to changes in the internal environment. The electronic analogues of pressure and flow can usually be dealt with in electronic systems by voltage or current limitations. There is, however, no analogue in an electronic system for the flow of a substance of different quality. In process systems there is an infinite variety of contained process material which may be intended to be present or may be present in abnormal conditions. There is also no direct electronic analogue for the fluid momentum that leads to hydraulic hammer.

The combination of differences in construction, duty and internal and external working environments, taken together with possible changes in these (in abnormal conditions) are described here as the *context* of a component. The opportunities for, and probabilities of exposure to, various changes in working conditions are dependant on the arrangement of components in which the component of interest is placed. This arrangement is, therefore, an important aspect of the context.

PROBLEMS WITH DATA SOURCES
for failure frequency of containment components

The features of process systems, outlined above, force the reliability analyst to resort to field data, collected from working applications, and to derive failure frequencies from this data. The collection or collation of such data is problematic because:

- production imperatives and culture often cause the data collected to be incomplete or in error
- operating conditions are not the same from application to application, even where the nominal service may be identical, yet the data collected must be pooled in order to give a usable frequency
- data collection protocols for the definition of failure events and for their allocation are not agreed upon between different organisations, nor are they reliably adhered to within individual organisations.

These, together with differences in resolution among organisations, lead to problems of the *level of aggregation* and of *data combination* (3). The data that is available is often quite amorphous (4).

THREATS TO A COMPONENT FROM ITS WORKING ENVIRONMENT

The failure, for example, of a filter designed to operate at 1 bar when it is exposed to 20 bar tells us nothing about the reliability of the filter in its intended environment. In the bench testing of filters, measures would be in place to prevent such exposure and if these measures failed then the test would be dismissed. Provided that the working environment also has measures in place to prevent such exposure, and that the failure of these measures is considered separately, then a useful application of failure frequencies is possible.

Where the threats to the internal environment of a component arise from the gross failure of other components, these will often be of sufficient interest that they will not be over-looked. In general, however, the changes to the internal environment of a containment component may be quite subtle in origin but nevertheless catastrophic in effect. The ability of these disturbances to be generated in respect of a particular application of the component will be highly dependent on the arrangement of components in the application.

For these reasons, it is not generally possible to establish that the field data collected in respect of failure of containment components is attributable to the component and not to its particular environment. Where this has been recognised, then classification of the environment can be attempted and the failure frequency qualified as relating to a particular class of environment.

Table 1 **Allocation of different failure rates to nominally similar equipment (direct acting relief valve) in different classes of service, after Hanks (5), for illustration only.**

Duty and application	Failure rate (per 10^6 hours)
Pressure relief of:	
machinery auxiliaries	1.8
process plant	4.3
cryogenic plant	3.5
condensate, methanol and odorant applications	8.3
Thermal relief of cryogenic plant	6.0

For example, five classifications of working environment have been used in the assessment of relief valve failure rates (5). These are shown in Table 1. However, it is very difficult to establish that the classifications chosen are sufficiently detailed and that any particular proposed application is well represented by one of the classifications defined.

Hurst et al (6) classified a large number of pipework and in-line component failures according to causes listed in Table 2. Whilst it may be difficult to agree on the classes defined and the allocation of individual cases, it is clear that many of the classifications relate to the context of the component and not to the component itself.

If no proper classification of the environmental factors is available then it is possible that the data collected and the 'failure frequency' derived from it cannot generally be used in relation to the component. In the extreme, the measured failure frequency is not indicative of the frequency with which the component will fail in circumstances that it was designed to survive, but is rather *the frequency with which the component experiences circumstances which it cannot survive.*

In a case where the environment is constantly hostile and not survivable even for a short period, the problem will normally be apparent from immediate failure. It is likely, in such cases, that either the design process has been inadequate (i.e. the mismatch between the component and the intended operating conditions should have been identified) or else that the combination of component and environment may become renowned as a new concern that must be watched for. Such concerns are difficult to maintain and, consequently, the related incidents tend to recur (7). Even where the effect is delayed, but is an inevitable consequence of the planned environment then the same response is likely. In these cases, where the link between operating conditions and failure is established the failure may or may not be attributed to the component, dependent on recording practice. However, where the normal operating conditions are tolerable, but transient or infrequent abnormal conditions are not, then it is less likely that the link between the particular contextual feature and the component failure will be revealed.

Table 2 **Classification of direct causes (for pipe and in-line component failures), after Hurst et al (6).**

Corrosion	Overpressure	Human error
Erosion	Vibration	Defective equipment
External loading	Temperature	Other
Impact	Wrong equipment	Unknown

Where characteristics of the context that will affect the expectation of failure of a component are known, then it is difficult to justify not reflecting these facts in the basic failure frequencies used. However, there are practical problems in achieving this:

- the complexity and the expense required to identify and to represent such characteristics
- the lack of a sound basis for modifying the failure frequencies in the absence of suitably documented historical data
- the lack of practical means of evaluating the applicability of contextual characteristics

Failures that are strongly context controlled have a weak influence on the quoted component failure rates because they are *diluted* by association with operating experience in qualitatively less hostile environments. This can lead to incorrect allocation of failure frequencies in QRA of a significant order of magnitude. The effect is illustrated schematically in Figure 1.

HYDRAULIC HAMMER

The hydraulic transients discussed here relate to momentum change caused by rapid restriction of a flow-path. Other related phenomena are not explicitly considered, though similar comments may apply.

Hydraulic hammer and associated problems are introduced in various texts (8). A brief introduction, sufficient for the purposes of this paper, is given in Appendix 1. A recent contribution which includes case histories is by Thorley (9). The difficulty of discounting hydraulic transients as potentially important events, even in small bore and short pipework is highlighted in Wood and Jones (10). More recently Liou (11) has shown that the approach set out by Wood and Jones is not necessarily conservative. A review of some recent work in this and related fields is given by Moody (12). The particular problem of flap valves on parallel pumps is highlighted. The arrangement in which this problem occurs is shown in Figure 2.

The difference in potential for exposure to hydraulic transients is an example of a variable characteristic of the context in which two otherwise identical containment components may be required to operate. It has been chosen as an example because:

- it exemplifies a variation in internal environment - though external examples can also be described these are less likely to lead to inappropriate allocation of a failure to the component of interest and some such events (e.g. falling objects) are often explicitly accounted for in QRA
- failure data sets are not normally classified according to this characteristic

- it is not a commonly understood phenomenon and is often neglected where it is not a self-evident or classically recognised problem (such as long large pipelines)
- the component initiating the problem will often not be the component that fails and can be quite remote from it.
- it can be caused by intermittent events, misbehaviour or intervention and so may not be identified as a contributory cause of a component failure.

This last point also means that the development of the transient will be characterised by a 'demand rate' (for example the frequency with which a sample point is opened and closed or the frequency with which a slam shut valve is called upon to act). This rate is in no sense characteristic of the component of interest. To identify a usable apparent failure rate (for QRA) the context must be quantified in terms of the demand rate, not just qualified in terms of the class of service.

Association of the component failure with an intermittent cause will be particularly difficult if many transient incidents precede failure or the 'demand' is caused by intermittent and unrevealed faults which leave no trace.

Other possible examples of contextual features, not discussed here include:

- over-pressure by thermal expansion of locked in liquid
- over-pressure by breakthrough of high pressure gas in a liquid system
- impact loading by slugs of liquid in gas lines

The susceptibility of containment components to hydraulic transients depends on their ability to withstand stress and stress cycling. The magnitude of the stress that they may be exposed to as a result of transients depends on

- flow velocity (preceding the transient event - not necessarily the intended flow velocity)
- density
- wave speed
- closure times of components (including, if appropriate, the component of interest)
- frictional losses in the line.

Clearly, these may vary for containment components that are otherwise considered to be in similar contexts characterised by, for example,

- operating temperature
- operating pressure
- process material (though this will usually fix the wave speed)

For identical components with the same process fluid, flow velocity will be a function of volumetric flow-rate. Depending on the design procedure followed, the design velocity can typically vary by over a range of about 10 to 1 (13). However the range of flow-rates that can be achieved in abnormal conditions may be even larger than this. For example, the inadvertent excess opening of the control valve may lead to high velocities. This point is particularly significant where the abnormally high flow triggers an event that develops the pressure transient. To pursue the same example, the opening of the control valve could trigger a high level alarm that causes a trip valve to close and induces a transient pressure. Uncontrolled reverse flows can also lead to situations in which the design velocity is exceeded.

Closure times of components can take any value, in principle. Short closure times are those of interest and, in practice, it is the ratio of closure time to pipe period that is important (see Appendix 1). This ratio will vary for lines of different length even where the closure times of associated components are the same. Again it must be appreciated that the closure times in abnormal conditions are of interest. For example, the reluctant and late, but sudden closure of a sticky non-return valve has been found to be a cause of damage (see Figure 2).

CONCLUSIONS

The very amorphous data on failure frequencies of containment components, and the various classifications for data that are used, are indicative that the failures are strongly characteristic of the context in which the components are deployed and are not intrinsic to the components. Consequently if we do not characterise the environment and allocate data accordingly then the basis for associating failure data with any particular planned employment of containment components is flawed. The context may need to be quantified in terms of a demand rate, not just qualified in terms of the class of service.

Hydraulic transients, for example, because they are transient, are probably under-recorded as instrumental in containment component failure. As a result failures due to single or repeated transients will have been diluted by association with the wealth of experience in operation of components that do not suffer from hydraulic transients. If it were possible to separate out the set of operating experience for which hydraulic transients are a problem, then a very much higher rate of failure - quite possibly higher than that of any general set of failure experience - would probably be established. Strictly, this is the 'demand rate' at which the transients are generated (or something that scales with this rate). Nevertheless the use of such a rate would be more appropriate to the QRA of systems with components in such hostile contexts.

It is not possible to be sure that context dependent causes (particularly transient, intermittent or unrevealed) are not significant in failure data. The error in failing to use appropriate data could be significant, even at the level of precision which is expected in QRA.

This argument can be generalised to other contextual features. The need to recognise these features and to adjust for them is clear. Without characterising the context of the containment components QRA is substantially weakened, but such characterisation is not easily achievable.

If a technique, such as HAZOP, which explores the context of the individual components, has not been used to try to find and to eliminate the particular threats that a component faces, then using generic failure data is questionable.

REFERENCES

1. CCPS, 1989, **Guidelines for Chemical Process Quantitative Risk Analysis.**
2. Smith, D.J., 1993, **Reliability, Maintainability and Risk** (Practical Methods for Engineers), 4th Edn, Butterworths.
3. Cannon, A.G. and Bendell, A., 1991, **Reliability Data Banks**, Elsevier, 13-18.
4. CCPS, 1989, **Guidelines for Process Equipment Reliability Data.**
5. Hanks, B.J., **Safety and Reliability 14(2)**, 1994.
6. Hurst, N.W., Bellamy, L.J, Geyer, T.A.W. and Astley, J.A., 1991, **J. Haz. Mat. 26**, 159-186.
7. Kletz, T.A., 1993, **Lessons from Disaster** (How organisations have no memory and accidents recur), I. Chem. E., Rugby.
8. Wylie, E.B. and Streeter V.L., 1983, **Fluid Transients**, FEB Press, Ann Arbor, Michigan USA.
9. Thorley, A.R.D., 1991, **Fluid Transients in Pipeline Systems**, D. & L. George.
10. Wood, D.J. and Jones, S.E., 1973, **Procs ASCE, J. of Hydraulics Division, HY1 99**, 167-178.
11. Liou, C.P., 1991, **J. Fluids Engineering 113**, 643-647.
12. Moody, F.J., **Trans ASME, J. Pressure Vessel Tech. 113**, 228-233.
13. Simpson, L.L. and Weirick, M.L, reprinted in Deutsch, D.J, 1980, Process Piping Systems, McGraw-Hill, 3-10.
14. Kletz, T.A., 1983, **Hazop and Hazan**, I. Chem. E., Rugby.

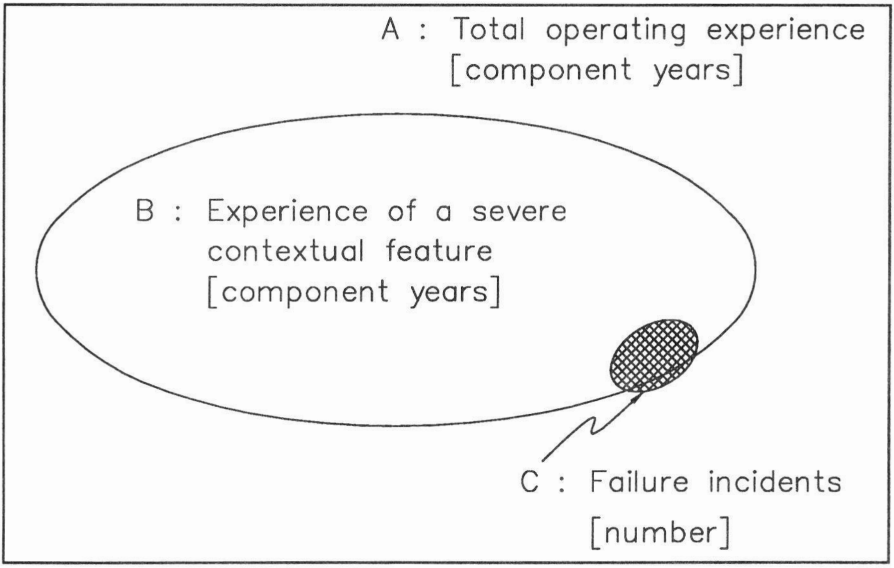

Figure 1 **A schematic Venn diagram illustrating the correlation between a contextual feature and failure incidents.**

The failures associated with an unidentified severe contextual feature are *diluted* in the estimation of failure rate.

The true expectation of failure frequency (given the contextual feature), ~C/B, is very much greater than the estimated frequency, ~C/A.

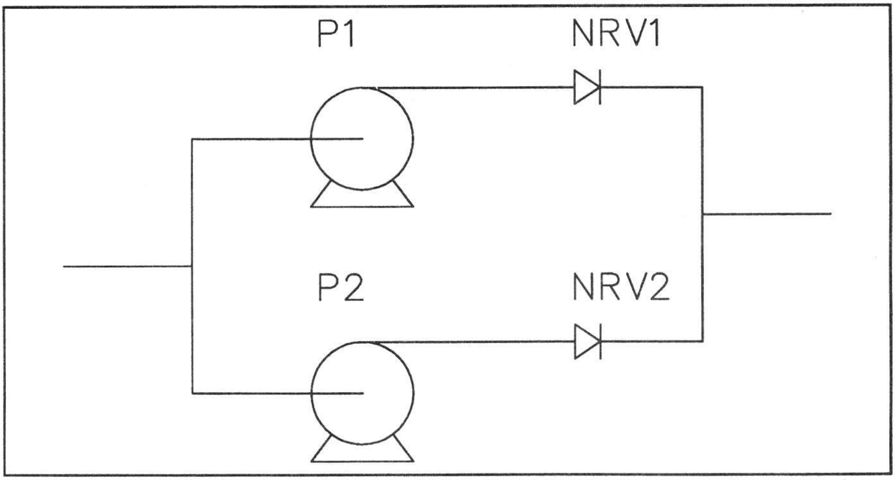

Figure 2 An arrangement of components that can lead to hydraulic transients.

Suppose that the pumps P1 and P2 are normally operating in parallel. On drive failure to one pump (say P1), a high velocity reverse flow can be established through that pump if the non-return valve (NRV1) does not respond quickly enough. If the eventual closure of the valve (NRV1) is fast then a large and damaging transient pressure can be generated.

A sticky flap-type non-return valve can exhibit this characteristic of late but fast closure.

The propensity for damage is due to the arrangement of the pumps and is not an intrinsic property of the pump.

This is a quite separate problem from the more widely appreciated hazard of pumps stopping on long lines.

Other modes of operation can also generate the problem. For example if P2 is normally idle, but the switch-over procedure is aimed at maintaining delivery so that P2 is started before P1 is stopped.

Appendix 1 : Some Principles of Hydraulic Hammer

The effect of *rapid* closure and the Joukowsky head

Consider a flow-path, such as that of the pipe illustrated in Figure A1. When this flow-path, becomes closed, for example by the operation of a valve, then the fluid must come to rest.

For a simplified case in which the closure is instant, the pipe wall is rigid and the flow is frictionless, a momentum balance can be used to find the associated change in pressure.

The slowing (to a stop) of the fluid requires a change in momentum and this requires forces to act at the point of closure, leading to a local rise in pressure. The size of the force is in proportion to the rate of change of momentum.

$$F = \frac{\mathrm{d}(mv)}{\mathrm{d}t} \qquad A1$$

Each particle of fluid experiences the same change in velocity Δv, from an initial velocity $v = v_0$, to a final velocity $v = 0$, so it is the rate at which the mass of fluid is brought to rest which determines the force.

$$F = \Delta v \frac{\mathrm{d}m}{\mathrm{d}t} \qquad A2$$

The rate at which fluid becomes stationary depends on the speed at which the change in pressure becomes established along the length of the flow-path.

A short period of time, Δt, after the closure event, the change in pressure at the point of closure will have propagated a distance $\Delta s = a\Delta t$ along the pipe. Here a is the wave speed, that is the speed of a pressure wave travelling through the system. In this simplified problem the wave speed is the local speed of sound.

The mass of fluid brought to rest in time Δt is then

$$\Delta m = \rho A \Delta s = \rho A a \Delta t \qquad A3$$

The force, which is required to achieve this is

$$F = \Delta v \frac{\Delta m}{\Delta t} = v_0 \rho A a \frac{\Delta t}{\Delta t} \qquad A4$$

So the pressure rise is

$$P_J = \frac{F}{A} = v_0 \rho A a \qquad A5$$

Expressed as a *head* this becomes

$$h_J = \frac{v_0 a}{g} \qquad A6$$

where the subscript J denotes the *Joukowsky* head, named after its empirical finder.

The above is **not** a worst-case analysis, but is sufficient to illustrate the scale of the potential pressure rise. Also the effect of closure on the fluid downstream has not been considered, though this can be the more significant in particular cases.

It is interesting to compare the Joukowsky head with the more familiar *kinetic* or *velocity* head which is generated when the momentum of a stream is changed continuously, such as where the flow path changes direction at an elbow. This kinetic pressure is of the order $v^2/2g$. In pipe flows of typical liquids the Joukowsky head exceeds the velocity head by three orders of magnitude.

Additional attention may need to be paid to the fact that transient pressures are associated with the *rapid* application of stresses which is often more capable of leading to damage than the same stresses applied gradually.

In a typical case, say for a = 1200 m s^{-1}, the Joukowsky head will be of the order of 360 m, which is often significant in relation to the weaker components in a line.

By extension of this argument, stresses three orders of magnitude greater than the normal reaction stresses in pipe support structures can be developed. Loss of containment can result from loss of support leading to failure of containment components even though the internal pressure has not exceeded the design envelope.

Slow Closure and the *Pipe Period*

If the flow-path closure is other than instant, then something other than a step change in pressure is established and propagated. Some components, notably pumps and vessels with vapour spaces, will respond by generating pressure waves (of the opposite sign) which propagate back towards the point of closure. If this returning wave arrives at the closure point before the closure is completed, then the pressure rise is modified. Otherwise the closure will still generate at least the rise predicted by the Joukowsky equation.

The time taken for a wave to travel from the point of closure to the point where a compensating wave is generated and back again is thus specially significant and is known as the *pipe period*.

Any closures for which elapsed time during closure exceeds the pipe period are termed *slow* closures. However slow closures can still produce appreciable pressure rises, even exceeding the Joukowsky pressure. No convenient general criterion by which pressure transients can be neglected has been established.

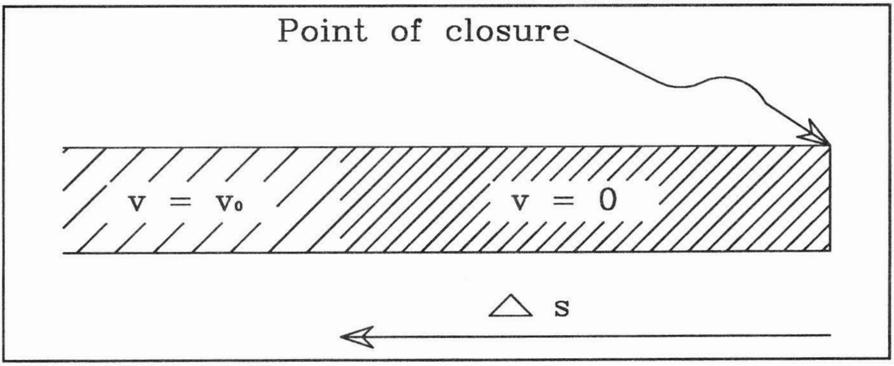

Figure A1 A schematic diagram of a pipe at some time Δt after closure of the flow-path.