Designing For Reliability

Identify Weak Spots by Asking 'What Can Go Wrong?'

By Steve Doty, P.E., Member ASHRAE

How important is extra reliability? Designs that maximize reliability may be at odds with other criteria, including energy efficiency. Therefore, there may be additional first costs and increased annual operating costs. Is this acceptable? Can the project budget support the reliability improvements? Identifying the costs involved helps pare down a list of wants into a more realistic list of needs. Doing this early helps establish a clear design path.

Consider an apartment building where fan coils are installed in each guestroom and a single hot water boiler is used. Single points of failure exist throughout this design, but it is commonly used and is considered acceptable.

The desire for increased reliability is linked to the consequence of a failure. If failure results in only an occasional nuisance, then using good equipment and having high construction quality control usually suffice. For example, in a climate with few cooling hours, a redundant chiller is difficult to justify based on thermal comfort alone. By contrast, a hospital in most climates needs redundant boilers and pumps. The focus on system reliability for manufacturing varies by product value. For example, the focus on golf balls is different than for satellites. In business terms, the cost of improving reliability is seen as insurance. If car insurance costs more than the car, it does not make business sense to buy car insurance.

Where reliability choices are integral to the design, it is important to understand the customer's views on what is

About the Author

Steve Doty, P.E., is an energy engineer for Colorado Springs Utilities in Colorado Springs, Colo.

This article is written around HVAC design, but the principles apply to other fields of engineering. Discussions of reliability options are based on protecting comfort or product losses. In all designs, safety is the first priority.

Option	Design Load Mbh (kW)	Equipment Redundancy	Arrangement Mbh (kW)	Installed Capacity Mbh (kW)	Remaining Capacity After 1 Failure Mbh (kW)	Remaining Capacity After 2 Failures Mbh (kW)
1	1,500 (440)	N + 0	1 at 1,500 (1 at 440)	1,500 (100%) (440) (100%)	0 (0)	0 (0)
2	1,500 (440)	N + 0	2 at 750 (2 at 220)	1,500 (100%) (440) (100%)	750 (50%) (220) (50%)	0 (0)
3	1,500 (440)	N + 0	3 at 500 (3 at 147)	1,500 (100%) (440) (100%)	1,000 (67%) (293) (67%)	500 (33%) (147) (33%)
4	1,500 (440)	N + 1	2 at 1,500 (1 at 440)	3,000 (200%) (880) (200%)	1,500 (100%) (440) (100%)	0 (0)
5	1,500 (440)	N + 1	3 at 750 (2 at 220)	2,250 (150%) (660) (150%)	1,500 (100%) (440) (100%)	750 (50%) (220) (50%)
6	1,500 (440)	N + 1	4 at 500 (4 at 147)	2,000 (133%) (586) (133%)	1,500 (100%) (440) (100%)	1,000 (67%) (293) (67%)
7	1,500 (440)	$(^2/_3 N) + 1$	2 at 1,000 (2 at 293)	2,000 (133%) (586) (133%)	1,000 (67%) (293) (67%)	0 (0)

Table 1: Options for equipment redundancy—equal-sized equipment.

important (project intent) so that the design is responsive to the customer's priorities. Discussion and documentation are useful to help the customer understand and agree to the level of reliability provided.

Beginning with a no-frills design, list points of failure and estimate the consequences and how high is the likeliness for failure. Consequences to consider include:

- Full or partial loss;
- Process impact from the loss;
- How long will it take to restore service; and
- Options for restoring service through repairs or temporary provisions.

The weak spot in all failure analysis methods is establishing the likeliness of a given failure. For example, what is the likeliness of the utility water supply being interrupted? There is no easy answer. However, the list of failures must be prioritized based on the combination of severity and likeliness. Assigning a one to 10 numerical weight for severity and likeliness is one method. How often a failure occurs may not be as important as how costly the failure would be.

Once the failure opportunities are prioritized, prepare options and costs to address each one. When possible, presenting this information in terms of cost/benefit allows the customer to make choices based on the business value of the improvements. This process also will serve to dispel any notion that their system is fail-proof.

Introducing "N"

Redundancy options applied to equipment presume the most likely failure will be an individual machine and not the infrastructure (an assumption that will be discussed later). The HVAC application begins with the design heating or cooling load and ***N*** represents the largest of the machines selected to serve the load. "N+1" then allows full capacity after any one unit failure.

Table 1 illustrates how to apply the N+ principle. Consider a base load of 1,500 Mbh (440 kW) heating output. A design option with no redundancy would be a single unit at 1,500 Mbh (440 kW), two at 750 Mbh (220 kW), or three at 500 Mbh (147 kW). N+0 and N+1 are shown to illustrate the pattern. N+2, N+3, etc., are possible, but are seldom used in practice except for extreme criticality. A complete doubling of maximum capacity (Option 4) is termed *100% redundancy*, and is common with smaller systems.

Option 7 is a commercial variation that uses two chillers or boilers at two-thirds of design capacity. This strategy leverages the reality that full-load conditions are seldom required. HVAC equipment sizing provisions such as built-in future capacity and initial start-up reserve capacity (*pull-up* allowance) provide some system redundancy without additional cost. Note that this example provides much of the redundancy with many of the benefits.

Table 1 shows equal size equipment for simplicity. However, any combination of equipment sizes can be evaluated. By setting N equal to the largest single unit, N+1 will protect against the worst case single equipment failure.

Observations from *Table 1*:

- Assigning the entire load to a single piece of equipment means all capacity is lost upon a single failure.
- Dividing the base load into smaller equipment increments means less is lost for a single failure, and for additional equipment failures.
- Using multiple smaller units reduces excess installed capacity and cost.

Argument for Multiple Small Units	Argument for Fewer Large Units
A system of multiple units fails softer on single and multiple failures.	Larger equipment may have higher full-load efficiency than smaller equipment.
Multiple units provide redundancy with less installed capacity and equipment cost because the "N = 1" extra unit is smaller.	Life span of large equipment is often longer than small equipment—life-cycle costs are different.
Smaller equipment is easier to manage in construction and easier to remove from the building at end of life.	With multiple large units running at part load, recovery after an equipment failure can be in seconds instead of minutes since all it has to do is ramp up. This technique is termed hot spare or rolling redundancy.
Smaller equipment usually is quicker to start than large equipment, lending itself more to automatic control and allowing cold spares instead of idling hot spares.	Multiple units require more taps to common piping, which are then new single points of failure.
Smaller incremental equipment will run nearer full load and may operate more efficiently compared to large equipment at low load.	Multiple units may take up more floor space due to multiple clearance areas.
	Some modular equipment designs focus on compactness and this may complicate maintenance, especially to isolate an individual unit sandwiched in the middle of a tandem assembly.

Table 2: Comparing strategies—Multiple small units versus fewer large units.

Modular Systems?

Based on the question, "What is left after a failure?" a design with multiple smaller components has merit compared to a design with fewer, larger components—that each failure causes less of a capacity loss (*Table 2*). We say this design fails *softly.*

Point of Failure: Piping Common to All Systems **Solutions:** • Pipe equipment in sets in lieu of common headers • Temporary connections • Heavier specification for the common piping—thicker pipe, higher pressure class, better valves, tighter field control • Redundant valves • Accessible for rapid repair	**Point of Failure:** Utility Water Supply **Solutions:** • Redundant feed, from opposite sides of utility street section valve • Storage • Built-up cooling towers with deep basins, designed for the time it takes to run dry • Provisions for portable truck supply
Point of Failure: Wiring Common to All Systems **Solutions:** • Wire equipment in sets in lieu of one main circuit breaker or source • Temporary connections • Heavier specification for the common wiring—reduced current loading, higher quality switches, tighter field control • Accessible for rapid repair	**Point of Failure:** Utility Electric Supply **Solutions:** • Twin utility feeds, preferably from different substations • On-site generation • Operable windows • Gas engine driven cooling • Thermal storage
Point of Failure: Switchgear Serving All Systems **Solutions:** • Split service—separate the equipment and leave a space between	**Point of Failure:** Utility Natural Gas Supply **Solutions:** • Dual fuel equipment and fuel oil storage • Thermal storage
Point of Failure: Central Automatic Controls **Solutions:** • Distributed stand-alone controls • Manual override provisions for end devices	**Point of Failure:** Building Issues Such As Foundation and Roof **Solutions:** • Occupy other than top floor (roof leaks) or basement (flooding) • TEFC motors indoors • Divide services among multiple buildings
Point of Failure: Transfer Switch **Solutions:** • This is tough to guard against • Maintenance bypass option • Temporary connections for downstream equipment	**Point of Failure:** Personnel, Especially for Complicated Systems **Solutions:** • Cross training • Documentation • Simple systems

Table 3: Single-point failure items other than equipment.

Beyond Equipment

Many opportunities for failure do not involve equipment. For high reliability designs, listing each single point of failure is an important part of design disclosure (*Table 3*); doing so will prompt the customer to consider operational contingency plans.

Chilled Water Systems vs. DX

For large cooling loads chilled water is the system of choice for a number of good reasons, but this choice creates new single points of failure. When the consequence of the failure is modest, chilled water may still be appropriate. However, when reliability is a high priority, air-cooled systems distributed by zone have the advantage. Since it is not centralized and does not use common piping, air-cooled equipment does not share the weaknesses related to the central installation philosophy. Consider the following single-point failure opportunities from the conventional central chilled water plant. Even with redundant equipment, the air-cooled design is inherently more reliable since it isn't central. It all comes back to having all the eggs in one basket—or gasket.

Central chilled water system weakness/single-point failures include:

- Main chilled water piping—headers and valves;
- Main condenser water piping—headers and valves;
- Single water supply for cooling towers;
- Single electric supply for chillers; and
- Ancillary damage from pipe rupture.

Despite the risks, it is not unusual for critical cooling loads to be served with chilled water. In some cases the lack of failure represents luck. In systems piped in steel, it speaks to the low probability of failure for this material when used for common piping. It may also suggest that reliability importance is not mission critical. For example, a data center with parallel offsite data storage capabilities *can* afford to go down once in awhile.

It may also indicate that energy cost is as compelling to the business as reliability.

Pipe Headers

Common piping is a single point of failure. All connections to a header/manifold, through the first valve (called the *root valve*), are all part of this single-point failure item. Avoiding brittle or fragile materials is a good approach because a drip is easier to manage than a burst. One way to select a pipe material for a single point of failure application is to imagine standing on top of it with a sledgehammer and pounding on it over and over, and select the material accordingly.

Even when the piping is suitably constructed and tough, valves need to be considered. Ask yourself, "If a valve leaks and needs to be repaired, then what?" Sometimes redundant valves are used to allow the second valve to be repaired through operation of the root valve. This prolongs, but does not eliminate, the inevitable system shutdown due to these valves. For all common piping systems it is only a matter of time before a shutdown is required.

Small connections to large header piping create opportunities to break off; one option is to specify not less than 2 in. (50 mm) connections to a header, then reduce down after the root valve.

In a noncorrosive environment, steel is a forgiving material due to its toughness, and a complete rupture of good quality steel pipe is unlikely. However, pipes manufactured with seams are inherently weaker than seamless pipe. Field connections are riskier than factory connections due to quality control concerns. *Study the specifications.*

Reducing Risk of Failures in Common Header Piping (Steel)

- Establish a service life that is well short (half) of normal expected life so it never gets old while in operation. This is a proven method for aircraft engines to maintain good reliability and safety. This affects life-cycle cost.
- Identify the common piping of interest on the construction drawings to communicate to contractors

where special attention is needed. Priority systems can be highlighted on electronic drawings during design.
- Create a separate strict specification section governing common piping. This will add cost but only to that portion of the work.
- Use 2 in. (50 mm) minimum connection size to reduce the chance of a small pipe breaking off a big pipe.
- Use thicker wall piping.
- Use seamless steel pipe and fittings, all welded connections, no coped connections or saddle welds, no threaded or grooved joints until after the root valve.
- Use high quality root valves.
- Perform rigorous pressure testing.
- Use strict welder certifications and independent field testing of welds.

Diminishing Benefits

There will always be *something* that can create a failure. Striving for absolute perfection is futile. Eventually, a point will be reached where additional measures provide little improvement and either create new points of failure or other compromises. Examples:

- With each addition of N+ equipment on a common header come new fittings, welds, and valves. When it comes to connections to common piping, less is more.
- A transfer switch is a common point between normal power and emergency power and a failure of this switch can take out *both* sources.
- Double-ended switch gear accommodates twin utility feeds, but includes a common point of failure: the tie breaker.
- Many variable speed drives have bypass options, but most do not allow energized maintenance, so a shutdown is required anyway.

Testing

For newly constructed systems it is important to establish confidence in what the system can and cannot do, and to identify early failure or equipment defect issues. Testing should impose a sustained and repeated *full* load on the equipment and fully take the system through all its operating modes. Documentation of initial testing, and periodic retesting, serves as a valuable training tool for operators. Design elements that cannot be tested once in service should be avoided. Testing work is ideally performed with operating staff but can be done with the assistance of a professional commissioning company.

Contingency Plan

Where reliability is crucial, a backup plan helps operating personnel to respond effectively. No plan can anticipate every contingency and it is not practical to have a backup for every possible failure. However, preparing and reviewing such a plan will serve to create awareness and to mitigate losses should a failure occur. Include in your plan:

- An overall review of priorities;
- Notations of all single points of failure;
- Curtailment actions for nonessential loads;
- Failure scenarios and the action steps needed to mitigate each;
- Locations of key elements, such as valves and switches;
- Contact information for emergency/temporary equipment and support; and
- One-line diagrams that show strategic points of operation.

Additional Study: Quantifying Reliability

Although beyond the scope of this article, there is a specific field of training for engineers tasked with managing and quantifying reliability; applications include aircraft safety and manufacturing defects. One established method is the Failure Mode and Effect Analysis (FMEA). With this method, failure items are arranged individually and in combinations using *and/or* logic chains to establish overall probability of failures. A one to 10 rating is assigned to provide weighting of each failure scenario for *degree of severity,*

SCENARIO:

MAKEUP WATER SUPPLY PRESSURE IS LOST AND THERE'S NO WATER. | IN 15 MINUTES, THE COOLING TOWER SUMP IS EMPTY. THE CHILLER HAS SHUT OFF. | WITHIN 10 MINUTES THE CHILLED WATER TEMPERATURE IS ABOVE 55°F (13°C). ALL MECHANICAL COOLING SHUTS DOWN. | THE DATA CENTER IS DUMPING DATA TO TAPES AND SHUTTING DOWN. | CLEANROOM CONDITIONS ARE LOST AND THE PRODUCT IS DISCARDED.

THE ROOT CAUSE OF THE DAMAGE IS LOSS OF WATER. THIS IS A FULL SHUTDOWN THAT OCCURS WITHIN 30 MINUTES, SO THERE IS NO TIME TO CUT OFF NONESSENTIAL LOADS. MITIGATION OPTIONS FOR WATER LOSS ARE REDUNDANT UTILITY WATER FEED, ON-SITE WATER STORAGE, DEEPER BUILT-UP COOLING TOWER BASIN, WATER TANKER CONTRACT, OR CONVERSION TO AIR-COOLED SYSTEMS. THE BOTTOM LINE IS THAT RELIABILITY MUST BE PART OF THE DESIGN BEFORE THESE PROBLEMS OCCUR.

probability of occurrence, and ability to detect, allowing a long list of failure possibilities to be prioritized. Like any estimate, the accuracy of the prediction is limited by any subjective values assigned. Still, a significant benefit of this method is identifying failure opportunities in complex systems that may not be evident using intuition and design experience alone.

10 Steps for Improving Reliability Through Design

Steps are in order of greatest effect.

1. Select systems that inherently have fewest single

points of failure. Equipment sets that depend less on shared resources are best.

2. Specify equipment that is inherently reliable. Often this means simplicity and fewer moving parts.
3. Arrange primary equipment in multiple 'baskets,' using N+ options, striving for equipment arrays that fail soft.
4. Identify remaining single-point failure items including common piping, wiring, and utility feeds. Prioritize them based on severity and likeliness. Adjust design type, or provide mitigating design treatment. Treat shared infrastructure more strictly in design than branch systems that are outside the boundary of the single-point failure zone.
5. For systems with shared distribution, make provisions to turn off nonessential loads.
6. Allow for using temporary equipment in response to a failure. Design provisions such as mechanical system tie in points in strategic locations, spare circuit breakers, and space for parked equipment can be of great assistance to the contractor if this work becomes necessary.
7. Avoid fragile materials and those that fail suddenly or totally in favor of those that have partial failure modes.
8. Be aware of the diminishing benefits of additional measures. Understand that no system is completely fail-proof. Avoid creating new single points of failure with design approaches.
9. Question all designs. "What happens if this fails?" and "What is left when this fails?" Document system limitations and create a contingency plan for operating personnel. Ensure the system design can accommodate periodic testing.
10. Get multiple opinions from other engineers. Ask them to be critical and find flaws.

Bibliography

ASTM A53/A53M-07, *Standard Specification for Pipe, Steel, Black and Hot-Dipped, Zinc-Coated, Welded and Seamless.*

Schwaller, D. 2003. "Hierarchy of HVAC design needs." *ASHRAE Journal* 45(8):41–44.

Turner, W., S. Doty, eds. 2007. *Energy Management Handbook,* 6th ed., Chap. 23, Energy Security and Reliability.