SIW SECURITY INFOWATCH.COM

INTEGRATORS

# How to Achieve Harmony in Security Design Projects

Analyzing common specification and implementation mistakes can help maximize the consultant-integrator relationship – which of course leads to a successful project and a happy client

Frank Pisciotta

> ***This article originally appeared in the March 2021 issue of Security Business magazine. When sharing, don't forget to mention @SecBusinessMag on Twitter and Security Business magazine on LinkedIn.***

Integrators and consultants can sometimes find themselves at odds during a project for a variety of reasons, but it does not have to be this way if everyone stays humble and focused on what is in the best interest of the end-user.

In 30 years as a consultant, I have made and observed some of these mistakes, and I learned from them to become a better partner in the security design process. Consultants write the specifications and prepare the drawings; integrators are expected to interpret those and provide pricing for the project. If anything gets out of balance from either the integrator, the consultant or even the end-user, the project is going to suffer substantially, and there are going to be losers in the process.

The integrator/consultant team should be working together to agree to a successful outcome – which includes a profit for the integrator, an effective security system for the end-user, and a satisfied reference for the consultant. If any one of these conditions is not met, the project cannot and should not be considered a success.

Harmony is achievable in security projects between the consultant and the integrator – with the proper coordination, communication and commitment, the consultant and the integrator can make each other's lives easier which is a benefit to the end-user. If a project ends with a different integrator than when it started, that is a shame, and something obviously went wrong – perhaps one of the causes in the charts that follow.

## Common Mistakes by the Consultant

It is easy for the consultant to abuse the authority vested by the end-user or architect and include petty and unreasonable expectations in the security specification – which in some cases include scapegoat clauses used to cover up a poor design. In other cases, a specification and design are flawed and the integrator(s) is left to sort it out.

In any case, common mistakes by the consultant inevitably trickle down to the integrator; thus, ensuring a harmonious relationship is incumbent on both sides understanding how to mitigate or solve them .

### Common Mistakes by the Consultant with Explanation and Solution

**1. Poor Spec Clause –** In the event that any subsection in the site-specific section of an RfP contradicts with information or specifications found in any other section of the document, the most stringent requirement or specification shall prevail. Should uncertainty exist, a Request for Clarification should be submitted to the project manager for an interpretation.

Explanation – Classic example of a practice to shift the responsibility for poor or incomplete design. Consultant can hold the integrator responsible for the worst-case scenario and creates a no-win bid situation for the integrator.

Solution – First, if a design cannot be completed properly, consider a design-build approach to the project; second, the consultant should complete the design with the appropriate schedules, bill of materials and device counts, and own the results.

**2. Poor Spec Clause –** Drawing requests which are unreasonable for the phase of work; asking for detailed labor-intensive drawings too early in the process.

Explanation – An example of an unreasonable drawing request would be to request a detailed riser diagram with a proposal. This is an unnecessary exercise for the integrator, and if the consultant has not taken the time to develop a riser, it is not reasonable to expect bidders to invest this level of effort before they have been awarded the project.

Solution – Detailed drawings such as riser drawings should not be requested until a bid has awarded and likely at the point when shop drawings are required at the beginning of construction.

**3. Poor Spec Clause –** It is possible that portions of the document contain text and language that does not apply to this specific project. When sections are clearly not appropriate, they should be disregarded.

Explanation – This is an extremely bad clause and practice. Specifications are typically too long as it is, and having extraneous information and expecting the integrator to pick and choose what clauses apply is setting a project up for failure.

Solution – Remove all text not needed.

**4. Poor Practice –** Failing to periodically vet the consultant's specification with trusted integrators to get candid feedback on clauses which may be unreasonable from the integrator's perspective.

Explanation – This demonstrates a lack of humility and unwillingness to look at the situation from the integrator's perspective. Unreasonable clauses can also unnecessarily inflate the cost of a project which is a detriment to the end-user, and in some extreme cases, may even result in a project being cancelled – which hurts everyone.

Solution – Consider an annual review with a different trusted integrator to get feedback on specification content.

**5. Poor Practice –** Failing to periodically review a specification and trim out content which is no longer needed. If you talk to any consultant, he or she will relate a story about getting burned on a project and adding a new clause to the specification to "prevent that from happening again."

Explanation – Allowing a specification to balloon up without governance and consolidation reduces the risk that the spec will get read – which is again a great danger to a project and can easily lead to discord and a lack of integrator profitability.

Solution – Embrace simplicity and always look for opportunities to streamline specifications.

**6. Poor Practice –** Failing to visit a job site early enough in the project to identify potential workmanship issues which are contrary to the drawings or specifications. For on-premises systems, the classic example is wiring and workmanship inside the enclosure or the IDF.

Explanation – Failing to visit the work site and getting errors corrected before they are repeated protects against schedule risk and decreased integrator profitability.

Solution – First, make a construction site visit early in the process to get things moving in the right direction early on; second, use the pre-bid meeting to remind the integrator about key workmanship clauses that will be checked regularly.

**7. Poor Practice –** Designing a system that will not work as intended. We have seen cases where the integrator spent so much time troubleshooting that there was a demand for a change order, which put the owner in the middle of a dispute.

Explanation – The consultant can get into a position of either over designing a system, or where multiple systems need to work together – failing to consult with the manufacturers' inside sales engineers or have a peer review of the design to confirm feasibility.

Solution – Consider leveraging manufacturers or peers in reviewing complex security designs to ensure that the integrator is not left to troubleshoot a faulty design.

**8. Poor Practice –** Failure to listen to alternative design options by the integrator.

Explanation – The consultant can sometimes be too prideful and not acknowledge the expertise of the integrator with the equipment and fears that credibility will be damaged by using the integrator's idea.

Solution – Respect the knowledge of the integrator and accept an alternative idea which delivers better results and lower costs for the end-user.

## Common Mistakes by the Integrator

When integrators work with a consultant, both parties should work within their respective areas of expertise. Consultants should refrain from over-designing; and in turn, integrators should play a part in the process by offering alternative design options that may deliver better results and lower costs for the owner.

Consultants should properly project the level of effort to properly design a system, including quality control measures to produce a workable and efficient design for the integrator. Integrators should avoid the common mistakes in the chart below:

### Common Integrator Mistakes with Explanation and Solution

**Mistake No. 1 –** Not reading the specification or failing to provide a copy of the specs and drawings to the technician(s) in the field.

Explanation – There is just no excuse not to read the specification if you choose to bid to such a project. It is irresponsible and risky to just jump to part two and see what equipment is specified.

Solution – The specs and drawings should be completely reviewed, and those documents provided to the technician(s) in the field.

**Mistake No. 2 –** Observing a design flaw in a specification and drawing and failing to bring that to the attention of the designer, knowing that this flaw will likely result in a change order after award.

Explanation – This gets into the ethical boundaries of project participants. Would the integrator believe that the overall harmony and relationship between the owner and consultant would be better if the integrator was transparent before the bid, or after forcing a large change order on the project or springing a change order after award?

Solution – Gain favor and a good reputation by raising the concern prior to the bid as this will demonstrate your competence in security system engineering and may increase your chances of getting an award – particularly in qualifications-based projects.

**Mistake No. 3 –** Failing to properly train the end-user on the proper use of the system. This might be one of the "all-time" most common problems in the security industry today.

Explanation – Technicians typically do not make good trainers, and starting with chapter one of the manual and finishing with the index is not a workable training strategy. Security systems are intended to reduce security risk, so the design, installation, operation and maintenance practices have to be perfectly aligned with the risk reduction strategy.

Solution – A proper risk-based training program needs to be developed in cooperation with the consultant, the integrator and the end-user. The need for a quick reference cheat sheet or summary tutorial for tasks which will only be performed infrequently.

**Mistake No. 4 –** Failing to complete the system or pre-commissioning performance verification before it is time for commissioning.

Explanation – This is simply bad practice and impacts every participant negatively. Poor performance results in unnecessarily long punch-lists and wastes project time and resources.

Solution – Ensure the system has been fully tested and written proof shown – in the form of system event reports – can result in a much more efficient commissioning test, saving time and money for all parties involved.

## Common Mistakes by the End-User

The client is an important part of this process that obviously cannot be ignored. Integrators who do not have the experience in risk assessment should encourage the end-user to use a risk assessment process (for example, the one we provide at www.securingpeople.com/physical-security-risk-assessment) as the foundation for the basis of design for technology deployment.

Here are the two common mistakes that clients tend to make:

**Mistake No. 1** – The scope of the project is a moving target and decisions are not made in a timely manner or changed frequently throughout the design or installation, resulting in inefficiencies for all parties.

Explanation – With luck, this type of client can be identified early in the process so that careful and deliberate decision-making can be made – and most importantly, documented – to defend change orders, which are never desirable but sometimes unavoidable.

Solution – If the project starts out with a risk assessment, it is easier to align the owner with an approach to the use and deployment of technology, otherwise people and opinions change over time. Additionally, all of the contractors involved (both consultant and integrator) must write tight proposals that clearly outline assumptions and deliverables.

**Mistake No. 2** – There is a project where a consultant is not involved. Due to lack of proper training, the end-user becomes disillusioned with a product and unnecessarily disparages the product and goes and gets a new vendor to replace an otherwise good product.

Explanation – The consultant can help the owner get to the root cause of the problem and help to negotiate a better outcome with independent supervision of the outcome. This can save a customer for the integrator.

Solution – Whenever a project owner is contemplating security technology and there is not a long-standing trusted integrator partnership or system standard, seek an independent consultant with no ties to manufacturers or hardware. Consider www.iapsc.org.

## Best Practices for Smooth Projects

The common mistakes in these charts may be a lot to digest, but here are some best practices that will help them be avoided, and thus, a successful project achieved. In these ways, we can all harmoniously serve the end-user client, which should be the sole focus of our work efforts:

- Humility by all parties – no competition or ego among consultant/integrator to see who is smarter.
- Never put the end-user in the middle of a dispute that is happening between the consultant and the integrator.
- Integrators should consider establishing a relationship with consultants in the area in advance of a project; conversely, consultants should be aware of the local, regional and national integrators in a given area.
- Integrators should read the bid documents and follow them.
- If one makes a mistake, own it, pay for it and preserve your word and reputation. In the end, that is all you have.

*Frank Pisciotta, CSC, is president of Business Protection Specialists Inc. (www.securingpeople.com), an independent security consulting firm focused on risk identification, regulatory compliance and security design services. He has managed more than 4,500 security-consulting engagements in his 30-year consulting career and earned his CPP from ASIS in 1994. He has also been certified as security consultant by the International Association of Professional Security Consultants. Email him at fp@securingpeople.com.*

**Source URL:** https://www.securityinfowatch.com/integrators/article/21213685/how-to-achieve-harmony-in-security-design-projects