SIA | PSA

Security Industry Careers Guide

Secure Your Future

Table of Contents

The Security Industry: Protecting People, Privacy, and Information

The world is full of risks – from pandemics and natural disasters to civil unrest, crime, war, and even online data breaches and identity theft. That's why individuals and organizations around the world invest billions in security technology to safeguard people, property, and information. From a video doorbell on a family's house to high-tech imaging systems used for baggage screening at the airport, the need for security impacts every part of society, including:

- Homes
- Retail stores
- Hospitals and healthcare facilities
- Schools and universities
- Transportation centers
- Manufacturing plants
- Infrastructure
- Stadiums, arenas, and public spaces

At the Security Industry Association (SIA), we represent the companies that manufacture, install, and support security solutions for all of these clients. And we welcome you to consider a career in our rapidly growing, constantly evolving, technologically innovative field, where you can develop and apply your skills to make the world safer for everyone.

A Secure Future

There are a wide range of fulfilling, well-paid, high-growth careers within the security industry, from entry-level technician roles installing and servicing systems to engineering positions focused on designing the next generation of security technology. There are also excellent career opportunities for software developers, salespeople, project managers, and more.

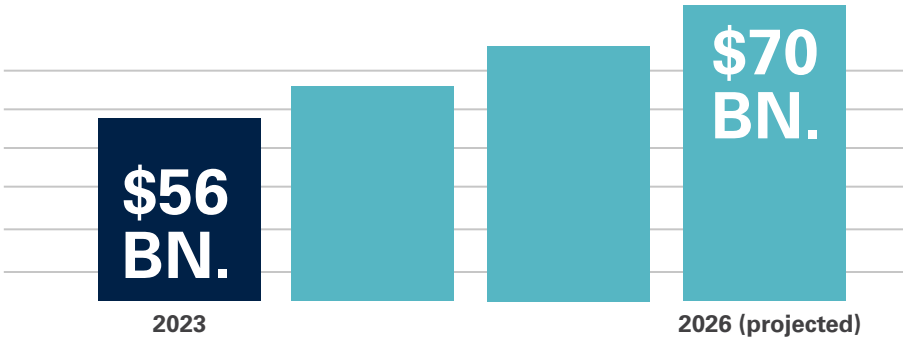
The educational requirements for security industry jobs vary considerably. Some positions can be learned on the job with a high school diploma, while others require advanced university degrees. And even if you enter the security industry in one role, there are often opportunities to advance or transition into other roles (for example, from engineering into sales or from installation into project management) as security companies are often committed to "promoting from within." Around 70%-80% of security industry professionals report that their previous position was in the security field.

The security industry has seen steady growth over many decades, and compensation, job security, and opportunities for advancement within the industry match or exceed comparable technical fields. **Increasing demand for security solutions has created a situation where companies need skilled workers more than ever, meaning there's never been a better time for new applicants!**

Security Industry Outlook: By the Numbers

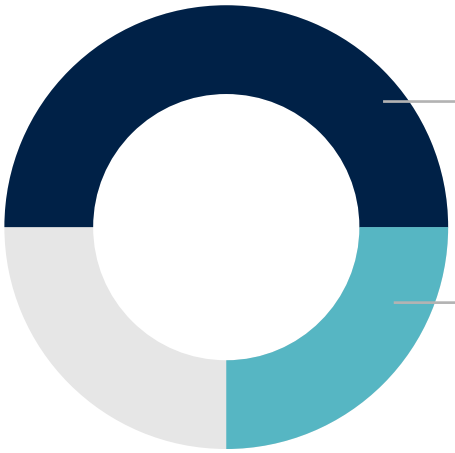
The market for security systems and equipment has experienced significant growth in recent years (especially in cybersecurity). See the following data from SIA'S industry survey:

The total value of the "physical" security equipment industry (excluding cybersecurity and "security services" such as guards and investigators) was **$56 billion in 2023** and is expected to increase to **$70 billion by 2026**.



Apart from a pandemic-era slowdown (due to supply chain shortages impacting all technology industries), **the industry has enjoyed steady growth over the past several decades and is forecasted to grow at 9% year-on-year.**

Companies in the security industry are optimistic about their futures, and looking to grow their organizations:



51%
Responded **"good."**

24%
Rated current business conditions as **"excellent."**

80% predict **even better conditions** in the near future.

Global Security Industry Employment

245,000
Security equipment manufacturers and distributors.

980,000
Providers of security services

Employers in the Security Industry

Many different types of companies are involved in designing security solutions, installing systems, and manufacturing the technology components that go into them. Each member of the "security ecosystem" offers a range of unique career opportunities.

End User (Client) Organizations

Every security project begins with the needs of an "end user" organization: it could be a factory looking for a way to monitor its facility, an apartment building looking to secure its doors and elevators, or a college campus concerned about student safety.

Security solutions are almost never "one size fits all." Most end users have specific requirements unique to their organizations and/or the facilities they need to secure, and will reach out to a security consultant to advise on their overall approach to security, from facility design to risk reduction strategies, in addition to the technical aspects of their security systems.

Security Consulting Firms

Security consultants work with end users to clarify performance requirements for the security solution based on the client's needs, industry standards, and any relevant laws or regulations (e.g., does an access control system comply with the requirements of the americans with disabilities act?). They will then design the system and provide detailed instructions (specifications) for how the system should be installed and operated.

The security consulting firm will assess any risks involved in the project, to help the client avoid cost overruns or schedule delays. They will also define the acceptance test criteria, so the end user can confirm whether the systems integrator implemented the system to specifications.

Systems Integrators and Installers

Systems integrators work with security consultants, handle the details of designing security systems and the hands-on work of building and installing those systems. Their responsibilities range from sourcing equipment and materials from dealers through installation and final testing to verify that the systems are working properly.

Often, the same company will handle both the "integrator" (design) and "installer" tasks for a project. However, for very large or complicated jobs, the work might be divided between multiple companies, with an integrator hiring out one or more installers to implement the system the integrator designed.

Technology Distributors

Security technology distributors serve as intermediaries between manufacturers and end users / integrators, providing the equipment and materials that go into security systems. In some cases, they might simply sell products, while in other cases they might offer services and support for solution design, installation, and training of operators, as well as maintenance after the sale.

Manufacturers

Manufacturers create the technology products that make up security systems, from video surveillance equipment to sensors for intrusion detection, access control systems, door locking hardware, notification systems, computer network infrastructure, and the software that manages all of these components.

"Manufacturers" can include both brand-name companies that manufacture their own products, as well as OEM (original equipment manufacturer) companies that design and manufacture products and components which other companies rebrand and sell.

Job Roles / Career Paths in Security

The security industry offers a wide range of career opportunities. The following sections describe the various roles within each category including:

Project Management

Project managers coordinate the work of other specialists, whether it's a team of engineers designing a new piece of equipment or an integrator's crew installing a system on site. While a project manager might or might not have hands-on technical skills, they need to understand how the various components of a system work together and know enough about every technical discipline to give clear directions to the team. They also need incredible organization and time management skills, to ensure that time and money are not wasted, as well as excellent communication skills, as they are often the go-between for the technical team, the client, and their company's management.

Project management is a great career path for people with a mix of technical, business, and interpersonal skills. Most project management roles require a college degree and some prior experience in the industry (e.g., as a technician or engineer).

Project Management Roles

- Security project manager (SPM)
- Product development manager
- Technical project manager
- Architectural & engineering program manager

Security Stories

Tia Eskandari

Director of Service, Southwest, Allied Universal Technology Services

After 18 years in retail management, I transitioned into the security industry through a referral from a friend. I joined a technology and systems integration company in 2019 as the regional service manager. I had a passion for project management and decided to work toward obtaining my project management professional (PMP) certification while I learned my new role. I was able to earn the certification in the spring of 2021 with support from the SIA Women in security scholarship program. When my company was acquired by Allied Universal, I became the director of service for the southwest region for Allied Universal technology services. I was responsible for driving the overall execution and performance of the field service staff and ensuring that we provide the best service to our customers. I learned a lot about the industry in a short time, and the connections I have made have been instrumental in my growth.

I had no idea where my path would lead me when I decided to join the security technology industry. I am grateful for all the opportunities I have been afforded and the amazing growth of our industry, especially for women.

Esteban Pastor

Sr. Product Manager, ZKTeco USA

After spending my 20s chasing the dream of becoming a rock star, touring the world, I had to face reality. I always had a passion for technology, and spent two years working for a camera manufacturer, but I was still seeking something more. I responded to an ad for technical support at an access control company, not realizing that my previous job had prepared me for a career in security. I immersed myself in learning everything I could about access control and security and discovered something I was truly passionate about. This allowed me to climb the ladder, advancing from technical support engineer to enterprise solutions specialist, product manager, and now senior product manager, collaborating with global teams on multiple products and solutions. Along the way, I've built meaningful connections and met incredible people.

With these years of experience, I'm excited about the future of this industry. The rapid pace of technological advancements keeps us on our toes, constantly evolving and bringing innovative solutions to life.

Engineering & Design

Engineers and designers develop new technologies and/or find ways to apply technology to solve specific security challenges. This could include an electrical engineer at an equipment manufacturer designing components for a biometric scanner, a systems engineer determining the best combination of cameras to monitor the grounds of a resort hotel, a CAD technician creating a 3D model of a stadium's security system, or an implementation engineer figuring out the best way to run cable to a hard-to-reach corner of an aircraft hangar.

Engineering and design is an excellent career path for people who enjoy technology, mathematics, and creative problem solving. Nearly all engineering roles require a college degree in a relevant field of engineering (e.g., electrical engineering, mechanical engineering, industrial design, systems engineering, etc.).

Engineering & Design Roles

- Engineering & design roles
- Systems engineer
- Implementation engineer
- Product development engineering & design roles
- Solutions engineer
- Drafter / computer-aided design (CAD) technician
- Specifications writer

Security Stories

Chris Gordon

Embedded Systems Engineer, Home Depot

While completing a degree in mechanical engineering technologies, I discovered a passion for security technology through my coursework and hands-on projects. I started my career as an apprentice at SAGE Integration, which laid the foundation for my expertise in security systems installation and maintenance. Following graduation, I transitioned into a systems engineer role at SAGE, immersing myself in the complexities of access control systems, CCTV, and weapons detection technologies.

Each project led to more challenging responsibilities, including leading implementations across multiple locations, with responsibility for testing security systems, optimizing new technologies, and presenting them to customers.

Today, as an embedded system engineer at the Home Depot, I oversee security services across 62 cities and 7 countries including weapons detection implementations, access control, CCTV systems, and other security measures.

What I find most rewarding is enhancing our customers' sense of safety. Witnessing their relief after resolving security concerns is an incredible reminder of the impact of my work in creating safer environments.

Maya Sears

Mechanical Engineer, Product Development, dormakaba

With a degree in mechanical and aerospace engineering, I initially aimed for a career in aerospace. However, during my senior year at Rose-Hulman Institute of Technology, I interned at dormakaba in product development. Despite my limited knowledge of the security industry, I was welcomed by a fantastic team of engineers who answered my questions and entrusted me with meaningful projects.

This experience opened my eyes to the immense potential and value within the security field, and after graduating, I returned to dormakaba full-time.

My role allows me to problem-solve and design, and provides a sense of satisfaction knowing that I contribute to the safety of those around me. Although I am still early in my career, my work as an engineer is incredibly rewarding. I am proud to be part of a field that is dynamic, essential, and is increasingly welcoming to women in traditionally male-dominated areas.

Installation, Service, & Quality Control

Technicians do the hands-on work of installing, connecting, and, testing the components of security solutions. This could include a quality control technician making sure a newly-manufactured batch of sensors is working properly to an installation technician placing those sensors in the walls and ceilings of a government facility or a service technician troubleshooting a malfunctioning camera on a client's site.

Some technician roles only require a high school diploma, two-year technical school degree, and/or an apprenticeship while offering highly competitive pay.

Installation, Service & Quality Control Roles

- Installation technician
  - Commercial
  - Residential
- Installation manager
- Service technician
- Quality control technician

Security Stories

Bobby Louissaint

Head of Technical Partnership Engagement, Meta

When I was younger, I always thought I would end up in the music industry as an engineer or similar role. However, when it came time to find a steady job, I had three friends working in security doing residential installations who were earning great money. Eventually, I joined them and started my career as a residential installer. I discovered that there were numerous opportunities within the industry, whether in residential, small business, or commercial settings.

Over my career, I've held various roles: technician, project manager, program manager, and leadership positions, and have found immense fulfillment in this field. I vividly remember the first time a system I installed played a part in saving lives during a fire at a large soda manufacturer in Downey, California. That experience made me appreciate how my work could make a difference. Furthermore, our industry has a significant, yet potentially unrecognized or untapped impact on the world, and it is incredibly rewarding to know that security is a necessity rather than a luxury.

Ruben Cuevas

Security Technician Superintendent, Preferred Technologies

I began my career in construction, but became curious about how security professionals I worked with installed their equipment: watching them set up cameras on lifts, pull wires for badge readers on doors, and install vehicle tag readers at gates, along with the tools they used.

I transitioned into the security industry field as a low-voltage technician, then worked my way up to lead technician, gaining valuable experience installing various types of security equipment, before being promoted to superintendent, overseeing projects in both commercial and industrial settings.

For me, this isn't just a job; it's a way to serve my community, ensuring that users are protected.

Cybersecurity and Digital Technology

Digital technology is critical to modern security, whether it's a team of cybersecurity experts protecting an organization's computer networks and data from malicious hackers or software engineers developing the code to process security camera images or AI / machine learning specialists finding new ways to detect suspicious patterns across all the different sensors in a facility's security system.

Cybersecurity, IT, and digital technology roles are excellent for people who enjoy coding and/or working computer hardware. Most positions require a degree, though some might only require a certification or two-year degree.

Cybersecurity & Digital Technology Roles

- Cybersecurity specialist
  - Integrator
  - Manufacturer
- Cybersecurity analyst
- IT / network specialist
- Application developer/programmer
- Applications engineer
- Machine learning / AI engineer

Security Stories

Will Knehr

Senior Manager of Information Security and Data Privacy, i-Pro Americas Inc

I started my career as a cryptologist in the Navy, where I worked to secure networks for the Department of Defense and other government agencies. The job primarily consisted of hardening networks against attackers, conducting threat hunt missions against advanced persistent threats, vulnerability analysis, and auditing secure networks for compliance. After I left the Navy, I went to work for one of the largest defense contractors in the world, running the cyber security operations center (CSOC) for the Defense Information Systems Agency and building specialized malware analysis labs for the National Security Agency.

I never thought about working in the security industry until I received a call out of the blue from a large security products manufacturing company that was looking for someone to come in and build a cybersecurity program from the ground up, and I haven't looked back since.

People in the security industry have been amazing to work with, welcoming me with open arms. A professional in this field can directly impact critical infrastructure for healthcare, schools, manufacturing, finance, and more, interacting with just about every technology you can think of. It's a rewarding, growing, fast paced industry with a lot to offer.

Technical Sales & Support

Security solutions are complex, and it takes a high degree of technical expertise as well as excellent communication and people skills to explain them in terms customers can understand.

Technical sales and support careers are excellent for people with a good balance of "people skills" and technical skills. Technical sales professionals usually come from an engineering or other technical background, and can often earn lucrative commissions. Education requirements for technical support positions will vary.

Operations Roles

- Sales engineer
- Technical support representative
- Technical trainer

Security Stories

Hannah Brauer

Associate Regional Sales Manager, i-Pro Americas Inc

I started my career in a very cutthroat industry working for large corporations where employees often felt like "just a number." Ready for change, I began searching for a company culture that aligned with my personal values and principles. Fortunately, I had the opportunity to join a new and innovative security camera manufacturer.

Working for a start-up company, I found myself in many high-level meetings I never imagined myself in so early in my career. In one of those meetings, I strongly expressed what I felt was a lack of productivity that day and insisted on each leader providing action items to address the issue (it had been a long day!). This caught the attention of our company's president who recognized the assertiveness and coordination I demonstrated during that meeting. He offered to create a new role for me within the company to oversee large projects and drive faster results.

I accepted the offer and for the next year and a half, I immersed myself in learning about our customers, channel partners, products, and operations. To my surprise, I loved it! One day I received a request from one of our midwest sales managers to help develop the territory and, once again, I was approached with a new position I never imagined – associate regional sales manager. The intent with this role was to add a junior salesperson to a territory that could be trained and mentored by a senior salesperson. I have been in a sales role for a year now and am still surprised at how much I enjoy my job. One of my favorite parts is working directly with customers and learning what they love about our products. I entered my career in HR with the desire to work with people, and the great thing about my sales role is I get to do that so much. A lot of the skills are transferable - negotiation, influencing change, organization, and communication - to name a few. I cannot say that I ever imagined this at the beginning of my career, but I have loved the twists and turns the security industry has thrown my way.

Pauline Powell

Sales Manager, LONG Building Technologies

After deciding to leave retail in 2009, I applied for an HR position with a large local security company. However, during the interview, they recognized my sales experience and persuaded me to take on an account executive role instead. In the beginning, I dedicated myself to learning the intricacies of security systems, building my own sales and marketing strategies. I quickly mastered operations and systems applications, selling more complex solutions and pushing the company to focus on commercial, government, and industrial clients. I broke the first-year sales record and continued to exceed my own expectations each year.

In 2013, I moved on to work in fire and property management before accepting an account executive position with LONG, where I helped launch their security division in Alaska and drive business growth. Sales soared consistently, placing me among the company's top salespeople year after year. As the company expanded, I took on mentoring, training, and leadership roles, which led to my recent promotion to sales manager. Today, I lead a team of nine account executives, supporting not only security sales but also HVAC service and building automation. I'm proud of my ability to bring diverse perspectives to sales strategies, mentor my team, and offer guidance to the leadership team in strategic planning and operations.

Other Roles

Security companies need talented professionals to handle their finances, human resources, marketing, warehouse operations, and all the other tasks that come with running a growing business. While this guide will focus on security-specific technical roles, security industry members also have a need for:

- Sales / business development
- Account managers / customer success
- Business operations
- Marketing
- Warehouse operations
- Procurement & purchasing
- Supply chain operations
- Service manager
- Support departments (HR, finance, legal, etc.)
- Executive leadership

Security Project Manager (SPM)

Alternative Job Titles
Project Lead, Job Manager, Installation Manager

Employed By
Integrators, Installers

Responsibilities

Security project managers (SPMs) oversee the installation/integration of new security systems as well as upgrades and expansions to existing systems. They're generally responsible for outlining the project's schedule, coordinating with the customer, directing the work of the project team members (including any external contractors hired to help with the job), and seeing the project through to a successful completion.

On a typical day, a security project manager might:

- Develop a plan for completing a new project based on the client's requirements and deadlines.
- Compare the number of hours worked and money spent to the overall progress of a project, to ensure the team is on track to deliver within budget and on schedule.
- Review the impact of any changes the client might request to the original scope of a project, and provide an estimate for how much those changes will impact the budget or schedule.
- Identify risks to the success of the project, and develop plans to address those risks.

Requirements

New project managers usually have a college degree in business administration, engineering, IT, or a related field plus five or more years of experience in the industry (usually in either a technician or engineering role). Obtaining a certified security project manager (CSPM) certification can improve chances of finding employment.

Compensation

Security project manager positions typically pay in the $75,000 to $110,000 range (plus bonuses), with the highest paid SPMs earning around $126,000 per year.

Work-Life Balance

The working hours and travel requirements for a SPMs can vary considerably depending on what company they work for, what projects they are managing, and the current stage of each project. SPMs overseeing low-complexity projects in their local areas might work a very consistent 40-hour week with little or no need for overnight travel. However, SPMs working on highly complex projects in different cities might work 50 or more hours per week and travel several days per month.

Because SPMs are ultimately responsible for the success of projects, they might need to put in extended hours when projects are on a tight deadline or when problems arise on a project.

Opportunities for Advancement

Successful security project managers might be promoted to "program manager," a role with broader responsibility for managing all aspects of their company's relationship with customers, including proposals, projects, and ongoing service and support.

Product Development Manager

Employed By Manufacturers

Responsibilities

Product development managers are responsible for coordinating the efforts of the engineers, designers, and technicians who create new technology products (or upgrades to existing products). It's their job to ensure that everyone on the team has the information and resources necessary to deliver a high-quality product on time and within budget.

On a typical day, a product development manager might:

- Review the specifications and requirements for a new product or proposed upgrade and create a plan for developing it, including budgets and schedules.
- Compare the number of hours worked and money spent to the overall progress of a project, to ensure the team is on track to deliver within budget and on schedule.
- Review the impact of any changes to the requirements / specifications, and provide an estimate for how much those changes will impact the budget or schedule.
- Report to their company's leadership on the progress of a development project.
- Identify risks to the success of the project, and develop plans to address those risks.

Requirements

Product development managers usually have a degree in engineering, IT, business administration, or a related field plus three or more years of experience in the industry, in either an engineering, design, or technician role. Obtaining an agile or scrum project management certification can improve chances of finding employment.

Compensation

Product development manager positions typically pay in the $120,000 to $150,000 range (plus bonuses), with the highest paid product development managers earning around $175,000 per year.

Work-Life Balance

A product development manager at an equipment manufacturer will usually have a highly structured work week, typically ranging between 40-50 hours with minimal need for travel. However, they might need to work extended hours during critical phases of a project and/or important presentations or meetings (depending on their company's culture regarding in-person vs. virtual meetings).

Opportunities for Advancement

Successful project managers might get promoted to "program manager," with broader responsibilities overseeing multiple products / solutions or specialize in user experience (UX) design, ensuring that products meet the needs of end users.

Technical Project Manager (TPM)

Employed By Integrators, Installers

Responsibilities

Technical project managers (TPMs) oversee the incorporation of software and IT components of new security systems (e.g., the computers that control cameras and sensors and the networks that connect them), as well as upgrades to existing systems). They discuss requirements with the customer, develop a plan (including schedule and budget), then oversee the work of the IT and software development teams.

On a typical day, a technical project manager might:

- Work with the engineering team to confirm the client's requirements are technically feasible.
- Make key choices about what software and services should be used in the system.
- Oversee the design of the overall software architecture to ensure that the various security systems – surveillance, access control, intrusion detection – can all work together cohesively.
- Identify what post-installation technical support, documentation, and maintenance services will be necessary to ensure the system operates successfully after deployment.
- Review the completed project to ensure that it meets technical specifications.

Requirements

Technical project managers typically have three to five years of project management experience in the security industry or a related field such as telecommunications. IT and project management certifications such as CompTIA Project+ are considered desirable by employers.

Compensation

Technical project manager positions typically pay somewhere between $115,000 and $140,000 (plus bonuses), with the highest paid TPMs earning around $150,000 per year.

Work-Life Balance

Technical project managers usually work 40-50 hours per week with minimal travel, though this can vary depending on the demands of their projects and the company they work for. TPMs may experience periods of increased workload when dealing with technical challenges or bringing projects to completion.

Opportunities for Advancement

Successful technical project managers may be promoted into more senior project management roles such as a technical lead or program manager, where they would be responsible for managing larger projects or multiple projects at once, or solution architect, where they have overarching responsibility for the design of all aspects of a solution / product.

Architectural & Engineering Program Manager

Alternative Job Titles
A&E Director

Employed By
Manufacturers

Responsibilities

Architectural & engineering (A&E) program managers work for manufacturers, and are responsible for customizing or upgrading products to meet specific client requirements. For instance, they might work with the product team to equip a surveillance camera with enhanced night vision for an extremely high-security site, or modify the physical appearance of security hardware to blend seamlessly into the decor of a luxury hotel.

A&E program managers often work directly with the sales department to determine how to respond to potential business opportunities. They also may also be involved with the R&D process in order to ensure that upcoming products align with the current and potential needs of customers.

On a typical day, an A&E program manager might:

- Work with architectural & engineering consultants to develop the technical specifications for specific client projects.
- Review and approve proposed designs, ensuring that they meet the specifications and requirements of the project they are being developed for.
- Provide project updates to relevant stakeholders, such as the client, outside contractors and consultants, and government agencies with a regulatory interest in the project.
- Review the status of existing projects to ensure that they have not deviated from the project's core technical specifications.

Requirements

This role requires a mix of commercial and technical expertise. A&E program managers typically have three or more years of sales and/or marketing experience, as well as a deep understanding of how technical specifications are developed and operationalized within architectural and engineering contexts.

Compensation

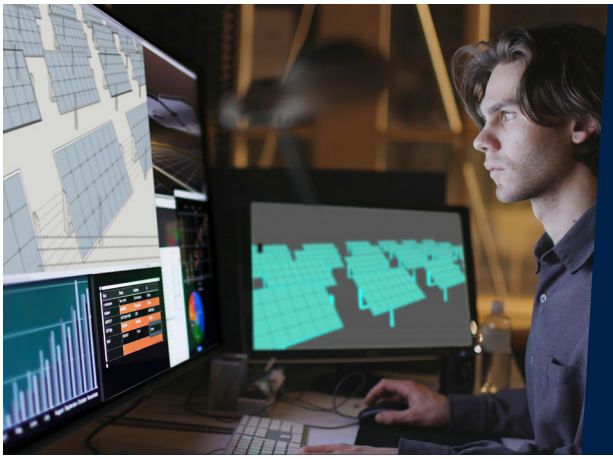
A&E program managers are usually paid $70,000 to $105,000 (plus bonuses), with the highest paid A&E program managers earning around $130,000 per year.

Work-Life Balance

The work-life balance associated with being an A&E manager can vary significantly depending on the project type and the phase of the project. When projects are at critical stages of development, the program manager may need to work extended hours. They may also be required to travel in order to meet with clients or perform site visits.

Opportunities for Advancement

Successful A&E program managers could potentially advance further into strategic leadership roles, such as engineering or technical director or become specialized consultants.



Systems Engineer

Alternative Job Titles
Electronic Security Systems Designer, Security Project Engineer, Development Engineer, Consulting Engineer

Employed By
Integrators, Installers, and some manufacturers that offer consulting services will also utilize Systems Engineers as part of their professional services offerings.

Responsibilities

Systems engineers are responsible for integrating the various components of a security project together into a single unified system. They select the hardware, software, and network components that are used in a security system, and they also determine how these components will be integrated with each other and the client's existing IT infrastructure.

After the initial system is designed, systems engineers oversee the testing and validation of the system, and configure the various components of the system to maximize performance.

On a typical day, a systems engineer might:

- Spend time developing the design and layout of a new layout by drafting schematics or creating network diagrams.
- Select the hardware and software components that will be necessary to meet the client's needs.
- Visit the work site in order to configure, test, and program various security systems and devices and ensure they are performing optimally.
- Develop the project documentation necessary to detail how the various components of the system should be installed, configured, and used.

Requirements

Systems engineers need to have a strong background in engineering or IT. Most companies require candidates for this position to have at least a bachelor's degree in electrical engineering, computer science, or information technology. Many of these roles also require significant experience within the security industry.

Compensation

Systems engineer positions typically pay in the $75,000 to $105,000 range (plus bonuses), with the highest paid systems engineers earning around $130,000 per year.

Work-Life Balance

A systems engineer's work-life balance will typically vary depending on the phase of the project. When approaching a tight deadline or during a critical period – for instance, during the installation process – they may need to work extended hours. Depending on the job, they may also need to be willing to travel to various work site locations.

Opportunities for Advancement

Successful systems engineers can move into technical sales, project management, program management (i.e., overseeing other engineers and project managers).

Implementation Engineer

Alternative Job Titles
Engineering Specialist

Employed By
Integrators, Installers

Responsibilities

An implementation engineer is responsible for taking the "on paper" designs for a security solution and translating it into a fully operational security system at the end user's facility. Implementation engineers are often called on to solve technical problems on the job, for instance if a team discovered that the electrical wiring in a client's building differs from the plans they were working on, and components might need to be repositioned or changed to accommodate it.

Implementation engineers develop an extensive understanding of security systems as well as the software applications that control it.

On a typical day, an implementation engineer might:

- Perform on-site assessments to ensure that all infrastructure necessary for the installation – such as brackets for mounting cameras, power supplies, etc. – have been properly implemented.
- Install or direct the installation of the security hardware that the system will rely upon to function.
- Configure and test the various hardware components.
- Document the installation process, including documenting any changes to the original design that were necessary.

Requirements

Junior-level implementation engineers are typically expected to have an understanding of basic engineering and programming principles. Senior-level engineers will be required to have advanced programming skills as well as a strong aptitude for engineering, and typically have at least five years of experience in an implementation engineering or adjacent role.

Compensation

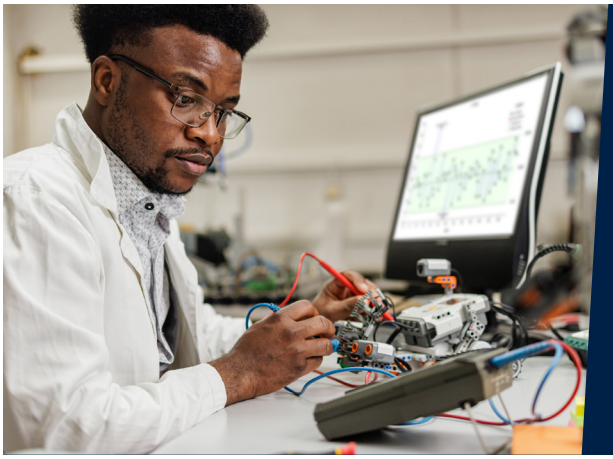
Junior implementation engineers are typically paid between $55,000 and $75,000, while senior-level implementation engineers are typically paid $85,000 to $100,000 (plus bonuses).

Work-Life Balance

Implementation engineers usually spend a significant amount of time working on-site, which may require them to travel depending on the work their company performs. They may also need to be on-call in the event that a system outage or other critical failure occurs. Due to the project-based nature of their job, the hours that an implementation engineer needs to work may vary depending on the phase of the projects they are involved in; during non-peak periods, implementation engineers may have significant flexibility when determining their schedules.

Opportunities for Advancement

Successful implementation engineers may advance to roles such as project manager or solutions architect, where they take on greater responsibility for overseeing the execution of security projects.



Product Development

Alternative Job Titles
Industrial Designer, Mechanical Engineer, Software Engineer, User Experience Engineer, Test Engineer, Mechanical Engineer, Electrical / Electronic Engineer, etc.

Employed By
Manufacturers

Responsibilities

Security technology products are designed and developed by multidisciplinary teams of specialists including electrical engineers, mechanical engineers, software engineers, industrial designers, and others, usually led by a project manager. For instance, a smart lock would need an electronics engineer to develop the circuitry, a mechanical engineer to develop the actual locking mechanism, a software engineer to program it, and an industrial designer to ensure it looks clean and attractive when installed on a door at a client's facility. In short, there are opportunities in the security industry for most every engineering specialty.

While their specific responsibilities will vary considerably depending on their specialty, product development engineers might:

- Discuss design specifications and limitations with designers and other engineers.
- Design, develop, and test the electronic components of security products.
- Select materials and components that are well-suited to the task, such as a durable, corrosion-resistant alloy for an outdoor lock.
- Test prototypes of the product to check that they behave as expected and meet the required standards.

Requirements

Product development engineers generally have bachelor's or advanced degrees in their specific engineering domain.

Compensation

Product development engineers make around $75,000 and $90,000 annually (plus bonuses), with the highest paid engineers earning around $140,000 per year.

Work-Life Balance

While a product development engineer might need to work additional hours in the days or weeks leading up to a deadline, typically they work a standard 35-50 hour work week. Travel might or might not be required depending on the specific nature of their products.

Opportunities for Advancement

Product development engineers might move into solution engineering, project management, or sales engineering roles, depending on their aptitudes and interests.

Solutions Engineer

Alternative Job Titles
Product Engineer, Software Engineer

Employed By
Manufacturers

Responsibilities

Solutions engineers ensure that a manufacturer's products, solutions, or software is aligned with the needs of their customers and the company's overall business strategy. They influence every part of developing products and custom solutions for high-profile clients, from early research and designs through product launch and support as clients begin implementing the product in their security systems.

They have a strong understanding of both engineering and business, and will work closely with the sales department, product development team, and client stakeholders to deliver a solution that meets and exceeds customers' expectations.

On a typical day, a solutions engineer might:

- Develop and propose a customized solution to address the needs of a potential customer, potentially designing bespoke solutions to address any unique needs that can't be met via standard product offerings.
- Gather feedback from customers and sales representatives and then present that feedback to the product team as guidance that can be used to ensure that the R&D process stays aligned with the needs of the market.
- Work with the sales team to determine how the company's products can be used to meet the needs of a potential customer, then assist in the development of the technical aspects of the sales team's proposal to that customer.

Requirements

Solutions engineers typically have a bachelor's degree in an engineering or technical discipline as well as at least three years in sales engineering or another customer-facing role.

Compensation

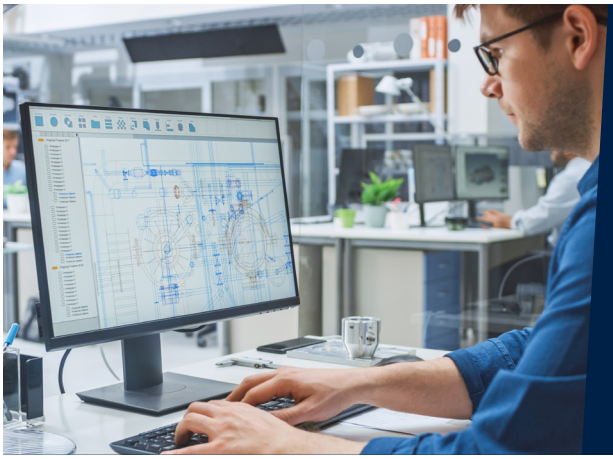
Solutions engineers are usually paid between $75,000 and $110,000 annually (plus bonuses), with the highest paid solutions engineers earning around $130,000 per year.

Work-Life Balance

Solutions engineers often need to travel frequently in order to meet with clients or provide on-site technical support. Due to the need to accommodate client schedules, they may need to hold these meetings outside of regular work hours. They are often able to work independently and with significant flexibility over their schedules as long as they are able to consistently meet their clients' needs.

Opportunities for Advancement

Successful solutions engineers may advance to roles such as product manager, where they take on greater responsibility for the overall performance of a manufacturer's product lines.



Computer-Aided Design (CAD) Technician

Alternative Job Titles
Drafter, CAD Operator, CAD Specialist, Building Information Modeling (BIM) Specialist

Employed By
Integrators, Installers, Manufacturers

Responsibilities

Computer-aided design (CAD) technicians, also known as drafters, are responsible for creating detailed technical drawings and plans for security systems and technology products, such as surveillance and alarm systems. They work closely with engineers and other technicians in order to understand the technical needs of the project and confirm that their CAD drawings meet those needs effectively.

On a typical day, a drafter might:

- Design precise schematics of a security system that will be used as blueprints by the installation team.
- Develop a schematic that shows the security system plan and the plan for the building it is being installed on. This schematic demonstrates how the security system should be integrated into the overall plan and will be designed to ensure that the security system complies with any building code requirements.
- Review a security system that has been successfully installed and create an "as-built" schematic that can be used to guide future maintenance, troubleshooting, and upgrades on the system.

Requirements

Most employers require a technical certificate in computer-aided design or engineering technology from a technical or vocational school. Programs that provide education on electrical systems, architecture, and construction can be particularly relevant for security system design.

Compensation

CAD technicians are typically paid between $66,000 and $75,000 (plus bonuses).

Work-Life Balance

CAD technicians typically work standard 9-5 business hours, and are less likely to be required to work overtime than many other security roles.

Opportunities for Advancement

Successful CAD technicians may advance to roles such as design engineer, where they take on greater responsibility for overseeing design projects, ensuring accuracy, and managing CAD standards and workflows.

Specifications Writer

Alternative Job Titles
Specification Business Development Manager

Employed By
Manufacturers, Consulting Firms

Responsibilities

Specifications writers are responsible for creating detailed documentation that describes the technical requirements and standards that a security system or product must meet. It is their job to take client requirements and turn them into clearly defined specifications that the project can follow when developing a product or implementing a security system.

Many specifications writers split their time between working with technical teams and sales / marketing teams to write the technical sections of bids and proposals.

On a typical day, a specifications writer might:

- Meet with product teams or clients so that they can fully understand the requirements of a given project, product, or service.
- Write the technical specifications for a security system, ensuring that those specifications reflect the client's requirements.
- Conduct research into industry standards, regulatory requirements, technical standards, and new technologies in order to ensure that their specifications reflect best practices and comply with all legal regulations.

Requirements

Specification writers typically have a degree in a technical discipline, with a strong emphasis on architecture for systems which are integrated within buildings or other architectural projects. Experience with technical writing is also a major asset and a knowledge of technical standards (e.g., ISO, NFPA), and regulations is also an asset.

Compensation

Specifications writers are usually paid between $60,000 and $95,000 annually, with the highest paid earning around $125,000 per year.

Work-Life Balance

Specifications writers have a project-based workload, which means that the size of their workload varies depending on the phase of the project. Their hours may extend beyond normal working hours during "peak" times of the year, such as when a key project deadline is approaching.

Opportunities for Advancement

A successful specifications writer may transition into a consulting, project management, sales engineer, or training role.

Installation Technician (Commercial and Residential)

Employed By
Installers, Integrators

Responsibilities

Installation technicians are responsible for installing the various components of security systems at a client's facility. Junior-level technicians will typically focus on installing basic components such as cabling and device mounts, and may connect some security devices to the system.

More senior technicians may install and connect the various devices such as sensors, cameras, access control systems, and network hardware, and perform some or all of the initial programming for those devices.

On a typical day, an installation technician might:

- Review the details of an installation project and ensure that they have all equipment and products necessary to complete the project successfully.
- Travel to the project site and install the mounting, wiring, cabling, and the devices themselves.
- Configure the devices to work with the security system, such as by adjusting camera angles, setting user permissions, and registering devices.
- Integrate the system with any existing IT infrastructure at the site, such as a building management system or pre-existing security services.

Requirements

Candidates for this role typically need a high-school diploma and must be proficient in the use of tools and equipment (drills, wire strippers, etc.) They also should generally have a fundamental understanding of wiring, circuits, and power supplies; familiarity with security systems is a major asset.

Compensation

Installation technicians are usually paid between $43,000 and $74,000 annually, with the highest paid installation technicians earning around $105,000 per year.

Work-Life Balance

Although the hours vary, the job often has clear start and end times, which allows workers to plan non-work activities effectively. The work is physically demanding, and working hours may vary from early morning to late evening depending on the needs of the client. Overtime can be required for projects with strict deadlines or projects that fall behind schedule during peak times.

Opportunities for Advancement

Installation technicians might be promoted to Installation manager, or transition into a service technician, technical support representative, trainer, or quality control technician role, or – with additional training – move into an engineering or project management role.

Service Technician

Alternative Job Titles
Service Engineer

Employed By
Installers, Integrators, Manufacturers

Responsibilities

Service technicians are responsible for repairing and maintaining security systems after installation. This could range from repairing or replacing broken or underperforming equipment to troubleshooting software or computer networking issues in a facility's control center. They will also perform routine and preventative maintenance to catch issues before they become a problem for the end user.

In smaller companies, installation technicians will also double as service technicians, while in larger companies they are separate roles.

On a typical day, a service technician might:

- Meet with a client to discuss concerns or issues with the performance of the system.
- Utilize diagnostic tools to assess the performance of various components of the system.
- Identify any problems or potential problems, apply solutions, or engage in troubleshooting efforts until a solution is found.
- Upgrade and modify existing installations to improve the performance or stability of the system.

Requirements

Service engineers will generally have at least three years of relevant experience. Their skill-level is expected to be equivalent or greater than the skill-level of a senior-level installation technician.

Compensation

Service technicians are usually paid between $54,000 and $72,000 annually, with the highest paid earning around $97,000 per year.

Work-Life Balance

Service technicians typically work standard full-time hours, and their shifts generally fall within normal business hours (e.g., 9-5). Many service technicians also have a certain number of "on-call" shifts that will require them to respond to urgent service requests or other issues. Because service technicians often have to do work on-site, they may be required to travel significant distances if their company has assigned them clients across a wide geographic area.

Opportunities for Advancement

Installation technicians might be promoted to service manager, or transition into an installation technician, technical support representative, trainer, or quality control technician role, or – with additional training – move into an engineering role.

Installation Manager

Alternative Job Titles
Installation Lead

Employed By
Integrators, Installers

Responsibilities

Installation managers (IMs) lead on-site teams during security system installations, upgrades, and expansions. They supervise the installation technicians, who might be internal employees or external contractors, and work with the project manager to make decisions about staffing, resources, and equipment needed onsite.

On a typical day, an installation manager might:

- Coordinate staffing needs for installation projects, assigning team members based on their skills and the needs of the project.
- Oversee the day-to-day activities of installation teams, providing supervision and support as needed.
- Assess the impact of client change requests on the project's timeline and budget, and provide updated quotes and schedules.
- Identify potential risks to project success, such as delays, equipment shortages, or technical issues, and develop contingency plans to address these challenges promptly.
- Ensure that all installations comply with relevant industry standards, regulations, and safety protocols.

Requirements

Installation managers usually have a college degree in business administration, engineering, IT or a related field plus five or more years of experience in the industry (usually in either a technician or engineering role). Supervisory experience is preferred, and strong project management skills are necessary. Obtaining a certified security project manager (CSPM) certification can improve chances of finding employment.

Compensation

Installation manager positions typically pay in the $75,000 to $110,000 range (plus bonuses), with the highest paid IMs earning around $120,000 per year.

Work-Life Balance

The work of an installation manager is often project-driven, with more regular hours during planning and post-installation, and more intense periods during installations that can lead to extended hours and travel. Installation managers might travel several days per month (depending on the size of their company) and intermittently work 50 or more hours per week, potentially including weekends.

Opportunities for Advancement

Successful installation managers can progress to senior roles such as security project managers (SPM) or operations manager. These positions oversee a broader range of operations and may involve managing multiple projects simultaneously.

Quality Control Technician

Alternative Job Titles
Quality Assurance

Employed By
Installers, Integrators, Manufacturers

Responsibilities

Quality control technicians ensure that the products sold by manufacturers and/or the security systems installed by integrators work as specified and meet any and all relevant requirements. This includes ensuring that components are tested and calibrated properly after they are installed / manufactured, evaluating installation / manufacturing procedures to ensure they align with quality control principles, and providing instruction to installers and factory staff to address any quality issues uncovered.

On a typical day, a quality control technician might:

- Perform functional testing of a recently installed security system or conduct audits of existing systems to ensure that all components work as expected in real-world circumstances.
- Test a sampling of products from a manufacturer's production lines, to ensure they meet all specifications
- Work with installation and/or engineering teams to improve quality and prevent problems before they occur.

Requirements

Quality control technicians typically have several years of experience working as Installation or service technicians or in a manufacturing role, having demonstrated a high degree of expertise and affection to detail. Knowledge of quality assurance methodologies such as ISO 9001 is also an asset.

Compensation

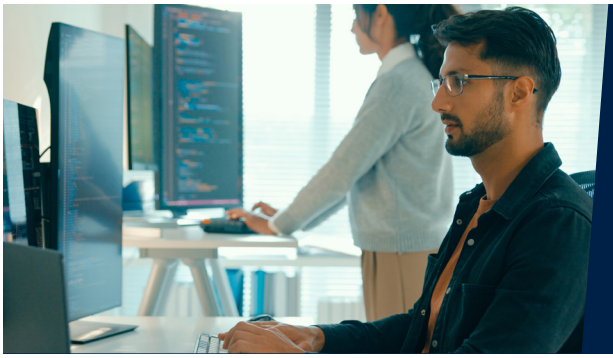
QC technicians positions typically pay in the $40,000 to $75,000 range annually.

Work-Life Balance

Quality control technicians typically work regular business hours, with only limited overtime requirements. They only face significant travel requirements if their company has installations at far-off sites or needs to inspect work being done at a vendor's factory that cannot be inspected by a different technician.

Opportunities for Advancement

Quality control technicians might move up to a junior engineering role, project management, or a position in operations or supply chain management.



Cybersecurity Specialist (Integrator)

Alternative Job Titles
Cybersecurity Manager

Employed By
Installers, Integrators

Responsibilities

Cybersecurity specialists ensure that the IT and networking components of security installations are adequately protected against any malicious actors who might try to breach the system, intercept communications, or access sensitive data.

This includes providing input into the design of the system, overseeing the installation process, and auditing the system at the conclusion of the installation.

They may also educate sales staff about a system's cybersecurity capabilities and liaise with the end user's internal cybersecurity team (or IT department).

On a typical day, a cybersecurity specialist might:

- Review the design of a security system to ensure that communication between various devices is secure, including by ensuring that individual devices and components have adequate security features and encryption.
- Implement firewalls and activity monitoring software at key points in the network in order to ensure that all access points are shielded and monitored.
- Collaborate with physical security teams in order to ensure that cybersecurity measures are integrated into the overall strategy for securing the system.

Requirements

Individuals in this field typically have at least three or more years of relevant experience as well as a degree in cybersecurity, computer science, systems engineering, or a related field. industry-related credentials like the security industry cybersecurity certification (SICC) and certified information systems security professional (CISSP) are also beneficial.

Compensation

Cybersecurity specialists are usually paid between $85,000 and $120,000 annually (plus bonuses), with the highest paid earning around $130,000 per year.

Work-Life Balance

Cybersecurity specialists generally work a standard weekly schedule within regular business hours. Outside of potentially needing to travel to sites for some tasks, travel is limited, and some businesses may allow some work (e.g., monitoring, auditing, analysis) to be done remotely. However, depending on the company, they may be required to respond to security incidents on an on-call basis and at irregular hours.

Opportunities for Advancement

Typically a cybersecurity analyst might advance to a more senior IT position, up to and including CIO, or work for a consulting firm that specializes in cybersecurity.

Cybersecurity Specialist (Manufacturer)

Alternative Job Titles
Cybersecurity Manager

Employed By
Manufacturers

Responsibilities

Cybersecurity specialists ensure that a manufacturer's products are not vulnerable to malicious actors trying to access them or intercept their communications. To that end, they are responsible for testing, and validating the cybersecurity aspects of the company's products and solutions, including "penetration tests" where they try to gain unauthorized access to the product, just like an actual attacker would.

Their role may also require them to provide cybersecurity services for the company's internal IT systems, and provide sales and support teams with guidance and advice about a product's security features.

On a typical day, a cybersecurity specialists might:

- Collaborate with product engineers to ensure that a product is secure-by-design, meaning that cybersecurity is a core part of the product's design and not an "additional feature."
- Interface with the application developers in charge of the product's software components to ensure that secure coding practices are followed.
- Test the security of a product by conducting penetration tests to identify vulnerabilities and assess the resilience of the product to attacks under different circumstances.
- Review the capabilities and functions of a device in order to ensure that it complies with industry standards as well as any applicable government regulations.

Requirements

Cybersecurity specialists typically have three or more years of experience, as well as a bachelor's degree in cybersecurity or a related field. Some companies will require cybersecurity specialists to have obtained a recognized industry credential such as a CISSP (certified information systems security professional) certificate.

Compensation

Cybersecurity specialists are usually paid between $90,000 and $130,000 annually (plus bonuses), with the highest paid earning around $140,000 per year.

Work-Life Balance

Most cybersecurity specialists work standard work hours; however, if they are deeply embedded in a product's development cycle then they may need to perform overtime in advance of certain deadlines. Some cybersecurity specialists may also be required to work on-call shifts and respond to emergencies such as breaches of a deployed product or the discovery of a significant vulnerability.

Opportunities for Advancement

Typically a cybersecurity specialist might advance to a more senior networking or software engineering position, or work for a consulting firm that specializes in cybersecurity.

IT/Network Specialist

Employed By Installers, Integrators

Responsibilities

IT/network specialists are responsible for designing or modifying the computer networks that connect security system components. This includes selecting both the hardware and software components of the network and integrating them into a cohesive whole.

Network specialists work closely with project design and service specialists to ensure that a security system's design is practical from a networking perspective, and also work closely with cybersecurity specialists to ensure that the system is secure.

On a typical day, a network specialist might:

- Outline a network architecture for a security system, including router, firewalls, and wireless access points.
- Collaborate with project managers and engineers to design the physical layout of the security system's network infrastructure, such as routers, access points, and cabling.
- Conduct systems checks and monitoring for client networks.
- Work with a cybersecurity specialist to patch a vulnerability in a client's network.

Requirements

IT/network specialists will generally have at least three years of relevant experience before moving into this role. They must have excellent programming skills in addition to experience designing and setting up networks. Certifications such as CompTIA Network+ or certified information systems security professional (CISSP) are considered desirable by employers.

Compensation

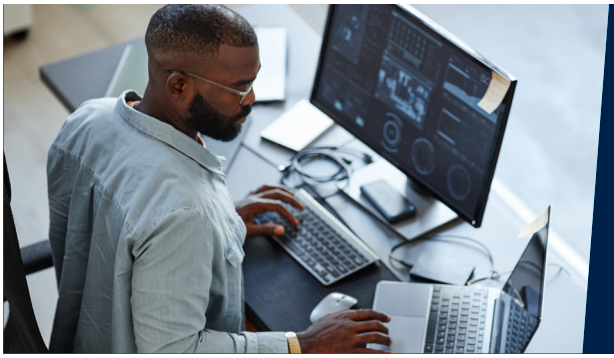
IT/network specialist positions typically pay in the $65,000 to $80,000 range (plus bonuses), with the highest paid network specialists earning around $95,000 per year.

Work-Life Balance

The work hours for an IT/network specialist can vary based on project demands and client needs. They generally work a standard 40-hour week, but may be required to work evenings, weekends, or on-call shifts to handle network emergencies or perform maintenance during off-peak hours. While there is potential for remote work, on-site presence is often needed for installations, upgrades, and troubleshooting.

Opportunities for Advancement

Successful IT/network specialists can advance to more senior IT positions, up to and including CIO. Specialists can also move into roles focused on cybersecurity, where they design and implement security protocols and systems to protect organizational networks. In larger organizations, there may also be opportunities to specialize in areas such as cloud networking, data center management, or IT strategy and governance.



Cybersecurity Analyst

Alternative Job Titles
Information Security Analyst, IT Security Analyst, Network Security Analyst

Employed By
Manufacturers, End Users, Integrators, Consulting Firms

Responsibilities

Cybersecurity analysts are responsible for protecting an organization's computer systems and networks from cyber threats and security breaches. This includes managing "Internet of Things (IoT)" devices installed on a network, including security equipment. Cybersecurity analysts play a crucial role in ensuring data privacy, identifying vulnerabilities, and implementing protective measures to safeguard an organization's data against theft or damage.

Additionally, they ensure that data can be restored effectively in the event of a disaster or security incident.

On a typical day, a cybersecurity analyst might:

- Monitor networks and systems for security breaches or intrusions using specialized software and tools.
- Work with IT to develop and update security protocols and policies to ensure they align with the latest industry standards and best practices.
- Perform vulnerability assessments and penetration tests to identify potential weaknesses in systems and recommend corrective actions.
- Investigate and respond to security incidents, working to mitigate risks and prevent future breaches.

Requirements

Many cybersecurity analysts have a college degree in computer science, information technology, cybersecurity, or a related field. Entry-level positions typically require at least one to three years of experience in IT or network security roles. Professional certifications such as certified information systems security professional (CISSP), certified ethical hacker (CEH), or CompTIA Security+ are highly valued and can improve employment prospects.

Compensation

Cybersecurity analyst positions typically pay in the $65,000 to $90,000 range annually depending on experience and location. Senior analysts or those with specialized skills or credentials can earn upwards of $100,000 per year, with additional compensation possible through bonuses or incentive programs.

Work-Life Balance

Cybersecurity analysts often work standard 40-hour weeks, but they may be required to work evenings or weekends in the event of a security breach or when implementing major security updates. Hours can vary depending on the size of the organization, the complexity of its IT systems, and may include on-call responsibilities.

Opportunities for Advancement

Cybersecurity analysts can advance to roles such as senior security analyst, security architect, or security manager. With experience and additional certifications, some may move into specialized roles focusing on areas like penetration testing, forensic analysis, or cloud security. Ultimately, experienced analysts might progress to chief information security officer (CISO) positions, overseeing an organization's entire security posture and strategy.

Application Developer / Programmer

Employed By Integrators, Manufacturers

Responsibilities

Application developers are responsible for developing, customizing, and supporting the software used in security systems and products. While their skill sets and job responsibilities might be similar to software developers in other industries, the unique nature of security products and systems require extreme attention to performance, reliability, and security of software applications.

On a typical day, an application developer might:

- Write and modify code to incorporate new features or fix issues.
- Work with quality assurance teams to identify and resolve problems.
- Create and maintain documentation, such as user manuals and technical guides to help clients and internal teams understand how to use, maintain, and troubleshoot the software
- Provide ongoing technical support for software applications.

Requirements

Application developers typically have a degree in computer science, software engineering, or a related field, along with experience in developing software applications for security systems or similar industries. Proficiency in programming languages such as Python, C++, Java, or JavaScript is often required, as well as experience with database management and networking. Knowledge of security protocols, encryption, and cybersecurity principles is highly beneficial.

Compensation

Application developer positions typically pay in the $70,000 to $80,000 range, with the highest paid earning around $95,000 per year.

Work-Life Balance

The work hours for an application developer can vary depending on the stage of development and client needs. They typically work a standard 40-hour week, but they may need to work additional hours during project deadlines, software deployments, or when urgent technical support is required. Remote work is common in this role, but on-site visits may be necessary for complex installations or troubleshooting.

Opportunities for Advancement

Successful application developers can advance to senior roles such as solutions architect, which entails greater responsibility for designing the overall software application. In larger organizations, there may also be opportunities to move into specialized areas such as cybersecurity, data analytics, or systems engineering.

Applications Engineer

Employed By Integrators, Installers

Responsibilities

Applications engineers in the security industry are responsible for integrating software applications into security systems. Unlike application developers, who focus on writing and modifying code to create software applications, applications engineers ensure these applications are properly configured, deployed, and maintained in real-world environments and properly integrated with end users' other hardware and software systems.

Application developers are often also responsible for providing ongoing software technical support to clients after installation.

On a typical day, an applications engineer might:

- Collaborate with installation teams to integrate software applications with various physical security devices such as cameras, alarms, and access controls.
- Engage directly with clients to understand their needs and the needs of the project.
- Conduct an on-site training session for clients to train them on using and managing their security software.
- Develop and maintain comprehensive documentation related to software configurations, integration processes, and compliance with industry standards.

Requirements

Application engineers typically have a degree in computer science, software engineering, or a related field, along with experience in developing software applications for security systems or similar industries. Proficiency in programming languages such as Python, C++, Java, or JavaScript is often required, as well as experience with database management and networking. Knowledge of security protocols, encryption, and cybersecurity principles is highly beneficial.

Compensation

Application engineer positions typically pay in the $70,000 to $90,000 range, with the highest paid earning around $100,000 per year.

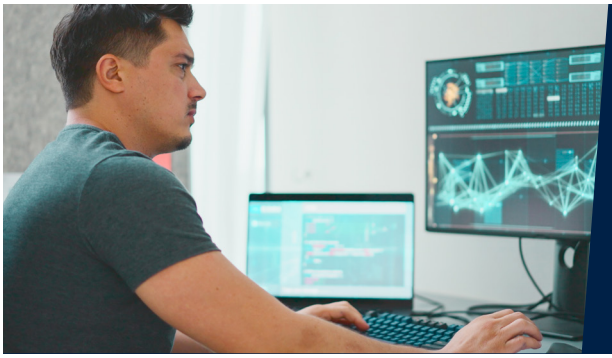
Work-Life Balance

Application engineers can vary depending on the stage of projects and client needs. They typically work a standard 40-hour week, but they may need to work additional hours to meet project deadlines or when urgent technical support is required.

Travel to client sites may be necessary for complex installations, troubleshooting, or training client staff.

Opportunities for Advancement

Application engineers might move into technical project management, application developer, or cybersecurity roles depending on their interests and attributes.



Machine Learning/Artificial Intelligence Specialist

Employed By Manufacturers

Responsibilities

Machine learning / AI specialists make use of data analytics, advanced algorithms, and machine learning models to improve the accuracy and automation of security systems. In practical terms, their work involves building algorithms and classification models that can monitor networks, automatically identify potential threats, and alert cybersecurity personnel as needed. They work closely with cybersecurity and data analysts to identify anomalies and improve the system's threat detection.

On a typical day, an ML/AI specialist might:

- Collect data from client security systems to train threat classification models on.
- Preprocess and categorize training data to ensure it is relevant, effective, and ready-to-use.
- Analyze system logs and performance metrics of deployed models to determine any adjustments or improvements to be made.
- Update and retrain models to better handle a particular class of cybersecurity threat.

Requirements

ML/AI specialists will typically have degrees in computer science or even specialized degrees and certifications in machine learning and artificial intelligence.

Compensation

ML/AI specialists are typically paid between $57,000 and $100,000 annually, with the highest paid ones earning around $120,000 per year.

Work-Life Balance

Today, most ML/AI specialists work a standard 35- to 50-hour week (with more hours required around project deadlines), with possible remote work and minimal need for travel.

Opportunities for Advancement

Successful ML/AI specialists may be able to advance to roles such as senior AI engineer (if present in their organization), or data science lead. As machine learning is a fast-growing and dynamic field, there are likely to be more opportunities for advancement or further specialization.

Sales Engineer

Alternative Job Titles
Technical Sales Representative, Pre-Sales Engineer

Employed By
Manufacturers, Integrators, Distributors

Responsibilities

Sales engineers help sales teams address any complex technical questions or special requirements customers might raise during the sales process. They are responsible for understanding a customer's security needs, working with the sales and engineering teams to identify solutions, then demonstrating how their company's products and services can solve a customer's specific security challenges. Additionally, they make sure that sales teams don't make inaccurate statements about the capabilities or cost of their company's solutions.

On a typical day, a sales engineer might:

- Analyze customer requirements and identify security solutions that address specific challenges.
- Prepare and deliver technical presentations / demonstrations that show the capabilities of a security system or product.
- Assist with writing proposals and responding to RFPs (requests for proposals), ensuring that all technical aspects are accurately addressed.
- Stay updated on the latest security technologies, industry trends, and competitors' products, to ensure they are able to answer any questions customers might ask.
- Conduct training sessions and provide ongoing technical support after a sale.

Requirements

Sales engineers typically have a college degree in engineering, computer science, or a related field, along with three to five years of experience in a product development / systems engineering or technical support role. Knowledge of security systems, including surveillance, access control, intrusion detection, and cybersecurity, is crucial. Sales engineers often benefit from certifications on the technical systems or product lines they work with.

Compensation

Sales engineer positions typically pay in the $80,000 to $100,000 range, plus commission and bonuses (which depending on the company, can be significant). Top performers often earn over $120,000 per year, depending on the complexity of the solutions and the volume of sales.

Work-Life Balance

The working hours and travel requirements for sales engineers can vary based on the company they work for, the territories they cover, and the specific needs of their customers. Sales engineers often travel to meet with customers and provide on-site support, which can mean frequent travel and varying hours, especially when deadlines approach or when working on large, complex projects.

Opportunities for Advancement

Successful sales engineers may advance to roles such as sales manager or solutions architect, where they take on greater responsibility for overseeing sales strategy and customer relationships or designing advanced, large-scale security solutions. They may also progress into senior management roles, such as director of sales engineering, where they manage a team of sales engineers and drive overall technical sales strategy for the company.

Technical Support Representative

Alternative Job Titles
Customer Support Technician, Technical Support Engineer

Employed By
Integrators, Installers, Manufacturers

Responsibilities

Technical support representatives assist customers by quickly troubleshooting, diagnosing, and resolving problems with security systems and equipment such as surveillance cameras, access control systems, intrusion alarms, and cybersecurity software. They might work for an integrator, providing assistance to end users after an installation, or possibly for a manufacturer, supporting integrators and end users throughout a product's life cycle.

In some cases, technical support representatives might talk a customer through resolving an issue, while other times they might dispatch a service technician to the customer's facility or even connect to the equipment via the internet to resolve the issue themselves.

In all cases technical support representatives play a critical role in ensuring customer satisfaction by resolving issues swiftly and maintaining the security system's integrity.

On a typical day, a technical support representative might:

- Respond to customer inquiries and support requests via phone, email, or live chat, addressing issues related to security systems and software.
- Troubleshoot problems and provide step-by-step guidance to resolve issues (e.g., configuration changes, software updates, hardware resets).
- Collaborate with other technical support staff and engineering teams.
- Create and update documentation.

Requirements

Technical support representatives may have an associate's or bachelor's degree. Some entry-level technical support representatives might learn about security technology on the job, while others have prior experience as a technician or another role within the industry. Strong communication skills, problem-solving abilities, and a customer service mindset are essential.

Compensation

Technical support representative positions typically pay in the $40,000 to $60,000 range, with opportunities for bonuses and overtime pay, depending on experience and the complexity of the support provided.

Work-Life Balance

Technical support representatives generally work in regularly scheduled shifts to ensure 24/7 support availability, which can include nights, weekends, and holidays, depending on the company and customer needs. Most support is provided remotely, though some roles may require on-site visits or travel to customer locations.

Opportunities for Advancement

A technical support representative position could eventually lead to roles in sales, customer success, training, field service, or even engineering and product development depending on an individual's interests and aptitude.

Trainer

Employed By Integrators, Installers, Manufacturers

Responsibilities

Trainers help manufacturers, integrators, and end users prepare people to install, operate, and maintain complex security systems and products. This could include training technicians to install an alarm system or training an end user's security team to operate cameras on site. Sometimes, trainers will contribute to the design of training programs, working together with the engineering, technical support, and sales and marketing teams to identify what skills and knowledge different audiences will need to fulfill their role in the security ecosystem.

On a typical day, a trainer might:

- Develop and/or update training materials including manuals, presentations, videos, and e-learning content, working with product teams to ensure they are current.
- Conduct training sessions in person or virtually, teaching participants how to install, operate, and troubleshoot security systems.
- Evaluate the effectiveness of training programs through assessments and feedback from participants.
- Tailor training programs to meet the specific needs of different audiences and clients.

Requirements

Trainers in the security industry typically have a background in security technology, engineering, or IT, often with several years of experience working as a technician, technical support representative, technical writer, or engineer. A bachelor's degree is usually preferred, but not always required. Certifications such as the certified professional facilitator (CPF) or certified professional in training management (CPTM) can enhance a trainer's qualifications.

Compensation

Trainer positions typically pay in the $50,000 to $70,000 range, with the potential for higher earnings based on experience, location, and the complexity of the training provided. Trainers may also receive additional compensation for travel, overtime, or specialized training sessions.

Work-Life Balance

Work-life balance for trainers can vary based on the nature of the training they provide. Trainers might need to travel to customer sites to conduct in-person training sessions. However, many trainers also conduct remote training sessions, which can provide more flexibility.

Opportunities for Advancement

Successful trainers might move up within the training department, or move into a technical support, product management, or sales role, leveraging their deep knowledge of security systems and strong communication skills.

Preparing for a Security Industry Career

If you're interested in joining the security industry, there are several ways to strengthen your resume and increase your chances of securing a job at a leading manufacturer, integrator, consulting firm, or end-user organization.

Degrees

Many security industry roles – particularly those related to engineering – require undergraduate or even graduate-level degrees in engineering, information technology, business administration or related fields.

However, many technician, technical support, and other roles might only require a two-year degree, or a combination of a two-year degree and certification. And it's often possible for individuals without a degree to enter and advance within the industry based through a combination of aptitude, practical experience, and/or certifications, without a formal degree.

Internships and Apprenticeships

Internship and apprenticeship programs allow you to develop industry-specific skills by working on a part-time or temporary basis. Generally, internships tend to be more informal while apprenticeships follow a more structured training program.

Internships

Many companies in the security ecosystem have internship programs, where students interested in a security career can work as an assistant to different teams and departments. This is a great way to see firsthand what a career in security is like, while gaining hands-on experience with cutting-edge security technologies and building a network with industry professionals who can help you in your career.

Apprenticeships

Apprenticeships provide an opportunity to "earn while you learn," working at a company in the security industry alongside seasoned professionals while completing a structured training program with classroom, self-study, and/or "on the job" training components.

To give one example, the Security Industry Association offers a 12-month apprenticeship initiative for security technicians and installers, with a focus on developing basic networking, IT, and cybersecurity skills through on-the-job training and one-to-one mentoring.

Programs like these are a great way to develop your knowledge of security technology and practices, and pave the way for long-term success in the field.

Certifications

Certifications offer a way to verify the skills you've acquired through on-the-job experience, apprenticeships, or an academic degree. A certification can make your resume more attractive to employers, as a complement or alternative to an academic degree. Most certification programs involve independent study assignments, documentation of relevant work experience, and/or an assessment test to demonstrate your skills and knowledge.

Some of the most popular certifications for the security industry include:

- Certified Security Project Manager (CSPM)
- Certified Protection Professional (CPP)
- Certified Information Security Manager (CISM)
- Physical Security Professional (PSP)
- Security Industry Cybersecurity Certification (SICC)
- Project Management Professional (PMP)
- CompTIA (A+, Security+, Network+)
- ISC2 CISSP
- Certified ScrumMaster (CSM)
- Certified Agile Professional

Many security device and technology manufacturers have certifications for specific equipment, product lines or software. A few examples include Assa ABloy, Axis Communications, Genetec, HID, SoftwareHouse, Milestone, etc.

Alternative Pathways

Security industry employers place a high value on candidates who already have practical, real-world experience working with electrical systems, driving vehicles, operating hand / power tools, or installing or repairing electronic equipment like stereos or AV systems. Many companies (particularly integrators) have "Skilled Through Alternative Routes" (STARS) initiatives specifically geared towards attracting people who acquired these skills from trade work or other non-academic paths – with or without a traditional degree.

Programs for Diverse Candidates and Veterans

The security industry is actively seeking candidates with diverse backgrounds and experiences, including veterans, women, and people from underrepresented communities.

Most employers in the security industry are equal employment opportunity companies who value the unique skills and perspectives that a diverse workforce can bring.

Military veterans also make excellent candidates for security industry positions because of their experience and familiarity with common security practices, such as conducting a risk assessment and working with similar types of devices and equipment.

Explore SIA
Student Membership

Security Industry Association (SIA)

The Security Industry Association is the leading professional organization for the security industry, and allows students to join at a discounted rate of $20 per year. Scan the QR code if you are interested in joining the Security Industry Association as a student member.

Scholarships

SIA Student Members are eligible to apply for competitive scholarships, including:

- **The RISE Scholarship,** which awards multiple $3,000 scholarships to be used for student loans, continuing education in the security industry, and professional training/certification.
- **The Women in Security Forum Scholarship**, which awards multiple $7,500 scholarships to be used for student loans, continuing education in the security industry, and professional training/certification.
- **The Denis R. Hébert Scholarship**, which awards two $5,000 scholarships to be used for certification, credentialing, or other post-secondary education programs related to identity management.
- **The Paul Ahern Scholarship,** which provides funds for recipients to enroll in SIA's OSDP Boot Camp.
- **The James Rothstein Business Scholarship**, which provides up to $3,000 of financial assistance to attend the Securing New Ground (SNG) conference.

Educational Events and Learning Resources

SIA Student Members receive free or reduced registration to educational events, as well as:

- Free access to the SIA Cornerstones learning modules.
- Access to SIA industry reports and market research papers.
- Access to the TIME mentorship program.
- Access to programs and content for young professionals via the RISE Program.

Networking and Employment Opportunities

Lastly, SIA Student Members can make use of the following networking opportunities:

- Access to internship listings and the Foundation for Advancing Security Talent (FAST) jobs board.
- Eligibility for the Security Systems Technician (SST) Apprenticeship Program.

Visit psasecurity.com

The PSA Network

The PSA network is a consortium of integrators that offers a wide range of resources and opportunities for students and young professionals, including:

- **Committees** on a variety of subjects (including leadership, technology, cybersecurity, marketing, etc.) that meet monthly to exchange knowledge and provide peer-to-peer networking and support.
- **Mentorship programs** that foster growth and knowledge transfer between experienced and new industry members, providing opportunities to gain valuable insight, develop new skills, and build lasting relationships that will help push your professional journey forward.
- **Scholarships** offering up to $2,500 in financial support toward higher education or industry certifications, for winning candidates.
- **PSA TEC Fellowship** where three selected individuals can attend PSA TEC, a leading educational conference in the security industry, all expenses paid.
- **PSA University,** an online platform offering access to educational content from industry experts across the network, featuring hundreds of courses to grow your knowledge and skills.

FAST (Foundation for Advancing Security Talent)

FAST is a partnership between the Electronic Security Association (ESA) and the Security Industry Association (SIA) dedicated to connecting passionate, innovative professionals with opportunities in the security industry. Among other resources, FAST offers:

- A security industry job board
- Free resume review
- Security industry career guides
- Networking events

www.securityindustry.org