IJMRSET

e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 9, September 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.54

☎ 6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 9, September 2023 |

| DOI:10.15680/IJMRSET.2023.0609004 |

The Significance of English Soft Skills for the Engineers

A. SRINIVAS

Mentor of English, Department of Humanities, Rajiv Gandhi University of Knowledge Technologies (RGUKT), IIIT Basar, Telangana, India

ABSTRACT: There has never been a better time to be an engineer. In many sectors, new technologies mean there are a growing number of opportunities for individuals with the right training and experience.Therefore, it can be frustrating when you think you've got the perfect CV but don't get that call back after your interview. The same applies when you don't get a promotion you think you're ready for. After all, you've got the right qualifications and technical abilities, so why didn't you get the job.Technical skills alone are no longer sufficient for many employers. Furthermore, technical skills alone will only take your career and levels of job satisfaction so far. So, what can you do.

KEYWORDS-english, soft-skills, engineers, significance, technical

I. INTRODUCTION

Too often, engineers focus only on their technical skills and abilities, largely ignoring soft skills. Soft skills, however, are very important in almost all roles and industries.

By paying attention to the following nine important soft skills for engineers, you'll make yourself more attractive to employers. You'll also become a more rounded engineer, enhancing your emotional intelligence and interpersonal skills, and improving your overall engineering abilities as soft skills work.
Communicating complex technical solutions in a way that clients understand is becoming increasingly important.

For example, as an engineer, you might have a tendency to focus on the technical detail when clients are often more interested in finding solutions to their specific problem and understanding the benefits to their business, i.e., they are not necessarily interested in abstract theories or high-level science, particularly at management level.

So, practice delivering highly technical information in as simple a way as possible while keeping your client's perspective in mind.

Another thing to highlight when discussing communication skills is the fact that this is a category rather than a specific or isolated skill. In other words, improving your communication skills will involve improving a range of other soft skills. You may not need all the soft communication skills in the list below, but they include:

- Active listening skills
- Writing skills
- Presentation skills

- Non-verbal communication skills
- Empathy
- Patience[1,2,3]

Problem-Solving

Problem-solving usually involves successfully considering the pros and cons of each solution and finding the path with the least risk involved.

Interviewers often consider problem-solving skills during the recruitment process because they show how candidates deal with challenges. After all, project managers and other leaders like having team members who don't bring every small difficulty to their doorstep.

Problem-solving skills can also help projects run more smoothly, as well as helping to improve the business overall.

You should also explore possibilities for improving other soft skills that are closely related to problem-solving skills. Examples include:

- Innovation skills
- Brainstorming skills
- Critical thinking skills
- Research skills

Having intellectual curiosity can also help improve your problem-solving skills. Being intellectually curious will help you think out-of-the-box, find solutions, and question why things are done the way they are.[5,7,8]

Organisation

In some situations, you can classify organisational skills as technical rather than soft. For example, good code needs to be well structured and organised. That said, there are also organisational skills you should improve that are non-technical.

These include punctuality, task management, and not taking on more tasks than you can handle.

Specific skills that come under the organisation soft skills umbrella include:

- Time management skills

- Goal-setting skills
- Planning skills
- Prioritisation skills

Finally with this one, there are apps available that help you stay organised, complementing your soft skills development.

Leadership

A good definition of leadership as a soft skill is taking responsibility for yourself and also for the people you work alongside. Remember, you don't have to be in a managerial position to be a leader. Leadership is also about things like keeping the right distance from a task (so you can see the bigger picture), setting the right example, and motivating others when things get tough.

Hone this skill, and don't forget to celebrate your leadership successes. Remember them as best practice examples, too, so you can use them as a stepping stone for promotion.

Areas you can work on in relation to leadership skills include some already highlighted, such as communication skills and organisational skills. Strategic thinking, personal development, and team development skills are also important.

Teamwork

There are many engineering tasks that you will do alone. Writing code is a good example. Individuals can't complete large engineering projects alone, however. Instead, they require teams and, by extension, teamwork.

As a result, teamwork is usually a non-negotiable soft skill in engineering. In other words, employers want you to be just as committed to successfully achieving team and company goals as you are to personal goals.

Adaptability

With rapidly advancing technologies, the reality of clients changing requirements, the increasing use of agile development techniques, and other factors, adaptability is an essential soft skill to improve. In fact, being willing and able to quickly adapt to situations is a skill highly valued by employers.

Creativity

In engineering, creativity is about finding new ways of looking at things. By developing this valuable soft skill, you'll be able to, for example, develop innovative products or project solutions. Creativity can also help you solve a problem or successfully deal with an unexpected situation.[9,10,11]

Interpersonal Skills and Emotional Intelligence

Interpersonal skills are, in a sense, an umbrella term for several soft skills, including active listening, social perceptiveness, and being able to handle feedback. They all centre on emotional intelligence.

While it may not be possible to have great relationships with colleagues and others in all situations, developing your interpersonal skills will help you, those around you, and the company you work for.

Customer service

Finally, giving customers more than they expect helps to nurture long-term and loyal relationships. After all, customers are crucial to the success of most businesses. As a result, companies are more focused on customers than ever before. Developing your own customer service skills will help you contribute to the company's efforts.

II. DISCUSSION

How to Improve Your Soft Skills

You can complete training courses to improve your soft skills. Experience is important, too, so be open to taking on leadership responsibilities while also being adaptable and flexible. For example, be willing to take on new roles or projects, even if they are outside your comfort zone.

You should always be ready to learn, embracing constructive feedback from wherever it comes from. Building strong relationships and regularly communicating with those who can help you grow and develop will help too.

Developing a Continuous Improvement Mindset

Becoming a master of the soft skills above is a lifelong objective, so don't expect to have all of them figured out quickly. Instead, focus on those you consider are your weakest, set goals, develop a plan, and constantly review your progress. The reward will be increased engineering success.

The Cybersecurity Risks Created by Industry 4.0's Increased Attack Surface

Businesses in all industries face an ever-increasing range of cybersecurity risks. This includes companies in the manufacturing sector. When you look at regulated industries such as pharmaceutical and medical device manufacturing, where patient safety is a top priority, cybersecurity risk levels can be even higher.

Industry 4.0 technologies and solutions almost always modify existing risks or create new ones. As a result, it is essential that cybersecurity is prioritised throughout every stage of every project that comes under the umbrella of Industry 4.0, digital transformation, smart manufacturing, and industrial automation.

It is also important to take a step back to take a wider view of cybersecurity in your organisation. This is because of one of the unintended consequences of Industry 4.0 technologies and solutions – the increased attack surface.

What is the Increased Attack Surface?

Some of the objectives of Industry 4.0 technologies include integration and the deepening of connections between systems. This can be systems on the production line, within the supply chain, or in other parts of the organisation, i.e., sales, R&D, purchasing, accounting, etc.[12,13,15]

Even systems that previously operated in silos can be brought into the new connected structure to make better use of data and to make efficiency savings and productivity gains.

However, each integration step you take on your smart manufacturing journey increases the cybersecurity attack surface that exists in your organisation. The same applies to every new connected device, platform, or piece of equipment. Connecting to cloud services and other resources external to the organisation significantly increases the attack surface too.

In other words, each new system or machine you integrate or connect is another potential target of attack.

You might even have legacy systems that were never designed to deal with the cybersecurity challenges that currently exist, never mind those that are yet to emerge.

Secure IT is Not Secure Enough in the Smart Manufacturing Era

One of the key cybersecurity challenges as manufacturers transition to smart factories is the fact that IT and OT (operational technology) are not synced up in terms of cybersecurity.

This situation arises because the team responsible for IT security is likely to have limited input in OT decisions and processes, plus there is generally no equivalent OT team responsible for security. In many situations, this can leave organisations unprepared for the enhanced cybersecurity threat created by the increased attack surface.

Dealing with These Enhanced Cybersecurity Threats in Smart Factories

The Industry 4.0 concept of integration is a crucial part of the solution to the cybersecurity risks created by expanding attack surfaces. We are not talking about integrating systems or equipment, however, but teams.

In practice, this means approaching cybersecurity in a more holistic way across all parts of the organisation, taking into account both IT and OT.
This integrated approach to cybersecurity will mitigate the threat of the increasing attack surface. For example, dealing with the gaps that arise in maturity assessments.

Cybersecurity maturity assessments are typically performed periodically. The time between assessments can often be too long, but there is also the issue of new Industry 4.0 solutions being implemented between cybersecurity maturity assessments. These solutions can increase the attack surface further, increasing risks and rendering the assessment out of date even though it is the most recent.

Taking a Holistic Approach to Cybersecurity in Manufacturing Organisations

While integrating your cybersecurity team across IT and OT is the solution, that team will require detailed knowledge of existing and emerging cybersecurity threats. It will also need in-depth knowledge of both IT and OT assets and network architectures, in addition to knowledge of both business and manufacturing processes.

Taking a holistic approach to cybersecurity also involves real-time auditing of IT and OT assets, regular maturity assessments and risk reviews, taking mitigating actions, and continuous monitoring.

While this is a more expansive approach to cybersecurity than currently exists in many manufacturing organisations, it will ensure the maximum level of protection across the entirety of the potential attack surface.
How Good Distribution Practice (GDP) differs from Good Manufacturing Practice (GMP)
Good distribution practice (GDP) and good manufacturing practice (GMP) are quality standards and guidelines that have the same ultimate objective – to ensure medical device and pharmaceutical products are safe, meet their intended use, and comply with regulations.[17]

GMP focuses on manufacturing processes, while GDP covers distribution activities. There are crossovers between both manufacturing and distribution, however. So, what are the main differences between GDP and GMP?

Definitions

To understand the key differences and how they impact operations, let's first look at the definitions of GMP and GDP.

What is Good Manufacturing Practice?

Good manufacturing practice involves consistently producing products that meet quality standards. This requires the implementation of a system where the aim is to minimise risks, from incorrect labelling of products to contamination to incorrect ingredients and everything in between. GMP systems cover all parts of the production process, from raw materials through to the production of the finished product.

What is Good Distribution Practice?

Good distribution practice involves maintaining the quality and integrity of products through all stages of the supply chain. It sets out minimum standards to ensure medical device and pharmaceutical products comply with regulations. GDP applies to warehousing, storage, and transportation, and it covers everything from storing and transporting products under the right conditions. Doing so, minimises the risk of product degradation, ensuring product integrity at the correct destination on time.

Unique Aspects of GDP

There are parts of GDP that are unique, so they don't apply to GMP guidance and standards. Those unique parts of GDP include guidance on transportation covering aspects such as temperature control, vehicle controls, and conducting risk assessments on transport routes. Guidance on brokers is also unique to GDP, i.e., guidance on those who facilitate transactions in the supply chain without ever handling the product.

Areas of Minimal Difference

While there are sections of guidance that are unique to GDP, there are also areas where there is minimal, if any, difference between GDP and GMP. These include:

- Quality management – both focus on ensuring members of staff are properly trained, and the facilities and equipment are fit for purpose. Management review meetings also feature in both, albeit with a bit more emphasis in GDP.

- Outsourced activities – minimal difference.

- Self-inspections – minimal difference.

- Complaints and returns – there are more details in GDP covering the control and management of product returns. Otherwise, there is minimal difference between the two standards.

Main Differences Between GDP and GMP

Aside from the unique aspects of GDP compared to GMP, the differences fall under four main headings:

- Personnel
- Equipment and premises
- Documentation
- Operations

Personnel

GMP talks about the role of Qualified Person while the focus of GDP is the role of Responsible Person. This isn't just a difference in words, though, as a Responsible Person has different responsibilities under the guidance. They can't, for example, certify the release of a product batch, whereas a Qualified Person can.

Equipment and Premises

The main difference between GDP and GMP is the additional controls included in GDP to cover products and materials that are either radioactive or highly sought-after on the black market.

There can be blurred lines in this area, though. Take the thermal mapping of storage areas as an example. Many facilities working to remain in compliance with GMP will have thermal mapping systems in place, even though they are not specifically required by GMP. However, thermal mapping is a requirement under GDP.

GDP also puts more emphasis on instrument calibration, particularly those instruments involved in product traceability processes.

Documentation

As might be expected, there is a reduced requirement in GDP for manufacturing and testing documentation, but an increased requirement for storage and personnel documentation.[14,15,16]

Operations

In GMP, these guidelines are covered under production, so the heading is different. In terms of the more practical specifics, GDP places more emphasis on fake product identification, supplier and customer approval, and exporting processes.

Not Just About Regulatory Compliance

Both GDP and GMP are important components for maintaining regulatory compliance when selling medical device and pharmaceutical products. The standards also have other benefits to businesses involved in these processes, including manufacturers as well as those further down the supply chain.

This includes helping to reduce the prevalence of fake medicines, improving the quality of products produced and delivered to patients/clinicians/customers, and minimising business risk in the manufacture and distribution of healthcare products.

Taking a Holistic Approach to Cybersecurity in the Transition to Becoming a Smart Factory

In a recent blog, we highlighted the cybersecurity risks that are created by the increasing attack surface in manufacturing organisations. As a quick recap, as you integrate systems, platforms, and equipment, and as you connect elements of your operation to the cloud, the potential attack surface in your organisation expands, exposing you to higher cybersecurity risks.

In our previous blog, we also highlighted the key to mitigating these risks – taking a holistic approach to cybersecurity as you transition to a Smart Factory. This means integrating your IT and OT (operational technology) teams and developing cybersecurity strategies, processes, and mitigation measures that cover all aspects of your organisation's technologies. This includes everything from your Manufacturing Execution System to the cloud applications used by your accounting team to the PLCs and SCADA systems running on the factory floor to the CRM used by your sales and marketing team.

What does this holistic approach to cybersecurity mean, though? What are the practical steps that should be taken by pharmaceutical, medical device, and technology manufacturers?

The Challenges of the Increasing Attack Surface

A good starting point is to have a clear understanding of the scale of the challenge when you integrate and connect devices and therefore increase the attack surface and potential risks. Some of the main points include:

- Many OT legacy systems have complex cybersecurity vulnerabilities.
- One of the reasons for the above point is the fact that OT equipment is traditionally older and less adaptable to change.
- Software upgrade and security patching processes often lack structure.
- The process of rolling out updates and security patches is more challenging with OT equipment. This is because OT equipment directly controls the production process. As a result, each upgrade and security patch must be risk assessed and qualified.
- Visibility across the entire operation is limited.

Industry 4.0 Cybersecurity Best Practices

A crucial component of Industry 4.0 cybersecurity is to make sure there is correct OT/IT bridge separation to isolate and protect OT equipment from external threats. This OT/IT bridge separation will also provide protection against the internal risks that are often present in large corporate IT networks.

This protection of OT equipment requires the implementation of robust architecture during connectivity design. This architecture needs to allow data through while at the same time preventing inward threats.

Other essential Industry 4.0 cybersecurity best practices include:

- Make cybersecurity an integral part of your smart manufacturing strategy.
- Take an end-to-end approach to cybersecurity that includes technology, processes, and people.

- Put in place a cybersecurity governance programme covering both IT and OT. This includes developing comprehensive cybersecurity procedures, controls, and policies. These procedures, controls, and policies should also be regularly reviewed and updated.[15,16,17]

- Put in place a strategy to continuously raise awareness of cybersecurity risks. This should apply at all organisational levels and should ensure constant vigilance while also providing education on new and emerging threats.

- Implement a strategy of continuous cybersecurity skills improvement throughout the organisation.

- Continuously focus on emerging threats as well as existing threats.

Getting it Right All the Time

There is a difficult and unfair reality about cybersecurity that is universal – those who seek to attack your organisation only have to be right once, whereas to properly protect your OT systems, you have to be right all the time.

This fact should not be a barrier to continuing on your Industry 4.0 journey as there are too many benefits to be ignored. However, cybersecurity considerations must be a core priority in everything you do and at all levels of the organisation.

III. RESULTS

An Overview of the Industry 4.0 Cybersecurity Risk Mitigation Process

In previous blogs in this series, we looked at one of the unintended consequences of implementing Industry 4.0 technologies and processes – the increased attack surface. In other words, the more equipment you connect, the larger the target for would-be attackers. We also looked at the challenges of dealing with this Industry 4.0 cybersecurity issue, and we outlined the main best practices.

In this final blog in the series, we outline the Industry 4.0 cybersecurity risk mitigation process. This process will help you overcome the challenges of cybersecurity and protect that ever-growing attack surface.

There are three main parts of this risk mitigation process:

1. Assess
2. Secure
3. Monitor

1. Assess Industry 4.0 Cybersecurity Risks

Cybersecurity Maturity Assessment

This part of the process starts by conducting a cybersecurity maturity assessment of your organisation with the aim of identifying risks to OT equipment and systems.

Risk Evaluation and Prioritisation

Once risks are identified, they need to be evaluated and prioritised to assess the probability of occurrence and the level of harm that could be caused. Those with a high probability of occurring and a high level of harm should be the highest priority.

Remember, however, that cybersecurity risk evaluation is not just about looking at the immediate threat. You also need to look at the root cause.

For example, one area that might be identified as high risk is malware knocking systems offline or putting data at risk. The probability of this occurring is high as malware attacks are commonplace. If such an attack is successful, it is likely to have a significant impact. Therefore, it makes sense to mitigate this risk.

Further analysis might reveal there is insufficient monitoring of malware and a poorly configured firewall. There might also be security patches that have not been applied.

You should put in place mitigation measures to harden these technology and process weak points. However, this doesn't necessarily get to the root cause of the problem. Let's track it back in reverse order:

- Malware isn't spotted, so it gets control of part of the system.
- It got through the firewall because it wasn't configured properly.
- It got to the firewall because a security patch wasn't applied to part of the system.
- The malware got into that part of the system because an individual with access used a USB device on a connected piece of equipment.
- The use of USB and similar devices is widespread because of a general lack of understanding of the cybersecurity risks they pose.[17]

There is definitely a technology problem in the above scenario. However, when you track the issue back to its root cause, it is also a people problem. Therefore, you need an end-to-end solution that includes technology, processes, and people:

- Technology – improve malware monitoring and firewall configuration
- Processes – ensure security patches are properly applied and develop a policy on the use of USB and similar devices
- People – conduct regular training for staff on cybersecurity risks and how to mitigate them

Once you have identified, evaluated, and prioritised the risks, the next step is to identify mitigation measures.

2. Secure Your OT Equipment

In this part of the risk mitigation process, it is important to understand that while a holistic approach is essential, the practicalities and realities of IT and OT can be contradictory.

This especially applies in fields like pharmaceutical and medical device manufacturing, as there are patient safety and compliance requirements. This creates situations where IT systems can be completely locked down for cybersecurity reasons while a certain degree of openness is required for OT systems to allow data to pass through.

Another example of the practical differences is the application of security patches. In most IT systems, security patches can be applied immediately. Greater care must be taken with OT systems, however, as the patch itself must be risk assessed and qualified. This is because applying a security patch could reduce the availability of a piece of equipment, impacting essential metrics like production line output and OEE (overall equipment effectiveness).

This is before you even consider the fact there will be OT systems and equipment operating on production lines that are no longer supported by the manufacturer, so security patches are not being developed.[15,17]

It is also important to take into account the nature of the equipment and systems being used, as this will also impact the steps required to make them secure. In IT security, equipment and systems are likely to be relatively new, while in the OT environment, it is not unusual to see equipment and systems that are decades old.

During the process of developing mitigation steps to secure your OT equipment against identified risks, there are some key points to consider:

Identity and Access Management

Identity and access management are essential cybersecurity components, but they are particularly important when third-party contractors are working on OT systems. If the contractor is physically present on the factory floor, they will have gone through the company’s security protocols. However, it is now increasingly possible for engineers to remotely work on manufacturing lines and equipment. Security measures for remote access are often much weaker than those in place for physical access, so there is usually room for improvement.

Use Reliable Partners and Vendors

It is also important to use trusted vendors and engineering teams that prioritise security when developing or updating systems and software. A track record of success is important too.

Reduce the Attack Surface Where Possible

A lot of the focus of Industry 4.0 cybersecurity involves securing the increasing attack surface, but there are also steps you can take to reduce potential access points for an attack. This includes removing unneeded systems and equipment

3. Monitor the Effective of Your Cybersecurity Risk Mitigation Measures

The final step in the risk mitigation process is the continuous monitoring of your mitigation measures, including through the use of automation and machine learning technologies.

You should also build in levels of redundancy wherever possible, so there are alternatives if a system or piece of equipment has to be taken offline for cybersecurity reasons.

Ensuring maximum resiliency is important, too, including ensuring you take regular system and data backups. You should also have an up-to-date disaster recovery plan, and it should be regularly tested, assessed, and reviewed.

An Ongoing Process

The process outlined above should become a constant feature of your operations, given the increasing fluidly of the manufacturing sector and the constantly changing nature of the cybersecurity threat profile. Prioritising cybersecurity and continuous vigilance are the solution.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 9, September 2023 |

| DOI:10.15680/IJMRSET.2023.0609004 |

SL Controls Shortlisted for Limerick Business Awards 2021

SL Controls has been shortlisted for an award at this year's Limerick Chamber of Commerce Business Awards. We are in the running for the Best Employer: Employee Talent Development & Workplace Wellness award.

It recognises companies that set high standards for wellness and talent development, and that create world-class working conditions for employees.

The other shortlisted companies in this award category are Three.ie and Kirby Engineering & Construction. The awards ceremony will take place on 19 November in the Limerick Strand Hotel.

Shauna Ryan, HR Manager at SL Controls said: "Employee wellness – both physical and mental – is a high priority for us at SL Controls. We have well-established programmes in place to promote and ensure wellness in the workplace. We are also committed to helping our employees find the right work-life balance while achieving what they want to achieve with their careers.

"Continuous professional development is also crucially important for us for a number of reasons, including the competitive nature of the recruitment landscape and the fact we operate in an industry that is constantly innovating. We support staff through training in a range of different ways to ensure we remain competitive as a company and to help our employees reach their full potential.

"To be recognised for these important priorities in our business is fantastic. We have been involved with the Limerick Chamber for many years now, and the awards ceremony is always a highlight on the regional business calendar. We are delighted to have been shortlisted in this category, and we are looking forward to the ceremony."

Project Management: The Importance of Economies of Repetition in Industry 4.0 Projects

One of the business outcomes that manufacturers want to achieve with Industry 4.0 projects is repeatability. Repeatability is about creating solutions that can be reliably and efficiently deployed multiple times. This goal of repeatability is also important in the delivery of Industry 4.0 and smart manufacturing projects.

In project management, this can be referred to as the economies of repetition. The economies of repetition involve creating structures and processes that make it possible to execute projects to a consistent minimum standard, with that standard constantly being enhanced and improved.

At SL Controls, we deliver economies of repetition in Industry 4.0 projects through TOTALproject.

What is TOTALproject?

TOTALproject defines our internal project management structure. It features a set of tools and templates, which we call the SL Controls project management Toolbox. TOTALproject is managed, improved, and updated by the SL Controls Project Management Office (PMO), and everything is documented in a SOP (Standard Operating Procedure).

The tools and templates in TOTALproject are based on the Project Management Institute's framework, so we are not redesigning the wheel. The goal of TOTALproject is to adapt tried and tested principles to our organisation and the delivery of projects specifically focused on our areas of expertise.

Project Management Toolbox

The SL Controls project management Toolbox includes governance structures and templates that our project managers and PMO use to ensure clear authority and accountability. The governance structures also ensure outputs and outcomes are clearly defined and controlled within each project and the PMO more generally.

Our project management Toolbox also ensures that lessons learned at the end of each project are communicated to all project managers and the wider SL Controls team. We have clearly defined processes to facilitate this sharing of knowledge to continuously raise standards.

We also have an ongoing focus on the development of our staff, providing training and professional development opportunities to increase the project management skills in the organisation. This includes helping our staff achieve PMP certification to become Project Management Professionals.

Benefits of Our Approach to Project Management

There are multiple benefits that come from our approach to project management at SL Controls. This includes company benefits as it ensures projects run more efficiently and cost-effectively. There are benefits to our employees, too, especially those who want to pursue a career path into project management.

The main benefits are for our customers, i.e., through the economies of repeatability. What does this mean in practice? There are three main points:

- Consistency in project delivery – TOTALproject and the project management structures we have put in place bring uniformity to project management at SL Controls. This ensures consistent standards on all projects.[11,12,13]
- Continuous improvement – while achieving consistency is important, standards are not fixed. Continuous improvement is central to our project management approach.
- Skills development – it is essential that we have the in-house skills available to deliver on the requirements of our clients. We achieve this through the development of our team, ensuring we have a pipeline of new project managers coming through.

The specifics of how we deliver projects depend on the requirements of our clients. For example, some clients already have robust project management structures, whereas on other projects if the client project management templates are not available, we will use our own. The principles and objectives of TOTALproject and our PMO remain the same – ensuring the economies of repetition in Industry 4.0 projects.

IV. CONCLUSIONS

Health and Safety and Remote Working at Client Sites

Throughout the Covid-19 pandemic and as we look to the future at SL Controls with increased home working arrangements, we have adapted our policies on health and safety. There is now much greater emphasis on ensuring consistent standards between health and safety in an SL Controls office location and when an employee is working from home.

For us at SL Controls, this also brought into sharp focus the fact we now have three distinct working conditions for our employees in terms of health and safety.

- Working in an SL Controls office
- Remote working from home
- Remotely working at a client site

Health and Safety for Remote Working at a Client Site

While working from home is currently a popular topic of discussion, remote working was common even before Covid-19. Remote working (outside of working from home) can take many forms, but at SL Controls, it typically means employees that travel to different client locations for all or some of the working week.
While this type of remote working has been common historically, it has not been common over the past 18+ months. As a result, we have taken steps to remind our team of important health and safety issues when working remotely.

Working at Client Locations

When working at client locations, our employees follow the health and safety policies and procedures of SL Controls and those of the company where they are working. This includes completing necessary risk assessments, understanding responsibilities, getting clarification when there is any confusion, and ensuring similar standards are applied for workstations and other working conditions.

Driving

Driving is an important health and safety consideration as there are many factors that are beyond an employer's or employee's control. Steps that we can take include checking the driver's licenses of our employees and reminding employees about staying safe when driving for work.

This includes taking practical steps such as making sure the vehicle is safe and properly maintained. At this time of year, things like tyres, washer fluid, and lights are particularly important as roads become more slippery in the winter months, there is often reduced visibility, and there is increased spray on windscreens.

We also advise employees to plan journeys in advance and ensure they are realistic about how long the journey will take. This advice includes leaving early enough, taking sufficient breaks, and taking into account bad weather, traffic, and the unexpected.

It is also important to emphasise being careful when driving in low light and when it's dark, as it is much more likely in the winter months to be driving in low light conditions both at the beginning and end of the day. Remaining alert and being well-rested are essential.

Other advice includes avoiding driving completely in exceptionally bad weather, and never using mobile phones while driving.

Covid-19 Considerations

Covid-19 is also a consideration for remote workers, so we also remind employees of the steps they should take to stay protected when working at a client site. This includes following the rules put in place by the client, in addition to following the more general advice of wearing a mask, regularly washing hands, and keeping a safe distance.

Travelling Overseas

While travelling overseas has been limited recently, it remains an important health and safety consideration for remote workers. Those considerations include everything from different driving conditions to crime and weather.[14]

Monitoring the Health and Safety of Remote Workers

At SL Controls, we have clear and consistent management systems that ensure employees working at client sites and other remote workers are safe. We also take steps to ensure our systems remain effective. This includes regularly reviewing risk assessments and including remote workers in decision-making.

Ongoing Improvement Process

As with most things in business, particularly in our industry, it is important not to stand still. Continuous improvement should always be the objective, including in all aspects of health and safety.

This continuous improvement approach enabled us to quickly adapt our health and safety processes when we moved to 100 percent remote working at the start of the pandemic. It will also ensure we continue to use best practices in health and safety when our employees work at client sites.[17]

REFERENCES

1. "application software". Oxford English Dictionary (Online ed.). Oxford University Press. (Subscription or participating institution membership required.)
2. ^ R. Shirey (August 2007). Internet Security Glossary, Version 2. Network Working Group. doi:10.17487/RFC4949. RFC 4949. Informational.
3. ^ "Application software". PC Magazine. Ziff Davis.
4. ^ Ryan, Thorne (2013-03-14). "Caffeine and computer screens: student programmers endure weekend long appathon". The Arbiter. Archived from the original on 2016-07-09. Retrieved 2015-10-12.
5. ^ Ceruzzi, Paul E. (2000). A History of Modern Computing. Cambridge, Massachusetts: MIT Press. ISBN 0-262-03255-4.
6. ^ a b Ulrich, William (August 31, 2006). "Application Package Software: The Promise Vs. Reality". Cutter Consortium. Cutter Benchmark Review. Archived from the original on 2 February 2016. Retrieved 2022-01-12.
7. ^ Dvorak, John (1989-07-01). "Looking to OS/2 for the next killer app is barking up the wrong tree. Here's where they really come from". PC Magazine. Ziff Davis. Retrieved 2022-03-25.
8. ^ "killer app". dictionary.com. Retrieved 2022-03-26. Origin of killer app 1985-1990
9. ^ Thom Holwerda (24 June 2011). "The History of 'App' and the Demise of the Programmer". www.osnews.com. Retrieved 2022-01-12.
10. ^ Gassée, Jean-Louis (2012-09-17). "The Silly Web vs. Native Apps Debate". Archived from the original on 2016-04-15. Retrieved 2013-07-14.
11. ^ Frechette, Casey (2013-04-11). "What journalists need to know about the difference between Web apps and native apps". Poynter. Retrieved 2017-01-04.
12. ^ Valums, Andrew (2010-02-10). "Web apps vs desktop apps". valums.com. Archived from the original on 2013-04-02. Retrieved 2013-07-14.
13. ^ "What Is a Horizontal Application?".
14. ^ "What Are Horizontal Services?". Archived from the original on 2013-10-31.
15. ^ "What is Application Software & Its Types | eduCBA". eduCBA. 2015-12-21. Retrieved 2017-03-24.
16. ^ Campbell-Kelly, Martin; Aspray, William (1996). Computer: A History of the Information Machine. New York: Basic Books. ISBN 0-465-02990-6.
17. ^ "Definition of desktop application". PCMAG. Retrieved 2022-01-07.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor
7.54

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com