July 01, 2023

April-June 2023

CILT Newsletter

The Chartered Institute of Logistics and Transport-India

How technology can ensure safety and save lives on Indian roads?

Technology-driven active safety measures such as vehicle alerts, remote prognostics, through the connectivity of an advanced driver assistance system, have proven to improve road safety by helping the driver manage or avoid emergency situations proactively.

TECHNOLOGY-DRIVEN ACTIVE SAFETY MEASURES

Advanced Driver Assistance Systems (ADAS) can be game changers for developing countries like India than for the west. This technology will break the vicious cycle of High Road Crash, Missing Safety Culture and create a virtuous cycle of Alert, Assist, Save and Learn for every road user and avoid millions of crash situations on an hourly basis.

The Chartered Institute of Logistics and Transport

EDITORIAL BOARD

Mr. Vinod Asthana

Dr. Veni Mathur

Mr. Rajiv Kochhar

Mr. Vaibhav Shah

NATIONAL COUNCIL MEMBERS OF CILT-INDIA

- **Hon'ble Shri Suresh Prabhu FCILT** — **Patron of CILT-India**
- **Shri Shanti Narain FCILT** — **Chairman Emeritus**
- **Shri N. Sivasailam FCILT** — **National Chairman**
- **Dr. Veni Mathur CMILT** — **Vice-Chairperson**
- **Shri Sharat C. Misra FCILT** — **Vice-Chairman**
- **Shri Vinod Asthana CMILT** — **Vice-Chairman**
- **Shri Sanjiv Garg CMILT** — **Secretary General**
- **Dr. Narender K. Tuli CMILT** — **Treasurer**
- **Shri Manish Puri CMILT** — **Member**
- **Dr. Manoj Singh CMILT** — **Member**
- **Shri Samir J. Shah FCILT** — **Member**
- **Shri Sachin S.Bhanushali CMILT** — **Member**
- **Shri Jakob Friis Sorensen CMILT** — **Member**
- **Dr. G. Raghuram FCILT** — **Member**
- **Shri Rajaji Meshram CMILT** — **Member**
- **Smt Ragini Yechry FCILT** — **Member**

CILT INDIA successfully completes

Three Months Weekend (On-line)

Professional Certificate Program in Terminal Management 2.0

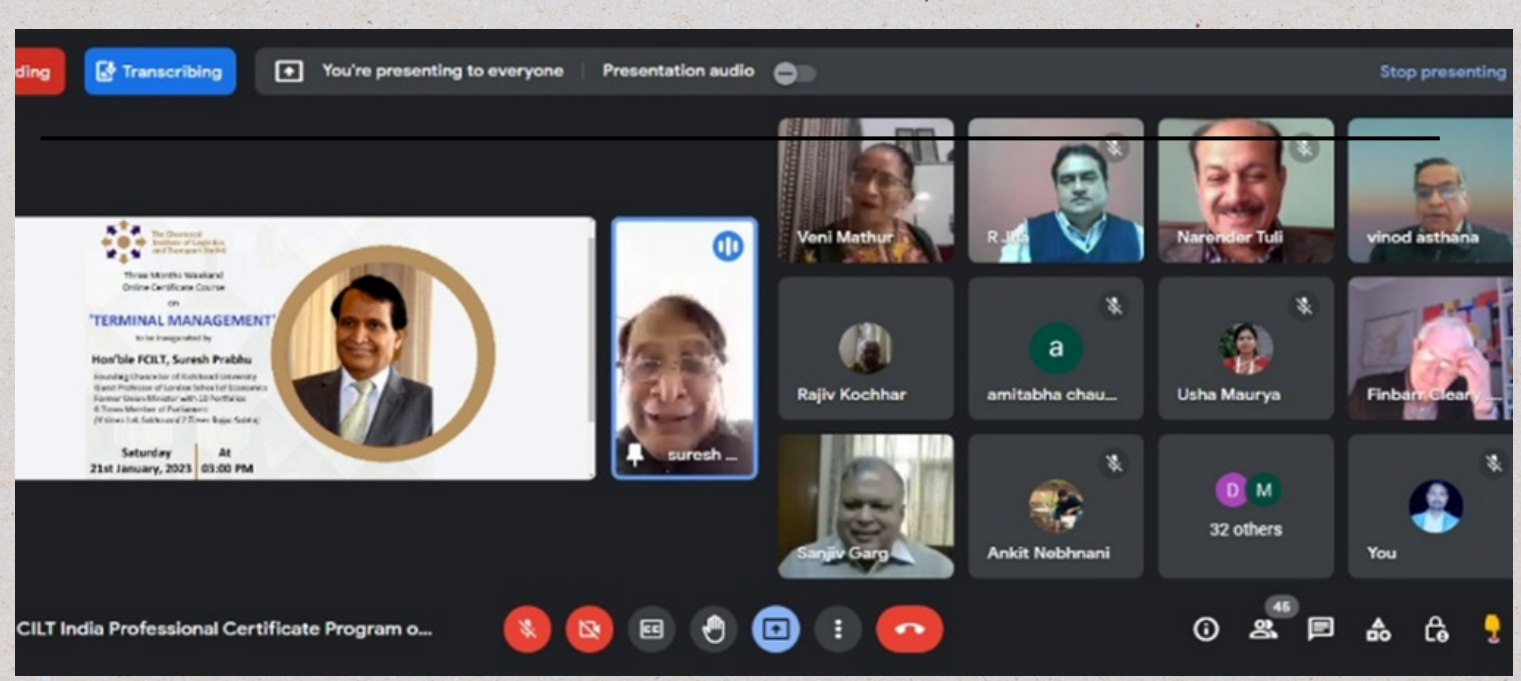
The Chartered Institute of Logistics and Transport - India (CILT India), is duly accredited by "The Chartered Institute of Logistics and Transport – International (www.ciltinternational.org)" and holds the territory status to conduct education and training Programmes in the field of logistics & transport in India.

With the announcement and implementation of "Gati Shakti Mission – A National Master Plan for Multimodal Connectivity", hundreds of terminals are planned to be established. CILT India has designed and developed an exclusive training program namely "Professional Certificate Program in Terminal Management".

This training program was meant for aspiring and in-service professionals to equip them with the necessary skills to leverage the current and emerging patterns. The objective of the program was to provide an excellent understanding of entire activities related to Policy, Plan & Design, Construct and operate various types of existing & futuristic terminals in a safe & environment friendly manner for efficient handling & movement of all types of goods.

The training program was conducted in on-line mode on weekends (i.e., on every Saturday & Sunday) for three to four hours and the duration of the program was for of 03 months, starting from 21st January – 09 April 2023.

The training program received a very good response from the industry and a total of 46 nominations for participation has been received from 7 Organizations, which included 01 PhD student from School of Planning and Architecture, 01 from Bennett University. Large Number of the participants from Adani,



Inauguration of Training Program on 21 January 2023

The training program was online inaugurate session on 21st January 2023, which was attended by :-

- Shri Sandeep Mehta CMILT, President Adani Ports & Sez Ltd.
- Shri N. Sivasailam, IAS, (Rtd.), and National Chairman of CILT India,
- Mr. Finbarr Cleary, International Vice President- International Business Forum (IBF)
- Ms. Reshma Yousuf CMILT, DGSA, CEO-CLLB, Malaysia
- Shri Sanjiv Garg, IRTS (Rtd.), and Secretary General of CILT India, and Managing Director, Pipavav Railway Corporation Limited, Former Additional Member, Railway Board
- Shri Vinod Athana IRTS (Rtd.) CMILT, Vice Chairman of CILT India, Former Managing Director, CRWC Ltd.
- Dr. Veni Mathur CMILT, Vice Chairperson, CILT India,

The list of organizations nominating the participants are as under:

Participant Organisations Name
Adani Logistics Ltd.
Gateway Rail Freight Limited
SAM surveyors and Adjusters
PWC India
MSMV Marketing
School of Planning and Architecture
Bennett University

During the course of this training program spanning over 24 days (12 Weekends), a total of 46 lecture sessions has been delivered covering entire aspects of terminal management by more than 33 eminent experts of the trade. These eminent experts include several serving topmost officials of Govt. of India,

Public Sector Undertakings and Private Corporate Houses. In addition, there were few eminent international experts as well, who took the sessions from Ireland & Malaysia to give a global perspective on the subject.

This training program also included two stage evaluation of participants, wherein participants were given two assignments meant to be submitted by them within the stipulated time frame. Based on the performance of the participants in this evaluation, the certificate issuance to participants of this training program were categorized into two parts:

- **Certificate of Proficiency:** The proficiency certificate has been awarded only to such participants, who qualified after the evaluation of both of their assignments, as submitted by them during this training program.

- **Certificate of Participation:** The participation certificate has been issued to all participants.

The award of 'Certificate of Proficiency' was categorized under three grades, based on the marks obtained by the respective participants post evaluation of both the assignments submitted by them, as under:

%ge of marks Obtained	Grade Awarded
80% and above	A+
60% and above but less than 80%	A
40% and above but less than 60%	B
Less than 40%	Not Qualified

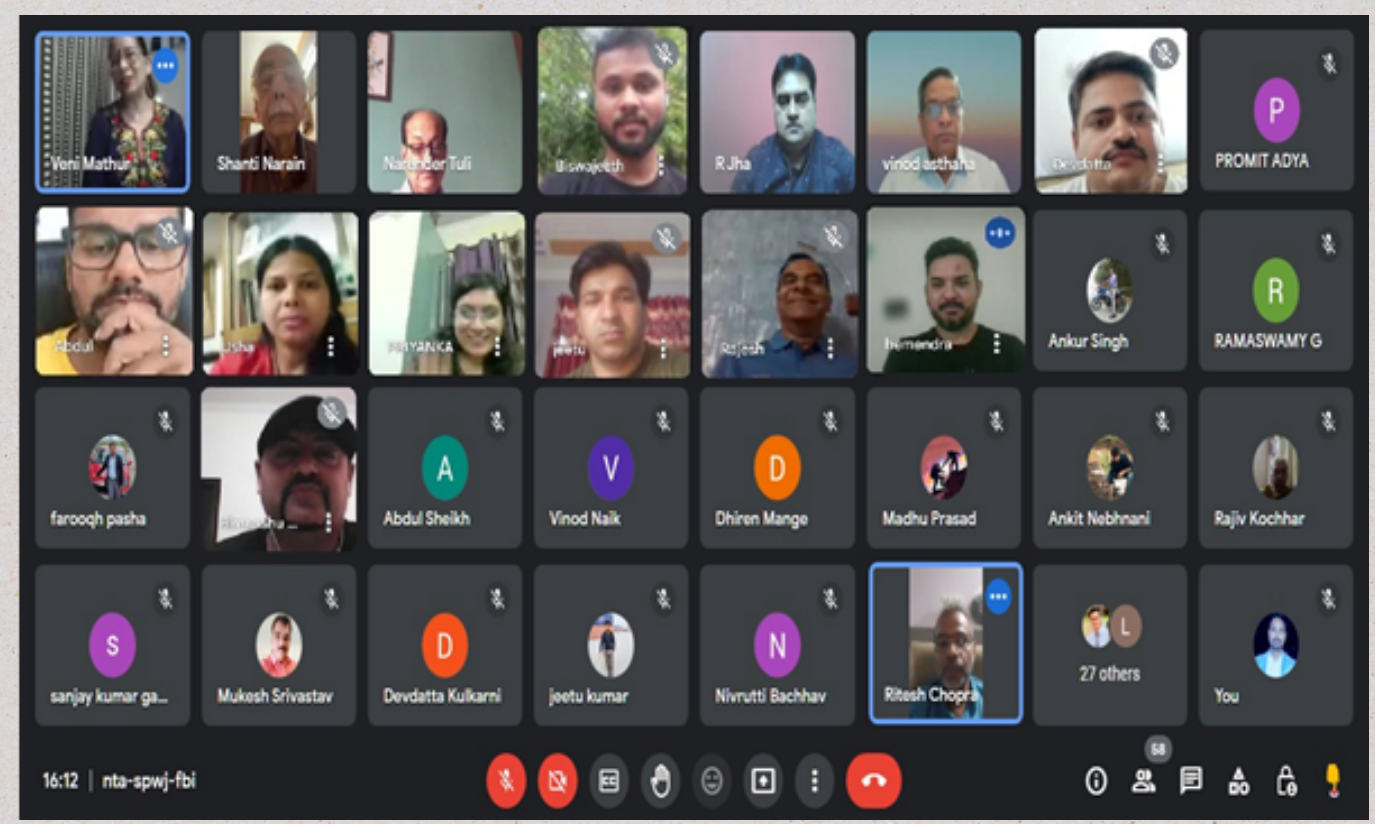
The training program concluded with valedictory on 09th April 2023. The course director Sh. Vinod Asthana summarized the audience about the entire training program with a target to make it widespread with bigger participation in future sessions. Thereafter, Sh. Shanti Narain, Chairman Emeritus – CILT India deliberated on the importance of terminal and the vital role it plays in the entire logistics value chain and assured the further improve on the quality of content in future.

Sh. Sanjiv Garg, General Secretary – CILT India has declared this training program as one of the most successful courses conducted so far by CILT India. He further discussed upon the need of reducing the higher logistics costs in India and also emphasized upon setting-up of standardization process in logistics.

Subsequent to this, feedback from some of the participants were also taken, who found the course content and speakers beyond their expectations and thanked CILT India for conducting such an excellent training program.

Finally, the valedictory was addressed by Sh. N. Sivasailam IAS (Retd.), National Chairman – CILT India, who thanked the Program Director and Associate Program Director for successfully conducting this training program. He deliberated upon the current scenarios of logistics and how redressal to issues be made. He also informed participants about evaluation of assignment / project as submitted by participants and declaration of results thereafter

The program concluded with a vote of thanks by Dr. Veni Mathur, Associate Course Director to all the attendees, participants, and their nominating organizations.



It's no longer products, its solutions

Girish Mirchandani, Editor, Transtopics / Trans India News Network

The road transport as well as the commercial vehicle industry has undergone a lot of changes in the last few years – not just in terms of products and services, but also in terms of deliverables to the respective customers. So, transportation of goods is not as simple as picking up goods from point A and delivering to point B – nor is selling a truck as simple as giving a truck to the customer. The entire process of deliverables has been redefined and companies are now not selling products or services, but they are selling Solutions.

However while it may sound pretty simple, but the process or the journey towards designing solutions has been a difficult one, with lots of research and data crunching. Companies, be it OEMs or transporters, have spent a lot of time, effort and funds to design solutions that make life simpler for the customers and besides quality products / solutions, give them the freedom to focus on their competence. And while we spoke of investing in designing these solutions, the providers have always been complaining that the monetary returns have been inadequate.

One of the toughest elements of the road transport industry has been 'Trucking'. All these years companies have been struggling with this element and how much ever they try to get things right, one of the spokes of the wheel gives way. Maintenance and upkeep of the trucks has always been a tough task – be it for fleet owners or for the smaller truckers. While the fleet owners have had their own workshops, once on the highways, the trucks are dependent on either the road side mechanics or the authorised service centre.

Until some time back, authorised service centres was not the most preferred option because of the cost and time taken. Therefore, the road side mechanics were the next best option – comparatively cheaper and faster. But these mechanics had their limitations. The smaller issues

limitations. The smaller issues could be taken care of, but major repairs and periodic service was still done with the authorised service centres. So, while the issues in the trucks were resolved one way or the other, the larger problem was that transporters had to be involved at every step.

Some years back, OEMs came up with the Annual Maintenance Contract (AMC) facility, which intended to take away the worries of servicing and maintenance from the customers. However, it was an expensive proposition at that time and somehow AMC did not gain popularity. But in the last few years, a lot has changed – not just for the OEMs, but also for the transporters.

The road transport business has become very demanding and transporters have been investing in putting up systems that make the transportation business better organised and systematic. Telematics has been once such innovation that has transformed many companies. Back in the day, telematics was all about knowing the location of the truck and it also seemed to be a very vital piece of information. But over the years, telematics has grown beyond just tracking the truck. The data available is being used for many more things – right from fleet management to driver behaviour to client servicing. The nextgen in the business is using the data available for many other ways that eventually improve efficiency and reduce cost.

The other big transformation in the transport industry has been the ERP systems, which make back end management more efficient. So from a back end perspective, what looked like haphazard operations some years ago, now seems like a better managed scenario with various factors being managed and operated with relative easy.

As a result of the above, armed with a lot of data, transporters are able to give their customers not just delivery of their cargo, but also transport related solutions. The ultimate aim is to being down the logistics cost and at the same time ensure that there are no delays in picking up or delivering the cargo. While the transporters, over the years, have strengthened their back end operations, their biggest area of concern has been fleet management, and the OEMs are well aware of this gap. Needless to say, they also have been working tirelessly to come up with a solution to these issues. And they have hit bulls eye in the last couple of years.

The OEMs have been on the edge for the last few years with the government introducing strict emission norms. There have been major technology transformations because of these upgrades, that too in a short span of time. The transition from BS III to BS IV resulted in a lot of electronics in the trucks and the transition to BS VI further complicated this, with more electronics. This transition to BS VI and now to BS VI Phase 2 wef from April 2023, is further going to enhance the effort to provide a complete solution to the truck owners. But before that, since the last few years, there has been a conscious shift to the AMC model. Not only has the cost become manageable, the service levels too have gone up significantly, with the OEMs pushing the dealers for increasing their capacity. At the same time, with service intervals going up, the trucks need to go to the service centre less often.

The transporters have realised the importance of periodical maintenance, since it ensures that the truck is performing to its best capability. Any kind of breakdown is something that transporters cannot afford, especially in contracts that are strictly time bound. Therefore it is in the best interest of the transporters to ensure that their trucks spend the maximum time on the road – and not in the service centres. As far as the BS VI trucks are concerned, the road side mechanics lack the capability as well as the tools to handle these trucks. So somehow these trucks by default have to come to the authorised service centre for any kind of scheduled maintenance or repairs.

The good part is that OEMs are now not talking about just the price of the truck. They are talking about a complete package, that includes service, maintenance and also add-on solutions such as tracking, driver behaviour, vehicle diagnostics and many more features. There is a complete dashboard that shares vital information on the truck and its behaviour and there is also a backend service centre that keeps an eye for any red flags.

Time and again we keep hearing that Logistics Cost has to come down. And one of the ways of doing that is to keep the trucks running on the roads for as long as possible. There can be some irregularities in getting load, which may put a brake on the truck. But having the truck to stay grounded at the workshop is definitely not acceptable. OEMs have put in a lot of effort and funds to make sure that trucks perform continuously, which leaves the transporters to focus on their core competence.

The other big cost centre for the transport industry is Tyres. It is heartening that even tyre companies are now talking about not just selling tyres, but solutions around tyres. There are a lot of options, including close monitoring of the performance of tyres and educating the transporters / truckers for getting more mileage from the tyres. At the same time, tyre companies are also offering add-ons such as constant tyre pressure monitoring and alerts, which not only increase tyre life, but also reduce fuel consumption – the largest component of the operating cost.

As India races towards its target of USD 5 trillion economy, one cannot deny the fact that road transport or logistics on the whole will be playing a very crucial part in this achievement. And in order to keep the wheels of road transport moving uninterrupted, OEMs and other suppliers are making sure that other elements of business related to the vehicle or components are handled by the manufacturer / supplier.

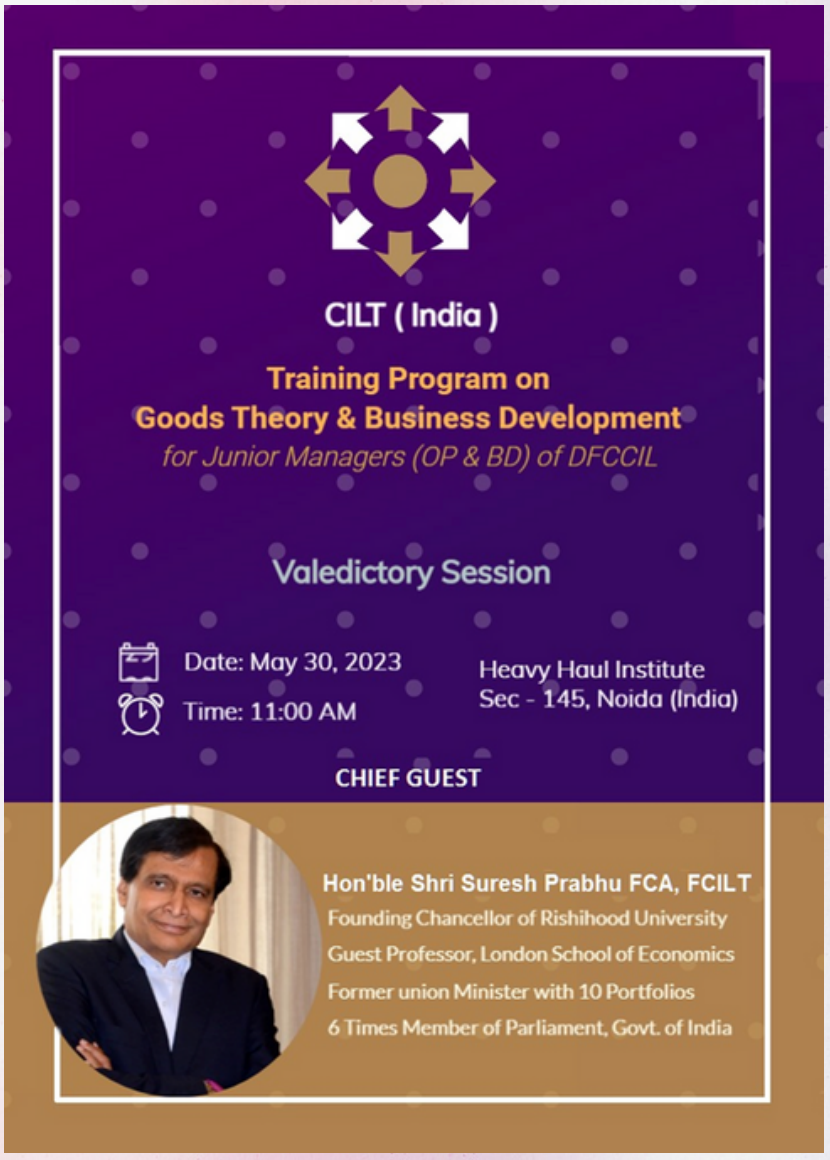
The road transport industry has made significant progress in the last few years and the adoption of advanced technology has been one of its biggest achievements. This is being translated to more business, more efficiency and better margins. It's just that all these elements have to support each other so that each one can continue to work on their core competence. And for those who are still offering just services, it is time to re-think your strategy and start working on Solutions.

CILT conducts Training Program on "Goods Theory & Business Development" for DFCCIL

Induction of First Batch of Trainees Jr. Manager (OP & BD)

The Chartered Institute of Logistics & Transport – India (CILT India) has conducted a 50 Hrs. classroom training program on "GOODS THEORY & BUSINESS DEVELOPMENT". This training program was spread over a period of five weeks starting from 25 April 2023 which finally concluded on 30 May 2023 with a valedictory session.

This training program was specifically meant for the first batch of trainee Jr. Managers (OP & BD) of DFCCIL (Dedicated Freight Corridor Corporation of India Ltd.), who will serve as front-line officers in the field and will deal with train operations, marketing & commercial functions. The physical classes for the said training program was conducted at their **Heavy Haul Institute (HHI), Noida.**



The valedictory session and certificate distribution of this training program was conducted on **30 May 2023 at HHI, Noida** wherein Hon'ble Sh. Suresh Prabhu FCA, FCILT, Former Union Minister with 10 portfolios including Ministry of Railways, has consented to be the Chief Guest and has delivered the Valedictory Lecture in online mode, despite being ill. Participants were also addressed by **Sh. Shanti Narain, Former Member Traffic (Indian Railways) and Chairman Emeritus – CILT India; Sh. Srinivas Nanduri, Director (Operations & Business Development), DFCCIL; Sh. Sanjiv Garg, MD – Pipavav Rail Corporation Ltd. & General Secretary – CILT India**.

The training program finally concluded with a vote of thanks by Sh. Vinod Asthana, Vice Chairman, CILT India at the valedictory session.

OPINION: HOW TECHNOLOGY CAN ENSURE SAFETY AND SAVE LIVES ON INDIAN ROADS

Rama Shankar Pandey, CEO, Tata Green Batteries

Technology-driven active safety measures such as vehicle alerts, remote prognostics, through the connectivity of an advanced driver assistance system, have proven to improve road safetyby helping the driver manageor avoid emergency situations proactively. This can be achieved by fusion of Telecommunication with informatics, capitalising on the quantum leap the scientists have taken in the domain of DataScience, Artificial Intelligence and Machine Learning.It will be a win-win for all stakeholders. And so we will see India free from all avoidable road deaths through technology for a purpose, #Technology4Safety.

Roads have becomecentral to human life and the symbolof national prosperity. Yet 3700 road deaths every day is a black-spot on worldtransportation. One day people may ask, is it worth?Is it sustainable?

In India, millions travel on roads; but daily 415 families do not get back their dear ones home. Road fatalities are the biggest cause of unnatural deaths among Indians. It is estimated that road accidents cost India about 3%-5% of its gross domestic product every year. India loses a city'sworth of population every year due to road crashes according to the Ministry of Road Transport & Highways of India data. With the evolution of the motorized vehicles, increasing speed limits and improving roads all over theworld, the boom of road transport is turning into a major bane to mankind. Without appropriate strategies to reduceroad accidents and deaths, it is becominga serious global crisis.

The National Crime Records Bureau data shows that India had about 1,55,622 deaths (due to road accidents) in 2022, with millions more sustaining serious injuries and living with long-term adverse health consequences. Globally,road traffic crashesare a leading cause of death among the young people, and the main cause of death among those aged 15–29 years.

Why road crashes?

Who is responsible for these deaths? More profound question should be how do we arrest the alarming Road Death numbers? For an answer we must look into the cultural reality of Indian Roads.

Understanding Road Crash is a complex science, yet an average Indian still treats it as a chance factor. Hence, many resort to luck/chance and Science takes a back seat. That is why so many superstitions like "Black Cat/Kaali Billi & Lemon Chilli/Nimbu Mirchi" are spread around the vehicles. It is also evident from our roads that we naturally do not follow Road Rules. .

The root cause remains the same. We don't believe that the Road Rules, the Life Saving Protocols, have a scientific background and hence most of us treat them more as law-compliance issues

The government is highly concerned about these deaths. Through world class regulation of Vehicles, Infrastructure, Licensing and Driving rules, it has demonstrated its strong intention to reduce road accidents and deaths. Still road crashes continue to occur because of inadequate enforcement of these laws and their violations by the road users. Majority of citizens violate simple road rules like Lane Discipline, Maintaining Safe Distance or wearing helmets, seat belts etc. Safety culture on our roads is grossly inadequate and it is obvious, as the majority of our masses still believe that road crashes are accidents by chance.

Countries where citizens respect the road rules and accidents occur owing to genuine human error, Government supports by bringing major Infrastructure reforms in a systemic approach. Our Safety Culture is very different from those countries. Our road designs and infrastructure have much higher density of black spots and our roads have become most dangerous in the world.

The more than 85% of two-wheeler riders and the mixed traffic of people who have no formal training to drive add to the unique complexity.

Technology has the answer

So what's the solution? Technology has the answer. The developed countries are looking at Autonomous Driving for their various specific needs. We in India also must not miss the biggest opportunity of our time to put Technology to its rightful use for arresting the alarming number of road accidents and deaths.

Replacing human drivers with autonomous soft bots in our cars may not and should not be our highest priority, as India r needs more skill-based employment generation in near term. We must assist our drivers, alert our road users and guide our infrastructure designers with technology that can become a game changer.

The early levels (0, 1 & 2) of **Advanced Driver Assistance Systems (ADAS)** can be game changers more for developing countries like India than for the west. This technology will break the vicious cycle of High Road Crash, Missing Safety Culture and Inadequate enforcement and create a virtuous cycle of Alert, Assist, Save and Learn for every road user and avoid millions of crash situations on an hourly basis.

The learning from this assistance will not be limited to the moment and to the drivers alone, but will further fuel design changes and safe interventions in vehicles and infrastructure on a large scale and will enable a quick turnaround towards a sustainable and safe road infrastructure. These ADAS systems generate millions of scientific data with various parameters from every road user.

The scientists can use this data insights to find root causes of a potential crash even if it has never happened (Near-misses of any potential Crash), and use it not only to alert and assist the drivers, but come up with fail safe interventions in infrastructure and vehicles. In today's technology paradigm, data is everything. Data insights are better policy directors than only having expert humans on the design table and ADAS builds that data for technology professionals to save Lives on the roads.

This new regime of 'Alert & Assist' can promise saving lives on the roads in a short time, compared to the current regime of world-class regulations with inadequate enforcements (both voluntary or forced). This can be achieved by fusion of Telecommunication with informatics, capitalising on the quantum leap the scientists have taken in the domain of Data Science, Artificial Intelligence and Machine Learning. Technology driven Active safety measures such as vehicle alerts, remote prognostics, through the connectivity of an advanced driver assistance system have proven to improve road safety by helping the driver manage or avoid emergency situations proactively.

Depending on cost continuum, an ADAS system can have Cameras, Radar/LIDAR, Ultrasonic Sensors with connected ecosystems and fuse all data to create insights in real time for alert, assistance and in higher level even automatic actions of brake and accelerator can be done, nearing to autonomous driving. The role of ADAS is to prevent deaths and injuries by reducing the number of accidents and the serious impact of those that cannot be avoided. Some of the safety critical alerts can be Pedestrian detection/avoidance, Lane departure warning/correction, Traffic Sign recognition, Automatic Emergency Braking, Blind Spot Detection, fatigue alert, Drowsiness Detection alarm etc.

On an elementary level, even a mobile application which can do elementary alert and assist can be of great help. These systems can build even Road Users Behaviour history and can be used for their own training or can be used as a Safe Driving Score to be incentivised by various service providers, including insurance companies, to win them for respecting the Road. This will trigger to build the missing Trust among Drivers/Road Users with Road System to support the Road rules, as they will have multiple gratifications to drive safely. Situation will be completely different from today, where 80K-90K traffic cops across the country are struggling to catch billions of violations. With this technology,

It will be a win-win for all stakeholders. And so we will see India free from all avoidable road deaths through technology for a purpose.

Seminar on Indian standard IS 18149: 2023 on 'Transportation of Dangerous Goods - Guidelines'

Service Sector Department of BIS conducted a Seminar on Indian standard IS 18149 : 2023 on 'Transportation of Dangerous Goods- Guidelines' in hybrid mode on 14 June 2023.

Objective of Seminar:

1. To create awareness about importance of standardization activities in Transportation of Dangerous Goods.
2. To understand the risk involved and importance of safety including labelling provisions and packaging of Dangerous Goods.
3. To provide an overview of Indian Standard, IS 18149:2023 – 'Transportation of Dangerous Goods – Guidelines'.
4. To identify organizations/individuals having expertise in these services who can contribute in formulation of future standards related to Dangerous Goods.

Shri S.K. Kanojia, Head (SSD) welcomed DDG (Standardization-II), the speakers and the delegates participating in the event including Service Providers, State Road Transport Authorities, and PSU's participating in the Seminar. He also shared the objectives of the Seminar with the participants.

Shri Sanjay Pant, DDG Standardization-II, inaugurated the seminar and appraised the speakers and the participants about importance of IS 18149:2023 and its effective implementation to ensure safety and quality services in transporting dangerous goods. He also thanked speakers for participating in the seminar and service sector department for organizing the event.

The seminar covered various aspects like present scenario of Transporting Dangerous Goods, Importance of Standardization in Transportation of Dangerous Goods, Importance of Safety and Role of DGSA, Marking and Labeling Provisions, Current Scenario of Petroleum Products, Packing and Stowage of Dangerous Goods and Overview on Salient Features of Indian Standard, IS 18149:2023 Transportation of Dangerous Goods - Guidelines.

The eminent speakers from Zuvan International Transport Ltd, IIT Delhi, Center for Logistics Leadership in Business (CLLB) – Malaysia, Chartered Institute of Logisitcs and Transport (CILT), Indian Oil Corporation Ltd (IOCL), Member Secretary of TED 24 - Transport Packages, Packaging Codes and Pallets Sectional Committee Sectional Committee and Member Secretary of Transport Services Sectional Committee, SSD 01 have given the presentations focussing on the objectives of the seminar.

The Seminar was attended by delegates from the government, Regulators, Service Providers, RTO's, State Road Transport Authorities, PSU's, individuals, and other stakeholders including the members of the relevant Sectional Committees of BIS. Around 30 physical and 300 virtual participants attended the event and appreciated the initiative taken by BIS for organizing this event.

Outcome/Way forward:

During the seminar, the participants were provided with comprehensive information about the published Indian standard, IS 18149:2023 Transportation of Dangerous Goods - Guidelines. In addition to this, the eminent domain area experts and members of Transport Services Sectional Committee, SSD 01, participated as speaker and shared their views and experiences on important aspects like present scenario of Transporting Dangerous Goods, Importance of Standardization in Transportation of Dangerous Goods, Importance of Safety and Role of DGSA, Marking and labeling Provisions, Current Scenario of Petroleum Products, Packing and Stowage of Dangerous Goods. The delegates interacted with the experts to resolve their doubts and queries in the event and appreciated BIS for organizing this event to help the stakeholders to update their knowledge about the subject and newly published Indian Standard IS 18149:2023.

The standard will provide guidelines to ensure the safety of the participants and stakeholders including vehicle owner's/transport agencies, contractors, consignors, consignees, loaders, unloaders, driver and vehicle crew carrying dangerous goods/substances.

Seminar on IS 18149: 2023 on 'Transportation of Dangerous Goods - Guidelines' at Indian Oil Bhavan

CILT India in association with BIS (Bureau of Indian Standards) has organised a workshop exclusively for IOCL (Indian Oil Corporation Ltd.) employees on "IS 18149:2023 Transportation of Dangerous Goods – Guidelines", at Indian Oil Bhawan, Yusuf Sarai, New Delhi on 15 June 2023. The workshop was represented by BIS & CILT India team involved in framing of IS 18149:2023 Standards, in addition to senior level IOCL officials. This initiative was very well appreciated by Mr. Sujoy Choudhury, Director (P& BD), Indian Oil Corporation Ltd.

Sh. Sujoy Choudhury Director (P&BD), IOCL felicitating Sh. Sanjiv Garg, Secretary General - CILT India

Workshop at Indian Oil Bhavan, New Delhi

Glimpse of Seminar at Indian Oil Bhavan

A Chain is only as strong as its weakest link

Sujay Goswami
Chartered Member, CILT - INDIA

Introduction

Threats to cyber security aim to exploit a company's weakest areas. An organisation's susceptibility to cyber risks in the supply chain is increasingly turning out to be their weakest point as they try to defend themselves and concentrate on bolstering their own cyber security. Organisations have been targeted through less-secure places in their supply chains numerous times in recent history, causing considerable financial and reputational harm. Developing a strong capacity to manage supply chain cyber risk and strengthen organisational cyber resilience involves several key steps. One may increase their organisation's cyber resilience by following these steps, which will assist them in identifying supply chain entities and supplier management proce-dures, assessing the cyber threat landscape to identify which suppliers are most crucial and in establishing systems to efficiently manage supply chain risk.

Risks associated with cyber security in the supply chain must be coordinated across the entire firm.

Supply Chain Risk Management (SCRM) is a collection of procedures used by businesses to detect, evaluate, and control risks in their supply chains.

ICT-SCRM: Supply Chain Risk Management is a crucial component of an organization's SCRM strategy that covers the risks posed by ICT assets and services, as well as their manufacturers, suppliers, and other supply-chain partners.

Cybersecurity in the supply chain is managed through the process of discovering, evaluating, and controlling both technology and human risk factors.

Cyber security risks in supply chains :

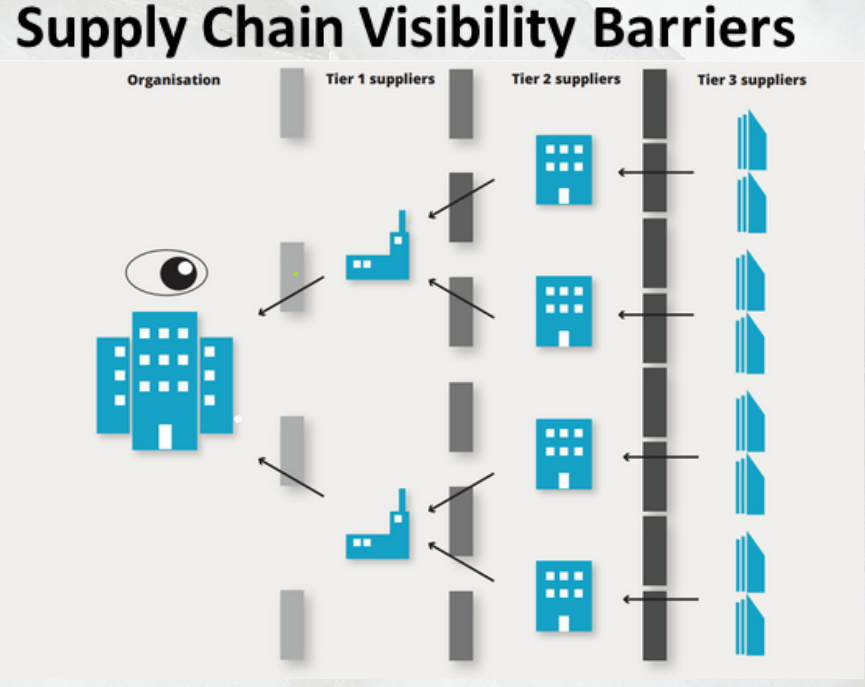
Digital interactions with supply chain organisations can happen from any element of a business. Thus, they are not just restricted to those who offer information and communications technology (ICT) services or infrastructure. Cyber threats to the supply chain are thus an enterprise-wide issue that calls for a business-led response to handle the very real dangers they provide.

Consider that Company A decides to launch a digital transformation project as an example of this idea. To help with the shift, its operation department works with a tier 1 supplier as a third-arty service provider. This service provider makes use of a tier 2 supplier's cloudbased customer platform, which is provided as a service.

All of Company A's customer information is transferred onto this cloud service as part of the transformation. Unfortunately, the service provider (tier 1) neglects to protect the administrative accounts they use to set up the cloud platform (tier 2) and a hostile actor gains access using their credentials and extracts files containing Company A's customer information.

"Cybersecurity is never just a technology problem; it's a problem of people, processes and knowledge."

The service provider (tier 1) is unaware that their administrative accounts have been compromised until Company A's operation department is approached by a malicious cyber actor who demands a ransom to remove the customer data or they would publicly reveal it. In recent years, the growing reliance of businesses on supplier-managed cloud services in place of conventional on-premises enterprise software has underlined the need for companies to get visibility into the direct and indirect suppliers present in their supply chains. In order to handle services or equipment, some vendors demand privileged system access. Cloud services frequently require additional apps and services to deploy, manage, and secure them, introducing new supply chain suppliers.



Manufacturing processes and services that are sophisticated and geographically interconnected have also resulted in increasingly complex hardware supply chains for example, the production of a single hardware item may involve dozens of component manufacturers and subcontractors, some of which have several degrees of separation from the primary manufacturer.

Targeted and opportunistic attacks

Complex supply chains can result in large attack surfaces, providing chances for malevolent cyber actors. If a huge organisation with robust cyber defences is an attacker's main target, they might search for another access point. This might occur through a service provider with access to the target's systems which is poorly protected. Infiltrating the service provider's weaker sections could successfully allow the attacker to bypass the main target's strong defences and wreak substantial harm. While targeted assaults frequently necessitate extensive planning, many other attacks are opportunistic and result in attackers conducting thorough audits of several businesses to find security flaws.

In this climate, firms must retain a good grasp of the cyber security risks in their supply chain and build an effective approach to identify, assess, and manage these risks.

"Your investment in cyber security may not protect you if attackers can breach your supply chain through a weak link."

Identify your Suppliers

Traditionally, suppliers who posed cyber security issues would be examined by an organization's IT department. However, many services now have information system components that can present cyber security threats and these services go beyond the jurisdiction of the IT team. Because of the fast global use of internet of things (IoT) devices and connected systems, plant machinery, equipment, building systems, and physical security systems are frequently internet-connected and may even enable remote access as part of maintenance and service schedules.

Furthermore, with free versions and credit card-based billing, cloud-based service consumption has gotten simpler. This allows any part of the organisation to employ new cloud services without seeking technical or budgetary authorisation. Before they are detected by the rest of the organisation, these services can swiftly become embedded in operational procedures. A strategy for completely identifying your suppliers must therefore consider the entire organisation and should go beyond ICT services and office-based solutions.

Recognise your supplier management processes.

Business processes are typically in place to develop new suppliers, manage relationships with existing suppliers, and offer visibility of purchasing choices inside the organisation. It is critical to make these processes accessible and to include cyber security teams so that they can effectively evaluate new vendors or examine substantial changes in existing suppliers.

The data acquired during the discovery phase must be organised into a governance model that clearly defines the roles and responsibilities for supplier management. Identifying the financial and technical authority for engaging new suppliers, as well as creating ownership for continuous supplier management, are all part of this process. It is critical that each supplier has a clearly defined owner inside the firm. Being responsible, Accountable, Supporting, Consulted, and Informed in each activity is a good way to capture the key accountabilities and responsibilities, and this should include the role that cyber security teams play in supporting supplier management and staying informed of any additions or changes in suppliers.

Understand your suppliers' security measures

It's crucial to keep an eye on your suppliers' security postures and make sure they understand your standards, especially if those suppliers are crucial to your business. Your contracts should expressly state and include any expectations you may have for the management and security of your assets and information by third parties, as well as for the protection and assurance levels necessary for the delivery of goods and services.

Understand your suppliers' and contractors' suppliers and contractors. Learn about your suppliers' current security arrangements, including the length of time they have been in place. Determine whether you are willing to allow your suppliers to utilise their own subcontractors to meet your contractual commitments. Understand what access your suppliers provide to their own subcontractors and how it affects your information and assets.

Establish and clearly communicate your vendors' basic security needs. These criteria may include personnel and physical security in addition to information security. For example, you may demand suppliers to do pre-employment checks to a given quality in order to verify that their employees are trustworthy and to decrease the danger of insider compromise. Think about the security consequences for your firm if a critical supplier changes ownership or major shareholding, or if it merges. If this has an influence on their appropriateness, a security evaluation of that provider may be required.

Ensure that security issues are included in your contractual processes. This means that supply chain and contract managers should collaborate closely with senior information security professionals at the tender development stage to establish your security needs and ask prospective suppliers to produce evidence that they can meet those criteria.

Consider the consequences if a supplier is unable to meet your requirements any longer, or if the contract must be terminated: do you have contract cancellation provisions? Do you have any requirements from that supplier about the return or disposal of your assets and information?

Identify your critical services and assets

You must establish a clear understanding of which of the assets and services (including third-party services) your company utilises, are most essential to achieving your goals in order to manage the cyber risks in your supply chain successfully. When you are aware of what needs protection the most, you can start setting priorities and allocating your scarce resources accordingly. Applying a technique known as a criticality analysis, which assesses the potential harm to your organisation caused by failures, outages, or other interruptions to each of the assets and services you use, is one way to accomplish this. Instead of being a one-time event that only happens during the procurement phase, evaluating criticality should be a continual activity.

Partner with vendors to improve cyber security

Strong, cooperative security relationships with your major suppliers can enhance information flow and help with coordination in the event of a security issue. You and your suppliers should share a same concern about supply chain risk. It's crucial that you pay attention to your suppliers' input, try to allay any worries they may have about your security measures, and, whenever you can, try to give them the assistance or information they need. Just as you might ask your suppliers to do security audits, you should be equally eager to comply with their requests and be as transparent as you can when sharing information about any potentially damaging security issues you could be addressing at the time. Giving your suppliers information about security incidents you've had may enable them to defend against assaults on their own systems.

Recognise the supply chain's cyber security concerns

You may start assessing the risks your supply chain might provide to each of your assets and services once you've decided which ones are the most important. Utilising cloud services, for instance, may increase your vulnerability to denial-of-service assaults on online systems, and using remote management services may raise the risk of compromised systems. Employees who work in supply chain management should be well-aware of cyber dangers and stay current on new security advances. In the past few years, there has been a steady rise in attacks on ICT infrastructure in supply chains. A new Accenture analysis claims that weak supply chain links now account for 50% of all security breaches. The threat is only going to increase as businesses shift their systems more frequently into cloud settings and as more employees operate from remote places. Therefore, it's crucial for businesses to gain a thorough awareness of the possible hazards posed by the suppliers, service providers, and consumers in their supply chains.

Agencies SHOULD continuously assess supply chain risks and alter mitigations and controls as necessary.

Examine and review supplier security in a systematic manner

While traditional procurement timelines might have included assessments of a supplier's cyber security procedures near the end of the sourcing process, in today's business environment it's critical that cyber security aspects be addressed by the involved teams across the organisation at an early stage. Although not a complete list, the practices listed below offer a helpful set of guidelines for supplier selection and risk management.

Ensure that all necessary parties have the chance to offer their opinions. Make sure to put all of your security demands in writing. When creating RFPs or contracts, be sure to specify your minimal security standards for providers. Your demands should be commensurate with the contract's level of related risk. Include clauses that allow you to audit the supplier's security as needed and that requires the provider to send you frequent security performance reports.

Think about how allowing suppliers to utilise their own subcontractors will affect security. Create a system for evaluating the cyber risk of potential suppliers. Due diligence on suppliers will aid in early detection of potential problems. Every firm has a distinct set of security requirements and a different level of risk tolerance, but any supplier may be assessed using a set of common indications of cyber security risk.

Discover the current controls landscape

It is feasible to identify the controls in place to help identify, protect, detect, respond, and recover from these risks if you are aware of the important assets of your company, the threats you face, and the potential effects that supplier relationships may have on threat levels. Maintaining a thorough awareness of any compliance obligations should also be part of this. Regulatory and compliance requirements must be precisely recognised and included in the controls framework, especially for foreign suppliers.

How to manage

Create a programme. Organisations need to create a programme for handling supply chain cyber threats that is suitable for their size, manpower, and other resources. Supply chain risk management (SCRM) initiatives were previously thought to be only possible for the larger businesses, but rising cyber dangers mean that all corporations now need to have a strategy in place. Smaller firms can nevertheless assign workers to execute supply chain cyber risk management tasks as part of their role, even if large enterprises may be able to set up a specialised team for this reason. A cyber risk management programme should have clearly defined roles and responsibilities.

launching the programme

The security state and practises of your supplier network should be evaluated and continuously reviewed as part of the supply chain cyber risk management strategy. The amount of detail you are able to reach relies on the number of suppliers you are managing; if this number is very high, you may need to devote the majority of your time and energy to a few suppliers who you have determined to be the most important to your company.

Establish a culture of cyber risk awareness throughout the supply chain

Because the cyber threat environment is continuously changing and staff members need to be informed, education initiatives should be ongoing. With a high culture of cyber security awareness, a business is less likely to suffer significant problems from assaults that rely on lax security procedures, such as email phishing-related data breaches. The key supply chain workers will probably benefit from this culture by being better able to evaluate suppliers and spot potential dangers in the supply chain.

Make sure there is continuing observation and improvement

The following recommendations can help to continuously strengthen the security of your supply chain:

- Plan regular evaluations of your own essential assets and systems. Any time a status changes, update your registers of systems and assets.
- Maintain an up-to-date list of your vendors and purchasing choices. Make sure to update the register if something changes.
- Continually assess each supplier's criticality status.
- Where feasible, demand security information from the subcontractors of your main suppliers.
- Establish a routine for reviewing your suppliers' security performance on a regular basis, and keep track of any status changes or departures from their contractual commitments. In a perfect world, a group of stakeholders from your organisation would monitor these assessments.
- Promote the exchange of security-related information with your suppliers and treat supply chain security as a shared concern.
- Keep in constant contact with your suppliers about security matters, such as new cyber hazards. Use technological tools that simplify collaboration without increasing risk.
- Be receptive to suggestions from providers on your own security. Be prepared to answer any questions they may have concerning your security measures

CONCLUSION:

It may seem like a difficult and complicated task to address supply chain cyber security risks, but organisations that adopt a methodical and cooperative approach will find themselves well-positioned to reduce risks, quickly adjust to changes in the business environment, and act quickly in the event of an incident.

One may determine which of their organization's information systems and assets needs the most resources devoted to their security against supply chain risks by evaluating the criticality of those systems and assets. The parts of their supply chain that require the greatest attention will become clear when you can identify which suppliers provide your most important resources and adjustments.

One can get crucial data to back up their choices by assessing the security posture of potential vendors during the procurement provide one should have a written agreement outlining their security standards and continuing expectations. It will be easier to ensure that security information is shared both ways by maintaining open, cooperative relationships with vendors. Your company is in a great position to minimise risks and allocate your cyber security resources to the most crucial areas by actively monitoring the cyber threat landscape, analysing threats against your own systems, assets, and processes, and updating controls as appropriate..

The process will be formalised and embedded in a structured way by establishing a programme for controlling supply chain cyber security risk and getting support from senior executives and board members. All impacted areas should be included in the risk management process, and the programme should be linked into the organization's larger risk assessment procedures. Recognise that human factors—rather than just technology—can frequently be what makes cyber mishaps possible.

Establish a strong culture of cyber security awareness by providing your workers, especially those in key roles, with high-quality training and direction. Make sure that the risk tolerances for your company are clear and easily accessible.

Finally, by keeping up a continuous supply chain monitoring programme, you can make sure that your records are up-to-date "snapshots in time" rather than static records that can't be trusted to give current risk information or guide future procurement decisions. Your security measures will be effectively strengthened with ongoing, small adjustments.

New Corporate Member (April – June 2023)

Name & Designation	Membership
ब्रेथवेट एंड कंपनी लिमिटेड BRAITHWAITE & CO. LTD. (भारत सरकार का उपक्रम) / (A Govt. of India Undertaking) (मिनीरत्न श्रेणी-1 कंपनी)/ (A MINIRATNA Category-1 Company) रेल मंत्रालय / Ministry Of Railways	OM/59/2023

New Individual Life Members (April-June 2023)

S.No.	Name & Designation	Membership
1	Shri Rajesh Prakash Sheth, CMILT National Manager, Marketing & Biz Development Expressway Cargo Movers Pvt Ltd	LM-1297
2	Shri S.R. Krishnan, CMILT Head Logistics, Alkaram Foodstuff Trading LLC-Dubai	LM-1298
3	Shri Parag Kochhar, CMILT Business Head, DP World - Mundra	LM-1299
4	Shri Akshyat Bhatia, CMILT Business Head, Maersk Line India Private Ltd, Gurugram	LM-1300
5	Shri Kabir Kewalramani, CMILT Exim Executive – Intern	LM-1301
6	Shri Kevin Boniface Coutinho, CMILT Nautical Faculty, Anglo-Eastern Maritime Training Centre	LM-1302
7	Shri Murlidhar Venkata Satya Inavolu, CMILT Founder & President, MVS Consultancy	LM-1303
8	Prof. Jitesh Thakkar, CMILT Professor, Gati Shakti Vishwavidyalaya	LM-1304
9	Prof. Manoj Choudhary, CMILT Vice Chancellor, Gati Shakti Vishwavidyalaya	LM-1305

S.No.	Name & Designation	Membership
10	Shri Gyan Abhishek, CMILT Head, Rail Operations, Maersk Line India Private Ltd.	LM-1306
11	Dr. Chandi Prasad Nanda, CMILT Professor and Dean Administration, Gati Shakti Vishwavidyalaya	LM-1307
12	Dr. Venkateswarlu Chintala, CMILT Programme Director, Engineering & Associate Prof Gati Shakti Vishwavidyalaya	LM-1308
13	Shri Aditya Kushwaha CMILT Solution Sales Manager, Maersk Line India Pvt Ltd	LM-1309
14	Shri Bino Issac Mathew, CMILT Deputy General Manager, Adani Logistics Ltd	LM-1310
15	Shri Pankaj Krishandev Mehta, CMILT Managing Director, Carrier Transicold India	LM-1311
16	Shahnwaz Akhtar, CMILT Procurement and Logistics Manager Tetra Tech for Trading and Contracting Co. Ltd.	LM-1312
17	Sunil Nandankar, CMILT Sr. Professor Materials Management, NAIR	LM-1313
18	Shri Ravi Pamnani, CMILT Associate Manager, Adani Logistics Ltd	LM-1314

The Chartered Institute of Logistics and Transport

Who We Are

The Chartered Institute of Logistics and Transport India is part of the leading, global professional body for those engaged in supply chain, logistics and transport – covering all sectors of the industry, namely air, land and sea, for both passenger and freight transportation.

Our primary objectives are to support our members in continuous professional development to future-proof their careers, as well as to work in close collaboration with the public and private sectors, Government agencies and the academia to develop opportunities and synergy for industry transformation and growth, underpinned by strategic thrusts in digitalisation and sustainability.

Contact Us

The Chartered Institute of Logistics and Transport

CILT –India, Headquarters, 3 Palam Marg,3 rd floor,
Vasant Vihar, New Delhi – 1100 057
Tel: +91-11-40809939
Email: info@ciltindia.in