"Practice of Professional Engineering" as defined in the Professional Engineers Act

"any act of planning, designing, composing, evaluating, advising, reporting, directing or supervising that requires the application of engineering principles and concerns the safeguarding of life, health, property, economic interests, the public welfare or the environment, or the managing of any such act"

CIE Scope of Practice

1. Planning and Design of Assured Communication Networks

By definition, assured communication networks include those supporting other critical infrastructures, as defined by the Government of Canada.[1] Any communications infrastructure whose failure, compromise, or unavailability can adversely affect society's well-being is critical, and must be secured against a broad spectrum of threats and failures.

The role of the CIE practitioner is concentrated at the systems level; i.e., it is concerned with the overall design of the network from the point of view of:

- *availability* (which encompasses performance) and reliability,
- *confidentiality* (protection against unauthorized access or exposure),
- *integrity* (protection against unauthorized modification/corruption, including "operations" security),
- privacy (restrictions on unauthorized disclosure),

and includes the design of secure operating and monitoring procedures.

It is not intended to encompass the configuration of network devices and interfaces (which is the purview of the network technician or technologist), nor is it intended to encompass the design of secure applications (which is the purview of the software analyst and/or designer). However, the CIE practitioner is expected to understand these works and take overall system responsibility for the work done.

CIE practitioners apply their engineering discipline – which includes comprehensive risk assessment and mitigation strategies – to develop and document requirements for network assurance and security, along with specifications and designs that will meet those requirements.

2. Implementation of Assured Communication Networks

As in most other engineering disciplines, there is a requirement for a licensed CIE practitioner to monitor, inspect/review, and provide oversight to the implementation of an assured network to

[1] Public Safety Canada, *National Strategy for Critical Infrastructure*, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf, 2009.

ensure that it is implemented in accordance with its designs. In some cases, issues will arise during implementation that may require the design to be revisited and possibly revised. Any such reviews and revisions cannot be left to persons less skilled than the designer without risking compromise of the network security. Thus, CIEs are expected to be involved in implementation of their designs, just as other engineers are. A CIE should "sign off" on the “as-built” implementation of an assured network as verification that it may be trusted.

3. Operational Oversight of Assured Communication Networks

Just as a certified aircraft must be operated in accordance with its Pilot Operating Handbook to be flown safely, so a secure network that has been properly designed and risk assessed must be operated in accordance with documented operating procedures to avoid failure or compromise.

The role of the CIE practitioner in operation of critical communications infrastructure is to provide the oversight necessary to ensure that its operation is in accordance with design limitations and secure practices, and to ensure that those practices are updated as and when required to reflect any changes in the design or configuration of the network.

This role includes ensuring that monitoring facilities are in place to detect any compromises of the network, and that appropriate corrective action is taken to address any threats detected.

It is not intended to encompass routine day-to-day operation and control of networks (which is the purview of network operators), or repair and configuration of network devices (which is the purview of network technicians and technologists).

Again, however, the CIE practitioner must understand the fundamental technologies and be able to run tests to assure that all implementation and maintenance work does not compromise the reliability and security of the network as originally designed.

4. Auditing and Risk Analysis of Network Infrastructure

As networks, network technology, and cyber-security threats are evolving rapidly, it will be necessary to evaluate existing network infrastructure on a regular basis to ensure that risks are properly identified and mitigated. Many existing networks were designed when technology was simpler and threats were fewer, without the end-to-end design undergoing formal risk analysis.

This scope of CIE practice emphasizes the critical engineering aspect of risk analysis in secure network design and operation. It also encompasses oversight of remedial analysis and contingency planning for corrective actions that may become necessary following a network failure or security breach.

5. Risk Analysis and Mitigation of Other Critical Infrastructure that is Dependent on Network Infrastructure

Since so much of society's critical infrastructure depends on network infrastructure, risk analysis and mitigation for infrastructures such as energy, finance, health care, public safety, and transportation will require knowledge of network infrastructure and its vulnerabilities. Communications infrastructure engineers will therefore be called upon to bring their specialized knowledge and skill to bear on designing, operating, and protecting other critical infrastructures.

CIE Body of Knowledge

Core Knowledge	Definition
Signals and systems	An understanding of the systems and their types, functions, and applications based on their input/output signals, input dependencies, the nature of their processing signals, and their certain characteristics such as leaner or non-linear systems. This also includes the perceptive knowledge of signals and their types and dependencies to time changes (discrete vs. continuous or analog vs. digital) and their functions and applications.
Transfer Theory	As Transfer theory is the main tool of classical control engineering, it is necessary for the CIE engineers to understand this function, which is the mathematical representation of the relationship between input and output of a system to be able to analyze the system's end to end behaviours
Digital Signal Processing	An understanding of the DSPs that are the key elements of the major industry CIE applications such as audio signal processing, audio compression, digital image processing, video compression, speech processing, speech recognition, digital communications, RADAR, SONAR, sensor array processing, spectral estimation, statistical signal processing. seismology, and biomedicine.
Real-time Systems	As real time systems are considered the major parts of the mission critical applications that are normally priority driven (QoS), a detail understanding of the real time systems, their dependencies to time, and their types of hard-real time and soft-real time systems are mandatory for CIE engineers.
Reliability	An understanding of the system reliability and differentiating it from other system characteristics such as high-performance or fast response time, and being able to address the major reliability issues as follows: 1. The system cannot safely be shut down for repair, or it is too inaccessible to repair. 2. The system must be kept running for safety reasons. 3. The system will lose large amounts of money when shut down.
Fault Tolerance	A general knowledge of Fault Tolerance that is the ability of a system to respond gracefully to an unexpected hardware or software failure. There

Core Knowledge	Definition
	are many levels of fault tolerance, the lowest being the ability to continue operation in the event of a power failure. Many fault-tolerant systems mirror all operations -- that is, every operation is performed on two or more duplicate systems, so if one fails the other can take over.
Communication	An understanding of the core elements of modern networking, including the knowledge of both legacy and evolving networking systems. Insight into the characteristics of networking which are not necessarily observable or obvious but are essential to CIE.
Communication/ Information Theory – Stochastic, Emergent and Non-deterministic systems	As networks grow and are interconnected they become extremely complex. This complexity has been compared to that of living biological organisms. This knowledge is required to appreciate the caution with which networks must be designed or changed, and to fully appreciate the risks inherent in CIE.
Digital Communication	An understanding of legacy, layer 2 analogue systems versus digital communications. And understanding of the recent evolution of layer 2 digital communications from older, point t point, time division multiplexing (TDM) technology to services such as Ethernet/MPLS and IP-based networking.
Telecommunication Protocols	Layer 3 and above protocols, with an emphasis of the IETF protocols including lower levels IP and higher level TCP, UDP and ICMP communications. Understanding of the distinction between unicast and multicast services. Understanding of basic elements of integrity and error correction, quality of service, flags, payloads and other variables and services which may be managed by protocols (as opposed to applications).
Wireless Communication	Layer 2 wireless protocols differ from layer 2 fixed line (fibre, copper) and impact speed and range in ways not seen with fixed line systems where these features are typically a function of the network element rather than the layer 2 protocol. Similarly, wireless network possess specific requirement associated with signal to noise, elevation and azimuth of antennae, Fresnel zones, attenuation and signal reflection, refraction.
Networks	An understanding of the relationships among networks, information assets and end-point devices; how to they relate and impact to one another in a logical manner and what are the intellectual tools and methods used to understand and define networks for the purposes of

Core Knowledge	Definition
	CIE.
Convergence	Convergence is the phenomena of information assets which were formally isolated on standalone networks moving to a common networking medium, most typically Internet protocols. Convergence is also the phenomena of fixed-line and wireless networking becoming transparent if not irrelevant to the application and user, whatever medium is most appropriate and available will be automatically used.
Computer Communications and Network Architecture	The logical design of networks to support the assurance properties of the assets they are intended to support. This includes but is not limited to techniques such as network zoning and requirements analysis such as capacity assessment and planning, redundancy planning and security architecture.
Distributed Computing	An understanding of who distributed and virtualized computing platforms function and how hardware and software services can be dispersed around the world in a manner completed transparent to application owners, administrators and users. Distributed computing imports heightened assurance requirements on networks, which in effect become part of the operating system – not just a means to move data from independent system to independent system.
Internet Protocols Communication	Internet protocols form the dense centre of networking technology, with (transparent) physical mediums and associated datalink protocols on one end, and application-specific protocols on the other. From layer 3 to layer 5 internet protocols dominate the moderate network totally and are fundamental elements of CIE.
Testing and Diagnostics	The centricity of networking to modern IT means that faults can appear to be network-related but in reality be application and device related; conversely, applications and device faults can have their roots in the network. In order to support high assurance and probably highly converged network, the tracing, tracking, determination or mooting of network faults is a functional imperative for a CIE engineer.
Risk management	An understanding of the practice of identifying possible threats to networks and network elements and the endpoints they support, judging the likelihood and potential severity of these threats and determining appropriate safeguards.
CIA of data in transit	Comprehending and assessing the requirements for confidentiality, integrity and availability of data on the network and as it passes through the network elements, including the borders between networks.

Core Knowledge	Definition
Threat Assessment and Mitigation	The ability to identify possible threats to networks whether they are natural or man-made, deliberate or accidental. The ability to judge the likelihood that a given threat will occur using quantitative and qualitative assessment techniques. The ability to judge the severity of impact associated with a given threat using quantitative and qualitative assessment techniques. Understanding how given controls and safeguards may be applied individually or as layers to mitigate threats, and the performance and financial costs associated with the controls and safeguards and potential new risks they may introduce themselves.
Governance	An understanding that CI engineering must be conducted in accordance with the laws of the jurisdiction in which it is practiced, and that data is subject to the laws of the jurisdictions it not only resides within, but also subject to the laws of jurisdictions it travels through at the time of transit.
CIE Regulatory Environment	Telecommunications is highly regulated in all modern economies. Depending on the jurisdiction, prices and services may be determined more or less by the regulator. Some services will be entirely defined in regulations while others entirely forborne. CIE regulations have a significant impact on the feasibility of any large-scale CIE undertaking, where networks connect outside a single, physical premise. A foundation understanding of CIE regulation avoids erroneous and costly designs assumptions or oversights.
Privacy	Privacy is about the appropriate management of, personally identifiable information. In the case of CI engineering this means the management of personally identifiable information as it move through the network. Privacy is a potent form of regulatory requirement in any western economy, usually associated with substantial sanctions for breech. Additionally, privacy requirements are often a business-language expression of security properties: confidentiality, integrity and availability. An understanding of privacy aids the prioritization and specification of a variety of design features such as zoning, monitoring, routing, encryption and network element management practices.
Sovereignty	Modern networks frequency route information in manners which can be transparent to users and even the original CIE designers. As data enters and traverses new networks it can become subject to shifting legal regimes, which can impact not only the assurance of the data but of the network path itself. Sovereignty issues are also fundamental consideration in the design of computing clouds, which in turn are entirely dependent on networks.