Conference abstracts

Morning session:

Session A1- Prof. Yizhaq Minchuk- Competition Strategy

(A1-01)

Dr. Doron Klunover
Shamoon College of Engineering (SCE), Beer Sheva, Israel

The Bankruptcy Problem: A Contest Approach

A contest is considered in which multiple players compete over shares of a prize, where a player's preferred share can be less than one. This setting can be viewed as a strategic effort-based approach to analyzing the bankruptcy problem. Specifically, instead of using a division rule to map players' claims onto shares, a lottery contest success function analogous to the proportional division rule is used to map effort onto shares. It is shown that under symmetry equilibrium aggregate effort often exceeds the value of the prize, while under asymmetry the equilibrium distribution of shares is analogous to a progressive sharing rule. Applications are discussed.

(A1-02)

Prof. Yizhaq Minchuk
Arieh Gavious, Hadas Tamam Ben Avrham
Shamoon College of Engineering (SCE), Beer Sheva, Israel
Ono Academic College

Attacker Sophistication and Cybersecurity Investment: A Multi-Defender Contest Model

Cyberattacks have become a defining challenge for modern economies, exposing systemic vulnerabilities across critical infrastructures, financial institutions, and public services. This paper develops a novel game-theoretic framework to analyze the strategic interaction between a single attacker and multiple defenders, distinguishing between non-sophisticated attacker (NSA), who select targets randomly, and sophisticated attacker (SA), who condition targeting based on defenders' relative defense levels. The model captures key dynamics such as risk dilution, overinvestment, and asymmetric exposure among defenders. We extend the analysis to incorporate three distinct policy interventions: reimbursement schemes, direct authorities investment in defence infrastructure, and mandated defenders efforts. Our results show that reimbursement mitigates underinvestment in NSA environments but is less effective under SA scenario; direct authority investment provides baseline protection but risks crowding out private initiative; and mandated effort can maximize social welfare, though at the cost of flexibility and potential overregulation. The findings highlight the importance of tailoring interventions based on attacker's sophistication. By bridging theoretical modeling with real-world cases such as WannaCry, the Bangladesh Bank heist, and the Colonial Pipeline ransomware attack, this study contributes to both the academic literature on cybersecurity economics and the policy debate on optimal governance of digital risk.

(A1-03)

Dr. Dvir Ross
Shamoon College of Engineering (SCE), Beer Sheva, Israel and Shenkar Colleges

Modeling Basketball Shooting Patterns Using Markov Chains: A Longitudinal Analysis of the Hot Hand Phenomenon

The "hot hand" phenomenon, where a player's success in consecutive shots is believed to indicate a streak of heightened performance, has been a subject of debate in sports analytics. In this study, we model basketball shot outcomes from the 2003-2004 to 2023-2024 NBA seasons as first-order and second-order Markov chains, capturing dependencies between successive shots. To account for game dynamics, we introduce resets to the Markov process at halftime and similar intervals. Dependency testing is conducted to evaluate the statistical significance of shooting streaks, revealing that the hot hand effect is not a significant phenomenon across this extensive dataset. By combining rigorous statistical modeling with longitudinal data analysis, this research challenges conventional beliefs about streak-based performance and provides a nuanced understanding of player behavior over two decades of professional basketball.

(A1-04)

Dr Dvir Ross
Nehoray Sade, Aviv Asraf
Shamoon College of Engineering (SCE), Beer Sheva, Israel

Data-Driven Risk-Adjusted Performance Analysis A Structural Complement to Classical Risk-Adjusted Ratios

This study asks when a structural price-path signal adds value beyond classical risk-adjusted ratios such as Sharpe, Sortino, Treynor, Calmar, and Information. Using daily adjusted-close data from 100 ETFs across 9 market eras and 180 train/test configurations, the paper proposes an exponential-fit score based on trend stability and deviation from the fitted path. The empirical results show a clear regime dependence: the proposed score is strongest in reversals and choppy markets ,while the classical ratios perform better in persistent trending regimes. Interpreted through a sign-based forecasting framework, the new score behaves like a mean-reversion signal, whereas the classical ratio family behaves more like momentum. The main contribution is not a universally superior metric, but a regime-aware complement to standard risk-adjusted performance analysis.

Session B1- Dr. Elroi Hadad- Data application in Economics and Finance

(B1-01)

Prof. Baruch Keren
Yossi Hadad
Shamoon College of Engineering (SCE), Beer Sheva, Israel

Computational Theory & Optimization

A Two-Stage Heuristic for Minimizing Machines and Operators in Cyclic Production Scheduling

This study introduces a two-stage heuristic algorithm for minimizing the number of machines and operators in cyclic production environments with multiple product types. The problem is formulated as a Bin Packing Problem (BPP), with the first stage allocating products to machines and the second assigning machines to operators under non-overlapping setup constraints. Each machine's schedule is modeled as a circular (donut-shaped) timeline to reflect cyclicality. Though BPP is NP-hard, the proposed heuristic provides near-optimal solutions and allows estimation of the optimality gap using lower bounds. Validation using real data from a plant producing 17 products showed notable reductions in required resources and operational costs. The model enhances scheduling efficiency and is applicable beyond manufacturing.

(B1-02)

Dr. Dima Alberg
Dr. Elroi Hadad
Shamoon College of Engineering (SCE), Beer Sheva, Israel

Tracking the Unseen: AI-Driven Dashboards for Real-Time Detection of Calendar Anomalies in Cryptocurrency Markets

This study introduces a novel AI-powered Business Intelligence Dashboard System (AIBIDS) designed to detect and visualize calendar-based anomalies in cryptocurrency returns. Focusing on Bitcoin as a case study, the system integrates unsupervised machine learning algorithms to identify periods of abnormal market behavior across multiple temporal resolutions. The proposed system leverages a star-schema OLAP data warehouse, enabling real-time anomaly detection, dynamic visualization, and drill-down exploration of market irregularities. Empirical results confirm the presence of pronounced calendar effects in Bitcoin returns, such as heightened anomalies during Q1 and Q4, and reveal model-specific sensitivities to local versus global volatility. Our novel platform offers a practical, scalable innovation for investors, analysts, and regulators seeking to monitor cryptocurrency markets more effectively, and contributes to the emerging FinTech literature on AI-driven anomaly detection and behavioral market dynamics.

Keywords: bitcoin; anomaly detection; autoencoder, AI models; Generative AI, Learning; Business Intelligence System

(B1-03)

Prof. Arik Sadeh
Osher Yosefian
HIT Holon Institute of Technology

Pricing and Quality Using a Data-Driven Approach

Traditionally, quality is defined by subjective expert opinions, consumer surveys, or simplistic engineering metrics. This study presents a comprehensive, step-by-step framework for developing a purely data-driven, objective, and quantitative Quality Index. The core philosophy is to let the market itself define quality. By analyzing historical transaction data, we can infer the latent characteristics and attributes that the market collectively values and is willing to pay a premium for. This is achieved by employing a machine learning technique to model the drivers of commercial success. The quality index in this study is based on cost, profit margins, and market price, as well as automotive-industry-relevant components such as Car Age, Year Quality Factor, and Manufacturer Reliability Score .

The study examines 60,000 observations of car sales by three automotive manufacturers over the last seven years. The Gradient Boosting Regressor, as an ML model, helped obtain a quality index for each car. This will be used to further optimize product pricing based on their quality and relevant inventory levels.

This empirically derived quality index serves for constructing an economically sound Optimal Pricing Model. We will delve into the tenets of Consumer Choice Theory, formulate a Random Utility Model, and derive a profit-maximization problem that allows a firm to strategically set prices based on a deep understanding of how consumers value both price and quality. The main goal is to bridge the gap between raw data and strategic, profit-maximizing decisions.

(B1-04)

Dr. Adi Katz
Shamoon College of Engineering (SCE), Ashdod, Israel
Yael Brender-Ilan
Ariel University, Department of Economics and Business Administration

The Serious Business of Humor: Insights into Digital Managerial Communication

As organizations increasingly rely on computer-mediated communication (CMC) to coordinate work, managers often use humor to make digital messages more engaging and persuasive. Yet research on managerial humor has produced inconsistent findings, suggesting that its effectiveness depends on context and the psychological processes it activates.

This presentation synthesizes findings from three experimental studies examining humor in managerial digital communication. The first study investigated humorous versus non-humorous managerial microcopy and found that humor can reduce motivation, perceived ability, and willingness to act, while highlighting the important role of employees' perceived task capability. The second study examined mandatory managerial requests under different task demands. The findings showed that humor increased compliance intentions, but through different mechanisms depending on task difficulty: by enhancing motivation for easy tasks and perceived ability for difficult tasks. The third study extended this work to visual managerial communication by examining humorous and non-humorous images embedded in managerial emails. While images improved task evaluations by reducing perceived effort and time demands, humorous images primarily increased amusement and affective engagement, without necessarily increasing intention to perform the requested task.

Taken together, the findings demonstrate that humor in digital managerial communication is neither uniformly beneficial nor detrimental. Rather, its effects depend on task characteristics, communication format, and the cognitive and affective pathways through which recipients process managerial messages. The presentation discusses implications for organizational communication, technology-mediated management, and the design of AI-assisted workplace messaging.

Session C1- Dr. Aviad Elyashar- Cyber Security

(C1-01)

Dr. Jonathan Cohen
Faculty of Computer and Information Science Ben Gurion University of the Negev

Stealthy False Data Injection Attack Detection in Power Systems

False Data Injection Attacks (FDIAs) pose serious threats to modern power systems by blending within normal operations, causing severe damage to the grid, underscoring the importance of effective countermeasures to reinforce cybersecurity resilience in evolving smart grids amid diverse operational conditions. We propose a carefully crafted, stealthy yet impactful FDIA scheme against power system state estimation and a corresponding robust anomaly detector based on simple normalization and eigenvalue principles. Specifically, we construct the stealthy FDIA by leveraging the pseudo-null space of the system Jacobian matrix. For detection, the power flow measurements undergo Pseudo-null Space Conserving Normalization to facilitate the extraction of the principal attack component via Singular Value Decomposition. We demonstrate the efficacy and scalability of our detection method, outperforming competitive learning-based detectors. Finally, we conduct a comprehensive scan of the stealth-noise parameter space, and numerically evaluate detection performance under varying system size, and noisy/partial observability.

(C1-02)

Mr. Javier Roasso
Jaidip Kotak, Aviad Elyashar, Robert Moskovitch, Asaf Shabtai and Rami Puzis
Ben Gurion University of the Negev
Shamoon College of Engineering (SCE), Beer Sheva, Israel

COPE: Common Operational Processes Enumeration

Industrial control systems (ICSs) lack a standardized ontology for de-scribing normal operational processes. This gap, which arises from the assumption that every process is unique, limits the development of scalable, process-aware security solutions and creates commu- nication barriers between security and operations teams. To ad-dress this deficiency, we propose the Common Operational Process Enumeration (COPE) framework, a hierarchical ontology which systematizes operational behaviors. COPE employs a four-level tax- onomy (Tactic, Technique, Sub-Technique, and Procedure), struc- turally inspired by the MITRE ATT&CK framework, to transform the vast amount of existing site-specific processes into a standard- ized, sharable terminology. This lexicon facilitates process-aware threat detection and the secure sharing of indicators of compromise (IOCs) without exposing proprietary details. To validate COPE's efficacy, we applied a systematic top-down methodology in three water system testbeds used to study ICS security. We identified and categorized 35 functional units (logical groupings of equipment performing a single function) and categorized them into a compact set of four unique Tactics that originate eight unique Techniques. The results reveal a high degree of reusability: over 80% of the identified functional units are described by just two Tactics (Stor- age and Filtering) and three Techniques. For instance, the Storage Tactic accounts for 71% of all functional units, while the Continuous Storage Monitoring Technique appears in 37% of units across the testbeds. This work demonstrates that common operational pat- terns exist and can be systematically identified and standardized. COPE provides the structured, contextual baseline of normal pro- cess behavior required to develop more intelligent, explainable, and scalable process-aware intrusion detection systems, while establish- ing a common language for incident response and cross-domain collaboration in ICS environments.

(C1-03)

Mr. Lavi Ben-Shimol
Ben Gurion University of the Negev

Cybersecurity & AI in Security Applications

LLMCloudHunter: Harnessing LLMs for Automated Extraction of Detection Rules from Cloud-Based CTI

As the number and sophistication of cyber attacks have increased, threat hunting has become a critical aspect of active security, enabling proactive detection and mitigation of threats before they cause harm. Open-source cyber threat intelligence (OSCTI) is a valuable resource for threat hunters; however, it often comes in unstructured formats requiring manual analysis. Previous studies aimed at automating OSCTI analysis are limited since (1) they failed to provide actionable outputs, (2) they did not utilize images in OSCTI sources, and (3) they focused on on-premise environments, overlooking the growing importance of cloud security. To address these gaps, we propose LLMCloudHunter, a novel framework leveraging large language models (LLMs) to automatically generate generic-signature detection rule candidates from textual and visual OSCTI data. We evaluated the quality of the rules generated by our framework using 20 annotated real-world cloud threat reports. Results show that LLMCloudHunter achieved 83% precision and 99% recall for extracting API calls made by the threat actor and 99% precision with 97% recall for indicators of compromise (IoCs). Additionally, 99.18% of the generated detection rule candidates were successfully compiled and converted into Splunk queries.

(C1-04)

Mr Ilya Feigin
Embedded Solutions 3000, COO.

Invisible Firewalls: The Next Evolution in Network Defense

This presentation examines a growing paradox in modern network security: firewalls remain a foundational security control, yet their visibility and centrality increasingly make them high-value targets for attackers. Drawing on market data, vulnerability trends, and real-world examples involving major firewall vendors such as Palo Alto Networks, Fortinet, and Check Point, the presentation analyzes how firewall weaknesses can expose entire networks to compromise.

The discussion addresses several recurring risk categories, including remote code execution, authentication bypass, information disclosure, misconfiguration, delayed patching, zero-day vulnerabilities, administrative compromise, and supply-chain exposure. Through visual examples, the presentation illustrates the firewall's role as a central traffic chokepoint, demonstrates potential attack paths using crafted malicious packets, and compares traditional exposed firewall architectures with an alternative protected architecture in which BNS/Invisicore appliances shield the firewall from internal and external discovery.

The central argument is that firewalls are essential, but they should no longer remain directly reachable, identifiable, or administratively exposed to attackers. The proposed Invisicore/InvisiHide approach introduces invisible security appliances on both sides of the firewall, allowing normal traffic inspection and filtering to continue while removing the firewall's visible network identity. Administrative access is restricted to controlled, time-limited, and strongly authorized sessions.

By reducing the firewall's discoverability and attack surface, this architecture aims to lower the risk of zero-day exploitation, unauthorized administration, lateral movement, and long-term attacker persistence. The presentation concludes that the next stage in firewall defense is not to replace the firewall, but to protect it by design—making it invisible, shielded, and significantly harder to target.

Session D1- Prof. Shlomo Greenberg- ML-based applications

(D1-01)

Mr. Avi Hazan

Avi Hazan[1], Elishai Ezra Tsur[2], and Shlomo Greenberg[3]
[1]Ben-Gurion University, [2]The Open University of Israel, [3] Shamoon College of Engineering (SCE), Beer Sheva, Israel

4SM: Selective Spiking State Space Models for Neuromorphic Sequence Learning

Modern AI models for sequences (like language or audio) are powerful but expensive to run. We asked: Can the brain's trick of communicating with sparse electrical spikes make these models faster and cheaper without losing accuracy? We built 4SM, a model where spiking neurons decide when and how the system updates its memory. Despite firing only a few spikes per neuron on average, 4SM matches or beats much denser models on tasks like digit recognition, speech commands, and long-range reasoning, even outperforming the well-known S4 baseline on ListOps. Spiking, it turns out, isn't just biologically inspired; it's genuinely efficient

(D1-02)

Dr. Erez Manor

Prof. Shlomo Greenberg
Ben-Gurion University, Shamoon College of Engineering (SCE), Israel

The Rise of TinyML: Bringing Intelligent Autonomy and Next-Gen Innovations to Extreme Edge Devices

Artificial Intelligence is undergoing a massive migration from centralized cloud datacenters directly into the physical environments where data is generated. Tiny Machine Learning (TinyML)—the deployment of machine learning models on resource-constrained, low-power microcontrollers and sensors—is the driving force behind this revolution. Operating with tight energy budgets (often below 1 milliwatt) and minimal memory footprints, TinyML enables real-time, ultra-low-latency, and entirely offline decision-making across consumer electronics, smart cities, healthcare wearables, and industrial automation. This lecture provides a comprehensive, high-level introduction to the foundations of the TinyML ecosystem.
phenomenon across this extensive dataset. By combining rigorous statistical modeling with longitudinal data analysis, this research challenges conventional beliefs about streak-based performance and provides a nuanced understanding of player behavior over two decades of professional basketball.

(D1-03)

Dr. Tom Trigano

Shamoon College of Engineering (SCE), Israel

Machine Learning for Activity Estimation in Spectroscopy Signals

The field of nuclear spectroscopy has received considerable interest in the last decades, particularly due to the exponential development of novel Machine Learning (ML) and Deep Learning (DL) techniques. However, the lack of annotated data often prevents their use at a large scale. In this presentation, we show how ML/DL methods can be used to extract the activity of a radioactive source directly from the time signal. Although simple, this illustration demonstrates that much remains to be done to fully leverage the potential of ML/DL techniques.

(D1-04)

Dr. Moshe Bensimon

Prof. Shlomo Greenberg
Shamoon College of Engineering (SCE), Israel

Computing Like the Brain: An Introduction to Neuromorphic Systems and Their Applications

This lecture introduces the fundamentals of neuromorphic computing, focusing on brain-inspired neural networks and the basic neuron model. We will explore key learning algorithms used in spiking neural networks (SNNs), and compare their advantages and limitations relative to traditional artificial neural networks (ANNs). The lecture will also highlight real-world applications, including sound processing, event-based image processing using event cameras, EEG signal analysis, and geophone-based sensing.

Afternoon Session:

<u>Session A2</u>- Dr. Natalia Vanetik- NLP and Applications

(A2-01)

Prof. Bozidar Ivankovic
Zdenko Bolfek, Božidar Ivanković
University of Applied Sciences Hrvatsko zagorje Krapina, Croatia

Artificial Intelligence, Automation and Structural Labour Shortages in the Croatian Labour Market

The paper analyses the transformation of the Croatian labour market from a prolonged period of high unemployment to a phase of structural labour shortages concentrated in several key sectors, in particular construction, tourism, retail trade, manufacturing, and transportation and storage. Based on available statistical data, it shows that these sectors record strong employment growth, a high number of registered job vacancies and increasing reliance on foreign labour, which raises questions about the long-term sustainability of a growth model based on extensive increases in the number of workers. The paper also examines the main channels through which artificial intelligence and automation affect the labour market – productivity enhancement, changes in the occupational structure and impacts on migration flows – and concludes that the sectors with the largest labour shortages are at the same time among those most exposed to the potential automation of routine and physically demanding tasks. It proposes a set of quantitative indicators for future monitoring of the effects of new technologies by sector (labour productivity, employment and occupational structure, dependence on foreign labour, intensity of investment in technology) and emphasises that the combination of systematic monitoring of these indicators and policies aimed at fostering investment in new technologies is a key precondition for harnessing the potential of artificial intelligence to alleviate structural labour shortages in Croatia.
Keyword. artificial intelligence, automation, labour market, labour productivity, structural labour shortages.

(A2-02)

Dr. Natalia Vanetik
Shamoon College of Engineering (SCE), Israel

Analyzing Rhetorical Evolution in Political Campaign Discourse

This study examines the rhetorical evolution of Donald J. Trump across two U.S. election cycles, comparing his 2020 campaign as an incumbent with his 2024 campaign as a challenger. Using approximately 64,000 speech-derived text segments, we apply a multi-layered NLP framework combining sentiment analysis, psychological lexical features, semantic drift estimation, topic modeling, and supervised classification. The results reveal a substantial rhetorical shift. In 2024, anger-related language increases markedly, while positive sentiment declines, indicating a more adversarial emotional tone. Topic modeling shows a transition from social and crisis-oriented themes in 2020 to economic and nationalist narratives in 2024. Semantic drift analysis further demonstrates systematic changes in the contextual use of key political terms. Classification experiments confirm that the two campaigns are highly distinguishable. Overall, the findings suggest that political discourse can influence information integrity through emotional framing, semantic recontextualization, and rhetorical emphasis, even without explicit misinformation.

(A2-03)

Mr. Idan-Chaim Cohen
Idan-Chaim Cohen[1,2], Noya Littor[2,3], Aviad Elyashar[2,4], Rami Puzis[2,3], and Odeya Cohen[1]
[1] Department of Nursing, Recanati School of Community Health Professions, Faculty of Health Sciences, Ben-Gurion University of the Negev, Beer-Sheva, Israel
[2] Cyber@BGU, Ben-Gurion University of the Negev, Beer-Sheva, Israel
[3] Stein Faculty of Computer and Information Science, Ben-Gurion University of the Negev, Beer-Sheva, Israel
[4] Department of Computer Science, Shamoon College of Engineering, Beer-Sheva, Israel

Machine Psychology in Safety-Critical Systems: The Case of Large Language Models in Disaster Management

Large language models are increasingly embedded in safety-critical systems, where outputs inform consequential decisions in domains such as medicine, infrastructure, and emergency response.

Because these models are trained on human-generated text, their outputs reflect patterns of human judgment, an emerging area of study termed machine psychology.

Two controlled experimental studies measured these patterns in a single high-stakes case: emergency and disaster management.

Across both studies, each testing eight language models from four providers, model judgments were systematically shifted by properties of the input that carry no factual relevance to the situation being assessed.

How information is framed, whether a probability is expressed as a frequency or a decimal, the affective tone of a report, and the degree of uncertainty in the data all moved severity ratings and resource-allocation decisions in measurable, directional ways.

Many cognitive biases documented in human decision-makers reappeared in the models.

The size of these effects varied widely across models, and prompt-based instructions intended to suppress them proved unreliable, in some cases overcorrecting.

This is a class of behavior that resists uniform correction and varies from one model to the next.

Characterizing this behavior before a model enters a setting where its output carries weight calls for structured assessment across three dimensions: machine psychology, information quality, and operational failure modes.

(A2-04)

Ms. Karin Shistik
Ben Gurion University of the Negev

State vs. Trait Anxiety in Causal Language Models

Psychological constructs in humans range along a state-trait continuum: traits persist across situations, while states fluctuate with context. Studies have shown that language models exhibit measurable psychological constructs, yet whether these constructs differ in contextual stability, as the state-trait distinction predicts, remains untested. We present the Questionnaire for Causal Language Models (QCLM), a psychometric framework that measures constructs through next-token probability distributions of base models. Applying QCLM to 35 causal language models under vanilla, stress, and neutral conditions, we assess two anxiety instruments targeting opposite ends of the state-trait continuum: STAI-S (state anxiety) and STAI-T (trait anxiety). Paired effect sizes and variance decomposition reveal that state anxiety is more sensitive to stress manipulation than trait anxiety: stimulus type accounts for a larger share of variance in state anxiety, while model identity contributes more to trait anxiety. These results provide empirical evidence that the state-trait distinction extends to language model behavior.

<u>Session B2</u>- Dr. Yehuda Ben-Shimol- ML-based Signal Processing

(B2-01)

Dr. Aviva Peeters
Yafit Cohen, Eitan Goldshtein, Alon Ben-Gal.
Shamoon College of Engineering (SCE), Israel

Data Science & Data Analytics

A Spatial Machine Learning Tool for Optimizing Sampling Distribution.

We present a spatial machine learning decision-support tool (DST) to optimize the distribution of samples or sensors in agricultural fields. The DST is based on a model that combines machine learning and spatial-statistical algorithms, to address spatial variability, especially the local spatial autocorrelation of multiple variables, and complex non-linear relations between variables. The method uses stratified-based sampling and an iterative process deriving spatial histograms, to find a subset which represents the spatial distribution of the entire dataset. The model uses remote-and proximal sensing data of plant, soil and environmental variables. The DST is accessible through a free, web-based interface, which outputs maps indicating optimal placement of samples or sensors within a field, and analytical outputs identifying the minimum required number of samples for optimal sampling and the accuracy for non-optimal configurations.

(B2-02)

Dr. Guy Tel Zur
Ben-Gurion University of Negev

Digital Twins as an additional security protection layer in industrial control systems (ICS)

Abstract For many years, cybersecurity awareness in Operational Technology (OT) systems was limited compared with Information Technology (IT) systems. This has changed significantly during the last two decades, as many Industrial Control Systems (ICS) have become interconnected with IT infrastructures and, in some cases, exposed directly or indirectly to the internet. As a result, the risk of cyberattacks against ICS has increased, and protecting critical industrial systems has become essential. This talk presents a complementary protection layer based on a Digital Twin (DT). A DT is a virtual representation of a physical system that runs continuously and is updated in real time. Unlike an offline simulation, a DT can operate in parallel with the physical system, receive selected measurements or trusted inputs, and predict the expected physical behavior. By comparing the physical system with the DT, discrepancies can be detected and displayed on the Human-Machine Interface (HMI). Such discrepancies may indicate sensor manipulation, actuator attacks, malware activity, or operational failures. The talk demonstrates the concept using a toy ICS project: a heated water container with temperature sensors, a heater actuator, and a controller. A physical model is developed and exported as an FMU, while an AI-assisted Digital Twin predicts the expected water temperature. The difference between the predicted and measured behavior is used as the basis for anomaly detection and for demonstrating DT-based cyber-physical protection

(B2-03)

Mr. Avishai Weizman
Itshak Lapidot, Yehuda Ben-Shimol Avishai Weizman
Ben-Gurion University of Negev

Spoofing-Robust Speaker Verification Based on Time-Domain Embedding

This study proposes a novel approach to spoofing-robust automatic speaker verification (SASV), focusing on logical access attacks. It introduces embeddings in the time domain based on the probability mass function (PMF) of speech waveform amplitudes in genuine and spoofed speech signals. This research highlights the role of gender separation and its positive impact on the spoofing detection task performance. The countermeasure system utilizes PMF-based embeddings, achieving equal error rates (EER) of 8.67% for males and 10.12% for females. Our study demonstrates that PMF-based embeddings capture valuable information for spoofing detection, as well as for the gender recognition task using PMF-based embeddings based on male and female groups. Our results are evaluated using the ASVspoof2019 database. Furthermore, fusing PMF-based embeddings with traditional countermeasures enhances generalization in SASV systems. This research suggests a promising direction for improving detection performance against spoofing attacks by combining PMF-based embeddings with traditional frequency-based embeddings.

(B2-04)

Dr. Yehuda Ben-Shimol
Alan Frid, Prof. Shlomo Greenberg
Ben-Gurion University of the Negev, Shamoon College of Engineering (SCE), Israel

Drones Detection using Deep Neural Network with RF and Acoustic Features

The use of drones has recently gained popularity in a diverse range of applications, such as aerial photography, agriculture, search and rescue operations, the entertainment industry, and more. However, misuse of drone technology can potentially lead to military threats, terrorist acts, as well as privacy and safety breaches. This emphasizes the need for effective and fast remote detection of potentially threatening drones. In this study, we propose a novel approach for automatic drone detection utilizing the usage of both radio frequency communication signals and acoustic signals derived from UAV rotor sounds. In particular, we propose the use of classical and deep machine-learning techniques and the fusion of RF and acoustic features for efficient and accurate drone classification. Distinct types of ML-based classifiers have been examined, including CNN- and RNN-based networks and the classical SVM method. The proposed approach has been evaluated with both frequency and audio features using common drone datasets, demonstrating better accuracy than existing state-of-the-art methods, especially in low SNR scenarios. The results presented in this paper show a classification accuracy of approximately 91% at an SNR ratio of −10 dB using the LSTM network and fused features.

Session C2- Dr. Marina Knyazhansky- Social Computational Intelligence

(C2-01)

Dr. Hagai Ilani
Lior Aronshtam, Elad Shufan
Ben-Gurion University of Negev

Fair Assignment of Plots to Tenants

This study explores generous maximum matching, a preference-based allocation method inspired by the challenge of assigning residential plots to tenants. Each tenant submits a strict and complete ranking of available plots. Unlike rank-maximal matching, which prioritizes maximizing top-choice assignments, generous maximum matching aims to minimize severe dissatisfaction—first reducing the number of tenants who receive their worst option, then second worst, and so on. We analyze structural properties of such matchings and prove that in any optimal solution, no more than one tenant gets their least-preferred plot, and at least one receives their top choice. More generally, in any Pareto-optimal matching, no more than k tenants receive one of their k least preferred plots. The generous maximum mechanism is not strategyproof. We show that tenants may manipulate their submitted preferences to avoid their least favorite plots.

(C2-02)

Dr. Marina Knyazhansky
Shamoon College of Engineering (SCE), Israel

VR Systems for Exposure-Based Treatment of Specific Phobias

Specific phobias are among the most common mental-health disorders (~10 % prevalence). Exposure therapy within CBT is the gold standard, yet recreating triggers such as flying, heights, or animals is often costly, impractical, or met with patient resistance. Virtual reality (VR) provides realistic but fully controllable environments. We developed three VR systems for graded exposure to acrophobia, aviophobia, and ailurophobia. Each platform follows CBT protocols, offering tiered scenarios, variable difficulty, and a clear sense of user control. The cat-phobia system, for example, guides users from passively observing a cat image to active interaction with a virtual cat. A mixed-methods case study tested the cat-phobia system on its creator with lifelong cat phobia. There was a significant improvement in her condition. These findings show that VR tools can deliver structured, effective exposure even for complex phobias and can serve as a trusted therapeutic space that blends control, presence, and self-reflection.

(C2-03)

Dr. Tammar Shrot
Naomi Korem, and Hadassa Daltrophe
Shamoon College of Engineering (SCE), Israel

A Permission-Based Approach to Minimizing Echo Chambers on Social Platforms

Echo-chambers in social media pose a growing threat to democratic discourse. Unlike other approaches that address this challenge through regulation that violates users' rights, our proposal preserves user autonomy by allowing them to decide whether to explore contrasting opinions. This study explores the effectiveness of applying regulation solely to users who have consented, examining whether such a strategy can encourage balanced information flow between ideologically divided communities within a network. We introduce a framework that models the diffusion of content across social media, incorporating elements such as users' connections, beliefs, and virality. Through simulations using real-world datasets and a range of parameter settings, we evaluate how the system performs. The findings reveal that engaging even a small proportion of consenting participants can markedly improve the spread of messages across ideological divides. Overall, this research highlights the promise of consent-based regulation as a pathway to more constructive and inclusive public discourse

(C2-04)

Naomi Korem,
Tammar Shrot, and Hadassa Daltrophe

What Machines Reveal about the Principle of Proportionality

The Principle of Proportionality is a cornerstone of Just War Theory, yet the advent of Lethal Autonomous Weapon Systems has intensified debates regarding its application. Conventional scholarship suggests proportionality requires qualitative, subjective judgment, which algorithmic systems inherently lack. Our talk reframes the inquiry, proposing that the difficulty of encoding proportionality into machines is not a technical failure but an epistemological "mirror" reflecting the principle's fundamental conceptual instability. We proceed in two stages. First, we provide theoretical and empirical reasons to suspect the comprehensibility of the proportionality principle. Second, we analyze various machine learning paradigms, including supervised, unsupervised, and reinforcement learning, to show that the inability to formalize a stable objective function prevents machines from learning the principle. We argue that if a principle cannot be taught or formalized, its comprehensibility to humans must be rigorously reconsidered. Rather than revealing machine limitations, the problem of teaching machines proportionality highlights the inherent indeterminacy of proportionality itself.

<u>Session D2</u>- Prof. Issac August- ***AI-based Spectral Imaging***

(D2-01)

Dr. Edward C. Wellman
University of Arizona

A Machine Learning Approach to estimating the intact strength of altered granites from Short Wave Infrared

This study investigates the use of machine learning and Shortwave Infrared (SWIR) hyperspectral imaging to estimate the Unconfined Compressive Strength (UCS) of altered granite. Advances in portable and lower-cost hyperspectral sensors provide new opportunities for non-destructive rock characterization using reflectance-based spectral data. Hyperspectral images of 32 altered granite core samples were acquired across the 1000–2500 nm SWIR range and analyzed to identify spectral features associated with mechanical rock strength.

The research focused on developing a machine learning workflow that integrates spectral preprocessing, feature extraction, and statistical analysis to classify rock samples into International Society of Rock Mechanics (ISRM) strength categories, including weak, moderately strong, and strong rock. Deviations from mean spectral responses were used to isolate significant spectral components related to alteration mineralogy and rock competency. A k-Nearest Neighbor (kNN) classifier achieved an overall classification accuracy of 90%, demonstrating the potential of hyperspectral data-driven models for geotechnical characterization. The study outlines a scalable framework for integrating machine learning and hyperspectral imaging into future drill core and surface rock strength assessments

(D2-02)

Dr. Dean N. Riley
School of Mining Engineering and Mineral Resources, University of Arizona, Tucson, AZ, USA

Optical and infrared spectroscopy mineral identification and volume estimates applied to forward modeling of cross-property rock physics models for some New Mexico granites.

Forward modeling and inversion of geophysical, geochemical, geomechanical and geological data in rock mechanics, rock physics, and mineral exploration and ore deposit characterization are unconstrained problems which are challenging for machine learning (ML) and artificial (AI) algorithms. Precise mineralogy identification and volume estimates are critical for the development of integrated geophysical and geological multi-modal ML/AI using cross-property rock physics models to effectively constrain geophysical and geological inversions for multi-sensor fusion for mineral exploration, mineral processing, metallurgical (re)processing and mine planning information. Reliable mineralogy identification with accurate volume estimates have traditionally been the limiting factor in this process. Development of these models has been challenging mostly from the lack of synchronized data collection of physical property measurements and optical and infrared spectroscopy. Rapid, accurate, and nondestructive characterization of core, thin section billets, and hand samples using optical and infrared spectroscopy can identify mineralogy and provide reasonable volume estimates of mineralogy thus improving rock physics and mineralogy cross-property relationships to constrain the geophysical and geological inversions in a unified framework. A proposed unified framework will be discussed using results from some New Mexico granites focused on the development of cross-property rock physics models based on mineralogy from optical and infrared spectroscopy to predict elastic properties (P- and S-wave acoustic velocities, or $V_p$and V_s), unconfined compressive strength (UCS), and other physical and mechanical properties for improvement of geophysical and geological inversions.

(D2-03)

Mr. David Martinko
Or Adir, Dr. Isaac Y August
Ben-Gurion University of Negev
Shamoon College of Engineering (SCE), Israel

Computational Spectroscopy Based on Event-Driven Signal Reconstruction Using Spiking Neural Networks

Hyperspectral imaging enables advanced material analysis and scene analysis. Recent advancements in computational hyperspectral sensing highlight systems integrating liquid crystal spectral encoders with event-based sensors. These sensors provide unique advantages, most notably ultra-fast temporal resolution and a wide dynamic range. Despite these benefits, the associated spectral reconstruction processes remain highly complex. To address this challenge, this project proposes a novel framework employing a Spiking Neural Network with a residual correction block for precise optical spectrum reconstruction. This work evaluates the feasibility and accuracy of this neuro-inspired approach. When evaluated against an analytical cumulative sum reconstruction and an Orthogonal Matching Pursuit spectral inversion algorithm, our findings demonstrate that the proposed SNN-driven residual model yields robust, noise-resistant spectral reconstruction with superior reliability.

Keywords:
Compressed Sensing; Event Camera; Hyper-spectral Imaging; Liquid Crystal; Spiking Neural Network (SNN)

(D2-04)

Ms. Or Bastiker
Shamoon College of Engineering (SCE), Israel

Error Modeling in the Sensing Matrix Describing Computational Spectrometers

In this project, the effects of errors in the sensing matrix on reconstruction quality in computational spectrometers within the optical domain are investigated. The objective of the project is to examine how uncertainties and deviations between the theoretical matrix, which ideally represents the system, and the actual behavior of the system influence the ability to reconstruct spectral information. The study considers scenarios in which noise, distortions, or errors are present in the matrix coefficients, and evaluates the sensitivity of the reconstruction process to these variations. In addition, a comparison is presented between the results obtained from the theoretical model and those derived from practical conditions, in order to assess the gap between them. The findings of this project contribute to a deeper understanding of practical limitations in computational optical systems and support the development of more robust, accurate, and reliable reconstruction methods.