CHEMICAL ENGINEERING TRANSACTIONS
VOL. 90, 2022
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Aleš Bernatík, Bruno Fabiano

ISBN 978-88-95608-88-4;; **ISSN** 2283-9216
DOI: 10.3303/CET2290068

A Bow-Tie Approach for the Identification of Scenarios Induced by Physical Intentional Attacks to Chemical and Process Plants

Matteo Iaiani, Alessandro Tugnoli*, Valerio Cozzani

LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, Italy
a.tugnoli@unibo.it

The possibility of inducing major accident scenarios by physical intentional attacks (e.g. terrorist attacks) to chemical and process plants processing and storing hazardous substances, has been increasingly recognized in the last decades. The identification of the credible security scenarios (chain from attack scenarios to major accident scenarios) is required by Security Vulnerability/Risk Assessment (SVA/SRA) methodologies, but an evident lack of supporting tools is present in the literature. The present study proposes a Bow-Tie approach for the identification of reference security scenarios to support hazard identification phase in SVA/SRA. The potential use of the results is demonstrated on a test case (industrial atmospheric tank storing a flammable liquid).

1. Introduction

Physical intentional attacks (e.g. terrorist attacks) to chemical and process plants processing and storing hazardous substances may generate major accident scenarios with severe consequences on humans, environment, and the assets (Landucci and Reniers, 2019). Past security-related incidents dramatically confirm that security of such installations must be considered as a major concern (Iaiani et al., 2021a). For example, the terrorist attack using drones laden with explosives against the Saudi Aramco Oil Processing Plant in 2019, severely damaged 14 storage tanks and 3 processing trains causing the release of the flammable material contained inside which led to multiple fires (cnbc.com, 2019).
The methodologies suitable for addressing security issues such as Security Vulnerability/Risk Assessment (SVA/SRA) methodologies (e.g. CCPS methodology, VAM-CF methodology, RAMCAP methodology, API RP 780 SRA methodology, and the one developed by the Hazardous Incidents Commission), as well as the novel and more complex approaches that were recently proposed in the literature (e.g. based on Bayesian Network, Markov Chains, Game Theory), require the identification of the credible major accident scenarios that can be generated by physical intentional attacks (Baybutt, 2018). However, despite the request for scenario identification, these methods do not provide any detailed practical procedure, and only occasionally checklists on sample security scenarios (cause-consequence chain from attack scenarios to major accident scenarios) are included. Furthermore, the techniques commonly used in the field of process safety for hazard identification such as HazOp, What if Analysis, FMEA, and MIMAH, do not account for security aspects (Mannan, 2012).
In the panorama outlined, the present study proposes a novel set of reference security scenarios using a Bow-Tie approach. The results support hazard identification phase in SVA/SRA and may also be used to integrate the scenarios considered in safety assessments (e.g. Safety Reports of European upper-tier Seveso plants) in order to yield a broader understanding of risk and to integrate in a single set the management of safety and security requirements (Boustras and Waring, 2020). The potential use of the reference security scenarios is demonstrated on a test case addressing a floating roof atmospheric tank for the storage of a flammable liquid.

Paper Received: 18 December 2021; Revised: 7 March 2022; Accepted: 3 May 2022
Please cite this article as: Iaiani M., Tugnoli A., Cozzani V., 2022, A Bow-Tie Approach for the Identification of Scenarios Induced by Physical Intentional Attacks to Chemical and Process Plants, Chemical Engineering Transactions, 90, 403-408 DOI:10.3303/CET2290068

2. The Bow-Tie approach

The method applied, based on a Bow-Tie approach, consists in the following steps: i) identification and validation of a reference set of Attack Scenarios (AS); ii) definition and validation of Attack Trees (AT) for a set of reference installations; iii) construction and validation of reference Bow-Tie (BT) diagrams for a set of families of hazardous substances frequently stored and processed in chemical and process plants.

Table 1: Set of Attack Scenarios (ASs) considered and related Reference Act of Interference (RAI).

AS code	Attack Scenario	Description	RAI code	Reference Act of Interference	Attack vector
#01	Deliberate interference with or w/o aids	Deliberate acts involving simple operations without the use of instruments or using tools that are present on site	#01-A	Closing/Opening manual valves	n.a.
			#01-B	Ramming installations and/or instrumentation	n.a.
#02	Arson using simple/incendiary means	Incendiary attacks	#02-A	Ignition of 50 L of gasoline contained in 2x25 L jerrycans	Heat load
			#02-B	Ignition of 1000 L of gasoline contained in an IBC tank with catch basin present in the target facility	Heat load
#03	Use of explosive	Use explosives to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	#03-A	Detonation of 50 kg of TATP carried inside a backpack	Overpressure
			#03-B	Detonation of 30 kg of TATP lifted by a drone	Overpressure
#04	Use of vehicle bomb	Use explosives (placed inside a vehicle) to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	#04	Detonation of 50000 kg of AN/dolomite (50/50) + diesel fuel contained inside a vehicle	Overpressure
#05	Shooting	Interference at close distance, using different types of weapons	#05	Shooting to equipment using 5.56×45mm NATO cartridge	Projectile impact
#06	Vehicle impact	Deliberate acts involving vehicles rammed against plant installations.	#06	Ramming installations using a large good vehicle (LGV)	n.a.

The set of Attack Scenarios (ASs) was identified from the analysis of the main SVA/SRA methodologies, focusing on the applicability in the context of the process industry. Cyber-attacks were explicitly considered out of the scope of the study given their specific mechanism which strongly depends on the design of the network system: dedicated works can be found in Iaiani et al. (2021b, 2021c). One or more Reference Act of Interference (RAI, example of an attack, defined considering credible worst-case situations in terms of instruments and/or materials available to the attacker) were defined for each AS based on information available in relevant literature in order to better support the identification and description of credible attack modes. In particular, Störfall-Kommission (2002) for typical deliberate interferences with or without the use of aids, Pert et al. (2006) for incendiary substances, Landucci et al. (2015) for types and quantities of explosives that can be potentially carried by a single man or by a vehicle, datasheets of heavy lift drones available in technical catalogues for information about common charges (valkyrie.pro, 2019), the standards EN 1063 and EN 1522 for type and characteristics of projectiles. ASs, corresponding RAIs, and attack vectors (heat load, overpressure, projectile impact) are all reported in Table 1. Depending on the characteristics of the target equipment (e.g. type, design pressure) the same AS will result in different damages. Therefore, in order to address this issue, three Attack Trees (ATs) were developed, corresponding to three reference installations (adapted from those proposed by Delvosalle et al. (2006)): atmospheric storage installations, pressurized storage installations, storage warehouses.

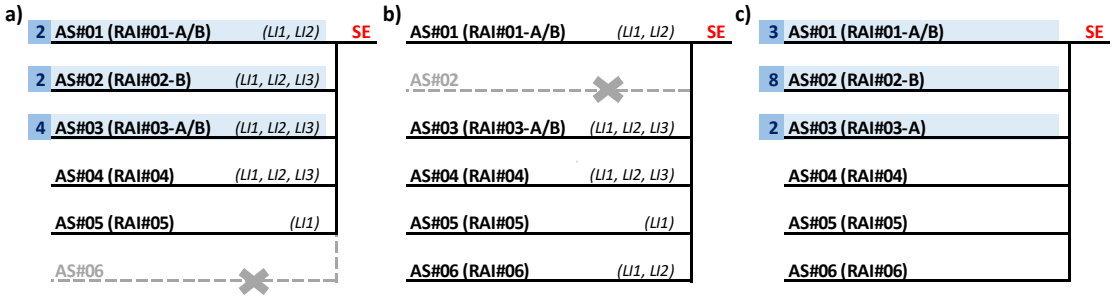

Figure 1: a) AT for atmospheric storage installations; b) AT for pressurized storage installations; c) AT for storage warehouses. Shaded branches are those validated by past security-related incidents. AS-codes and RAI-codes are defined in Table 1. LI: Loss Intensity.

ATs are graphs that represent all the attack modes (ASs and RAIs) which lead to a specific Security Event (SE), intended as a Loss of Physical Integrity (LPI) and/or a Loss Of Containment (LOC) of the hazardous material stored in the reference installation. In case of LOC of fluids, according to Cozzani et al. (2013), three different Loss Intensities (LIs) were used for characterizing the SE: LI1 - release from a 10 mm average release diameter; LI2 - release of the entire vessel inventory in 10 min and full-bore rupture of connected pipework; LI3 - instantaneous release of the entire vessel content. In particular, in order to define the ATs for each reference installation, the possibility of each AS to cause a LOC according to the above-defined LIs, or a LPI, was assessed.The assessment was based on the definitions of the set of adopted RAIs, taking into account the specific features of the attack vectors.Finally, Bow-Tie diagrams (BTs) were built combining Attack Trees (ATs, left side of the SE) with Event Trees (ETs, right side of the SE). ETs were generated according to the method proposed in step 6 of the MIMAH procedure for the most frequent families of hazardous substances stored and processed in the process industry: flammable liquids, flammable pressurized gasses, flammable gasses, flammable cryogenic liquids, toxic pressurized gasses, pressurized liquefied toxic gasses, and oxidizing solids. Validation of the proposed ATs and BTs was carried out using information available in a database collecting past security-related incidents that occurred worldwide in the Chemical&Petroleum (C&P) sector (Iaiani et al., 2021a): elements of the BT that were recorded at least one time were considered possible to occur again and therefore validated.

3. Attack Trees for reference installations

Figure 1 shows the ATs that were developed for atmospheric storage installations (Panel-a), pressurized storage installations (Panel-b), and storage warehouses (Panel-c). AS-codes and RAI-codes are defined in Table 1. Shaded branches in the ATs (light blue color) are those validated with past security-related incidents (number in tags refer to the number of incidents).Looking at the AT for atmospheric storage installations (Panel-a of Figure 1), there is historical evidence of a SE caused by the majority of the attack scenarios considered in the present study, i.e. deliberate interferences with or without the use of aids available on site (AS#01), incendiary attacks (AS#02), use of explosives (AS#03) both carried by a single man and by a heavy lift drone. No attacks consisting in the detonation of explosives contained inside vehicles (AS#04) or in shooting (AS#05) were recorded for atmospheric storages in the database; however, these two attacks are deemed to be potentially able to damage atmospheric installations as highlighted in the studies of Landucci et al. (2015) and Woodward (1978). On the contrary, vehicle impact attacks (AS#06) are not considered credible for this type of installations due the typical presence of catch basins or bunds around atmospheric storage tanks. This conclusion is also supported by the lack of recorded incidents featuring this AS.No incident collected in the database reported a SE involving a pressurized storage installation (see AT in Panel-b of Figure 1). However, all the ASs considered in the present study have the potential to cause damage to pressurized equipment units, with the exception of incendiary attacks given the low duration of the fires associated to ignition of 50 L (RAI#02-A) and 1000 L (RAI#02-B) of gasoline (< 1 min in case of unconfined pools) if compared to the typical time to failure (ttf) of these installations (minimum ttf of 1 min for atmospheric installations and of 5 min for pressurized installations according to Cozzani et al. (2006)). Thirteen (13) incidents reported a SE involving a storage warehouse as reported in the AT shown in Panel-c of Figure 1. It is important to remark that attackers have to reach the warehouse interior area, bypassing the physical barriers in place (attack that occurs outside the

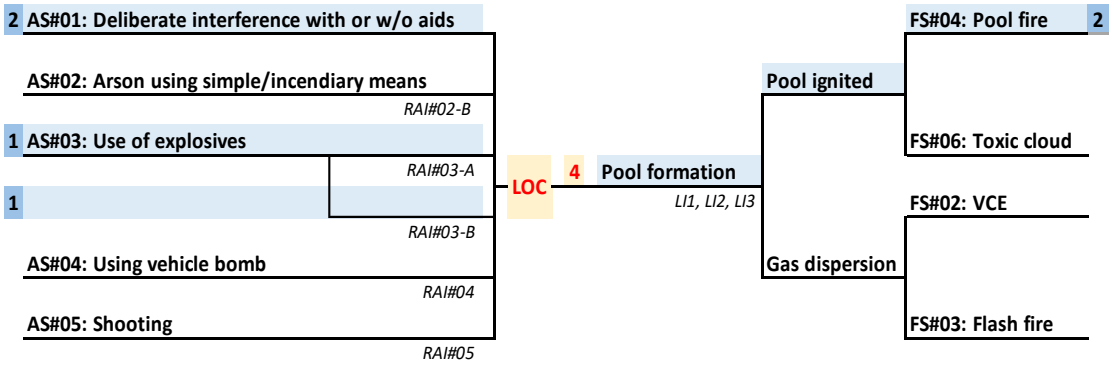

Figure 2: Reference BT for atmospheric storage of flammable liquids. Shaded branches are those validated by past security-related incidents. AS-codes and RAI-codes are defined in Table 1. LI: Loss Intensity.

warehouse are not accounted in the analysis). Due to the very frequent presence of flammable materials stored (e.g. paint products, solvents) that can be ignited, the incendiary attack (AS#02) resulted the most recorded followed by deliberate interferences (AS#01) and attacks involving explosives (AS#03) carried by the attackers themselves (RAI#03-A). On the contrary, the use of explosives lifted by drones (RAI#03-B) was not observed due to the fact that storage buildings are typically enclosed areas and access of drones may be difficult.
The use of a vehicle bomb inside a storage warehouse (AS#04) was not validated, but damage is considered certain in case of successful detonation. A similar consideration was done for shooting attacks (AS#05) as no validation was possible (no incident reporting this AS was recorded), but perforation of the low-volume containers used for the storage of liquids and powders is considered certain for shooters within the interior area of storage warehouses given their low thickness. Similar assumptions apply to vehicle impact attacks (AS#06). Given the different nature of the containers if compared to the one of steel-made storage tanks, release loss intensities have no meaning in case of storage warehouses, and thus they are not reported in the reference AT.

4. Reference Bow-Tie diagram for the storage of flammable liquids

For the sake of brevity, only the reference BT developed for the atmospheric storage of flammable liquids (i.e. liquids having a flash point of not more than 93 °C) is shown and discussed (see Figure 2). The tree on the left side of the SE (a LOC in the specific case) is the AT developed for atmospheric storage installations (see Panel-a of Figure 1), while the one on its right side is the ET generated with the MIMAH procedure.
The formation of a pool of flammable liquid is the primary event that follows a LOC, which was validated by four past security-related incidents (see tags in the BT): in two cases this event was generated by deliberate interferences involving simple operations without the use of instruments or using tools that are present on site (AS#01), while in the other two cases it was caused by attacks involving the use of explosives (AS#03).
A pool fire is the major accident scenario that occurs in case of immediate ignition of the flammable vapors evaporating from the pool. For example, this was validated by the incident occurred on 14/07/2015 in France where 2000 tons of naphtha and 1000 tons of gasoline were released from the storage tanks resulting in pool fires after the detonation of explosive devices (RAI#03-A)(eMars database), and by the one occurred on 14/09/2019 in Saudi Arabia where the release and ignition of oil from 14 storage tanks of the Saudi Aramco Oil Processing Plant was caused by a drone attack (RAI#03-B)(cnbc.com, 2019).
In case combustion conditions produce large amounts of toxic compounds, a toxic cloud is associated to the pool fire, and toxic effects are added to those related to the heat load.
Overall, the formation of a pool is deemed credible for all the ASs considered. However, its ignition (i.e. pool fire formation) is highly probable only in case of incendiary attacks, while in case of attacks using explosive devices (AS#03 and AS#04), ignition is deemed possible, but not certain as demonstrated by past security-related incidents occurred in other sectors, such as the one of transportation of oil and gas via pipeline (Global Terrorism Database).
Finally, the secondary event “gas dispersion” is excluded in case of low volatile liquids, and in case of incendiary attacks (AS#02) given the presence of an immediate source of ignition. If a delayed ignition of the gas cloud occurs, a vapor cloud explosion (VCE) or a flash fire may happen depending on several factors such as the reactivity of the substance involved, the turbulence of the gas cloud, the confinement, and the explosive gas mass.

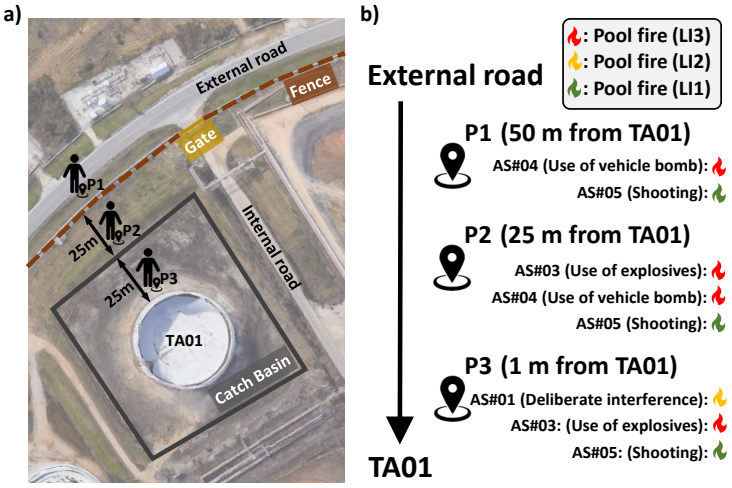

Figure 3: a) Layout of the site considered in the test case showing the atmospheric storage tank TA01, the catch basin, the site fence, the internal and external roads, the gate, and positions P1, P2, and P3; b) Reference security scenarios suggested for TA01 based on the position reached by the attacker (P1, P2, P3).

5. Test case

The test case addresses an atmospheric floating roof storage tank storing a low volatile flammable liquid (TA01). The layout of the site area of interest is shown in Figure 3 (Panel-a). Three alternative potential locations reached by the attacker were considered: P1 (outside the fence), P2 (between the fence and the catch basin), and P3 (proximity of TA01, inside the catch basin).

The reference BT shown in Figure 2 is applicable to the layout considered and was used to define reference security scenarios based on the position reached by the attacker (P1, P2, P3, see Panel-b of Figure 3).

The hazardous properties and storage conditions of the flammable liquid exclude the possibility of a large vapor cloud formation from the evaporation of spilled pools, and therefore both VCE and flash fire are excluded. Moreover, also a toxic cloud is excluded as outdoor uncontrolled combustion is not expected to create large clouds of acute toxic compounds.

A damage caused by deliberate interferences with or without the use of aids (RAI#01-A and RAI#01-B) is only possible from position P3 due to the fact that the attacker has to reach TA01 (LI2 expected in case of use of aids present on site, e.g. disc grinder or cutting torch, while LI1 in case of manipulation of small valves present on TA01). The attacker is then expected to ignite the spilled liquid, leading to pool fires (worst-case).

The pool fire modelling (performed according to the Yellow Book of TNO), showed that a damage caused by incendiary attacks is only possible in case of an incendiary device which involves large quantities of flammable material (e.g. 1000 L of gasoline contained in IBC tanks as in RAI#02-B) and at close distances to TA01 (< 5m). Therefore, only from position P3 a damage is possible: however, this requires to move IBC tanks within the catch basin area (e.g. with a crane) where they are not normally present and this is not deemed credible, and thus no damage from incendiary attacks is considered.

The information on the effects of the peak overpressure provided in Landucci et al. (2015) allowed to conclude that in case of attacks involving explosives (AS#03), a damage is possible from positions P2 and P3 for both the two RAIs considered (a LI3 release is achievable). Moreover, the detonation of explosives may cause the ignition of the pool of the released liquid generating a fire (worst-case scenario).

Similar considerations apply to the detonation of a vehicle bomb (AS#04) from both the positions accessible to vehicles (P1 and P2), since vehicle access to P3 is prevented by the presence of the catch basin. This AS resulted a very critical attack pattern as in the case of detonation of 50000 kg of AN/dolomite (50/50) + diesel fuel inside a vehicle (RAI#04), the effects of the peak overpressure are able to cause damage at a distance of about 150 m (Landucci et al., 2015), far farther than the distance between P1 and TA01 (50 m).

In case of shooting attacks (AS#05), a perforation is reasonably possible from each of the three positions considered. However, only a release loss intensity LI1 is expected in this case (the diameter of the hole is nearly the same as that of the projectile). Immediate ignition was conservatively assumed in this case (worst-case scenario).

Finally, the presence of the catch basin makes the vehicle impact attacks (AS#06) not able to cause damage to tank TA01. Overall, the security scenarios identified may be used in SVA/SRA and may be compared those considered in safety assessments (e.g. Safety Reports of European upper-tier Seveso plants) in order to yield

a broader understanding of risk and to integrate in a single set the management of safety and security requirements.

6. Conclusions

The present study proposes a novel set of reference security scenarios triggered by physical intentional attacks to chemical and process plants using a Bow-Tie (BT) approach. The developed reference BTs (Attack Trees on the left side of the Security Event and the Event Trees on its right side) were validated by past security-related incidents occurred worldwide in the chemical and process facilities in the last decades. Attack Trees were developed for three reference target installations: atmospheric storage installations, pressurized storage installations, and storage warehouses, considering for each of them, a set of attack scenarios able to cause physical damage. Event Trees were generated with the MIMAH procedure for the most frequent families of hazardous substances stored and processed in the chemical and process industry. A test case addressing a floating roof atmospheric tank storing a flammable liquid was used to demonstrate the potential use of the developed reference security BTs in supporting security hazards identification.
Overall, the present study provides contribute to fill the existing gap in the availability of practical approaches for the identification of security scenarios which are requested in the application of SVA/SRA methodologies and other methods for quantitative security risk evaluation. Moreover, the developed reference security BTs may be used to integrate the list of major accident scenarios considered in the Safety Reports of European upper-tier Seveso plants in order to yield a more complete understanding of risk and to define a single set of safety/security requirements (integrated management of safety and security risks).

Acknowledgments

This work was supported by INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) in the framework of the 4th SAF€RA call.

References

Baybutt P., 2018, On the completeness of scenario identification in process hazard analysis (PHA), J. Loss Prev. Process Ind., 55, 492–499.
Boustras G., Waring A., 2020, Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context, Saf. Sci., 132, 104942.
cnbc.com, 2019, Satellite photos show extent of damage to Saudi Aramco plants [WWW Document]. URL https://www.cnbc.com/2019/09/17/satellite-photos-show-extent-of-damage-to-saudi-aramco-plants.html (accessed 11.6.20).
Cozzani V., Gubinelli G., Salzano E., 2006, Escalation thresholds in the assessment of domino accidental events, J. Hazard. Mater., 129, 1–21.
Cozzani V., Tugnoli A., Bonvicini S., Salzano E., 2013, Threshold-Based Approach, in: Domino Effects in the Process Industries: Modelling, Prevention and Managing, Elsevier B.V., 189–207.
Delvosalle C., Fievez C., Pipart A., Debray B., 2006, ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries, J. Hazard. Mater., 130, 200–219.
Iaiani M., Casson Moreno V., Reniers G., Tugnoli A., Cozzani V., 2021a, Analysis of events involving the intentional release of hazardous substances from industrial facilities, Reliab. Eng. Syst. Saf., 212, 107593.
Iaiani M., Tugnoli A., Bonvicini S., Cozzani V., 2021b, Major accidents triggered by malicious manipulations of the control system in process facilities, Saf. Sci., 134, 105043.
Iaiani M., Tugnoli A., Macini P., Cozzani V., 2021c, Outage and asset damage triggered by malicious manipulation of the control system in process plants, Reliab. Eng. Syst. Saf., 213, 107685.
Landucci G., Reniers G., 2019, Preface to special issue on quantitative security analysis of industrial facilities, Reliab. Eng. Syst. Saf.
Landucci G., Reniers G., Cozzani V., Salzano E., 2015, Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios, Reliab. Eng. Syst. Saf., 143, 53–62.
Mannan S., 2012, Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control, 4th ed. Elsevier, UK: Butterworth-Heinemann.
Pert A.D., Baron M.G., Birkett J.W., 2006, Review of Analytical Techniques for Arson Residues, J. Forensic Sci., 51, 1033–1049.
Störfall-Kommission (SFK), 2002, SFK–GS–38 - Combating Interference by Unauthorised Persons.
valkyrie.pro, 2019, VALKYRIE HEAVY PRO New 2019 - datasheet [WWW Document]. URL https://www.valkyrie.pro/ (accessed 7.13.21).
Woodward R.L., 1978, The penetration of metal targets by conical projectiles, Int. J. Mech. Sci., 20, 349–359.